NOKIA

7450 ETHERNET SERVICE SWITCH
7750 SERVICE ROUTER
7950 EXTENSIBLE ROUTING SYSTEM
VIRTUALIZED SERVICE ROUTER

CLASSIC CLI COMMAND REFERENCE GUIDE
RELEASE 22.2.R1

3HE 18381 AAAA TQZZA 01

Issue: 01

February 2022

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2022 Nokia.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table of Contents

1 Getting Started 5
2 Classic CLI Overview 11
3 Command Trees 61
4 3 Commands 545
5 a Commands 551
6 b Commands 1077
7 c Commands 1235
8 d Commands 1541
9 e Commands 1951
10 f Commands 2279
11 g Commands 2499
12 h Commands 2609
13 i Commands 2785
14 j Commands 3209
15 k Commands 3213
16 l Commands 3245
17 m Commands 3615
18 n Commands 4189
19 o Commands 4313
20 p Commands 4421
21 q Commands 5091

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22 r Commands 5205
23 s Commands 5647
24 t Commands 6475
25 u Commands 6771
26 v Commands 6885
27 w Commands 7041
28 x Commands 7093
29 y Commands 7103
30 z Commands 7105

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

1 Getting Started

This guide contains command descriptions for the classic SR OS CLI commands that are used to manage the SR OS.

In this guide, the term CLI refers to the classic CLI unless otherwise specified.

This guide does not include **clear**, **monitor**, **show**, or **tools** commands. These commands are documented in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide*.

Note: This guide generically covers Release 22.*x*.R*x* content and may contain some content that will be released in later maintenance loads. Refer to the *SR OS 22.x*.R*x* Software Release Notes, part number 3HE 18412 000*x* TQZZA, for information about features supported in each load of the Release 22.*x*.R*x* software.

The full set of CLI commands supported by the SR OS is documented in three related guides that are listed in Table 1.

Table 1 **Documentation for SR OS CLI Commands**

Guide Title	Classic CLI Commands	MD-CLI Commands
7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide	All **clear**, **monitor**, **show**, and **tools** commands	All **clear**, **monitor**, **show**, and **tools** commands
7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide	All other commands	—
7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide	—	All other commands

1.1 Command Tree

The SR OS CLI command tree is a hierarchical inverted tree. The highest level is the root level. Below this level are other tree levels with the major command groups; for example, **configuration** commands and **admin** commands are levels below root.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In the tree, you can click on a command to link directly to the command description.

Note: Commands that are listed in the tree but are not linked to an associated description are available on one or more platforms but are not currently described in the guide.

1.2 Command Descriptions

Command descriptions are listed in alphabetical order by command name.

Figure 1 shows an example of a command description.

Figure 1 **Command Description Example**

aa-sub-study

Syntax as-sub-study *study-type*

Context [Tree] (config>app-assure>group>statistics aa-sub-study)

Full Context configure application-assurance group statistics aa-sub-study

Description This command enables the context to configure accounting and statistics collection parameters per application assurance special study subscribers.

Parameters *study-type* — Specifies special study protocol subscriber stats.

Values application, protocol

sw3044

Table 2 describes the fields that may be shown for a command. Not all fields are applicable for all commands.

Table 2 **Command Description Fields**

Field	Description
Command Name	Name of the command
Syntax	Command syntax required to execute the command. See Table 3 for information on syntax symbols.
Context	Path to the command as it is displayed in the CLI prompt. Clicking on [Tree] links to the command in the CLI tree.
Full Context	Complete contextual path to perform the command

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 2 **Command Description Fields (Continued)**

Field	Description
Platforms	Hardware platforms on which the command is available, including: 7450 ESS-7, 7450 ESS-12, 7750 SR-1, 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-a4, 7750 SR-a8, 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-20e, 7950 XRS-40, VSR
Description	Description of the command functionality and any restrictions
Default	Command default value
Parameters	Descriptions of command parameters
Values	Values allowed for the parameter
Default	Parameter default value

Note: Some SR OS features are platform-specific and therefore may not be available or visible on all platforms. Refer to the *SR OS 22.x*.R*x* Software Release Notes, part number 3HE 18412 000*x* TQZZA, for information on platform support.

All options for enumerated types and numerical ranges are listed in the command descriptions; however, not all options or ranges are valid on all platforms.

1.3 Navigational Aids

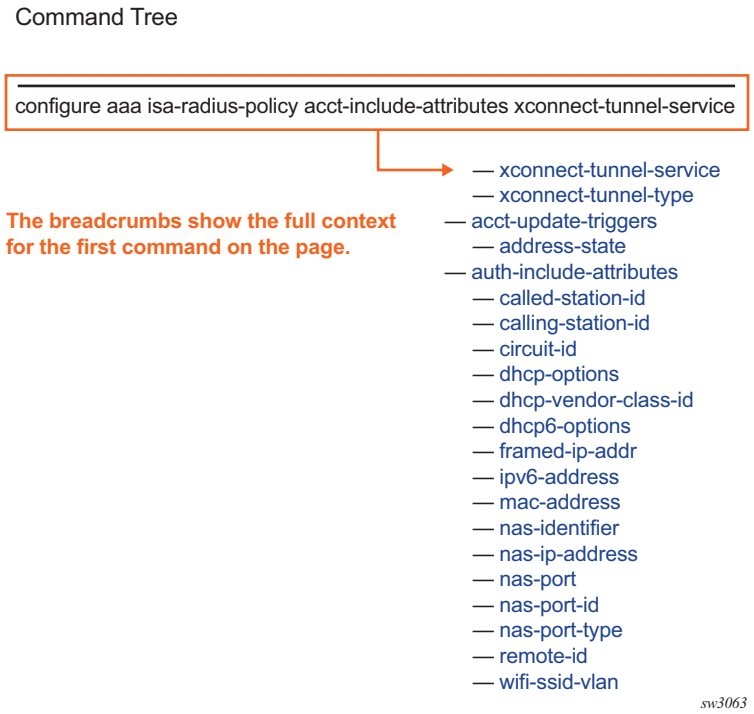
The following aids help you navigate the guide and find specific commands.

1.3.1 Context Path

In the CLI tree section, the complete contextual path to the first command on the page is shown at the top of the page, as shown in Figure 2.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Figure 2 **Command Tree Navigation**



1.3.2 Searching

The Context field in each command description shows, in parentheses, the full path to the command as displayed in the CLI prompt. This form of the contextual path often abbreviates terms. For example:

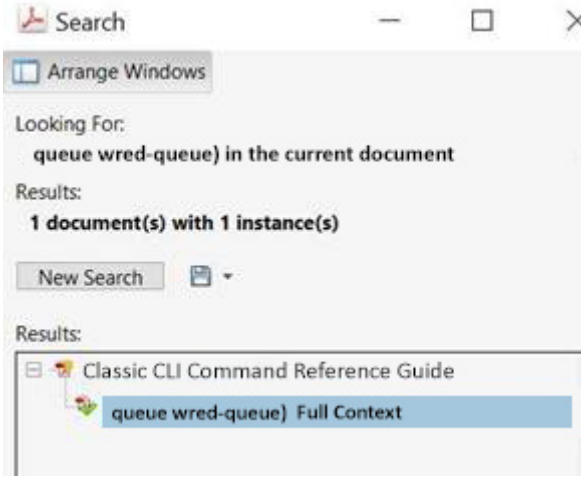
(cfg>qos>qgrps>egr>qgrp>queue wred-queue)

To search this guide for a specific command using the Acrobat search function, enter the command name and append a closing parenthesis in the search window. For more efficient searching, add the previous level of the contextual path before the command name.

If you add the context and closing parenthesis, the resulting search returns only matching Context entries. It will not return instances of the same command found elsewhere in the guide. Figure 3 shows an example of a search.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Figure 3 **Search Window**



1.3.3 Linking to the Tree

Clicking on [Tree] in a command description context links directly to the command in the CLI tree. Figure 4 shows the [Tree] element.

Figure 4 **Link to CLI Tree**

aa-sub-study

Syntax	as-sub-study *study-type*
Context	[Tree] (config>app-assure>group>statistics aa-sub-study)
Full Context	configure application-assurance group statistics aa-sub-study
Description	This command enables the context to configure accounting and statistics collection parameters per application assurance special study subscribers.
Parameters	*study-type* — Specifies special study protocol subscriber stats.
Values	application, protocol

sw3061

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2 Classic CLI Overview

In this chapter, “CLI” refers to the classic CLI unless otherwise specified.

2.1 CLI Structure

The SR OS CLI is a command-driven interface accessible through the console, Telnet, or secure shell (SSH). The CLI can be used for the configuration and management of routers.

The SR OS CLI command tree is a hierarchical inverted tree. The operational root level is the highest level of this tree. When the user enters a CLI session, the user is in the operational root context. Below this level are other tree levels for the major command groups; for example, **configure** commands and **show** commands are levels below the operational root level.

The CLI is organized so that related commands with the same scope are at the same level or in the same context. Sublevels or subcontexts have related commands with a more refined scope.

Note: The CLI engine used to execute scripts is the primary CLI engine configured with **config**>**system**>**management-interface**>**cli**>**cli-engine** {[**classic-cli**] [**md-cli**]}.

2.2 Navigating in the CLI

Table 3 describes command syntax symbols used in this guide.

Table 3 **Command Syntax Symbols**

Symbol	Description
|	A vertical line indicates that only one of the parameters within the brackets or braces can be selected.
[ ]	Brackets indicate optional parameters.
{ }	Braces indicate that one of the parameters must be selected.
[{ }]	Braces within square brackets indicate that the parameters are optional, but if one is selected, the information within the braces is required.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 3 **Command Syntax Symbols (Continued)**

Symbol	Description
Bold	**Bold** indicates commands and keywords.
Italic	*Italics* indicates that you must enter text for the parameter.

2.2.1 CLI Contexts

Use the CLI to access, configure, and manage Nokia routers. CLI commands are entered at the command line prompt. Access to specific CLI commands is controlled by the permissions set by your system administrator. Entering a CLI command makes navigation possible from one command context (or level) to another.

When the user enters a CLI session, the user is in the operational root context. Navigate to another level by entering the name of successively lower contexts. For example, at the command prompt (#), enter **configure** or **config**. See Command Completion for alternative syntax for the same command.The active context displays in the command prompt.

```
A:cses-E11# config
A:cses-E11>config#
```

In a CLI context, enter commands at that context level by entering the text. Press <Enter> to move to a lower context. The user can also include commands from lower context at one context level as long as the command and parameter syntax is correct.

The following example shows two methods to navigate to a service SDP ingress level.

Method 1:

```
A:cses-E11# configure service epipe 6 spoke-sdp 2:6 ingress
*A:cses-E11>config>service>epipe>spoke-sdp>ingress#
```

Method 2:

```
A:cses-E11>config# service
A:cses-E11>config>service# epipe 6
*A:cses-E11>config>service>epipe# spoke-sdp 2:6
*A:cses-E11>config>service>epipe>spoke-sdp# ingress
*A:cses-E11>config>service>epipe>spoke-sdp>ingress#
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The CLI returns an error message if the syntax is incorrect. For example, if the user enters **rooter** for the **root** command, it would result in an error.

```
*A:cses-E11>config# rooter
Error: Bad command.
```

The command parameter is the means by which a value is passed to the command processing program. The user must enter the value according to the syntax rules and, where applicable, the defined range. In the previous example, “6” and “2:6” are the parameter values that the user must enter to execute the command. The value “6” is the value for the Epipe service identifier parameter. For the value “2:6”, “2” is the value for the SDP identifier parameter and “6” is the value for the virtual circuit identifier.

2.2.2 Operational Root and Global Commands

The commands in Table 4 are available at the operational root level of the CLI hierarchy. For the command descriptions, see the respective command sections in this guide. For descriptions of the **clear**, **monitor**, **show**, and **tools** commands, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide*.

Table 4 **Operational Root Commands**

Command	Description
admin	Enters the administrative context for system operations
bof	Enters the context to configure the boot options file
clear	Clears statistics or resets the operational state
configure	Enters the configuration context
[**no**] **debug**	Enters the context to enable or disable debugging and specify debug options
[**no**] **enable-dynamic-services-config**	Enters the context to manually modify the dynamic services in the current CLI session
[**no**] **enable-vsd-config**	Enters the context to manually modify the VSD configuration in the current CLI session
environment	Enters the environment configuration context
file	Enters the context for file system commands
help	Displays help in the CLI

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 4 **Operational Root Commands (Continued)**

Command	Description
monitor	Enters the context to monitor statistics
password	Enters the context to change the user CLI login password
show	Shows operational information
tools	Enters the tools context for troubleshooting and debugging

Global commands are commands that can be entered at any level in the CLI hierarchy. To display the list of all system global commands, enter **help globals** in the CLI.

The global commands are listed in Table 5. For the command descriptions, see the respective command sections in this guide.

Table 5 **Global Commands**

Command	Description
back	Navigates to the parent context
candidate	Enters the context to configure candidate parameters
echo	Echoes the text that is typed in. The primary use is to display messages to the screen within an exec file.
enable-admin	Enables the user to become a system administrator
exec	Executes the contents of a text file as if they were CLI commands entered at the console
exit	Returns to the previous higher context
help	Displays help in the CLI
history	Displays a list of the most recently entered commands
logout	Terminates the CLI session
mrinfo	Requests multicast router information
mstat	Traces a multicast path from a source to a receiver and displays multicast packet rate and loss information (IGMP-based)
mstat2	Traces a multicast path from a source to a receiver and displays multicast packet rate and loss information (UDP-based)
mtrace	Traces a multicast path from a source to a receiver (IGMP-based)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 5 **Global Commands (Continued)**

Command	Description
mtrace2	Traces a multicast path from a source to a receiver (UDP-based)
oam	Provides OAM test suite options. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide*.
ping	Verifies the reachability of a remote host
pwc	Displays the present or previous working context of the CLI session
sleep	Causes the console session to pause operation (sleep) for 1 s or for the specified number of seconds. The primary use is to introduce a pause in the execution of an exec file.
ssh	Opens a secure shell connection to a host
telnet	Connects to a host using Telnet
traceroute	Determines the route to a destination address
tree	Displays a list of all commands at the current level and all sublevels
write	Sends a console message to a specific user or to all users with active console sessions

2.2.3 CLI environment Commands

The CLI **environment** commands listed in Table 6 are found in the **environment** context of the operational root of the CLI tree. These commands control session preferences for a single CLI session. For more information on the commands, see the respective command sections in this guide.

Table 6 **CLI environment Commands**

Command	Description
alias	Enables the substitution of a command line by an alias
create	Enables or disables the use of a create parameter check
kernel	Enables or disables the kernel
more	Enables the CLI output to be displayed one screen at a time, awaiting user input to continue
reduced-prompt	Configures the maximum number of higher-level CLI context nodes to display by name in the CLI prompt for the current CLI session

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 6 **CLI environment Commands (Continued)**

Command	Description
saved-ind-prompt	Saves the indicator in the prompt
shell	Enables or disables the shell
suggest-internal-objects	Enables the suggestion of internally created objects while auto-completing
terminal	Configures the terminal screen length for the current CLI session
time-display	Specifies whether time should be displayed in local time or UTC
time-stamp	Specifies whether the timestamp should be displayed before the prompt

2.2.4 CLI monitor Commands

The CLI **monitor** commands display specified statistical information related to the monitor subject (such as filter, port, QoS, router, service, and VRRP) at a configurable interval until a count is reached. The CLI **monitor** commands are found in the **monitor** context of the operational root of the CLI tree.

The **monitor** command output displays a snapshot of the current statistics. The output refreshes with subsequent statistical information at each configured interval and is displayed as a delta to the previous output.

The <Ctrl-c> keystroke interrupts a monitoring process. Monitor command configurations cannot be saved. You must enter the command for each monitoring session. If the maximum limits are configured, you can monitor the statistical information for a maximum of 60 × 999 s ~ approximately 1000 min.

The CLI **monitor** commands contexts are listed in Table 7. For more information on the commands, see the respective command sections in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide*.

Table 7 **CLI monitor Commands**

Command	Description
card	Enables monitoring of ingress FP queue groups
ccag	Enables CCAG port monitoring for traffic statistics. This command is supported on the 7450 ESS and 7750 SR; additional restrictions may apply.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 7 **CLI monitor Commands (Continued)**

Command	Description
cpm-filter	Monitors the command output for CPM filters
eth-cfm	Enables 802.1ag CFM statistics monitoring
filter	Enables IP and MAC filter monitoring at a configurable interval until that count is reached
lag	Enables Link Aggregation Group (LAG) monitoring to display statistics for individual port members and the LAG
management-access-filter	Enables management access filter monitoring
oam-pm	Enables operations, administration, and management (OAM) performance monitoring
port	Enables port traffic monitoring. The statistical information for the specified ports displays at the configured interval until the configured count is reached.
qos	Enables arbiter and scheduler statistics monitoring
router	Enables virtual router instance monitoring at a configurable interval until that count is reached
service	Monitors commands for a particular service
test-oam	Enables monitoring of OAM performance

2.3 Getting Help in the CLI

The **help** system commands and the ? key display different types of help in the CLI. Table 8 lists the help commands.

Table 8 **Online Help Commands**

Command	Description
help	Describes the help system
help globals	Displays information about global commands
help edit	Displays information about all editing keystrokes
help special-characters	Displays information about all special characters that can be entered at the command prompt

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 8 **Online Help Commands (Continued)**

Command	Description
?	Displays context-sensitive help information and displays a full list of options and commands available from the current context When entered at the root context, displays a full list of top-level contexts and global commands
command ? *command parameter* ? *command* **keyword** ?	Displays the available syntax options for the command, lists the associated parameters and keywords, and lists all commands available from the *command* context
string?	Lists all commands available in the current context that start with *string*
command string? *command parameter string*? *command* **keyword** *string*?	Lists all commands, parameters, or keywords available in the *command* context that start with *string*
string<Tab>	Completes a partial command name (auto-completion) or lists available commands that match *string*

The **tree** and **tree detail** system commands are useful when searching for a command in a lower-level context.

The following example shows a partial list of the **tree** and **tree detail** command outputs on a 7750 SR.

```
*A:cses-E11>config# tree

+---router
| +---aggregate
| +---allow-icmp-redirect
| +---allow-icmp6-redirect
| +---autonomous-system
| +---bfd
| | +---abort
| | +---begin
| | +---bfd-template
| | | +---echo-receive
| | | +---multiplier
| | | +---receive-interval
| | | +---transmit-interval
| | | +---type
| | +---commit
| +---bgp
| | +---add-paths
| | | +---ipv4
| | | +---ipv6
| | | +---label-ipv4
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
| | | +---label-ipv6
| | | +---vpn-ipv4
| | | +---vpn-ipv6
| | +---advertise-external
| | +---advertise-inactive
| | +---aggregator-id-zero
| | +---auth-keychain
| | +---authentication-key
| | +---backup-path
| | +---best-path-selection
| | | +---always-compare-med
| | | +---as-path-ignore
| | | +---deterministic-med
| | | +---ignore-nh-metric
| | | +---ignore-router-id
| | +---bfd-enable
| | +---cluster

*A:cses-E11>config# tree detail
...
+---router [<router-name>]
| +---no aggregate <ip-prefix/ip-prefix-length>
| | aggregate <ip-prefix/ip-prefix-length> [summary-only] [as-set]
[aggregator <as-number:ip-address>] [black-hole [generate-icmp]]
[community <comm-id>]
| | aggregate <ip-prefix/ip-prefix-length> [summary-only] [as-set]
[aggregator <as-number:ip-address>] [community <comm-id>] [indirect
<ip-address>]
| +---allow-icmp-redirect
| | no allow-icmp-redirect
| +---allow-icmp6-redirect
| | no allow-icmp6-redirect
| +---autonomous-system <autonomous-system>
| | no autonomous-system
| +---bfd
| | +---abort
| | +---begin
| | +---bfd-template <[32 chars max]>
| | | no bfd-template <[32 chars max]>
| | | +---echo-receive <milli-seconds>
| | | | no echo-receive
| | | +---multiplier <[3..20]>
| | | | no multiplier
| | | +---no receive-interval
| | | | receive-interval <milli-seconds>
| | | +---no transmit-interval
| | | | transmit-interval <milli-seconds>
| | | +---no type
| | | | type {cpm-np}
| | +---commit
| +---bgp
| | no bgp
| | +---add-paths
| | | no add-paths
| | | +---ipv4 send <send-limit>
| | | | ipv4 send <send-limit> receive [none]
| | | | no ipv4
| | | +---no ipv6
| | | | ipv6 send <send-limit>
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
| | | | ipv6 send <send-limit> receive [none]
| | |   +---label-ipv4 send <send-limit>
| | |   label-ipv4 send <send-limit> receive [none]
| | |   no label-ipv4
| | +---label-ipv6 send <send-limit>
| | |   label-ipv6 send <send-limit> receive [none]
| | |   no label-ipv6
| | | +---no vpn-ipv4
| | | | vpn-ipv4 send <send-limit>
| | | | vpn-ipv4 send <send-limit> receive [none]
| | | +---no vpn-ipv6
| | | | vpn-ipv6 send <send-limit>
| | | | vpn-ipv6 send <send-limit> receive [none]
| | +---advertise-external [ipv4] [ipv6] [label-ipv4] [label-ipv6]
| | | no advertise-external [ipv4] [ipv6] [label-ipv4] [label-ipv6]
| | +---advertise-inactive
| | | no advertise-inactive
| | +---aggregator-id-zero
| | | no aggregator-id-zero
| | +---auth-keychain <name>
| | +---authentication-key <authentication-key|hash-key> [hash|hash2|custom]
```

2.4 The CLI Command Prompt

By default, the CLI command prompt indicates the device being accessed, the active CPM, and the current CLI context. For example, the prompt: **A:cses-E11>config>router>if#** indicates that the active CPM is CPM A, the user is on the device with the hostname **cses-E11**, and the current context **config**>**router**>**interface**. In the prompt, the separator used between contexts is the “>” symbol. The active CPM can be A or B on the 7750 SR, and A, B, C, or D on the 7950 XRS.

At the end of the prompt, there is either a pound sign (#) or a dollar sign ($). A “#” at the end of the prompt indicates the context is an existing context. A “$” at the end of the prompt indicates the context has been newly created. Contexts are newly created for logical entities when the user first navigates into the context.

Because there can be a large number of sublevels in the CLI, the **environment** command **reduced-prompt** *no of nodes in prompt* allows the user to control the number of levels displayed in the prompt.

Allowed values in strings are printable, 7-bit ASCII characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes. Double quotes within a string are not supported. For example:

```
*A:cses-E11>config>router# interface "primary#1"
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When changes are made to the configuration file, a “*” appears in the prompt string (*A:cses-E11), indicating that the changes have not been saved. When an **admin save** command is executed, the “*” disappears. This behavior is controlled by the **saved-ind-prompt** command in the **environment** context.

2.5 Displaying Configuration Contexts

The **info**, **info detail**, and **objective** commands display the configuration for the current level. The **info** command shows non-default configurations. The **info detail** command shows the entire configuration for the current level, including defaults. The **info objective** command provides an output objective that controls the configuration parameters to be displayed.

The following example displays the output from the **info** command and the **info detail** command.

```
*A:cses-E11>config>router# interface system
*A:cses-E11>config>router>if# info
----------------------------------------------
            address 10.10.0.1/32
----------------------------------------------
*A:cses-E11>config>router>if#


*A:cses-E11>config>router>if# info detail
----------------------------------------------
            address 10.10.10.103/32 broadcast host-ones
            no description
            no arp-timeout
            no allow-directed-broadcasts
            tos-marking-state trusted
            no local-proxy-arp
            no proxy-arp
            icmp
                mask-reply
                redirects 100 10
                unreachables 100 10
                ttl-expired 100 10
            exit
            no mac
            no cflowd
            no shutdown
----------------------------------------------
*A:cses-E11>config>router>if#
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2.6 exec Files

The **exec** command allows you to execute a text file of CLI commands as if it were typed at a console device.

The **exec** command and the associated exec files can be used to conveniently execute a number of commands that are always executed together in the same order. For example, an **exec** command can be used to define a set of commonly used standard command aliases.

The **echo** command can be used within an exec command file to display messages on screen while the file executes.

Arguments can be specified with the **exec** command. These arguments are passed in to be used inside the text file that includes the CLI commands. The passing of arguments with the **exec** command only works in the classic CLI. The passing of arguments with the **exec** command cannot be used in the MD-CLI.

For example, if the file cf3/Test.txt contains the following set of CLI commands:

```
echo $(1)
echo $(2)
echo $(3)
```

then executing the following commands:

 # exec cf3:/Test.txt -arguments var1=10 var2=20 var3=30

or

 # exec cf3:/Test.txt -arguments 10 20 30

produces the following output:

```
10
20
30
```

2.7 CLI Script Control

SR OS provides centralized script management for CLI scripts that are used by CRON and the Event Handling System (EHS). A set of script policies and script objects can be configured to control such things as:

- where scripts are located (local compact FTP server)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- where to store the output of the results
- how long to keep historical script result records
- how long a script may run

If the scripts are located on local compact flash devices, the user must ensure that the scripts are on the compact flash devices of both CPMs so that operation of EHS continues as expected if a CPM switchover occurs.

Only one script can execute at a time. An SNMP table (smRunTable in the DISMAN-SCRIPT-MIB) is used as both an input queue of scripts waiting to be executed and for storage of records for completed scripts. If the input queue is full, the script request is discarded.

2.8 Entering CLI Commands

The following sections outline the steps to entering CLI commands.

2.8.1 Command Completion

The CLI supports both command abbreviation and command completion. If the keystrokes entered are enough to match a valid command, the CLI displays the remainder of the command syntax when the <Tab> key or spacebar is pressed. When typing a command, the <Tab> key or spacebar invokes auto-completion. If the keystrokes entered are sufficient to identity a specific command, auto-completion completes the command. If the letters are not sufficient to identify a specific command, pressing the <Tab> key or spacebar displays commands matching the letters entered.

System commands are available in all CLI contexts.

2.8.2 Unordered and Unnamed Parameters

In a command context, the CLI accepts command parameters in any order as long as the command is formatted in the proper command keyword and parameter syntax. Command completion works as long as enough recognizable characters of the command are entered.

The following output shows the command syntax for **static-route-entry**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
*A:cses-E11>config>router# static-route-entry ?
 - no static-route-entry <ip-prefix/prefix-length> [mcast]
 - static-route-entry <ip-prefix/prefix-length> [mcast]

<ip-prefix/prefix-*> : ipv4-prefix    - a.b.c.d (host bits must be 0)
                       ipv4-prefix-le - [0..32]
                       ipv6-prefix    - x:x:x:x:x:x:x:x   (eight 16-bit pieces)
                                        x:x:x:x:x:x:d.d.d.d
                                        x - [0..FFFF]H
                                        d - [0..255]D
                       ipv6-prefix-le - [0..128]
<mcast>              : keyword - Indicates that static-route being configured
                       is used for mcast table only

 [no] backup-tag      - Create/Configure or Delete/Deconfigure backup tag for
                        static-route-entry
 [no] black-hole      + Create/Configure or Delete/Deconfigure blackhole
                        nexthop for static-route-entry
 [no] community       - Create/Configure or Delete/Deconfigure community for
                        static-route-entry
 [no] indirect        + Create/Configure or Delete/Deconfigure indirect
                        next-hop for static-route-entry
 [no] next-hop        + Create/Configure or Delete/Deconfigure next-hop for
                        static-route-entry
 [no] tag             - Create/Configure or Delete/Deconfigure tag for
                        static-route-entry
```

Some SR OS CLI commands have multiple unnamed parameters. For example, the **subrate** *csu-mode rate-step* command has both a *csu-mode* parameter and a *rate-step* parameter that do not have leading keywords. SR OS uses a best-match algorithm to select which parts of the user input are intended to be used for each unnamed parameter. This best-match algorithm depends on the specific command.

In some cases, it is not possible for the algorithm to be 100% accurate, and the SR OS may assign an unintended value to a parameter when two unnamed parameters have similar constraints and syntax. For example, the **environment alias** *alias-name alias-command-name* command may reverse the *alias-name* and *alias-command-name* parameters if the first parameter entered is more than 80 characters.

2.8.3 Editing Keystrokes

When entering a command, special keystrokes allow for editing of the command. Table 9 lists the command editing keystrokes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 9 **Command Editing Keystrokes**

Editing Action	Keystrokes
Stop the current command	<Ctrl-c>
Delete current character	<Ctrl-d>
Delete text up to cursor	<Ctrl-u>
Delete text after cursor	<Ctrl-k>
Move to beginning of line	<Ctrl-a>
Move to end of line	<Ctrl-e>
Get prior command from history	<Ctrl-p>
Get next command from history	<Ctrl-n>
Move cursor left	<Ctrl-b>
Move cursor right	<Ctrl-f>
Move back one word	<Esc><b>
Move forward one word	<Esc><f>
Convert rest of word to uppercase	<Esc><c>
Convert rest of word to lowercase	<Esc><l>
Delete remainder of word	<Esc><d>
Delete word up to cursor	<Ctrl-w>
Transpose current and previous character	<Ctrl-t>
Enter command and return to operational root prompt	<Ctrl-z>
Refresh input line	<Ctrl-l>

2.8.4 Absolute Paths

CLI commands can be executed in any context by specifying the full path from the CLI root. To execute an out-of-context command, enter a forward slash (*/*) or backward slash (\) at the beginning of the command line. The commands are interpreted as absolute paths. Spaces between the slash and the first command return an error.

```
*A:cses-E11# configure router
*A:cses-E11>config>router# interface system address 10.2.3.4
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
*A:cses-E11>config>router# /admin save
*A:cses-E11>config>router# \clear router interface
*A:cses-E11>config>router#
```

The "/" or "\" cannot be used as an absolute path at the beginning of the command string of the **environment alias** command. The command may change the current context depending on whether it is a leaf command. This is the same behavior the CLI performs when CLI commands are entered individually; for example:

```
*A:cses-E11# admin
*A:cses-E11>admin# save
```

or

```
*A:cses-E11# admin save
*A:cses-E11#
```

An absolute path command behaves in the same way as manually entering a series of command line instructions and parameters.

For example, beginning in an IES context service ID 4 (IES 4):

```
config>service>ies> /clear card 1
```

behaves in the way same as the following series of commands:

```
config>service>ies>exit all
clear card 1
configure service ies 4 (returns you to your starting point)
config>service>ies
```

If the command takes you to a different context, the following occurs:

```
config>service>ies>/configure service vpls 5 create
```

becomes:

```
config>service>ies>exit all
configure service vpls 5 create
config>service>vpls>
```

2.8.5 History

The CLI maintains a history of the most recently entered commands. The **history** command shows the most recently entered CLI commands.

```
*A:cses-E11# history
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
   1 environment terminal length 48
   2 environment no create
   3 show version
   4 configure port 1/1/1
   5 info
   6 \configure router isis
   7 \port 1/1/2
   8 con port 1/1/2
   9 \con port 1/1/2
  10 \configure router bgp
  11 info
  12 \configure system login-control
  13 info
  14 history
  15 show version
  16 history
*A:cses-E11# !3

A:cses-E11# show version
TiMOS-B-0.0.I2016 both/i386 Nokia 7450 ESS Copyright (c) 2000-2016 Nokia
All rights reserved. All use subject to applicable license agreements.
Built on Sun Oct 12 20:01:13 PDT 2008 by builder in /rel0.0/I2016/panos/main
A:cses-E11#
```

2.8.6 Entering Numerical Ranges

The SR OS CLI allows the use of a single numerical range as an argument in the command line. This range can be a set or a sequence of numbers, or a combination of both.

A set is a range of numerical values, from a minimum to a maximum, incremented by 1. For example:

```
configure service vpls [1..10] create customer 1
```

A sequence is a list of discrete integer elements, in any order. For example:

```
configure service vpls [1,2,3] no shutdown
```

A sequence can contain sets as well as integer elements. For example:

```
configure service vpls [4..6,7,8..10] no shutdown
```

For example, it is possible to shut down ports 1 through 10 on an XMA/MDA 1 in chassis slot 1. A port can be denoted by "*slot*/*mda*/*port*", where *slot* is the slot number, *mda* is the XMA/MDA number and *port* is the port number. To shut down ports 1 through 10 on an XMA/MDA 1 in slot 1, the command is entered as follows:

```
configure port 1/1/[1..10] shutdown
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

<Ctrl-c> can be used to abort the execution of a range command.

CLI commands can contain ranges of hexadecimal values. This allows ranges to be used when working with data normally expressed in hexadecimal instead of decimal, such as IPv6 or MAC addresses. For example:

```
#config>service>vpls>sap$ static-mac aa:bb:[0x19..0x21]:dd:ee:ff create
#config>service>vpls>sap$ info
----------------------------------------------
                static-mac aa:bb:19:dd:ee:ff create
                static-mac aa:bb:1a:dd:ee:ff create
                static-mac aa:bb:1b:dd:ee:ff create
                static-mac aa:bb:1c:dd:ee:ff create
                static-mac aa:bb:1d:dd:ee:ff create
                static-mac aa:bb:1e:dd:ee:ff create
                static-mac aa:bb:1f:dd:ee:ff create
                static-mac aa:bb:20:dd:ee:ff create
                static-mac aa:bb:21:dd:ee:ff create
----------------------------------------------
```

A range can also be a reference to a previous range in the same command. This reference takes the form [$*x*], where *x* is an integer between 0 and 5. For example:

```
configure service vprn [11..20] router-id 10.20.[$0].1
```

This gives vprn 11 the router-id "10.20.11.1", vprn 12 the router-id "10.20.12.1", and so on.

Specifying a range in the CLI does have limitations. These limitations are summarized in Table 10.

Table 10 **CLI Range Use Limitations**

Limitation	Description
Up to 6 ranges (including references) may be specified in a single command, and they may not combine to more than 1000 iterations of the command.	For example, ports on two adapter cards can be shut down in one command by using two ranges: **configure port 1/[1..2]/[1..10]**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 10 **CLI Range Use Limitations (Continued)**

Limitation	Description
Ranges within quotation marks are interpreted literally.	In the CLI, enclosing a string in quotation marks (“*string*”) causes the string to be treated literally and as a single parameter. For example, several commands in the CLI allow the configuration of a descriptive string. If the string is more than one word and includes spaces, it must be enclosed in quotation marks. A range that is enclosed in quotes is also treated literally. For example, **configure router interface "A[1..10]" no shutdown** creates a single router interface with the name “A[1..10]”. However, a command such as: **configure router interface A[1..10] no shutdown** creates 10 interfaces with names A1, A2 .. A10.
Command completion does not work when entering a range.	After entering a range in a CLI command, command and key completion, which normally occurs by pressing the <Tab> key or spacebar, does not work. If the command line entered is correct and unambiguous, the command works properly; otherwise, an error is returned.

2.8.7 Pipe/Match

SR OS supports the pipe feature to search one or more files for a character string or pattern.

When using the pipe or **match** command, the variables and attributes must be spelled correctly. The attributes follow the command and must come before the expression or pattern. The following are examples of how to use the pipe/**match** command to complete different tasks:

- Task: Capture all the lines that include “echo” and redirect the output to a file on the compact flash:

  admin display-config | match “echo” > cf1:\test\echo_list.txt
- Task: Display all the lines that do not include “echo”:

  admin display-config | match invert-match “echo”
- Task: Display the first match of “vpls” in the configuration file:

  admin display-config | match max-count 1 “vpls”
- Task: Display everything in the configuration after finding the first instance of “interface”:

  admin display-config | match post-lines 999999 interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Task: Display a count of the total number of lines of output instead of displaying the output itself:

  admin display-config | match interface | count

Command syntax:

match *pattern* **context** {**parents** | **children** | **all**} [**ignore-case**] [**max-count** *lines-count*] [**expression**]

match *pattern* [**ignore-case**] [**invert-match**] [**pre-lines** *pre-lines*] [**post-lines** *lines-count*] [**max-count** *lines-count*] [**expression**]

where:

```
pattern         string or regular expression
context         keyword:  display context associated with the matching line
parents         keyword:  display parent context information
children        keyword:  display child context information
all             keyword:  display both parent and child context information
ignore-case     keyword
max-count       keyword:  display only a specific number of instances of matching
                          lines
lines-count     1 — 2147483647
expression      keyword:  pattern is interpreted as a regular expression
invert-match    keyword
pre-lines       keyword:  display some lines prior to the matching line
pre-lines       0 — 100
post-lines      keyword:  display some lines after the matching line
lines-count     1 — 2147483647
```

For example:

```
A:Dut-C# show log log-id 98 | match ignore-case "sdp bind"
"Status of SDP Bind 101:1002 in service 1001 (customer 1) changed to admin=up oper=u
p flags="
"Processing of a SDP state change event is finished and the status of all affected S
DP Bindings on SDP 101 has been updated."


A:Dut-C# show log log-id 98 | match max-count 1 "service 1001"
"Status of service 1001 (customer 1) changed to administrative state: up,
operational state: up"

A:Dut-C# admin display-config | match post-lines 5 max-
count 2 expression "OSPF.*Config"
echo "OSPFv2 Configuration"
#--------------------------------------------------
        ospf
            timers
                spf-wait 1000 1000 1000
            exit
echo "OSPFv2 (Inst: 1) Configuration"
#--------------------------------------------------
        ospf 1
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
            asbr
            router-id 10.0.0.1
            export "testall"
*A:Dut# admin display-config | match debug_mirror
            profile "debug_mirror"


*A:Dut# admin display-config | match context parent debug_mirror
#--------------------------------------------------
    system
        security
            profile "debug_mirror"


*A:Dut# admin display-config | match context all debug_mirror
#--------------------------------------------------
    system
        security
            profile "debug_mirror"
                default-action deny-all
                entry 10
                exit


*A:Dut# show log event-control | match ignore-case pre-lines 10 SyncStatus
L  2016 tmnxLogOnlyEventThrottled        MA  gen          0           0
MCPATH:
   2005 tmnxMcPathSrcGrpBlackHole        MI  thr          0           0
   2006 tmnxMcPathSrcGrpBlackHoleCleared MI  thr          0           0
   2007 tmnxMcPathAvailBwLimitExceeded   MI  thr          0           0
   2008 tmnxMcPathAvailBwLimitCleared    MI  thr          0           0
MC_REDUNDANCY:
   2001 tmnxMcRedundancyPeerStateChanged WA  gen          0           0
   2002 tmnxMcRedundancyMismatchDetected WA  gen          0           0
   2003 tmnxMcRedundancyMismatchResolved WA  gen          0           0
   2004 tmnxMcPeerSyncStatusChanged      WA  gen          0           0
```

Table 11 describes regular expression symbols and their interpretation (similar to what is used for route policy regexp matching). Table 12 describes character class expressions.

Table 11 **Regular Expression Symbols**

String	Description
.	Matches any single character
[ ]	Matches a single character that is contained within the brackets [abc] matches “a”, “b”, or “c” [a-z] matches any lowercase letter [A-Z] matches any uppercase letter [0-9] matches any number

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 11 **Regular Expression Symbols (Continued)**

String	Description
[^]	Matches a single character that is not contained within the brackets [^abc] matches any character other than “a”, “b”, or “c” [^a-z] matches any single character that is not a lowercase letter
^	Matches the start of the line (or any line, when applied in multiline mode)
$	Matches the end of the line (or any line, when applied in multiline mode)
()	Defines a “marked subexpression” Every matched instance will be available to the next command as a variable
*	A single character expression followed by “*” matches zero or more copies of the expression
{m,n}	Matches least *m* and at most *n* repetitions of the term
{m}	Matches exactly *m* repetitions of the term
{m,}	Matches *m* or more repetitions of the term
?	The preceding item is optional and matched at most once
+	The preceding item is matched one or more times
-	Used between start and end of a range
\	An escape character to indicate that the following character is a match criteria and not a grouping delimiter
>	Redirects output

Table 12 **Character Class Expressions**

Character Class	Characters Matched [1]	Description
[:alnum:]	‘ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789’	Alphanumeric characters
[:alpha:]	‘ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz’	Alphabetic characters
[:blank:]	‘ \t’	Space and Tab
[:cntrl:]	‘\007\b\t\n\v\f\r\1\2\3\4\5\6\16\17\20 \21\22\23\24\25\26\27\30 \31\32\33\34\35\36\37\177’	Control characters
[:digit:]	‘0123456789’	Digits

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 12 **Character Class Expressions (Continued)**

Character Class	Characters Matched [1]	Description
[:graph:]	‘ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789 !\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~’	Visible characters
[:lower:]	‘abcdefghijklmnopqrstuvwxyz’	Lowercase letters
[:print:]	‘ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!\"#$%&'()*+,-./ :;<=>?@[\\]^_`{|}~ ’	Visible characters and the Space character
[:punct:]	‘!\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~’	Punctuation characters
[:space:]	‘\t\n\v\f\r ‘	Whitespace (blank) characters
[:upper:]	‘ABCDEFGHIJKLMNOPQRSTUVWXYZ’	Uppercase letters
[:xdigit:]	‘0123456789ABCDEFabcdef’	Hexadecimal digits

Note:

1. Characters matching the character class are delimited by single quotation marks (‘).

Character class expressions must be enclosed within brackets. The expression [[:digit:]] is treated as a regular expression containing the character class “digit”, while [:digit:] is treated as a regular expression matching “:”, “d”, “i”, “g”, or “t”.

2.8.8 Pipe/Count

The SR OS supports a pipe/**count** command (...| **count**) that provides a count of the number of lines that would have otherwise been displayed. The pipe/**count** command is particularly useful when used in conjunction with the pipe/**match** command in order to count the number of output lines that match a specified pattern.

For example:

```
*A:dut-c# show service service-using vprn

===============================================================================
Services [vprn]
===============================================================================
ServiceId    Type      Adm  Opr  CustomerId Service Name
-------------------------------------------------------------------------------
1            VPRN      Down Down 1
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
44            VPRN      Up   Up   1
100           VPRN      Down Down 1
102           VPRN      Up   Up   1
235           VPRN      Down Down 1
1000          VPRN      Down Down 1000
-------------------------------------------------------------------------------
Matching Services : 6
-------------------------------------------------------------------------------
===============================================================================
*A:dut-c# show service service-using vprn | match Down | count
Count: 4 lines
*A:dut-c#
```

2.8.9 Pipe/reverse-dns

The SR OS supports a command pipe/**reverse-dns** (...| **reverse-dns**) that processes the input to the pipe by performing a reverse DNS lookup on any IPv4 or IPv6 address strings. For each line where an address string is identified and where the reverse DNS lookup locates a match, the output of the lookup is inserted as the next line in the display. If no match is found, nothing is printed. If the output line is more than 80 characters, the line is truncated.

For example:

```
A:Dut-C# ping 135.243.195.220 router-instance "management" | reverse-dns
PING 135.243.195.220 56 data bytes
  (135.243.195.220) sauron.lab.sk.alcatel-lucent.com
64 bytes from 135.243.195.220: icmp_seq=1 ttl=63 time=1.42ms.
...
---- 135.243.195.220 PING Statistics ----
  (135.243.195.220) sauron.lab.sk.alcatel-lucent.com

A:Dut-C# echo 2001:4860:4860::8888 | reverse-dns
2001:4860:4860::8888
  (2001:4860:4860::8888) dns.google
```

2.8.10 Range Operator Support of Regular Expression Match

The user can include a regular expression inside the range operator of any **clear**, **config**, **show**, or **tools** CLI commands. The beginning and ending of the regular expression must be delimited with the "/" symbol.

SR OS performs the following steps:

- auto-completes the command to get all the possible names

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- performs a match of the regular expression against all the names
- executes the command for the names for which the match was successful

Note: The order of execution is the same as the order in which the names are listed in the output display of the CLI **info** command or in the output display when you invoke the auto-complete function using the <Tab> key. If the execution of the command fails for one of the matching object names, the execution is aborted and the remaining matching object names are not processed.

For example (assume the following SR-TE LSP names are configured on the router):

```
*A:bkvm35# show router mpls sr-te-lsp
===============================================================================
MPLS SR-TE LSPs (Originating)
===============================================================================
LSP Name                        To              Tun      Protect     Adm    Opr
                                                Id       Path
-------------------------------------------------------------------------------
sr-te-pce                       192.0.2.198     1        N/A         Up     Dwn
RENO194_DET190_LSP1_Profile10   192.0.2.190     2        N/A         Up     Dwn
RENO194_DET190_LSP3             192.0.2.190     3        N/A         Up     Dwn
RENO194_ATL224_LSP1             192.0.2.224     4        N/A         Up     Dwn
-------------------------------------------------------------------------------
LSPs : 4
===============================================================================
```

The following command displays the subset of all SR-TE LSPs with names that include the expression "LSP":

show router mpls sr-te-lsp [/LSP/]

The SR OS expands this command into the following individual commands:

show router mpls sr-te-lsp RENO194_DET190_LSP1_Profile10

show router mpls sr-te-lsp RENO194_DET190_LSP3

show router mpls sr-te-lsp RENO194_ATL224_LSP1

The output of the three **show** commands is displayed in the following example:

```
*A:bkvm35# show router mpls sr-te-lsp [/LSP/]
===============================================================================
MPLS SR-TE LSPs (Originating)
===============================================================================
LSP Name                          To              Tun      Protect     Adm   Opr
                                                  Id       Path
-------------------------------------------------------------------------------
RENO194_DET190_LSP1_Profile10     192.0.2.190     2        N/A         Up    Dwn
-------------------------------------------------------------------------------
LSPs : 1
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
===============================================================================
===============================================================================
MPLS SR-TE LSPs (Originating)
===============================================================================
LSP Name                            To              Tun     Protect    Adm  Opr
                                                    Id      Path
-------------------------------------------------------------------------------
RENO194_DET190_LSP3                 192.0.2.190     3       N/A        Up   Dwn
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
===============================================================================
MPLS SR-TE LSPs (Originating)
===============================================================================
LSP Name                            To              Tun     Protect    Adm  Opr
                                                    Id      Path
-------------------------------------------------------------------------------
RENO194_ATL224_LSP1                 192.0.2.224     4       N/A        Up   Dwn
-------------------------------------------------------------------------------
```

2.8.10.1 Regular Expression Symbols in a Regular Expression Match Operation

The user can use all the regular expression symbols listed in Table 11 and Table 12 inside the regular expression to match.

For example, the user can list all LSP names that begin with the string "RENO194_" followed by the string "ATL" as follows:

```
*A:bkvm35# show router mpls sr-te-lsp [/^RENO194_\['ATL'\]/]
===============================================================================
MPLS SR-TE LSPs (Originating)
===============================================================================
LSP Name                        To              Tun     Protect     Adm    Opr
                                                Id      Path
-------------------------------------------------------------------------------
RENO194_ATL224_LSP1             38.120.48.224   4       N/A         Up     Dwn
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
```

Note: The following conventions are used in the previous example.

- Use the character "^", which matches the start of the string, directly inside the regular expression to indicate a match at the start of the string. However, if you want to match it as a character, enter it as "\\^".
- Use the range delimiter with the escape symbol in front "\[" inside the regular expression because the range delimiter encloses the regular expression.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 13 summarizes special rules governing the use of some of the regular expression symbols inside a regular expression match operation. Any symbol from Table 11 or Table 12 that is not listed in Table 13 can be used directly inside a regular expression match operation.

Table 13 **Rules Governing Regular Expression Symbols**

String	Description
?	[/\?/] if using as a regular expression and [/\\\?/] if using to match the character ?
[ ]	[/\[\]/] if using as a regular expression and [/\\\[\\\]/] if using to match the characters []
$	[/$/] if using as a regular expression and [/\\$/] if using to match the character $
\	[/\\\\/] if using to match the character \
/	[/\/] if using to match the character /
‘	[/\'/] if using to match the character '
*	[/*/] if using to match the character *
.	[/\./] if using as a regular expression and [/\\\./] if using to match the character .
+	[/\\+/] if using to match the character +
,	[/\,/] if using to match the character ,
^	[/\\^/] if using to match the character ^
(	[/\\(/] if using to match the character (
)	[/\\)/] if using to match the character)
space	[/\ /] if using to match the character space

The SR OS does not support the combination of a partial string with a regular expression match operation.

For example, if the operator wants to display the SR-TE LSP names that begin with the string "RENO194_ATL", if part of the string is entered directly and the rest of the string is entered inside a regular expression, the command returns no match. The following example demonstrates the incorrect syntax:

```
*A:bkvm35# show router mpls sr-te-lsp RENO194_[/ATL/]
```

To obtain a match, the entire string must be inside the regular expression. The following example demonstrates the correct syntax for finding a match:

```
*A:bkvm35# show router mpls sr-te-lsp [/^RENO194_ATL/]
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
===============================================================================
MPLS SR-TE LSPs (Originating)
===============================================================================
LSP Name                        To              Tun      Protect     Adm    Opr
                                                Id       Path
-------------------------------------------------------------------------------
RENO194_ATL224_LSP1             38.120.48.224   4        N/A         Up     Dwn
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
```

2.8.11 Redirection

The SR OS supports redirection (>), which allows the operator to store the output of a CLI command as a local or remote file.

For example:

```
'ping <customer_ip> > cf3cf1:/ping/result.txt'
'ping <customer_ip> > ftp://ron@ftp.nokia.com/ping/result.txt'
```

In some cases, only part of the output might be applicable. The pipe/**match** and redirection commands can be combined:

```
ping 10.0.0.1 | match expression "time.\d+" > cf3cf1:/ping/time.txt
```

This records only the RTT portion (including the word “time”).

2.9 vi Editor

The “vi”sual editor (vi) is a file editor that can edit any ASCII file. This includes configuration files, exec files, and the BOF.

VT100 terminal mode is supported. However, if a different terminal mode is configured, there is no noticeable negative effect.

When a configuration file is changed, a validation check is executed to see if the user is allowed to view or perform configuration changes. When a user modifies the configuration file using the vi editor, these checks do not occur. Because of this, the vi editor is only available to a user with administrator privileges. If others require access to the vi editor, their profile must be modified to allow the access. Access permission for the file directory where the file resides must be performed before a user can open, read, or write a file processing command. If a user does not have permission to access the directory, the operation is denied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When opening a file, a resource check verifies that sufficient resources are available to process the file. If there are insufficient resources, the operation is denied and the operator is informed of that event.

Multiple sessions are allowed and are limited only by the memory resources available on the node.

2.9.1 Summary of vi Commands

The vi editor operates in two modes:

- Command mode — this mode causes actions to be taken on the file

  In this mode, each character entered is a command that does something to the text file being edited; for example, the character “O” typed in command mode causes the vi editor to enter insert mode.
- Insert mode — entered text is inserted into the file

  In insert mode, every character typed is added to the text in the file. Pressing <Esc> turns off insert mode.

2.9.2 Using the vi Commands

Use the commands in the following tables to start and end vi edit sessions, move around in a file, enter new text, modify, move, and delete existing text, and read from and write to other files.

Table 14 describes the commands to cut, paste, and delete text.

Table 14 **Cutting and Pasting or Deleting Text**

vi Command	Description
"	Specify a buffer to be used with any of the commands using buffers. Follow the " character with a letter or a number, which corresponds to a buffer.
d	Delete text. The “dd” command deletes the current line. A count specifies the number of lines to delete. Whatever is deleted is placed into the buffer specified with the " command. If no buffer is specified, the general buffer is used.
D	Delete to the end of the line from the current cursor position.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 14 **Cutting and Pasting or Deleting Text (Continued)**

vi Command	Description
p	Paste the specified buffer after the current cursor position or line. If no buffer is specified (with the " command), 'p' uses the general buffer.
P	Paste the specified buffer before the current cursor position or line. If no buffer is specified (with the " command), “P” uses the general buffer.
x	Delete the character under the cursor. A count specifies how many characters to delete. The characters after the cursor are deleted.
X	Delete the character before the cursor.
y	Yank text, putting the result into a buffer. The “yy” command yanks the current line. Entering a number yanks that many lines. The buffer can be specified with the " command. If no buffer is specified, the general buffer is used.
Y	Yank the current line into the specified buffer. If no buffer is specified, the general buffer is used.

Table 15 describes the commands to insert new text.

Table 15 **Inserting New Text**

vi Command	Description
A	Append at the end of the current line.
I	Insert from the beginning of a line.
O	Enter insert mode in a new line above the current cursor position.
a	Enter insert mode; the characters typed in are inserted after the current cursor position. A count inserts all the text that was inserted that many times.
i	Enter insert mode, the characters typed in are inserted before the current cursor position. A count inserts all the text that was inserted that many times.
o	Enter insert mode in a new line below the current cursor position.

Table 16 describes the commands to move the cursor within the file.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 16 **Moving the Cursor Within the File**

vi Command	Description
^B	Scroll backward one page. A count scrolls that many pages.
^D	Scroll forward half a window. A count scrolls that many lines.
^F	Scroll forward one page. A count scrolls that many pages.
^H	Move the cursor one space to the left. A count moves that many spaces.
^J	Move the cursor down one line in the same column. A count moves that many lines down.
^M	Move to the first character on the next line.
^N	Move the cursor down one line in the same column. A count moves that many lines down.
^P	Move the cursor up one line in the same column. A count moves that many lines up.
^U	Scroll backward half a window. A count scrolls that many lines.
$	Move the cursor to the end of the current line. A count moves to the end of the following lines.
%	Move the cursor to the matching parenthesis or brace.
^	Move the cursor to the first non-whitespace character.
(	Move the cursor to the beginning of a sentence.
)	Move the cursor to the beginning of the next sentence.
{	Move the cursor to the preceding paragraph.
}	Move the cursor to the next paragraph.
|	Move the cursor to the column specified by the count.
+	Move the cursor to the first non-whitespace character in the next line.
-	Move the cursor to the first non-whitespace character in the previous line.
_	Move the cursor to the first non-whitespace character in the current line.
0	Move the cursor to the first column of the current line.
B	Move the cursor back one word, skipping over punctuation.
E	Move forward to the end of a word, skipping over punctuation.
G	Go to the line number specified as the count. If no count is given, go to the end of the file.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 16 **Moving the Cursor Within the File (Continued)**

vi Command	Description
H	Move the cursor to the first non-whitespace character at the top of the screen.
L	Move the cursor to the first non-whitespace character at the bottom of the screen.
M	Move the cursor to the first non-whitespace character in the middle of the screen.
W	Move forward to the beginning of a word, skipping over punctuation.
b	Move the cursor back one word. If the cursor is in the middle of a word, move the cursor to the first character of that word.
e	Move the cursor forward one word. If the cursor is in the middle of a word, move the cursor to the last character of that word.
h	Move the cursor one character position to the left.
j	Move the cursor down one line.
k	Move the cursor up one line.
l	Move the cursor one character position to the right.
w	Move the cursor forward one word. If the cursor is in the middle of a word, move the cursor to the first character of the next word.

Table 17 describes the commands to move the cursor around the screen.

Table 17 **Moving the Cursor Around the Screen**

vi Command	Description
^E	Scroll forwards one line. A count scrolls that many lines.
^Y	Scroll backwards one line. A count scrolls that many lines.
z	Redraw the screen with the following options: • z<return> puts the current line on the top of the screen. • z. puts the current line on the center of the screen. • z- puts the current line on the bottom of the screen. If you specify a count before the z command, it changes the current line to the line specified. For example, 16z. puts line 16 on the center of the screen.

Table 18 describes the commands to replace text.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 18 **Replacing Text**

vi Command	Description
C	Change to the end of the line from the current cursor position.
R	Replace characters on the screen with a set of characters entered, ending with <Esc>.
S	Change an entire line.
c	Change until cc changes the current line. A count changes that many lines.
r	Replace one character under the cursor. Specify a count to replace a number of characters.
s	Substitute one character under the cursor, and go into insert mode. Specify a count to substitute a number of characters. A dollar sign ($) is placed at the last character to be substituted.

Table 19 describes the commands to search for text or characters in the file.

Table 19 **Searching for Text or Characters**

vi Command	Description
,	Repeat the last f, F, t or T command in the reverse direction.
/	Search the file downwards for the string specified after the /.
;	Repeat the last f, F, t or T command.
?	Search the file upwards for the string specified after the ?.
F	Search the current line backwards for the character specified after the F command. If found, move the cursor to the position.
N	Repeat the last search done by / or ?, except in the reverse direction.
T	Search the current line backwards for the character specified after the T command, and move to the column after the character if it is found.
f	Search the current line for the character specified after the f command. If found, move the cursor to the position.
n	Repeat the last search done by / or ?.
t	Search the current line for the character specified after the t command, and move to the column before the character if it is found.

Table 20 describes the commands to manipulate character and line formatting.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 20 **Manipulating Character and Line Formatting**

vi Command	Description
~	Switch the case of the character under the cursor.
<	Shift the lines up to the left by one shiftwidth. << shifts the current line to the left and can be specified with a count.
>	Shift the lines up to the right by one shiftwidth. >> shifts the current line to the right and can be specified with a count.
J	Join the current line with the next one. A count joins that many lines.

Table 21 describes the commands to save and quit.

Table 21 **Saving and Quitting**

vi Command	Description
ZZ	Exit the editor, saving if any changes were made.

Table 22 describes miscellaneous commands.

Table 22 **Miscellaneous Commands**

vi Command	Description
^G	Show the current filename and the status.
^L	Clear and redraw the screen.
^R	Redraw the screen removing false lines.
^[	Cancel a partially formed command (escape key).
^^	Go back to the last file edited.
!	Execute a shell (not supported).
&	Repeat the previous :s command.
.	Repeat the last command that modified the file.
:	Begin typing an EX editor command. The command is executed when the user presses <Enter>.
@	Type the command stored in the specified buffer.
U	Restore the current line to the previous state before the cursor entered the line.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 22 **Miscellaneous Commands (Continued)**

vi Command	Description (Continued)
m	Mark the current position with the character specified after the m command.
u	Undo the last change to the file. Typing u again will redo the change.

2.9.3 EX commands

The vi editor is built upon another editor, called the EX. The EX editor only edits by line. From the vi editor you use the : command to start entering an EX command. The following list is not complete; however, it includes the most commonly used commands. If more than one line is to be modified by certain commands (such as :s and :w), the range must be specified before the command. For example, to substitute lines 3 through 15, the command is :3,15s/from/this/g.

Table 23 describes the EX commands.

Table 23 **EX commands**

vi Command	Description
:ab string strings	Abbreviation. If a word is typed in vi corresponding to string1, the editor automatically inserts the corresponding words. For example, the abbreviation :ab usa United States of America inserts the words United States of America whenever the word usa is typed in.
:map keys new_seq	Mapping. This lets you map a key or a sequence of keys to another key or sequence of keys.
:q	Quit vi. If there have been changes made, the editor issues a warning message.
:q!	Quit vi without saving changes.
:s/pattern/ to_pattern/ options	Substitute. This substitutes the specified pattern with the string in the to_pattern. Without options, it only substitutes the first occurrence of the pattern. If a g is specified, all occurrences are substituted.
:set [all]	Sets some customizing options to vi and EX. The :set all command gives all the possible options.
:una string	Removes the abbreviation previously defined by :ab.
:unm keys	Removes the mapping defined by :map.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 23 **EX commands (Continued)**

vi Command	Description (Continued)
:vi filename	Starts editing a new file. If changes have not been saved, the editor displays a warning.
:w	Write out the current file.
:w filename	Write the buffer to the filename specified.
:w >> filename	Append the contents of the buffer to the filename.
:wq	Write the buffer and quit.

2.10 Configuration Rollback

The Configuration Rollback feature provides the ability to undo configurations and revert to previous router configuration states while minimizing impacts to services.

This feature gives the operator better control and visibility over the router configurations and reduces operational risk while increasing flexibility and providing powerful recovery options.

Configuration rollback is useful in cases where configuration changes are made but the operator later decides not to keep the changes (for example, experimentation or when problems are identified in the configuration during actual network operation).

The advantages of this feature include the following.

- Changes made to the router configuration are performed with minimal impact on services being provided by the SR because the router does not need to be rebooted.
- There is no impact in areas of the configuration that did not change.

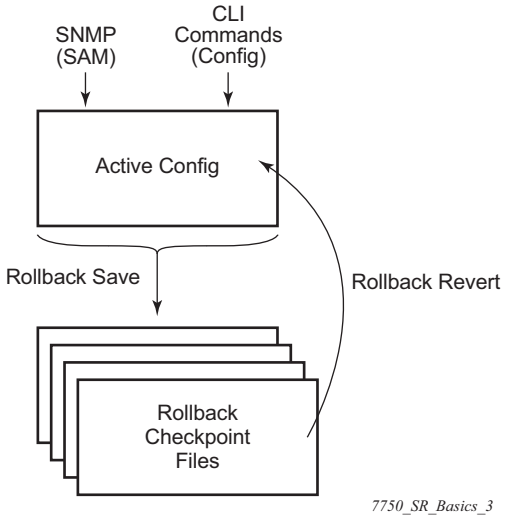
With the rollback feature, the operator can smoothly revert to previous configurations.

Configuration parameters that are changed or items that the changed configuration has dependencies on are removed (revert to default) and the previous values are restored, which may briefly impact services.

A history of changes is preserved using checkpoint IDs, which allows rollback to different points, as well as examination of changes made, as shown in Figure 5.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Figure 5 **Rollback Operation**



2.10.1 Feature Behavior

The following list describes detailed behavior of the rollback feature, including the applicable CLI commands.

- The user can create a rollback checkpoint and later revert to this checkpoint with minimal impact to services.

  ```
  admin>rollback# save [comment comment-string]
  comment-string: a char comment associated with the
  checkpoint, maximum 255 characters
  ```

- Rollback checkpoints include all current operationally active configurations:
  - changes from direct CLI commands in the configuration branch
  - SNMP sets
- Rollback checkpoints do not include BOF configurations. The BOF file and BOF configuration are not part of a rollback save or rollback. A rollback does not change the BOF configuration. The BOF contains basic information for the node and does not change frequently; changes are mostly made during initial commissioning of the node.
- A rollback save feature can be automatically executed (for example, scheduled monthly) using the CRON facility of SR OS.
- The latest rollback checkpoint file uses the suffix .rb. The next latest rollback checkpoint file has the suffix “.rb.1”, the next oldest has the suffix “rb.2”, and so on.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
file-url.rb  <--- latest rollback file
file-url.rb.1
...
file-url.rb.9  <--- oldest rollback file
```

- When a **rollback save** is executed, the system shifts the file suffix of all the previous checkpoints by 1 (new ID = old ID + 1). If there are already as many checkpoint files as the maximum number supported, the last checkpoint file is deleted.
- The maximum number of rollback checkpoints is configurable and defaults to 10, which includes the latest file and files 1 through 9.
- The locations and names of the rollback checkpoint files are configurable to be local (on the compact flash) or remote. The *file-url* must contain a path/directory and filename with no suffix. The .rb suffix for rollback checkpoint files is automatically appended to the rollback checkpoint files.

  ```
  config>system>rollback# rollback-location file-url
  ```
- There is no default rollback location. If a rollback location is not specified or it is cleared using **no rollback-location**, and a **rollback save** is attempted, the **rollback save** fails and returns an error message.
- The entire set of rollback checkpoint files can be copied from the active CPM CF to the standby CPM CF. This synchronization is done using the following command:

  ```
  admin>redundancy# rollback-sync
  ```
- The operator can enable an automatic synchronization of rollback checkpoint files between the active CPM and standby CPM. When this automatic synchronization is enabled, a **rollback save** causes the new checkpoint file to be saved to both the active and standby CPMs. The suffixes of the old checkpoint files on both active and standby CPMs are incremented.

  Automatic synchronization only causes the new checkpoint file to be copied to both CFs. The older checkpoint files are not automatically copied from active to standby but can be copied manually with **admin redundancy rollback-sync**.
- The **config>redundancy>synchronize {boot-env | config}** and **admin>redundancy>synchronize {boot-env | config}** commands do not apply to rollback checkpoint files. These commands do not manually or automatically synchronize rollback checkpoint files. The dedicated **rollback-sync** commands must be used to synchronize rollback checkpoint files.
- Rollback files can be deleted using a dedicated rollback checkpoint deletion command.

  ```
  admin>rollback# delete {latest-rb | checkpoint-id}
  ```

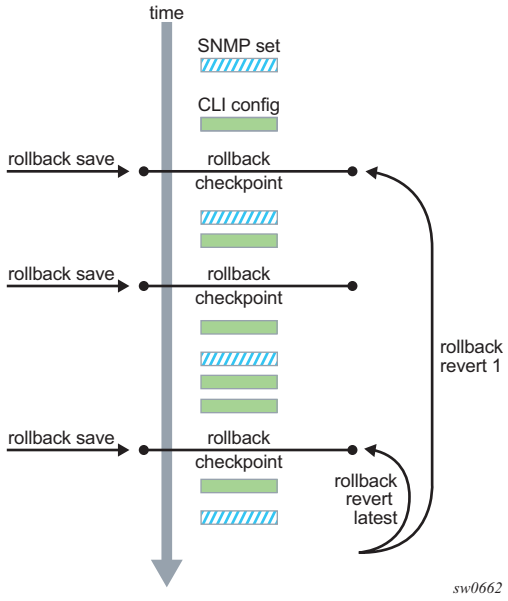

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Deleting a rollback checkpoint causes the suffixes to be adjusted (decremented) for all checkpoints older that the one that was deleted in order to close the “hole” in the list of checkpoint files and create room to create another checkpoint.
- If **config>redundancy>rollback-sync** is enabled, a **rollback delete** also deletes the equivalent checkpoint on the standby CF and shuffles the suffixes on the standby CF.
- If an operator manually deletes a rollback checkpoint file using **file delete**, the suffixes of the checkpoint files are not shuffled, nor is the equivalent checkpoint file deleted from the standby CF. This manual deletion creates a “hole” in the checkpoint file list until enough new checkpoints have been created to roll the “hole” off the end of the list.

• Figure 6, shows how a configuration is rolled back to a previous configuration (a saved rollback checkpoint). The previous configuration is loaded and takes operational effect.

```
admin>rollback# revert [latest-rb | checkpoint-id]
```

Figure 6 **Configuration Rollback**



• A rollback revert does not affect the currently stored rollback checkpoint files; files are not deleted or renumbered. This means that if an operator issues the command **rollback revert 3** and then issues the **rollback save** command, the resulting rollback checkpoint files *file-url.rb* and *file-url.rb.4* contain the same rollback state/configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The **boot-good-exec** or **boot-bad-exec** command is not automatically executed after a rollback.
- Impacts to the running services are minimized during a rollback:
  - There is no impact in areas of the configuration that did not change.
  - Configuration parameters that are changed or items that the changed configuration has dependencies on are removed (revert to default) and the previous values are restored, which may briefly impact services. The following are examples of service impact.
    - If the currently active configuration contains **configure port 5/1/1 dwdm tdcm dispersion -1000** and the rollback checkpoint contains **configure port 5/1/1 dwdm tdcm dispersion -1010**, the operational dispersion transitions from -1000 to 0 and then back to -1010 for port 5/1/1, which causes a traffic interruption.
    - If changing neighbor 1 of an MC-APS port, the port must be configured as **no neighbor** and then configured as neighbor 2. Moving through the **no neighbor** intermediate state requires the working and protection circuits to be torn down and rebuilt. This impacts the 7450 ESS and 7750 SR.
- A rollback undoes any SNMP sets or direct CLI configuration commands that occurred since the last checkpoint creation.
- During the period when a node is processing a **rollback revert**, both CLI commands from other users and SNMP commands continue to be processed. The only commands that are blocked during a **rollback revert** are other rollback commands, including **revert**, **save**, and **compare**. Only one **rollback** command can be executing at a time on a node.
- Commands are available to view and compare the various rollback checkpoints to current operating and candidate configurations.
- Rollback checkpoint files are not guaranteed to be in any particular format. They are not interchangeable with normal configuration files or executable scripts. A normal configuration file from an **admin save** cannot be renamed as a rollback checkpoint and then referenced for a **rollback revert** operation. Only rollback checkpoint files generated with **rollback save** can be used for rollback revert operations.
- If a hardware change is made after a **rollback save**:
  - a rollback can be executed as long as the hardware change was an addition of hardware to the node (for example, a new card or IOM was installed in a previously empty slot)
  - a rollback is not guaranteed to work if hardware was removed or changed (for example, an XCM/IOM was removed, or an XMA/MDA was swapped for a different XMA/MDA type)
- Rollback across a change to the following parameters is not supported:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

  - **chassis-mode**
  - **configure isa application-assurance-group minimum-isa-generation**
- Rollback is supported even after an **admin reboot** is performed or the primary configuration in the BOF is changed and an **admin reboot** is performed. The **admin reboot** command does not “break the chain” for rollback.
- Lawful intercept configuration under the **config**>**li** branch is not affected by a rollback or rescue. LI configuration is not saved in the rollback checkpoint or rescue file, and a rollback revert does not affect any configuration under the **config>li** branch.
- Any configuration or state change performed under the debug branch of the CLI is not saved in the rollback checkpoint file or impacted by a rollback.
- Rollbacks to a checkpoint created in a more recent release are not supported (for example, a node running in 9.0r5 cannot roll back to a checkpoint created in 9.0r7).
- The following list captures some side effects and specific behaviors of a rollback revert. Some of these side effects are not related purely to configuration, that is, in the CLI configuration branch, and may have interactions with tools commands, RADIUS, and so on.
  - SAA jobs that are running when a rollback revert is initiated and need configuration changes due to the rollback, are stopped. If the SAA job is a continuous type, it is restarted as part of the rollback revert after the configuration changes have been applied, just as if the operator had typed **no shutdown** for the continuous SAA job. Non-continuous SAA jobs that were modified by the rollback need to be manually restarted if they need to be run again.
  - If **max-nbr-mac-addr** is reduced as part of the revert and the number of MAC addresses in the forwarding database is greater than the **max-nbr-mac-addr**, the rollback is aborted before any actions are taken and an informative error message is provided. The operator must take actions to remove the MAC addresses if they wish to proceed with the rollback.
  - If active subscribers or subscriber hosts or DHCP lease states are present, some associated configuration changes may be blocked, just as those same changes would be blocked if an operator tried to make them using the CLI.
  - When trying to delete an SLA profile being used by active subscriber hosts, or trying to change a NAT policy in a subscriber profile, if certain configuration changes associated with the hosts or lease states are required as part of the rollback but those changes are blocked, then for each blocked configuration item a warning is printed, that particular configuration item is not changed, and the rollback continues. This is supported on the 7450 ESS and 7750 SR.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- After a multi-chassis peer shutdown or if configuration changes have been made that affect the contents of the distributed database (for example, synchronization tag creation or deletion), further configuration changes related to that peer may be temporarily refused. The duration of the temporary configuration freeze depends on the size of the distributed database. A rollback attempting to make those refused configuration changes fails and an error message is provided to the CLI user.
- If a **force-switchover** command (for example, **tools perform service id 1 endpoint "x" force-switchover spoke-sdp-fec 1**) has been applied to a **spoke-sdp-fec** of a dynamic multi-segment pseudowire, and a rollback revert needs to change the admin state of the **spoke-sdp-fec** (for example, to modify **spoke-sdp-fec** parameters that may be dependent on the admin state), the rollback revert automatically removes the **force-switchover** and the node reverts to whatever is the best spoke SDP in the redundant set.
- Rollback impacts the configuration state of the router, and as with normal operator CLI or SNMP configuration changes, additional actions or steps may need to occur before certain configuration changes take operational effect. Some examples include the following.
  - Configuration changes that require a manual **shutdown** command and then **no shutdown** command in order to take operational effect also need this manual **shutdown/no shutdown** command in order to take operational effect after a rollback if the rollback changes those configuration items. Some examples include the following.
  - Changes to autonomous system or confederation values require a BGP **shutdown**/**no shutdown** command.
  - Changes to VPRN **max-routes** require a **shutdown/no shutdown** command on the VPRN service.
  - Changes to OSPF or IS-IS **export-limit** require a **shutdown/no shutdown** command on OSPF or IS-IS.
  - For configuration changes to an MSAP policy that normally require a **tools perform subscriber-mgmt eval-msap** command to take operational effect on subscribers that are already active, if a rollback changes the MSAP policy configuration, the operator must run the **eval-msap** tools command to have the changes applied to the active subscribers.
- Any uncommitted changes (for example, the **begin** command was entered and some changes were made, but the **commit** command was never entered) in the following areas are lost or cleared when a rollback revert is initiated:
  - **config>app-assure>group policy**
  - **config>router>policy-options**
  - **config>system>sync-if-timing**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Some **card** and **mda** commands require a reboot, removal, or rebuild of an entire card or XMA/MDA. When these commands need to be executed as part of a rollback, the impacted cards and MDAs are listed in a warning and the operator is prompted with a single y/n prompt to proceed. This prompt will not occur for a rollback initiated via SNMP or if the operator uses the **now** keyword with the **rollback revert** command. Some examples of **card** and **mda** commands that may cause a prompt are:
  - **config>card>card-type**
  - **config>card>mda**
  - **config>card>mda>mda-type**
- Although the use of the <Ctrl-c> key combination is not recommended during a rollback revert, it is supported via CLI or SNMP. Interrupting a rollback revert may leave the router in a state that is not necessarily between the old active configuration and the rollback checkpoint, as the rollback processing may have been in the middle of tearing things down or rebuilding configurations. A strong warning is issued in this case to indicate that the operator must examine the configuration and potentially issue another rollback revert to return to a known and coherent configuration.
- An HA CPM switchover during a rollback revert causes the rollback operation to abort. The newly active CPM has an indeterminate configuration. When an HA switchover occurs during a rollback (or within a few seconds of a rollback completing), the operator is advised to repeat the rollback revert operation to the same checkpoint.
- A rollback revert operation does not check authorization of each command that is applied during the revert. Permission to execute the revert operation, that is, authorization to execute the **admin rollback revert** command, should only be given to users who are allowed to initiate a rollback revert. It is generally recommended that only system administrators be allowed access to the file system where the rollback files are stored so that they cannot be manually edited.

2.10.2 Rollback and SNMP

The SR OS has SNMP support for rollback status and control. See the TIMETRA-SYSTEM-MIB for details (for example, items such as tmnxSysRollbackStarted).

When the router is doing a rollback revert, SNMP managers see a tmnxSysRollbackStarted trap, then a rapid set of “config change” traps, and finally, the tmnxSysRollbackStatusChange trap.

During the period when a router is processing a rollback revert, both CLI commands from other users and SNMP commands continue to be processed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2.10.3 Rescue Configuration

A special rescue configuration checkpoint can be created that an operator can revert to at any time. The rescue configuration has its own keyword (**rescue**) and does not use the same rolling suffix indices as the normal rollback checkpoints. This allows the operator to easily return to the rescue configuration state without having to consider a checkpoint index, and ensures that the rescue checkpoint is always available and does not roll off the bottom of the list of checkpoints.

The operator should define a basic rescue configuration that is known to work and give appropriate management access to the node.

The location and filename of the rescue file are configurable. The SR OS appends the .rc suffix to the specified rescue filename.

2.10.4 Operational Guidelines

The following points offer some operational guidance on the use of rollback.

- The **admin save** and **admin rollback save** commands should be performed periodically.
- The **admin save** command can be used to back up a complete configuration file that can be used during router reboot, with the following considerations:
  - used with a reboot as a last resort
  - performed after any major hardware changes or major service changes
  - performed after any software upgrade
- The **admin rollback save** command can be used to create a rollback checkpoint as follows:
  - to be used for intermediate checkpoints that can be recovered with minimal impact to services
  - to be performed each time a moderate number of configuration changes have been made
  - to be performed after any hardware changes
  - to be performed after any software upgrade
  - to be scheduled with CRON (for example, once every one or two weeks)
- A new **admin rollback save rescue** must be created when hardware is changed.
- Rollback checkpoint files are not editable, or compatible or interchangeable with configuration files generated with **admin save**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The repeated use of the **admin rollback save**, **admin rollback delete**, and **admin rollback revert** commands over the course of weeks or months is not recommended without also executing an occasional **admin save**. In a serious situation, use one of the saved configurations as the primary configuration for an **admin reboot**.
- For a software upgrade, it is recommended that a rollback checkpoint be created using **admin rollback save**, in addition to saving the configuration with **admin save**, after an upgrade has been performed and the system is operating as expected. This ensures that a good checkpoint that is fully compatible with the new release is available at a point shortly after the upgrade.
- An operator can create a set of rollback checkpoints to support busy or quiet days or weekends or weekdays and use CRON to shift between them.
- It is beneficial to create a rollback checkpoint before a rollback revert is initiated, especially if significant configuration changes have been applied since the last checkpoint was created. If the rollback is especially significant, that is, there are a lot of major changes, it is also a good practice to perform an **admin save** in case a full reboot is required to recover from an issue.
- A rollback failure may occur in some limited cases where the node needs a long time to complete one of the resulting configuration changes. If a rollback (for example, **rollback revert 5**), fails during execution, it should be attempted again. The second attempt typically completes the remaining configuration changes required to fully revert to the desired checkpoint.
- When a new backup CPM is commissioned, the user executes the **admin redundancy rollback-sync** command to copy the entire set of rollback files from the active CPM CF to the new standby CPM CF. If the operator wants the system to automatically copy new rollback checkpoints to both CFs whenever a new checkpoint is created, the **configure redundancy rollback-sync** command should be enabled.
- An HA CPM switchover during a rollback revert causes the rollback operation to abort. The newly active CPM has an indeterminate configuration. A log event is created in this case to warn the operator. When an HA switchover occurs during a rollback or within a few seconds of a rollback completing, the operator is advised to repeat the rollback revert operation to the same checkpoint.
- A rollback checkpoint stores the rollback location and the **local-max-checkpoints** and **remote-max-checkpoints** values, and it is possible that a rollback revert operation may change those values. If an operator changes the **local-max-checkpoints** or **remote-max-checkpoints** values, it is recommended that all the existing checkpoints be deleted to prevent a subsequent rollback revert from changing the maximum values to any of the previous values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If a warning prompt (**y/n**) is displayed when a rollback revert is initiated, it is highly recommended that the operator respond **no** to the warning prompt the first time, save a rollback checkpoint before attempting this rollback revert, execute the revert again, and respond **yes**. If the rollback encounters problems, a revert to the saved checkpoint can be used to return to the initial configuration state.

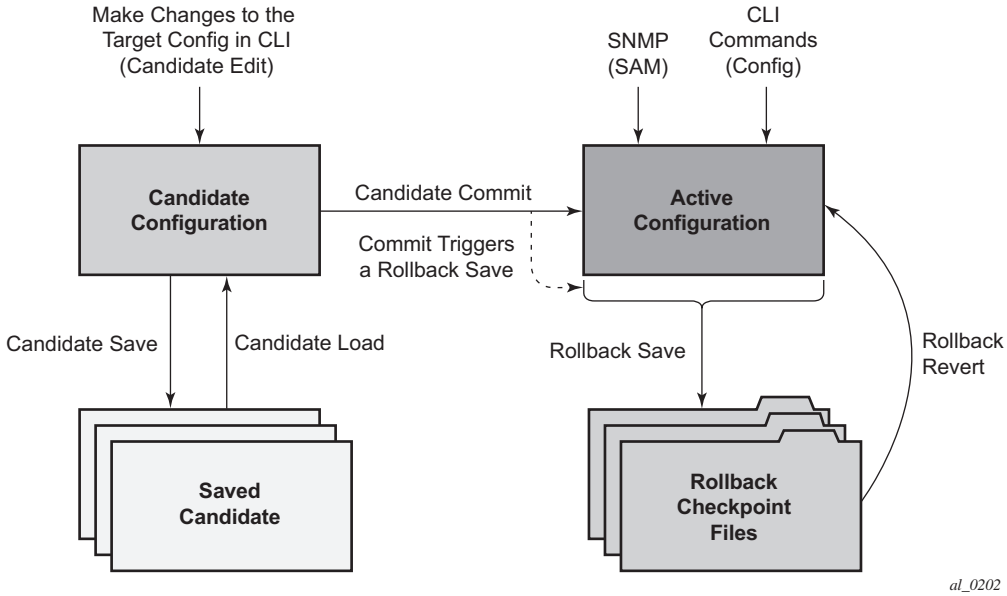
2.11 Transactional Configuration

Transactional configuration allows an operator to edit a candidate configuration (a set of configuration changes) without causing operational changes in the router (the active or operational configuration). When the candidate configuration is complete, the operator can explicitly commit the changes to make the entire new configuration become active.

Transactional configuration gives the operator better control and visibility over their router configurations and reduces operational risk while increasing flexibility.

The transactional configuration and configuration rollback functions combine to provide the operational model depicted in Figure 7.

Figure 7 **Router Configuration with Rollback and Transactions**



© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2.11.1 Basic Operation

In order to edit the candidate configuration, the operator must first enter the candidate edit mode (edit-cfg) with the **candidate>edit** command. The operator can enter and quit the configuration mode as many times as they wish before finally committing the candidate configuration.

In edit-cfg mode, the operator builds a set of candidate configuration changes using the same CLI tree as the standard line-by-line, non-transactional configuration. Tab completion and keyword syntax checking is available.

Just as there is a single operational active configuration that can be modified simultaneously by multiple users in the SR OS, there is also a single global candidate configuration instance. All users make changes in the same global candidate configuration, and a **commit** operation by any user commits the changes made by all users.

Users can exclusively create a candidate configuration by blocking other users and sessions of the same user from entering edit-cfg mode by specifying the **exclusive** parameter. The **config>system>management-interface>cli>classic-cli>allow-immediate** command can be used to enforce the use of candidate configuration, instead of allowing immediate line-by-line configuration changes.

If a **commit** operation is successful, all of the candidate changes take operational effect and the candidate is cleared. If there is an error in the processing of the commit, or a **commit confirmed** is not confirmed and an auto-revert occurs, the router returns to a configuration state with none of the candidate changes applied. The operator can then continue editing the candidate and try a commit later.

All commands in the candidate configuration must be in the correct order for a commit to be successful. Configuration that depends on other candidate objects must be placed after those objects in the candidate. A set of candidate editing commands (**copy**, **insert**, and so on) are available to correct and reorder the candidate configuration.

The edit-cfg mode is primarily intended for building a candidate configuration while navigating the **configure** branch of the CLI. Many CLI commands in branches other than **configure** are supported while in edit-cfg mode, but access to some CLI branches and commands are blocked, including:

- **exec** command
- **enable-admin** command
- **enable-dynamic-services-config** command
- **admin** branch
- **bof** branch

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **debug** branch
- **tools** branch

The candidate configuration can be saved to a file and subsequently loaded into a candidate configuration. A saved candidate is similar to, but not the same as, an SR OS configuration file generated with an **admin save** command. The saved candidate cannot be used in general as a configuration file and may not **exec** without failures.

There is no SNMP access to the candidate configuration and no SNMP management of candidates, although any configuration changes made using transactional configuration are reported via the standard SR OS SNMP change traps and basic candidate status information is available via SNMP.

A commit may fail for a number of reasons, including:

- misordering: the candidate configuration has changes that are not in the correct order, that is, an object is referred to before it is actually created
- invalid options and combinations: although many syntax errors are eliminated during the candidate editing process, the candidate configuration may contain combinations of configurations and options that are not valid and are rejected when the SR OS attempts to have them take operational effect
- out of resources: rhe application of the candidate may exhaust system resources, such as queue resources

Error messages are provided for commit failures to help the operator take the necessary actions to correct the candidate.

Standard line-by-line, non-transactional CLI and SNMP commands are not blocked during the creation or editing of a candidate or the processing of a commit. These commands take immediate operational effect when <Enter> is pressed.

2.11.2 Transactions and Rollback

By default, the SR OS automatically creates a new rollback checkpoint after a **commit** operation. The rollback checkpoint includes the new configuration changes made by the commit. An optional **no-checkpoint** keyword can be used to prevent the auto-creation of a rollback checkpoint after a commit. If the commit fails, no new rollback checkpoint is created.

When the **commit confirmed** option is used, a rollback checkpoint is created after the processing of the commit and exists whether the commit is automatically reverted or not.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Transactional configuration relies on the rollback mechanism to operate. Any commands and configurations that are not supported in a rollback revert are also not supported in edit-cfg mode; for example, changes to **chassis-mode**.

2.11.3 Authorization

Authorization works transparently in edit-cfg mode and no unique or new local profile or TACACS+ permissions rules are required other than allowing access to the **candidate** branch. For example, if an operator has permission to access the **configure filter** context, they automatically also have access to the **configure filter** context when in edit-cfg mode.

If the operator's profile allows access to the candidate **load** and **save** commands, the operations load and save only those items that the user is authorized to access.

The candidate view only displays the items that the user is authorized to access.

The candidate editing commands (such as adding lines, removing lines, and delete operations) only allow operations on items that the user is authorized to access.

The candidate **commit** and **discard** commands, along with **admin rollback revert**, operate on the entire candidate and impact all items; authorization does not apply.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3 Command Trees

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

admin

3.1 admin Commands

- admin
  - application-assurance
    - group
    - group
      - url-list
    - upgrade
  - certificate
    - clear-ocsp-cache
    - cmpv2
      - cert-request
      - clear-request
      - initial-registration
      - key-update
      - poll
      - show-request
    - convert-file
    - crl-update
    - display
    - est
      - cacert
      - enroll
      - renew
    - export
    - gen-keypair
    - gen-local-cert-req
    - import
    - reload
    - secure-nd-export
    - secure-nd-import
  - clear
    - lockout
    - password-history
  - compare
  - debug-save
  - disconnect
  - display-config
  - enable-tech
  - ipsec
    - display-key
    - transport-mode
      - display-key
  - nat
    - save-deterministic-script
  - reboot
  - redundancy
    - cert-sync
    - force-switchover
    - rollback-sync

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

admin redundancy synchronize

- synchronize
- reset-policy-exclusive
- rollback
  - compare
  - delete
  - revert
  - save
  - view
- satellite
  - eth-sat
    - reboot
    - sync-boot-env
    - tech-support
  - tdm-sat
    - reboot
    - sync-boot-env
    - tech-support
- save
- set-time
- system
  - license
    - activate
    - validate
  - security
    - hash-control
      - custom-hash
  - system
  - telemetry
    - grpc
      - subscription
        - subscription cancel-all
- tech-support
- view

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bof

3.2 bof Commands

- bof
  - address
  - auto-boot
  - autoconfigure
    - ipv4
      - dhcp
    - ipv6
      - dhcp
  - autonegotiate
  - console-speed
  - dns-domain
  - duplex
  - encrypt
  - encryption-key
  - ess-system-type
  - fips-140-2
  - ip-mtu
  - li-local-save
  - li-separate
  - license-file
  - password
  - persist
  - primary-config
  - primary-dns
  - primary-image
  - save
  - secondary-config
  - secondary-dns
  - secondary-image
  - speed
  - static-route
  - system-base-mac
  - system-profile
  - tertiary-config
  - tertiary-dns
  - tertiary-image
  - wait

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.3 candidate Commands

— candidate
  — commit
  — confirm
  — copy
  — delete
  — discard
  — edit
  — goto
  — insert
  — load
  — quit
  — redo
  — replace
  — save
  — undo
  — view

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4 configure Commands

— configure

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.1 configure aaa Commands

- aaa
  - acct-on-off-group
    - description
  - diameter
    - node
      - connection-timer
      - description
      - ipv6-source-address
      - peer
        - address
        - connection-timer
        - default-peer
        - preference
        - route
          - route index
          - preference
        - shutdown
        - watchdog-timer
      - python-policy
      - router
      - source-address
  - diameter-peer-policy
    - applications
    - connection-timer
    - description
    - ipv6-source-address
    - origin-host
    - origin-realm
    - peer
      - address
      - connection-timer
      - destination-host
      - destination-realm
      - preference
      - shutdown
      - transaction-timer
      - transport
      - watchdog-timer
    - proxy
      - mcs-peer
      - router
      - shutdown
    - python-policy
    - router
    - source-address
    - transaction-timer
    - vendor-support
    - watchdog-timer
  - isa-radius-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure aaa isa-radius-policy acct-include-attributes

- acct-include-attributes
  - acct-delay-time
  - acct-trigger-reason
  - called-station-id
  - calling-station-id
  - circuit-id
  - class
  - credit-control-quota
  - dhcp-options
  - dhcp-vendor-class-id
  - dhcp6-options
  - frame-counters
  - framed-ip-addr
  - framed-ip-netmask
  - framed-ipv6-prefix
  - hardware-timestamp
  - inside-service-id
  - ipv6-address
  - mac-address
  - millisecond-event-timestamp
  - multi-session-id
  - nas-identifier
  - nas-ip-address
  - nas-port
  - nas-port-id
  - nas-port-type
  - nat-subscriber-string
  - octet-counters
  - outside-ip
  - outside-service-id
  - port-range-block
  - release-reason
  - remote-id
  - session-time
  - subscriber-data
  - subscriber-id
  - ue-creation-type
  - user-name
  - wifi-rssi
  - wifi-ssid-vlan
  - xconnect-tunnel-home-address
  - xconnect-tunnel-local-ipv6-address
  - xconnect-tunnel-remote-ipv6-address
  - xconnect-tunnel-service
  - xconnect-tunnel-type
- acct-update-triggers
  - address-state
  - soft-quota-exhausted
- auth-include-attributes
  - called-station-id
  - calling-station-id
  - circuit-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure aaa isa-radius-policy auth-include-attributes dhcp-options

- dhcp-options
- dhcp-vendor-class-id
- dhcp6-options
- framed-ip-addr
- ipv6-address
- mac-address
- nas-identifier
- nas-ip-address
- nas-port
- nas-port-id
- nas-port-type
- remote-id
- wifi-ssid-vlan
- xconnect-tunnel-home-address

- description
- nas-ip-address-origin
- password
- periodic-update
- python-policy
- **servers**
  - access-algorithm
  - retry
  - router
  - server
    - accounting
    - authentication
    - coa
    - ip-address
    - secret
    - shutdown
  - source-address-range
  - timeout
- user-name-format

- l2tp-accounting-policy
  - accounting-type
  - acct-tunnel-connection-fmt
  - description
  - include-radius-attribute
    - calling-station-id
    - nas-identifier
    - nas-port
    - nas-port-id
    - nas-port-type
    - radius-accounting-server
  - radius-accounting-server
    - access-algorithm
    - retry
    - router
    - server
    - source-address
    - timeout
  - radius-server-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure aaa l2tp-accounting-policy request-script-policy

- request-script-policy
- shutdown
- radius-coa-port
- radius-script-policy
  - action-on-fail
  - description
  - primary
    - script-url
    - shutdown
  - secondary
    - script-url
    - shutdown
- radius-server-policy
  - accept-script-policy
  - acct-on-off
  - acct-request-script-policy
  - auth-request-script-policy
  - buffering
  - description
  - python-policy
  - request-script-policy
  - servers
    - access-algorithm
    - buffering
      - acct-interim
      - acct-start
      - acct-stop
    - disable-stickiness
    - health-check
      - down-timeout
      - test-account
        - interval
        - password
        - shutdown
        - user-name
    - hold-down-time
    - ipv6-source-address
    - retry
    - router
    - server
    - source-address
    - timeout
- route-downloader
  - base-user-name
  - default-metric
  - default-tag
  - description
  - download-interval
  - max-routes
  - password
  - radius-server-policy
  - retry-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure aaa route-downloader shutdown

- shutdown
- wpp
  - portal-groups
    - portal-group
      - description
      - portal
      - shutdown
  - system-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.2 configure application-assurance Commands

- application-assurance
  - aarp
    - description
    - master-selection-mode
    - peer
    - peer-endpoint
    - priority
    - shutdown
  - bit-rate-high-wmark
  - bit-rate-low-wmark
  - cflowd
    - field
  - datapath-cpu-high-wmark
  - datapath-cpu-low-wmark
  - flow-attribute
    - attribute
  - flow-setup-high-wmark
  - flow-setup-low-wmark
  - flow-table-high-wmark
  - flow-table-low-wmark
  - group
    - aa-sub-congestion-detection
      - rtt-threshold
      - rtt-threshold-rat
      - rtt-threshold-tolerance
      - shutdown
    - aa-sub-remote
    - access-network-location
      - source
        - rtt-threshold
        - rtt-threshold-rat
        - rtt-threshold-tolerance
          - characteristic
          - tcp-mss-adjust
          - url-filter
    - aqp-initial-lookup
    - certificate-profile
      - certificate
      - description
      - shutdown
    - cflowd
      - collector
        - description
        - shutdown
      - comprehensive
        - app-group
        - application
        - flow-rate
        - flow-rate2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group cflowd comprehensive shutdown

- shutdown
- template
  - dynamic-fields
    - field
    - shutdown
  - field-selection
- direct-export
  - collector
    - address
      - shutdown
    - description
  - vlan-id
- export-override
  - prefix
- obfuscation
  - aes-128-encryption
  - aes-256-encryption
- rtp-performance
  - app-group
  - application
  - audio-template
    - dynamic-fields
      - field
      - shutdown
    - field-selection
  - flow-rate
  - flow-rate2
  - shutdown
  - video-template
    - dynamic-fields
      - field
      - shutdown
    - field-selection
  - voice-template
    - dynamic-fields
      - field
      - shutdown
    - field-selection
- shutdown
- tcp-performance
  - app-group
  - application
  - flow-rate
  - flow-rate2
  - shutdown
  - template
    - dynamic-fields
      - field
      - shutdown
    - field-selection
- template-retransmit
- volume

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group cflowd volume rate

- rate
- shutdown
- template
  - dynamic-fields
    - field
    - shutdown
  - field-selection
- description
- dns-ip-cache
  - description
  - dns-match
    - domain
    - server-address
  - ip-cache
    - high-wmark
    - low-wmark
    - size
    - static-address
  - shutdown
- event-log
  - buffer-type
  - max-entries
  - shutdown
  - syslog
    - address
    - description
    - facility
    - port
    - severity
    - vlan-id
- gtp
  - event-log
  - gtp-filter
    - description
    - event-log
    - gtp-in-gtp
    - gtp-tunnel-database
      - default-tunnel-endpoint-limit
      - validate-gtp-tunnels
      - validate-sequence-number
      - validate-source-ip-addr
    - imsi-apn-filter
      - default-action
      - entry
        - action
        - apn
        - mcc-mnc-prefix
        - src-gsn
    - max-payload-length
    - message-type
      - default-action
      - entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group gtp gtp-filter message-type-gtpv2

- message-type-gtpv2
  - default-action
  - entry
- gtpc-inspection
- mode
- shutdown
- http-enrich
- description
- field
  - anti-spoof
  - calling-line-id
  - encode
  - name
  - static-string
- rat-enrichment
  - rat-type
- shutdown
- tls-extension
  - subtype
- http-error-redirect
- description
- error-code
- http-host
- participant-id
- shutdown
- template
- http-match-all-requests
- http-notification
- description
- interval
- script-url
- shutdown
- template
- http-redirect
- captive-redirect
  - vlan-id
- description
- redirect-https
- redirect-url
- shutdown
- tcp-client-reset
- template
- http-x-online-host
- ip-prefix-list
- description
- prefix
- policer
- action
- adaptation-rule
- cbs
- congestion-override
  - cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group policer congestion-override cir

- cir
- mbs
- pir
- congestion-override-stage2
  - cbs
  - cir
  - mbs
  - pir
- description
- flow-count
- gtp-traffic
- mbs
- rate
- rate-percentage
- rate-percentage-stage2
- tod-override
  - cbs
  - description
  - flow-count
  - mbs
  - rate
  - shutdown
  - time-range
- policy
  - abort
  - app-filter
    - entry
      - application
      - description
      - expression
      - flow-setup-direction
      - http-match-all-requests
      - http-port
      - ip-protocol-num
      - network-address
      - protocol
      - server-address
      - server-port
      - shutdown
  - app-group
    - charging-group
    - description
    - export-id
  - app-profile
    - aa-sub-suppressible
    - capacity-cost
    - characteristic
    - description
    - divert
  - app-qos-policy
    - entry
      - action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group policy app-qos-policy entry action abandon-tcp-optimization

- abandon-tcp-optimization
- bandwidth-policer
- dns-ip-cache
- drop
- error-drop
- flow-count-limit
- flow-rate-limit
- fragment-drop
- gtp-filter
- http-enrich
- http-error-redirect
- http-notification
- http-redirect
- mirror-source
- overload-drop
- remark
  - dscp
  - fc
  - priority
- sctp-filter
- session-filter
- tcp-mss-adjust
- tcp-validate
- tls-enrich
- url-filter
  - default-action
  - description

- description
- match
  - aa-sub
  - aa-sub-tethering-state
  - app-group
  - application
  - characteristic
  - charging-group
  - dscp
  - dst-ip
  - dst-port
  - flow-attribute
    - confidence
  - ip-protocol-num
  - src-ip
  - src-port
  - traffic-direction
- shutdown

- app-service-options
  - characteristic
    - default-value
    - value
- application
  - app-group
  - charging-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group policy application charging-group export-id

- export-id
- description
- export-id
- begin
- charging-group
  - description
  - export-id
  - notify-start-stop
- commit
- custom-protocol
  - description
  - expression
  - shutdown
- default-charging-group
- default-tethered-charging-group
- diff
  - ip-protocol-num
- description
  - ip
- policy-override
  - policy
    - characteristic
- port-list
  - description
  - port
- sctp-filter
  - description
  - event-log
  - ppid
    - default-action
    - entry
  - ppid-range
- session-filter
  - default-action
  - description
  - entry
    - action
      - http-redirect
    - description
    - match
      - dns-ip-cache
      - dscp
      - dst-ip
      - dst-port
      - ip-protocol-num
      - src-ip
      - src-port
- shallow-inspection
- statistics
  - aa-admit-deny
    - accounting-policy
    - collect-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group statistics aa-admit-deny gtp-filter-stats

- gtp-filter-stats
- policer-stats
- policer-stats-resources
- sctp-filter-stats
- session-filter-stats
- tcp-validate-stats

- aa-partition
  - accounting-policy
  - collect-stats
  - tethering-summary
  - traffic-type
- aa-sub
  - accounting-policy
  - aggregate-stats
  - app-group
  - application
  - charging-group
  - collect-stats
  - description
  - exclude-tcp-retrans
  - max-throughput-stats
  - protocol
  - radius-accounting-policy
  - usage-monitoring
- aa-sub-study
  - aa-sub
  - accounting-policy
  - collect-stats
- app-group
  - accounting-policy
  - collect-stats
- application
  - accounting-policy
  - collect-stats
- protocol
  - accounting-policy
  - collect-stats
  - shutdown
- threshold-crossing-alert
  - error-drop
    - high-wmark
  - fragment-drop-all
    - high-wmark
  - fragment-drop-out-of-order
    - high-wmark
  - gtp-filter
    - default-gtp-tunnel-endpoint-limit
      - high-wmark
    - gtp-in-gtp
      - high-wmark
      - default-action
        - high-wmark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group statistics threshold-crossing-alert gtp-filter imsi-apn entry

- entry
  - high-wmark
- imsi-apn-filter
  - default-action
    - high-wmark
  - entry
    - high-wmark
- max-payload-length
  - high-wmark
- message-type
  - default-action
    - high-wmark
  - entry
    - high-wmark
  - header-sanity
    - high-wmark
- message-type-gtpv2
  - default-action
    - high-wmark
  - entry
    - high-wmark
- missing-mandatory-ie
  - high-wmark
- tunnel-endpoint-limit
  - high-wmark
- tunnel-resource-limit
  - high-wmark
- validate-gtp-tunnels
  - high-wmark
- validate-sequence-number
  - high-wmark
- validate-src-ip-addr
  - high-wmark
- gtp-sanity-drop
  - high-wmark
- overload-drop
  - high-wmark
- policer
  - high-wmark
- sctp-filter
  - packet-sanity
    - high-wmark
  - ppid
    - default-action
      - high-wmark
    - entry
      - high-wmark
  - ppid-range
    - high-wmark
- session-filter
  - default-action
    - high-wmark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group statistics threshold-crossing-alert session-filter entry

- entry
  - high-wmark
- tcp-validate
  - high-wmark
- tcp-optimizer
  - dack-timeout
  - description
  - init-cwnd-size
  - init-ss-threshold
  - network-rtt-threshold
  - tcp-stack
- tcp-validate
  - description
  - event-log
  - strict
- template
- tethering-detection
  - shutdown
  - single-device
    - expected-ttl
  - cbs
  - mbs
- transit-ip-policy
  - def-app-profile
  - description
  - detect-seen-ip
  - dhcp
    - shutdown
  - diameter
    - application-policy
    - shutdown
  - ipv6-address-prefix-length
  - radius
    - authentication-policy
    - seen-ip-radius-acct-policy
    - shutdown
    - static-aa-sub
  - static-aa-sub
    - ip
  - sub-ident-policy
  - transit-auto-create
    - inactivity-mon
    - inactivity-monitor
    - shutdown
- transit-prefix-policy
  - description
  - entry
    - aa-sub
    - match
      - aa-sub-ip
      - network-ip
  - static-aa-sub

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group transit-prefix-policy static-remote-aa-sub

- static-remote-aa-sub
- url-filter
  - apply-function-specific-behavior
  - default-action
  - description
  - http-redirect
  - http-request-filtering
  - icap
    - custom-x-header
    - default-action
    - http-redirect
    - server
      - description
      - shutdown
    - vlan-id
  - local-filtering
    - allow-list
    - default-action
    - deny-list
      - default-action
      - http-redirect
  - shutdown
  - web-service
    - classification-overrides
      - entry
    - classifier
    - default-action
    - default-profile
    - dns-server
    - fqdn
    - http-redirect
    - profile
      - category
      - description
    - vlan-id
  - url-list
    - decrypt-key
    - description
    - expression-match
    - file
    - shutdown
    - size
  - wap1x
    - shutdown
  - aqp-initial-lookup
- http-enrich
  - field
- http-error-redirect
  - error-code
  - template
- http-notification
  - template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance http-redirect

- **http-redirect**
  - **template**
- **packet-rate-high-wmark**
- **packet-rate-low-wmark**
- **protocol**
  - **description**
  - **shutdown**
- **radius-accounting-policy**
  - **description**
  - **interim-update-interval**
  - **radius-accounting-server**
    - **access-algorithm**
    - **retry**
    - **router**
    - **server**
    - **source-address**
    - **timeout**
  - **significant-change**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.3 configure bfd Commands

- bfd
  - seamless-bfd
    - reflector
      - description
      - discriminator
      - local-state
      - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.4 configure bmp Commands

- bmp
  - shutdown
  - station
    - connection
      - connect-retry
      - local-address
      - router
      - station-address
      - tcp-keepalive
        - keep-count
        - keep-idle
        - keep-interval
        - shutdown
    - description
    - family
    - initiation-message
    - report-local-routes
    - shutdown
    - stats-report-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.5 configure call-trace Commands

- call-trace
  - buffering
  - location
    - disable
    - size-limit
  - max-files-number
  - primary-cf
  - trace-profile
    - applications
    - debug-output
    - description
    - events
    - live-output
    - size-limit
    - time-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.6 configure card Commands

- card
  - card-type
  - fail-on-error
  - filter-profile
  - fp
    - egress
      - hs-fixed-high-thresh-delta
      - hs-pool-policy
      - wred-queue-control
        - buffer-allocation
        - resv-cbs
        - shutdown
        - slope-policy
    - fp-resource-policy
    - hi-bw-mcast-src
    - ingress
      - access
        - queue-group
          - accounting-policy
          - collect-stats
          - description
          - policer-control-override
            - max-rate
            - priority-mbs-thresholds
              - min-thresh-separation
              - priority
                - mbs-contribution
          - policer-control-policy
          - policer-override
            - policer
              - cbs
              - mbs
              - packet-byte-offset
              - rate
              - stat-mode
      - dist-cpu-protection
        - dynamic-enforcement-policer-pool
        - description
      - mcast-path-management
        - bandwidth-policy
        - shutdown
      - network
        - pool
          - amber-alarm-threshold
          - red-alarm-threshold
          - resv-cbs
          - slope-policy
        - queue-group
          - accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure card fp ingress network queue-group collect-stats

- collect-stats
- description
- policer-control-override
  - max-rate
  - priority-mbs-thresholds
    - min-thresh-separation
    - priority
      - mbs-contribution
- policer-control-policy
- policer-override
  - policer
    - cbs
    - mbs
    - packet-byte-offset
    - rate
    - stat-mode
  - queue-policy
- policy-accounting
  - classes
  - policers
- ingress-buffer-allocation
- init-extract-prio-mode
- stable-pool-sizing

mda
- access
  - egress
  - ingress
- atm
  - mode
- clock-mode
- egress-xpl
  - threshold
  - window
- event
  - action
- fail-on-error
- ingress-xpl
  - threshold
  - window
- mda-type
- network
  - egress
  - ingress
- power-priority-level
- reset-on-recoverable-error
- shutdown
- sync-e
- upgrade
- xconnect
  - mac
    - description
    - loopback

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure card mda xconnect mac loopback bandwidth

- bandwidth
- description
- power-save
- reset-on-recoverable-error
- shutdown
- upgrade
- virtual-scheduler-adjustment
  - internal-scheduler-weight-mode
  - rate-calc-min-int
  - sched-run-min-int
  - slow-queue-threshold
  - task-scheduling-int
- xiom
  - fail-on-error
  - mda
    - mda-type
    - power-priority-level
    - shutdown
    - sync-e
    - xconnect
      - mac
        - description
        - loopback
          - bandwidth
          - description
  - reset-on-recoverable-error
  - shutdown
  - upgrade
  - xiom-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.7 configure cflowd Commands

- cflowd
  - active-flow-timeout
  - analyze-gre-payload
  - analyze-l2tp-traffic
  - analyze-v4overv6-traffic
  - cache-size
  - collector
    - aggregation
      - as-matrix
      - destination-prefix
      - protocol-port
      - raw
      - source-destination-prefix
      - source-prefix
    - autonomous-system-type
    - description
    - export-filter
      - family
        - ipv4
        - ipv6
        - l2-ip
        - mcast-ipv4
        - mcast-ipv6
        - mpls
      - interface-list
        - router
        - service
          - ies
          - vprn
      - router
    - router
    - shutdown
    - template-set
  - enhanced-distribution
  - export-mode
  - inactive-flow-timeout
  - inband-collector-export-only
  - overflow
  - rate
  - sample-profile
    - metering-process
    - sample-rate
  - shutdown
  - template-retransmit
  - use-vrtr-if-index

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure connection-profile

3.4.8 configure connection-profile Commands

— connection-profile
  — description
  — member

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.9 configure connection-profile-vlan Commands

- connection-profile-vlan
  - description
  - vlan-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure esa

3.4.10 configure esa Commands

- esa
  - description
  - host-port
  - shutdown
  - vm
    - cores
    - description
    - host-port
    - memory
    - shutdown
    - vm-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.11 configure eth-cfm Commands

- eth-cfm
  - default-domain
    - bridge-identifier
      - id-permission
      - mhf-creation
      - mip-ltr-priority
  - domain
    - association
      - auto-mep-discovery
      - bridge-identifier
        - id-permission
        - mhf-creation
        - mip-ltr-priority
        - vlan
      - ccm-hold-time
      - ccm-interval
      - facility-id-permission
      - remote-mepid
  - md-auto-id
    - ma-index-range
    - md-index-range
  - redundancy
    - mc-lag
      - propagate-hold-time
      - standby-mep-shutdown
  - slm
    - inactivity-timer
  - system
    - grace-tx-enable
    - sender-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.12 configure eth-ring Commands

- eth-ring
  - ccm-hold-time
  - compatible-version
  - description
  - guard-time
  - node-id
  - path
    - description
    - eth-cfm
      - mep
        - alarm-notification
          - fng-alarm-time
          - fng-reset-time
        - ccm-enable
        - ccm-ltm-priority
        - ccm-padding-size
        - control-mep
        - description
        - eth-test-enable
          - bit-error-threshold
          - test-pattern
        - grace
          - eth-ed
            - max-rx-defect-window
            - priority
            - rx-eth-ed
            - tx-eth-ed
          - eth-vsm-grace
            - rx-eth-vsm-grace
            - tx-eth-vsm-grace
        - low-priority-defect
        - mac-address
        - one-way-delay-threshold
        - shutdown
    - rpl-end
    - shutdown
  - revert-time
  - rpl-node
  - shutdown
  - sub-ring
    - interconnect
      - propagate-topology-change

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.13 configure eth-tunnel Commands

- eth-tunnel
  - ccm-hold-time
  - description
  - ethernet
    - encap-type
    - mac
  - lag-emulation
    - access
      - adapt-qos
      - per-fp-ing-queuing
    - path-threshold
  - mac
  - path
    - control-tag
    - description
    - eth-cfm
      - mep
        - alarm-notification
          - fng-alarm-time
          - fng-reset-time
        - ccm-enable
        - ccm-ltm-priority
        - ccm-padding-size
        - control-mep
        - description
        - eth-test-enable
          - bit-error-threshold
          - test-pattern
        - grace
          - eth-ed
            - max-rx-defect-window
            - priority
            - rx-eth-ed
            - tx-eth-ed
          - eth-vsm-grace
            - rx-eth-vsm-grace
            - tx-eth-vsm-grace
        - low-priority-defect
        - mac-address
        - one-way-delay-threshold
        - shutdown
    - member
    - precedence
    - shutdown
  - protection-type
  - revert-time
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.14 configure filter Commands

- **filter**
  - copy
    - ip-filter
    - ipv6-filter
    - mac-filter
  - dhcp-filter
    - default-action
    - description
    - entry
      - action
      - option
  - dhcp6-filter
    - default-action
    - **description**
    - entry
      - action
      - option
  - gre-tunnel-template
    - description
    - ipv4
      - destination-address
      - gre-key
      - skip-ttl-decrement
      - source-address
  - ip-exception
    - description
    - entry
      - description
      - match
        - dst-ip
        - dst-port
        - icmp-code
        - icmp-type
        - src-ip
        - src-port
    - filter-name
    - renum
    - scope
  - ip-filter
    - chain-to-system-filter
    - default-action
    - description
    - embed-filter
    - entry
      - action
        - drop
        - drop-extracted-traffic
        - extended-action
          - remark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure filter ip-filter entry action fc

- fc
- forward
- forward-when
- gtp-local-breakout
- http-redirect
- ignore-match
- l2-aware-nat-bypass
- nat
- rate-limit
- reassemble
- remark
- tcp-mss-adjust

- description
- egress-pbr
- filter-sample
- interface-disable-sample
- log
- match
  - destination-class
  - dscp
  - dst-ip
  - dst-port
  - fragment
  - icmp-code
  - icmp-type
  - ip
  - ip-option
  - multiple-option
  - option-present
  - packet-length
  - port
  - **src-ip**
  - src-mac
  - src-port
  - src-route-option
  - tcp-ack
  - tcp-cwr
  - tcp-ece
  - tcp-fin
  - tcp-ns
  - tcp-psh
  - tcp-rst
  - tcp-syn
  - tcp-urg
  - ttl
- pbr-down-action-override
- sample-profile
- sticky-dest
- group-inserted-entries
- renum
- scope
- shared-radius-filter-wmark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure filter ip-filter sub-insert-credit-control

- sub-insert-credit-control
- sub-insert-radius
- sub-insert-shared-pccrule
- sub-insert-shared-radius
- sub-insert-wmark
- type

- ipv6-exception
  - description
  - entry
    - description
    - match
      - dst-ip
      - dst-port
      - icmp-code
      - icmp-type
      - port
      - src-ip
      - src-port
  - renum
- ipv6-filter
  - chain-to-system-filter
  - default-action
  - description
  - embed-filter
  - entry
    - action
      - drop
      - drop-extracted-traffic
      - extended-action
        - remark
      - fc
      - forward
      - forward-when
      - http-redirect
      - ignore-match
      - nat
      - rate-limit
      - remark
      - tcp-mss-adjust
    - description
    - egress-pbr
    - filter-sample
    - interface-disable-sample
    - log
    - match
      - ah-ext-hdr
      - destination-class
      - dscp
      - dst-ip
      - dst-port
      - esp-ext-hdr
      - flow-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure filter ipv6-filter entry match fragment

- fragment
- hop-by-hop-opt
- hop-limit
- icmp-code
- icmp-type
- ip
- packet-length
- port
- routing-type0
- src-ip
- src-mac
- src-port
- tcp-ack
- tcp-cwr
- tcp-ece
- tcp-fin
- tcp-ns
- tcp-psh
- tcp-rst
- tcp-syn
- tcp-urg
- pbr-down-action-override
- sample-profile
- sticky-dest
- group-inserted-entries
- renum
- scope
- shared-radius-filter-wmark
- sub-insert-credit-control
- sub-insert-radius
- sub-insert-shared-pccrule
- sub-insert-shared-radius
- sub-insert-wmark
- type

- log
  - description
  - destination
  - shutdown
  - summary
    - shutdown
    - summary-crit
  - wrap-around
- mac-filter
  - default-action
  - description
  - embed-filter
  - entry
    - action
      - drop
      - forward
      - http-redirect
      - ignore-match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure filter mac-filter entry action rate-limit

- rate-limit
- description
- log
- match
  - dot1p
  - dsap
  - dst-mac
  - etype
  - inner-tag
  - isid
  - outer-tag
  - snap-oui
  - snap-pid
  - src-mac
  - ssap
- pbr-down-action-override
- sticky-dest
- renum
- scope
- type

- match-list
  - ip-prefix-list
    - apply-path
      - bgp-peers
    - description
    - prefix
    - prefix-exclude
  - ipv6-prefix-list
    - apply-path
      - bgp-peers
    - description
    - prefix
    - prefix-exclude
  - port-list
    - description
    - port
  - protocol-list
    - description
    - protocol
- md-auto-id
- filter-id-range
- redirect-policy
  - description
  - destination
    - description
    - ping-test
      - drop-count
      - interval
      - source-address
      - timeout
    - priority
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure filter redirect-policy destination unicast-rt-test

- unicast-rt-test
- notify-dest-change
- router
- shutdown
- sticky-dest

- redirect-policy-binding
  - binding-operator
  - redirect-policy
- system-filter
  - ip
  - ipv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure fwd-path-ext

3.4.15 configure fwd-path-ext Commands

- fwd-path-ext
  - fpe
    - description
    - multi-path
    - multi-path-list
      - path
    - path
    - pw-port-extension
    - srv6
      - interface-a
        - qos
      - interface-b
        - mtu
        - qos
    - sub-mgmt-extensions
    - vxlan
  - sdp-id-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.16 configure gmpls-tun-grp Commands

- gmpls-tun-grp
  - description
  - far-end
  - member
    - glsp
    - shutdown
  - member-threshold
  - mode
  - shutdown
  - type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.17 configure group-encryption Commands

- group-encryption
  - encryption-keygroup
    - active-outbound-sa
    - description
    - esp-auth-algorithm
    - esp-encryption-algorithm
    - keygroup-name
    - security-association
  - group-encryption-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure info

3.4.18 configure info Commands

— info

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure interface-group-handler

3.4.19 configure interface-group-handler Commands

- interface-group-handler
  - member
  - shutdown
  - threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.20 configure ipsec Commands

- ipsec
  - cert-profile
    - entry
      - cert
      - key
      - rsa-signature
      - send-chain
        - ca-profile
    - shutdown
  - client-db
    - client
      - client-identification
        - idi
        - peer-ip-prefix
      - client-name
      - credential
        - pre-shared-key
      - description
      - private-interface
      - private-service
      - shutdown
      - ts-negotiation
      - tunnel-template
    - description
    - match-list
      - idi
      - peer-ip-prefix
    - shutdown
  - ike-policy
    - auth-method
    - auto-eap-method
    - auto-eap-own-method
    - description
    - dpd
    - ike-mode
    - ike-transform
    - ike-version
    - ikev1-ph1-responder-delete-notify
    - ikev2-fragment
    - ipsec-lifetime
    - limit-init-exchange
    - lockout
    - match-peer-id-to-cert
    - nat-traversal
    - own-auth-method
    - pfs
    - relay-unsolicited-cfg-attribute
      - internal-ip4-address
      - internal-ip4-dns

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure ipsec ike-policy relay-unsolicited-cfg-attribute internal-ip4-netmask

- internal-ip4-netmask
- internal-ip6-address
- internal-ip6-dns
- send-idr-after-eap-success
- ike-transform
  - dh-group
  - ike-auth-algorithm
  - ike-encryption-algorithm
  - ike-prf-algorithm
  - isakmp-lifetime
- ipsec-transform
  - esp-auth-algorithm
  - esp-encryption-algorithm
  - extended-sequence-number
  - ipsec-lifetime
  - pfs-dh-group
- ipsec-transport-mode-profile
  - description
  - dynamic-keying
    - auto-establish
    - cert
      - cert-profile
      - default-result
      - primary
      - status-verify
        - default-result
        - primary
      - trust-anchor-profile
    - ike-policy
    - local-id
    - pre-shared-key
    - transform
  - max-history-esp-key-records
  - max-history-ike-key-records
  - replay-window
- radius-accounting-policy
  - include-radius-attribute
    - acct-stats
    - called-station-id
    - calling-station-id
    - framed-ip-addr
    - framed-ipv6-prefix
    - nas-identifier
    - nas-ip-addr
    - nas-port-id
  - radius-server-policy
  - update-interval
- radius-authentication-policy
  - include-radius-attribute
    - called-station-id
    - calling-station-id
    - client-cert-subject-key-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure ipsec radius-authentication-policy include-radius-attribute nas-identifier

- nas-identifier
- nas-ip-addr
- nas-port-id
- password
- radius-server-policy
- show-ipsec-keys
- static-sa
  - authentication
  - description
  - direction
  - protocol
  - spi
- trust-anchor-profile
  - trust-anchor
- ts-list
  - local
    - entry
      - address
      - protocol
  - remote
    - entry
      - address
      - protocol
- tunnel-template
  - clear-df-bit
  - copy-traffic-class-upon-decapsulation
  - description
  - encapsulated-ip-mtu
  - icmp-generation
    - frag-required
      - interval
      - message-count
  - icmp6-generation
    - pkt-too-big
      - interval
      - interval
      - message-count
  - ip-mtu
  - pmtu-discovery-aging
  - private-tcp-mss-adjust
  - propagate-pmtu-v4
  - propagate-pmtu-v6
  - public-tcp-mss-adjust
  - replay-window
  - sp-reverse-route
  - transform

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.21 configure isa Commands

- isa
  - description
    - tcp-adv-func
  - shutdown
    - accounting-policy
    - collect-stats
  - application-assurance-group
    - backup
    - description
    - divert-fc
    - fail-to-open
    - flow-attribute
    - http-enrich-max-pkt
    - isa-capacity-cost-high-threshold
    - isa-capacity-cost-low-threshold
    - isa-overload-cut-through
    - minimum-isa-generation
    - overload-sub-quarantine
      - shutdown
    - partitions
    - primary
    - qos
      - egress
        - from-subscriber
          - pool
            - resv-cbs
            - slope-policy
          - port-scheduler-policy
          - queue-policy
          - wa-shared-high-wmark
          - wa-shared-low-wmark
        - to-subscriber
          - pool
            - resv-cbs
            - slope-policy
          - port-scheduler-policy
          - queue-policy
          - wa-shared-high-wmark
          - wa-shared-low-wmark
    - shared-resources
      - gtp-tunnel-database
      - tcp-adv-func
      - web-service-url-filter
    - shutdown
    - statistics
      - performance
        - accounting-policy
        - collect-stats
    - transit-prefix-ipv4-entries

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure isa application-assurance-group transit-prefix-ipv4-remote-entries

- transit-prefix-ipv4-remote-entries
- transit-prefix-ipv6-entries
- transit-prefix-ipv6-remote-entries
- vm-traffic-distribution-by-ip
- vm-traffic-distribution-by-teid

- description
  - description
- lns-group
  - description
  - esa-vm
  - mda
  - port-policy
  - shutdown
- nat-group
  - active-mda-limit
  - description
  - esa-vm
  - failed-mda-limit
  - inter-chassis-redundancy
    - flow-timeout-on-switchover
    - ip-mtu
    - keepalive
    - local-ip-range-start
    - monitor-oper-group
    - monitor-port
    - preferred
    - remote-ip-range-start
    - replication-threshold
    - router
  - mda
  - radius-accounting-policy
  - redundancy
  - scaling-profile
  - session-limits
    - reserved
    - upnp-mappings
    - watermarks
  - shutdown
  - suppress-lsn-events
  - suppress-lsn-sub-blks-free
- shutdown
- tunnel-group
  - active-mda-number
  - backup
  - description
  - esa-vm
  - ipsec-responder-only
  - mda
  - multi-active
  - primary
  - reassembly
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure isa tunnel-group stats-collection

- stats-collection
  - isa-dp-cpu-usage
- video-group
  - ad-insert
  - analyzer
  - description
  - enable-rt-client
  - esa-vm
  - fcc-server
  - local-rt-server
  - primary
  - resv-ret
  - shutdown
  - stream-selection
  - watermark
    - bandwidth
      - fcc
      - ret
      - total
    - session
      - fcc
      - ret
      - total
  - esa-vm
- wlan-gw-group
  - active-iom-limit
  - active-mda-limit
  - description
  - distributed-sub-mgmt
    - isa-aa-group
    - isa-aa-oversubscription-factor
  - esa-vm
  - iom
  - mda
  - nat
    - lsn
    - radius-accounting-policy
    - session-limits
      - reserved
      - upnp-mappings
      - watermarks
    - suppress-lsn-events
    - suppress-lsn-sub-blks-free
  - port-policy
  - scaling-profile
  - shutdown
  - tunnel-port-policy
  - watermarks
    - mark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.22 configure lag Commands

- lag
  - access
    - adapt-qos
    - bandwidth
    - booking-factor
    - per-fp-egr-queuing
    - per-fp-ing-queuing
    - per-fp-sap-instance
  - adaptive-load-balancing
  - bfd
    - disable-soft-reset-extension
    - family
      - bfd-on-distributing-only
      - local-ip-address
      - max-admin-down-time
      - max-setup-time
      - multiplier
      - receive-interval
      - remote-ip-address
      - shutdown
      - transmit-interval
  - description
  - dynamic-cost
  - encap-type
  - eth-cfm
      - alarm-notification
        - fng-alarm-time
        - fng-reset-time
    - mep
      - ais-enable
        - client-meg-level
        - interface-support-enable
        - interval
        - low-priority-defect
        - priority
      - alarm-notification
        - fng-alarm-time
        - fng-reset-time
      - bit-error-threshold
      - ccm-enable
      - ccm-ltm-priority
      - ccm-padding-size
      - ccm-padding-size
      - ccm-tlv-ignore
      - collect-lmm-stats
      - csf-enable
        - multiplier
      - description
        - low-priority-defect

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure lag eth-cfm mep eth-test-enable

- eth-test-enable
  - bit-error-threshold
  - test-pattern
- facility-fault
- grace
  - eth-ed
    - max-rx-defect-window
    - priority
    - rx-eth-ed
    - tx-eth-ed
  - eth-vsm-grace
    - rx-eth-vsm-grace
    - tx-eth-vsm-grace
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown

- hash-weight-threshold
- hold-time
- lacp
- lacp-mux-control
- lacp-xmit-interval
- lacp-xmit-stdby
- link-map-profile
  - description
  - failure-mode
  - link
- mac
- mode
- monitor-oper-group
- per-link-hash
- port
- port-threshold
- port-type
- port-weight-speed
- selection-criteria
- shutdown
- standby-signaling
- weight-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.23 configure li Commands

- li
  - li-filter
    - li-ip-filter
      - description
      - entry
        - description
        - match
          - dst-ip
          - dst-port
          - fragment
          - src-ip
          - src-port
    - li-ipv6-filter
      - description
      - entry
        - description
        - match
          - dst-ip
          - dst-port
          - src-ip
          - src-port
    - li-mac-filter
      - description
      - entry
        - description
        - match
          - dst-mac
          - src-mac
  - li-filter-associations
    - li-ip-filter
      - ip-filter
      - ip-filter-name
    - li-ipv6-filter
      - ipv6-filter
      - ipv6-filter-name
    - li-mac-filter
      - mac-filter
      - mac-filter-name
  - li-filter-block-reservation
    - li-reserved-block
      - description
      - ip-filter
      - ip-filter-name
      - ipv6-filter
      - ipv6-filter-name
      - mac-filter
      - mac-filter-name
      - start-entry
  - li-filter-lock-state

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure li li-source

- li-source
  - ip-filter
  - ipv6-filter
  - li-ip-filter
  - li-ipv6-filter
  - li-mac-filter
  - mac-filter
  - nat
    - classic-lsn-sub
      - intercept-id
      - session-id
    - dslite-lsn-sub
      - intercept-id
      - session-id
    - ethernet-header
      - intercept-id
      - session-id
    - l2-aware-sub
      - intercept-id
      - session-id
    - nat64-lsn-sub
      - intercept-id
      - session-id
  - port
  - sap
  - shutdown
  - subscriber
  - wlan-gw
    - dsm-subscriber
      - intercept-id
      - session-id
    - intercept-id
    - session-id
- log
  - log-id
    - description
    - filter
    - from
    - netconf-stream
    - shutdown
    - time-format
    - to
- mirror-dest-reservation
- mirror-dest-template
  - layer-3-encap
    - direction-bit
    - ip-src
    - router
    - udp-dst
    - udp-src
- radius
  - mirror-dest-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure li save

- save
- use-outside-ip-address
- x-interfaces
  - correlation-id
    - ipoe
    - pppoe
  - ine-identifier
  - lics
    - lic
      - address
      - authentication
        - password
        - private-ki
        - sequence-group
      - description
      - lic-identifier
      - port
      - router
  - shutdown
  - user-db
  - x1
    - address
    - peer
    - port
    - timeouts
      - message-timeout
  - x2
    - address
    - peer
    - timeouts
      - keep-alive
      - request
  - x3
    - address-range
    - alarms
      - cpu-alarm
      - memory-alarm
      - throughput-alarm
    - li-group
    - peers
      - peer
    - session-limit
    - timeouts
      - keep-alive
      - request
      - target-retry-wait

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.24 configure log Commands

- log
  - accounting-policy
    - align
    - collection-interval
    - custom-record
      - aa-specific
        - aa-sub-attributes
          - all
          - app-profile
          - app-service-options
        - aa-sub-counters
          - all
          - long-duration-flow-count
          - medium-duration-flow-count
          - short-duration-flow-count
          - total-flow-duration
          - total-flows-completed-count
        - from-aa-sub-counters
          - all
          - flows-active-count
          - flows-admitted-count
          - flows-denied-count
          - forwarding-class
          - max-throughput-octet-count
          - max-throughput-packet-count
          - max-throughput-timestamp
          - octets-admitted-count
          - octets-denied-count
          - packets-admitted-count
          - packets-denied-count
        - to-aa-sub-counters
          - all
          - flows-active-count
          - flows-admitted-count
          - flows-denied-count
          - forwarding-class
          - max-throughput-octet-count
          - max-throughput-packet-count
          - max-throughput-timestamp
          - octets-admitted-count
          - octets-denied-count
          - packets-admitted-count
          - packets-denied-count
      - policer
        - e-counters
          - exceed-profile-octets-discarded-count
          - exceed-profile-octets-forwarded-count
          - exceed-profile-octets-offered-count
          - exceed-profile-packets-discarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log accounting-policy custom-record policer e-counters exceed-profile-packets-forwarded-count

- exceed-profile-packets-forwarded-count
- exceed-profile-packets-offered-count
- in-plus-profile-octets-discarded-count
- in-plus-profile-octets-forwarded-count
- in-plus-profile-octets-offered-count
- in-plus-profile-packets-discarded-count
- in-plus-profile-packets-forwarded-count
- in-plus-profile-packets-offered-count
- in-profile-octets-discarded-count
- in-profile-octets-forwarded-count
- in-profile-octets-offered-count
- in-profile-packets-discarded-count
- in-profile-packets-forwarded-count
- in-profile-packets-offered-count
- out-profile-octets-discarded-count
- out-profile-octets-forwarded-count
- out-profile-octets-offered-count
- out-profile-packets-discarded-count
- out-profile-packets-forwarded-count
- out-profile-packets-offered-count
- uncoloured-octets-offered-count
- uncoloured-packets-offered-count

- i-counters
  - in-profile-octets-discarded-count
  - in-profile-octets-forwarded-count
  - in-profile-octets-offered-count
  - in-profile-packets-discarded-count
  - in-profile-packets-forwarded-count
  - in-profile-packets-offered-count
  - out-profile-octets-discarded-count
  - out-profile-octets-forwarded-count
  - out-profile-octets-offered-count
  - out-profile-packets-discarded-count
  - out-profile-packets-forwarded-count
  - out-profile-packets-offered-count
  - uncoloured-octets-offered-count
  - uncoloured-packets-offered-count

- queue
  - e-counters
    - all
    - in-profile-octets-discarded-count
    - in-profile-octets-forwarded-count
    - in-profile-packets-discarded-count
    - in-profile-packets-forwarded-count
    - out-profile-octets-discarded-count
    - out-profile-octets-forwarded-count
    - out-profile-packets-discarded-count
    - out-profile-packets-forwarded-count
  - i-counters
    - all
    - all-octets-offered-count
    - all-packets-offered-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log accounting-policy custom-record queue i-counters high-octets-discarded-count

- high-octets-discarded-count
- high-octets-offered-count
- high-packets-discarded-count
- high-packets-offered-count
- in-profile-octets-forwarded-count
- in-profile-packets-forwarded-count
- low-octets-discarded-count
- low-octets-offered-count
- low-packets-discarded-count
- low-packets-offered-count
- out-profile-octets-forwarded-count
- out-profile-packets-forwarded-count
- uncoloured-octets-offered-count
- uncoloured-packets-offered-count

- ref-aa-specific-counter
- ref-policer
  - e-counters
    - exceed-profile-octets-discarded-count
    - exceed-profile-octets-forwarded-count
    - exceed-profile-octets-offered-count
    - exceed-profile-packets-discarded-count
    - exceed-profile-packets-forwarded-count
    - exceed-profile-packets-offered-count
    - in-plus-profile-octets-discarded-count
    - in-plus-profile-octets-forwarded-count
    - in-plus-profile-octets-offered-count
    - in-plus-profile-packets-discarded-count
    - in-plus-profile-packets-forwarded-count
    - in-plus-profile-packets-offered-count
    - in-profile-octets-discarded-count
    - in-profile-octets-forwarded-count
    - in-profile-octets-offered-count
    - in-profile-packets-discarded-count
    - in-profile-packets-forwarded-count
    - in-profile-packets-offered-count
    - out-profile-octets-discarded-count
    - out-profile-octets-forwarded-count
    - out-profile-octets-offered-count
    - out-profile-packets-discarded-count
    - out-profile-packets-forwarded-count
    - out-profile-packets-offered-count
    - uncoloured-octets-offered-count
    - uncoloured-packets-offered-count
  - i-counters
    - in-profile-octets-discarded-count
    - in-profile-octets-forwarded-count
    - in-profile-octets-offered-count
    - in-profile-packets-discarded-count
    - in-profile-packets-forwarded-count
    - in-profile-packets-offered-count
    - out-profile-octets-discarded-count
    - out-profile-octets-forwarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log accounting-policy custom-record ref-policer i-counters out-profile-octets-offered-count

- out-profile-octets-offered-count
- out-profile-packets-discarded-count
- out-profile-packets-forwarded-count
- out-profile-packets-offered-count
- uncoloured-octets-offered-count
- uncoloured-packets-offered-count

- ref-queue
  - e-counters
    - all
    - in-profile-octets-discarded-count
    - in-profile-octets-forwarded-count
    - in-profile-packets-discarded-count
    - in-profile-packets-forwarded-count
    - out-profile-octets-discarded-count
    - out-profile-octets-forwarded-count
    - out-profile-packets-discarded-count
    - out-profile-packets-forwarded-count
  - i-counters
    - all
    - all-octets-offered-count
    - all-packets-offered-count
    - high-octets-discarded-count
    - high-octets-offered-count
    - high-packets-discarded-count
    - high-packets-offered-count
    - in-profile-octets-forwarded-count
    - in-profile-packets-forwarded-count
    - low-octets-discarded-count
    - low-octets-offered-count
    - low-packets-discarded-count
    - low-packets-offered-count
    - out-profile-octets-forwarded-count
    - out-profile-packets-forwarded-count
    - uncoloured-octets-offered-count
    - uncoloured-packets-offered-count
  - significant-change
- default
- description
- include-system-info
- record
- shutdown
- to

- app-route-notifications
  - cold-start-wait
  - route-recovery-wait
- event-control
- event-damping
- event-handling
  - handler
    - action-list
      - entry
        - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log event-handling handler action-list entry min-delay

- min-delay
- script-policy
- shutdown
- description
- shutdown
- event-trigger
- event
- description
- shutdown
- trigger-entry
- debounce
- description
- event-handler
- log-filter
- shutdown
- location
- file-id
- description
- location
- rollover
- filter
- default-action
- description
- entry
- action
- description
- match
- application
- message
- number
- router
- severity
- subject
- action
- match
- log-id
- description
- filter
- from
- netconf-stream
- python-policy
- shutdown
- time-format
- to
- route-preference
- services-all-events
- service
- snmp-trap-group
- description
- trap-target
- syslog
- address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log syslog description

- description
- facility
- level
- log-prefix
- port
- tls-client-profile
- throttle-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.25 configure macsec Commands

- macsec
  - connectivity-association
    - cipher-suite
    - clear-tag-mode
    - delay-protection
    - description
    - encryption-offset
    - macsec-encrypt
    - replay-protection
    - replay-window-size
    - shutdown
    - static-cak
      - active-psk
      - mka-hello-interval
      - mka-key-server-priority
      - pre-shared-key
        - cak
        - ckn
  - mac-policy
    - dest-mac-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.26 configure mcast-management Commands

- mcast-management
  - bandwidth-policy
    - admin-bw-threshold
    - description
    - falling-percent-reset
    - mcast-pool
    - t2-paths
      - primary-path
        - queue-parameters
          - cbs
          - drop-tail
            - low
              - percent-reduction-from-mbs
          - mbs
          - cbs
          - mbs
      - secondary-path
        - number-paths
        - queue-parameters
          - cbs
          - drop-tail
            - low
              - percent-reduction-from-mbs
          - mbs
        - number-paths
          - cbs
          - mbs
  - chassis-level
    - mmrp-impm-override
    - per-mcast-plane-capacity
      - mcast-capacity
      - redundant-mcast-capacity
      - total-capacity
    - round-robin-inactive-records
      - keepalive-override
        - keepalive-override
      - keepalive-override
  - mcast-reporting-dest
    - description
    - dest-ip-addr
    - max-tx-delay
    - shutdown
    - udp-dst-port
  - multicast-info-policy
    - bundle
      - admin-bw
      - bw-activity
      - channel
        - admin-bw

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure mcast-management multicast-info-policy bundle channel bw-activity

- bw-activity
- explicit-sf-path
- keepalive-override
- preference
- primary-tunnel-interface
- source-override
  - admin-bw
  - bw-activity
  - explicit-sf-path
  - keepalive-override
  - preference
  - primary-tunnel-interface
  - video
    - analyzer
      - alarms
        - cc-error
        - non-vid-pid-absent
        - pat-repetition
        - pat-syntax
        - pcr-repetition
        - pid-pmt-unref
        - pmt-repetition
        - pmt-syntax
        - report-alarm
        - tei-set
        - ts-sync-loss
        - vid-pid-absent
      - description
    - description
    - fcc-channel-type
    - fcc-min-duration
    - fcc-server
    - local-fcc-port
    - local-rt-port
    - local-rt-server
    - reorder-audio
    - rt-buffer-size
    - rt-server
    - stream-selection
    - video-group
- video
  - analyzer
    - alarms
      - cc-error
      - non-vid-pid-absent
      - pat-repetition
      - pat-syntax
      - pcr-repetition
      - pid-pmt-unref
      - pmt-repetition
      - pmt-syntax
      - report-alarm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure mcast-management multicast-info-policy bundle channel video analyzer alarms tei-set

- tei-set
- ts-sync-loss
- vid-pid-absent
- description
- description
- fcc-channel-type
- fcc-min-duration
- fcc-server
- local-fcc-port
- local-rt-port
- local-rt-server
- reorder-audio
- rt-buffer-size
- rt-server
- stream-selection
- video-group
- cong-priority-threshold
- description
- ecmp-opt-threshold
- explicit-sf-path
- keepalive-override
- preference
- primary-tunnel-interface
  - bw-activity
  - explicit-sf-path
- video
  - analyzer
    - alarms
      - cc-error
      - non-vid-pid-absent
      - pat-repetition
      - pat-syntax
      - pcr-repetition
      - pid-pmt-unref
      - pmt-repetition
      - pmt-syntax
      - report-alarm
      - tei-set
      - ts-sync-loss
      - vid-pid-absent
    - description
  - description
  - fcc-channel-type
  - fcc-min-duration
  - fcc-server
  - local-fcc-port
  - local-rt-port
  - local-rt-server
  - reorder-audio
  - rt-buffer-size
  - rt-server
  - source-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure mcast-management multicast-info-policy bundle video stream-selection

- **stream-selection**
- video-group
- description
- video-policy
  - video-interface
    - extended-unicast
    - fcc-session-timeout
    - hd
      - dent-threshold
      - fcc-burst
      - fcc-server
      - local-rt-server
      - mc-handover
      - rt-rate
    - max-igmp-latency
    - max-sessions
    - pip
      - dent-threshold
      - fcc-burst
      - fcc-server
      - local-rt-server
      - mc-handover
      - rt-rate
    - ret-session-timeout
    - rt-payload-type
    - rt-rate
    - sd
      - dent-threshold
      - fcc-burst
      - fcc-server
      - local-rt-server
      - mc-handover
      - rt-rate
    - subscriber-bw-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.27 configure mirror Commands

- mirror
  - mirror-dest
    - description
    - enable-port-id
    - encap
      - layer-3-encap
        - direction-bit
        - gateway
          - ip
          - udp
        - router
    - endpoint
      - description
      - revert-time
    - fc
    - pcap
      - file-url
    - remote-source
      - far-end
      - spoke-sdp
        - control-channel-status
          - acknowledgment
          - refresh-timer
          - request-timer
          - shutdown
        - control-word
        - egress
          - vc-label
        - ingress
          - l2tpv3
            - cookie
          - vc-label
        - pw-path-id
          - agi
          - saii-type2
          - taii-type2
        - shutdown
    - sampling-rate
    - sap
      - cem
        - packet
        - rtp-header
      - egress
        - ip-mirror
          - sa-mac
        - qos
      - endpoint
      - endpoint
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure mirror mirror-dest slice-size

- slice-size
- spoke-sdp
  - control-channel-status
    - acknowledgment
    - refresh-timer
    - request-timer
    - shutdown
  - control-word
  - egress
    - l2tpv3
      - cookie
    - shutdown
    - vc-label
  - ingress
    - l2tpv3
      - cookie
    - vc-label
  - precedence
  - pw-path-id
    - agi
    - saii-type2
    - taii-type2
  - shutdown
- mirror-source
  - ip-filter
  - ipv6-filter
  - mac-filter
  - port
  - sap
  - shutdown
  - subscriber

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.28 configure oam-pm Commands

- oam-pm
  - bin-group
    - bin-type
      - bin
        - lower-bound
      - delay-event
      - delay-event-exclusion
      - exclude-from-avg
    - description
    - shutdown
  - session
    - bin-group
    - description
    - ethernet
      - dest-mac
      - dmm
        - data-tlv-size
        - delay-template
        - interval
        - shutdown
        - test-duration
      - lmm
        - availability
          - flr-threshold
          - hli-force-count
          - shutdown
          - timing
        - enable-fc-collection
        - interval
        - loss-events
          - avg-flr-event
          - chli-event
          - hli-event
          - unavailability-event
          - undet-availability-event
          - undet-unavailability-event
        - shutdown
        - test-duration
      - priority
      - remote-mepid
      - slm
        - data-tlv-size
        - flr-threshold
        - hli-force-count
        - loss-events
          - avg-flr-event
          - chli-event
          - hli-event
          - unavailability-event

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure oam-pm session ethernet slm loss-events undet-availability-event

- undet-availability-event
- undet-unavailability-event
- shutdown
- test-duration
- timing
- source
- ip
- allow-egress-remark-dscp
- dest-udp-port
- destination
- do-not-fragment
- dscp
- fc
- forwarding
- pattern
- profile
- router
- router-instance
- source
- source-udp-port
- ttl
- twamp-light
- allow-ipv6-udp-checksum-zero
- delay-template
- interval
- loss
- flr-threshold
- hli-force-count
- timing
- loss-events
- avg-flr-event
- chli-event
- hli-event
- unavailability-event
- undet-availability-event
- undet-unavailability-event
- pad-size
- record-stats
- shutdown
- test-duration
- meas-interval
- accounting-policy
- boundary-type
- clock-offset
- event-mon
- delay-events
- loss-events
- shutdown
- intervals-stored
- event-mon
- delay-events
- loss-events

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure oam-pm session measurement-interval event-mon shutdown

- shutdown
- mpls
  - dm
    - delay-template
    - interval
    - pad-tlv-size
    - reflect-pad
    - shutdown
    - test-duration
  - dscp
  - fc
  - lsp
    - mpls-tp-static
      - lsp
    - rsvp
      - lsp
      - udp-return-object
    - rsvp-auto
      - from
      - lsp-template
      - to
      - udp-return-object
  - pattern
  - profile
  - ttl
- streaming
  - delay-template
    - description
    - fd-avg
    - ifdv-avg
    - sample-window
    - shutdown
    - window-integrity

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure open-flow

3.4.29 configure open-flow Commands

- open-flow
  - of-switch
    - aux-channel-enable
    - description
    - echo-interval
    - echo-multiple
    - flowtable
      - max-size
      - no-match-action
      - switch-defined-cookie
    - logical-port-status
    - of-controller
      - tls-client-profile
      - vprn
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.30 configure port Commands

- port
  - access
    - egress
      - resv-cbs
      - slope-policy
    - pool
      - amber-alarm-threshold
      - red-alarm-threshold
      - resv-cbs
      - slope-policy
    - ingress
      - pool
        - amber-alarm-threshold
        - red-alarm-threshold
        - resv-cbs
        - slope-policy
  - aps
    - advertise-interval
    - hold-time
    - hold-time-aps
    - mode-annexb
    - neighbor
    - protect-circuit
    - rdi-alarms
    - revert-time
    - switching-mode
    - working-circuit
    - wtr-annexb
  - connector
    - breakout
    - rs-fec-mode
  - ddm-events
  - description
  - dist-cpu-protection
  - dwdm
    - coherent
      - compatibility
      - cpr-window-size
      - dispersion
      - mode
      - report-alarms
      - rx-los-reaction
      - rx-los-thresh
      - sweep
      - target-power
    - frequency
    - tdcm
  - ethernet
    - access

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet access bandwidth

- bandwidth
- booking-factor
- egress
  - description
  - queue-group
    - accounting-policy
    - agg-rate
      - limit-unused-bandwidth
      - queue-frame-based-accounting
      - rate
    - collect-stats
    - description
    - host-match
    - hs-turbo
    - queue-overrides
      - queue
        - adaptation-rule
        - burst-limit
        - cbs
        - drop-tail
          - low
            - percent-reduction-from-mbs
        - mbs
        - monitor-queue-depth
        - parent
        - percent-rate
        - rate
    - scheduler-override
      - scheduler
        - parent
        - rate
    - scheduler-policy
  - vport
    - agg-rate
      - limit-unused-bandwidth
      - queue-frame-based-accounting
      - rate
    - agg-rate-limit
    - description
    - egress-rate-modify
    - host-match
    - hw-agg-shaper-scheduler-policy
    - limit-unused-bandwidth
    - mon-hw-agg-shaper-sch
    - mon-port-sch
    - port-scheduler-policy
    - scheduler-policy
- ingress
  - queue-group
    - accounting-policy
    - collect-stats
    - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet access ingress queue-group queue-overrides

- queue-overrides
  - queue
    - adaptation-rule
    - cbs
    - drop-tail
      - low
        - percent-reduction-from-mbs
    - mbs
    - monitor-queue-depth
    - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
- accounting-policy
- autonegotiate
- collect-stats
- crc-monitor
  - sd-threshold
  - sf-threshold
  - window-size
- dampening
  - half-life
  - shutdown
  - suppress-threshold
- discard-rx-pause-frames
- dot1q-etype
- dot1x
  - macsec
    - exclude-mac-policy
    - exclude-protocol
    - rx-must-be-encrypted
    - sub-port
      - ca-name
      - eapol-destination-address
      - encap-match
      - max-peer
      - shutdown
  - max-auth-req
  - per-host-authentication
    - allowed-source-macs
      - mac-address
    - authenticator-init
    - shutdown
  - port-control
  - quiet-period
  - radius-plcy
  - radius-server-policy
  - re-auth-period
  - re-authentication
  - server-timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet dot1x shutdown

- shutdown
- supplicant-timeout
- transmit-period
- tunnel-dot1q
- tunnel-qinq
- tunneling

- down-on-internal-error
- down-when-looped
  - keep-alive
  - retry-timeout
  - shutdown
  - use-broadcast-address
- duplex
  - shutdown
- efm-oam
  - accept-remote-loopback
  - discovery
    - advertise-capabilities
      - link-monitoring
  - dying-gasp-tx-on-reset
  - grace-tx-enable
  - grace-vendor-oui
  - hold-time
  - ignore-efm-state
  - link-monitoring
    - errored-frame
      - event-notification
      - sd-threshold
      - sf-threshold
      - shutdown
      - window
    - errored-frame-period
      - event-notification
      - sd-threshold
      - sf-threshold
      - shutdown
      - window
    - errored-frame-seconds
      - event-notification
      - sd-threshold
      - sf-threshold
      - shutdown
      - window
    - errored-symbols
      - event-notification
      - sd-threshold
      - sf-threshold
      - shutdown
      - window
    - local-sf-action
      - event-notification-burst
      - info-notification

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet efm-oam link-monitoring local-sf-action info-notification critical-event

- critical-event
- dying-gasp
- local-port-action
- shutdown
- mode
- peer-rdi-rx
- critical-event
- dying-gasp
- event-notification
- link-fault
- shutdown
- transmit-interval
- trigger-fault
- tunneling
- egress
- hs-port-pool-policy
- hs-scheduler-overrides
- group
- max-rate
- scheduling-class
- hs-scheduler-policy
- hs-secondary-shaper
- aggregate
- low-burst-max-class
- rate
- class
- rate
- description
- scheduler-policy
- egress-rate
- egress-scheduler-override
- level
- max-rate
- egress-scheduler-policy
- elmi
- mode
- n393
- t391
- t392
- encap-type
- eth-bn-egress-rate-changes
- eth-cfm
- mep
- ais-enable
- client-meg-level
- interface-support-enable
- interval
- low-priority-defect
- priority
- alarm-notification
- fng-alarm-time
- fng-reset-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet eth-cfm mep ccm-enable

- ccm-enable
- ccm-ltm-priority
- ccm-padding-size
- ccm-tlv-ignore
- collect-lmm-stats
- csf-enable
  - multiplier
- description
- eth-bn
  - receive
  - rx-update-pacing
  - low-priority-defect
- eth-test-enable
  - bit-error-threshold
  - test-pattern
- facility-fault
- grace
  - eth-ed
    - max-rx-defect-window
    - priority
    - rx-eth-ed
    - tx-eth-ed
  - eth-vsm-grace
    - rx-eth-vsm-grace
    - tx-eth-vsm-grace
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown

- hold-time
  - scheduler-policy
- ingress-rate
- lacp-tunnel
- lldp
- lldp
  - dest-mac
    - admin-status
    - notification
    - port-id-subtype
    - tunnel-nearest-bridge
    - tx-mgmt-address
    - tx-tlvs
- load-balancing-algorithm
- mac
- min-frame-length
- mode
- mon-port-sch
- mtu
- network
  - accounting-policy
  - collect-stats
  - egress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet network egress queue-group

- queue-group
  - accounting-policy
  - agg-rate
    - limit-unused-bandwidth
    - queue-frame-based-accounting
    - rate
  - collect-stats
  - description
  - hs-turbo
  - policer-control-policy
    - policer-control-policy
  - queue-overrides
    - queue
      - adaptation-rule
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs
      - monitor-queue-depth
      - percent-rate
      - rate
  - scheduler-policy
    - adaptation-rule
    - cbs
    - rate
- egress-port-queue-overrides
  - queue
    - monitor-queue-depth
- queue-policy
- pbb-etype
- ptp-asymmetry
- qinq-etype
- report-alarm
- rs-fec-mode
- sflow
- shutdown
- single-fiber
- speed
- ssm
  - code-type
  - esmc-tunnel
  - shutdown
  - tx-dus
- symbol-monitor
  - sd-threshold
  - sf-threshold
  - shutdown
  - window-size
- util-stats-interval
- xgig
- hybrid-buffer-allocation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port hybrid-buffer-allocation egr-weight

- egr-weight
- ing-weight
- modify-buffer-allocation-rate
  - egr-percentage-of-rate
  - ing-percentage-of-rate
- monitor-agg-egress-queue-stats
- multilink-bundle
  - fragment-threshold
  - ima
    - atm
      - cell-format
      - min-vp-vpi
    - link-delay
    - max-bandwidth
    - test-pattern-procedure
      - shutdown
      - test-link
      - test-pattern
    - version
  - interleave-fragments
  - member
  - minimum-links
  - mlfr
    - ack-timeout
    - egress
      - qos-profile
    - frame-relay
      - lmi-type
      - mode
      - mode
      - n391dte
      - n392dce
      - n392dte
      - n393dce
      - n393dte
      - t391dte
      - t392dce
    - hello-interval
    - identifier
    - ingress
      - qos-profile
    - retry-limit
  - mlppp
    - egress
      - qos-profile
    - endpoint-discriminator
    - ingress
      - qos-profile
    - magic-number
    - multiclass
    - stateless-aps-switchover
  - mrru

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port multilink-bundle protect-bundle

- protect-bundle
- red-differential-delay
- short-sequence
- working-bundle
- yellow-differential-delay

- network
  - egress
    - pool
      - amber-alarm-threshold
      - red-alarm-threshold
      - resv-cbs
      - slope-policy
  - oper-group
  - otu
    - async-mapping
    - fec
    - otu2-lan-data-rate
    - pm-tti
      - expected
      - mismatch-reaction
      - tx
    - psi-payload
      - expected
      - mismatch-reaction
      - tx
      - tx
    - report-alarms
    - sd-threshold
    - sd-threshold-clear
    - sf-sd-method
    - sf-threshold
    - sf-threshold-clear
    - shutdown
    - sm-tti
      - expected
      - mismatch-reaction
      - tx
  - pxc-pxc-id.sub-port-id
  - shutdown
  - sonet-sdh
    - clock-source
    - framing
    - group
    - hold-time
    - loopback
    - path
      - access
        - egress
          - vport
            - agg-rate
              - limit-unused-bandwidth
              - rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port sonet-sdh path access egress vport description

- description
- egress-rate-modify
- host-match
- limit-unused-bandwidth
- mon-port-sch
- port-scheduler-policy
- queue-frame-based-accounting
- scheduler-policy

- atm
  - cell-format
  - custom-buffer-mode
    - buffer-pool
    - vc-threshold
  - ilmi
    - egress
      - traffic-desc
    - ingress
      - traffic-desc
    - keep-alive
    - protocol
    - shutdown
  - min-vp-vpi
  - vp
  - vpi
- cisco-hdlc
  - down-count
  - keepalive
  - up-count
- crc
- description
- egress-scheduler-override
  - level
  - max-rate
- egress-scheduler-policy
- encap-type
- frame-relay
    - qos-profile
  - frf-12
    - egress
      - qos-profile
    - fragment-threshold
  - lmi-type
  - mode
  - n391dte
  - n392dce
  - n392dte
  - n393dce
  - n393dte
  - t391dte
  - t392dce
- load-balancing-algorithm
- mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port sonet-sdh path mode

- mode
- mtu
- network
  - accounting-policy
  - collect-stats
  - queue-policy
- payload
- ppp
  - keepalive
- report-alarm
- scramble
- shutdown
- signal-label
- trace-string

- report-alarm
- section-trace
- single-fiber
- speed
- suppress-lo-alarm
- threshold
- tx-dus

- tdm
  - buildout
    - qos-profile
  - ds1
    - bert
    - bit-error-insertion
    - channel-group
      - atm
        - cell-format
        - min-vp-vpi
      - cisco-hdlc
        - down-count
        - keepalive
        - up-count
      - crc
      - description
      - egress-scheduler-override
        - level
        - max-rate
      - egress-scheduler-policy
      - encap-type
      - frame-relay
        - egress
        - frf-12
          - egress
            - qos-profile
          - fragment-threshold
        - identifier
        - lmi-type
        - mode
        - n391dte

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port tdm ds1 channel-group frame-relay n392dce

- n392dce
- n392dte
- n393dce
- n393dte
- t391dte
- t392dce
- idle-cycle-flag
- idle-payload-fill
- idle-signal-fill
- load-balancing-algorithm
- mac
- mode
- mtu
- network
- accounting-policy
- collect-stats
- queue-policy
- ppp
- ber-sf-link-down
- compress
- keepalive
- scramble
- shutdown
- speed
- timeslots
- clock-source
- framing
- invert-data
- loopback
- network
- remote-loop-respond
- report-alarm
- shutdown
- signal-mode
- threshold
- ds3
- atm
- cell-format
- mapping
- min-vp-vpi
- bert
- bit-error-insertion
- channelized
- cisco-hdlc
- down-count
- keepalive
- up-count
- clock-source
- crc
- description
- egress-scheduler-override
- level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port tdm ds3 egress-scheduler-override max-rate

- max-rate
- egress-scheduler-policy
- encap-type
- feac-loop-respond
- frame-relay
  - frf-12
    - egress
      - qos-profile
    - fragment-threshold
  - lmi-type
  - mode
  - n391dte
  - n392dce
  - n392dte
  - n393dce
  - n393dte
  - t391dte
  - t392dce
- framing
- idle-cycle-flag
- load-balancing-algorithm
- loopback
- mac
- mdl
- mdl-transmit
- mode
- mtu
- network
  - accounting-policy
  - collect-stats
  - queue-policy
- ppp
  - keepalive
- report-alarm
- scramble
- shutdown
- subrate

- e1
  - bert
  - bit-error-insertion
  - channel-group
    - atm
      - cell-format
      - min-vp-vpi
    - cisco-hdlc
      - down-count
      - keepalive
      - up-count
    - crc
    - description
    - egress-scheduler-override
      - **level**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port tdm e1 channel-group egress-scheduler-override max-rate

- max-rate
- egress-scheduler-policy
- encap-type
- frame-relay
  - frf-12
    - egress
      - qos-profile
    - fragment-threshold
  - identifier
  - lmi-type
  - mode
  - n391dte
  - n392dce
  - n392dte
  - n393dce
  - n393dte
  - t391dte
  - t392dce
- idle-cycle-flag
- idle-payload-fill
- idle-signal-fill
- load-balancing-algorithm
- mac
- mode
- mtu
- network
  - accounting-policy
  - collect-stats
  - queue-policy
- ppp
  - ber-sf-link-down
  - compress
  - keepalive
- scramble
- shutdown
- speed
- timeslots

- clock-source
  - level
- framing
- invert-data
- loopback
- national-bits
- network
- report-alarm
- shutdown
- signal-mode
- threshold

- e3
  - atm
    - cell-format
    - min-vp-vpi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port tdm e3 bert

- bert
- bit-error-insertion
- cisco-hdlc
  - down-count
  - keepalive
  - up-count
- clock-source
- crc
- description
- egress-scheduler-override
  - level
  - max-rate
- egress-scheduler-policy
- encap-type
- frame-relay
  - frf-12
    - egress
      - qos-profile
    - fragment-threshold
  - lmi-type
  - mode
  - n391dte
  - n392dce
  - n392dte
  - n393dce
  - n393dte
  - t391dte
  - t392dce
- framing
- idle-cycle-flag
- load-balancing-algorithm
- loopback
- mac
- mode
- mtu
- network
  - accounting-policy
  - collect-stats
  - queue-policy
- ppp
  - keepalive
- report-alarm
- scramble
- shutdown

- hold-time
- lbo
- length

- transceiver
  - digital-coherent-optics

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.31 configure port-policy Commands

— port-policy
  — description
  — egress-scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.32 configure port-xc Commands

- port-xc
  - pxc
    - description
    - port
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure pw-port

3.4.33 configure pw-port Commands

- pw-port
  - description
  - dot1q-etype
  - encap-type
  - oper-group
  - qinq-etype

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.34 configure python Commands

- python
  - python-policy
    - cache
      - entry-size
      - max-entries
      - max-entry-lifetime
      - mcs-peer
      - minimum-lifetimes
        - high-availability
        - multi-chassis-redundancy
        - persistence
      - persistence
      - shutdown
    - description
    - dhcp
    - dhcp6
    - diameter
    - gtpv1-c
    - gtpv2-c
    - pppoe
    - radius
    - syslog
    - vsd
    - vsd
  - python-script
    - action-on-fail
    - description
    - primary-url
    - protection
    - secondary-url
    - shutdown
    - tertiary-url

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.35 configure qos Commands

- **qos**
  - adv-config-policy
    - child-control
      - bandwidth-distribution
        - above-offered-allowance
          - delta-consumed-agg-rate
          - delta-consumed-higher-tier-rate
          - unconsumed-agg-rate
          - unconsumed-higher-tier-rate
        - above-offered-cap
        - enqueue-on-pir-zero
        - granularity
        - internal-scheduler-weight-mode
        - limit-pir-zero-drain
        - lub-init-min-pir
      - offered-measurement
        - add
        - fast-start
        - fast-stop
        - granularity
        - high-rate-hold-time
        - max-decrement
        - sample-interval
        - time-average-factor
    - description
  - atm-td-profile
    - clp-tagging
    - description
    - descriptor-type
    - policing
    - service-category
    - shaping
    - traffic
    - weight
  - copy
    - adv-config-policy
    - atm-td-profile
    - hs-attachment-policy
    - hs-pool-policy
    - hs-port-pool-policy
    - hs-scheduler-policy
    - mc-fr-profile-egress
    - **mc-fr-profile-ingress**
    - mlppp-profile-egress
    - mlppp-profile-ingress
    - named-pool-policy
    - network
    - network-queue
    - policer-control-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos copy port-scheduler-policy

- port-scheduler-policy
- post-policer-mapping
- queue-group-egress
- queue-group-ingress
- sap-egress
- sap-ingress
- scheduler-policy
- shared-queue
- slope-policy
- fp-resource-policy
  - aggregate-shapers
    - auto-creation
    - hw-agg-shapers
  - description
  - ports
    - hqos-mode
  - queues
    - ingress-percent-of-total
- hs-attachment-policy
  - description
  - low-burst-max-class
  - queue
  - wrr-group
- hs-pool-policy
  - description
  - mid-tier
    - mid-pool
      - allocation-percent
      - parent-root-pool
      - port-bw-oversub-factor
      - slope-policy
  - root-tier
    - root-pool
      - allocation-weight
      - slope-policy
  - system-reserve
- hs-port-pool-policy
  - alt-port-class-pools
    - class-pool
      - allocation
      - parent-mid-pool
      - slope-policy
  - description
  - std-port-class-pools
    - class-pool
      - allocation
      - parent-mid-pool
      - slope-policy
- hs-scheduler-policy
  - description
  - group
  - max-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos hs-scheduler-policy scheduling-class

- scheduling-class
- hw-agg-shaper-scheduler-policy
  - congestion-threshold
  - description
  - group
  - max-rate
  - monitor-threshold
  - sched-class
- match-list
  - ip-prefix-list
    - description
    - prefix
  - ipv6-prefix-list
    - description
    - prefix
  - port-list
    - description
    - port
- mc-fr-profile-egress
  - class
    - max-queue-size
    - mir
    - weight
  - description
- mc-fr-profile-ingress
  - class
    - reassembly-timeout
  - description
- md-auto-id
  - qos-policy-id-range
- mlppp-profile-egress
  - class
    - fc
    - max-queue-size
    - mir
    - weight
  - description
  - fc
- mlppp-profile-ingress
  - class
    - reassembly-timeout
  - description
- network
  - description
  - egress
    - dscp
    - fc
      - de-mark
      - dot1p
      - dot1p-in-profile
      - dot1p-out-profile
      - dscp-in-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos network egress fc dscp-out-profile

- dscp-out-profile
- lsp-exp-in-profile
- lsp-exp-out-profile
- port-redirect-group
- ip-criteria
  - entry
    - action
    - description
    - match
      - dscp
      - dst-ip
      - dst-port
      - fragment
      - icmp-type
      - src-ip
      - src-port
  - renum
- ipv6-criteria
  - entry
    - action
    - description
    - match
      - dscp
      - dst-ip
      - dst-port
      - fragment
      - icmp-type
      - src-ip
      - src-port
  - renum
- prec
- remarking

- ingress
  - default-action
  - dot1p
  - dscp
  - fc
    - fp-redirect-group
  - ip-criteria
    - entry
      - action
      - description
      - match
        - dscp
        - dst-ip
        - dst-port
        - fragment
        - src-ip
        - src-port
    - renum
  - ipv6-criteria
    - entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos network ingress ipv6-criteria entry action

- action
- description
- match
  - dscp
  - dst-ip
  - dst-port
  - fragment
  - src-ip
  - src-port
- renum
- ler-use-dscp
- lsp-exp
- scope
- network-queue
- description
- fc
  - multicast-queue
  - queue
- hs-attachment-policy
- hs-wrr-group
  - adaptation-rule
  - hs-class-weight
  - rate
- queue
  - adaptation-rule
  - avg-frame-overhead
  - cbs
  - drop-tail
    - low
      - percent-reduction-from-mbs
  - hs-alt-port-class-pool
  - hs-class-weight
  - hs-mbs
  - hs-wred-queue
  - hs-wrr-weight
  - mbs
  - port-parent
  - rate
- policer-control-policy
- description
- root
  - max-percent-rate
  - max-rate
  - priority-mbs-thresholds
    - min-thresh-separation
    - priority
      - mbs-contribution
  - profile-preferred
- tier
  - arbiter
    - description
    - parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos policer-control-policy tier arbiter percent-rate

- percent-rate
- rate

- port-scheduler-policy
  - description
  - dist-lag-rate-shared
  - group
    - monitor-threshold
    - percent-rate
    - rate
  - hqos-algorithm
  - level
  - max-rate
  - monitor-threshold
  - orphan-override
- post-policer-mapping
  - description
  - fc
    - maps-to
- queue-group-redirect-list
  - match
  - type
- queue-group-templates
  - egress
    - queue-group
      - description
      - fc
        - **queue**
      - hs-attachment-policy
      - hs-wrr-group
        - adaptation-rule
        - hs-class-weight
        - percent-rate
        - rate
      - policer
        - adaptation-rule
        - adv-config-policy
        - cbs
        - description
        - enable-exceed-pir
        - high-prio-only
        - mbs
        - packet-byte-offset
        - parent
        - percent-rate
        - profile-capped
        - rate
        - stat-mode
      - profile-capped
      - queue
        - adaptation-rule
        - adv-config-policy
        - burst-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos queue-group-templates egress queue-group queue cbs

- cbs
- drop-tail
  - exceed
    - percent-reduction-from-mbs
  - high
    - percent-reduction-from-mbs
  - highplus
    - percent-reduction-from-mbs
  - low
    - percent-reduction-from-mbs
- dynamic-mbs
- hs-alt-port-class-pool
- hs-class-weight
- hs-wred-queue
- hs-wrr-weight
- mbs
- packet-byte-offset
- parent
- percent-rate
- port-parent
- queue-delay
- rate
- wred-queue
- queues-hqos-manageable
  - queue

- ingress
  - queue-group
    - description
    - policer
      - **adaptation-rule**
      - adv-config-policy
      - cbs
      - description
      - high-prio-only
      - mbs
      - packet-byte-offset
      - parent
      - percent-rate
      - profile-capped
      - rate
      - stat-mode
    - profile-capped
    - queue
      - adaptation-rule
      - adv-config-policy
      - burst-limit
      - cbs
      - cir-non-profiling
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos queue-group-templates ingress queue-group queue packet-byte-offset

- packet-byte-offset
- parent
- percent-rate
- rate

- sap-egress
  - description
  - dot1p
  - dscp
  - dynamic-policer
    - cbs
    - mbs
    - packet-byte-offset
    - parent
    - range
    - stat-mode
  - ethernet-ctag
  - fc
    - de-mark
    - de-mark-inner
    - de-mark-outer
    - dot1p
    - dot1p-inner
    - dot1p-outer
    - dscp
    - policer
    - prec
    - queue
  - hs-attachment-policy
  - hs-wrr-group
    - adaptation-rule
    - hs-class-weight
    - percent-rate
    - rate
  - ip-criteria
    - entry
      - action
      - description
      - match
        - dscp
        - dst-ip
        - dst-port
        - fragment
        - src-ip
        - src-port
    - renum
  - ipv6-criteria
    - entry
      - action
      - description
      - match
        - dscp
        - dst-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos sap-egress ipv6-criteria entry match dst-port

- dst-port
- src-ip
- src-port
- renum
- parent-location
- policer
  - adaptation-rule
  - adv-config-policy
  - cbs
  - description
  - enable-dscp-prec-remarking
  - enable-exceed-pir
  - high-prio-only
  - mbs
  - packet-byte-offset
  - parent
  - percent-rate
  - port-parent
  - profile-capped
  - profile-out-preserve
  - rate
  - scheduler-parent
  - stat-mode
- policers-hqos-manageable
- post-policer-mapping
- prec
- queue
  - adaptation-rule
  - adaptation-rule
  - adv-config-policy
  - agg-shaper-weight
  - avg-frame-overhead
  - burst-limit
  - cbs
  - drop-tail
    - exceed
      - percent-reduction-from-mbs
    - high
      - percent-reduction-from-mbs
    - highplus
      - percent-reduction-from-mbs
    - low
      - percent-reduction-from-mbs
  - fir-burst-limit
  - hs-alt-port-class-pool
  - hs-class-weight
  - hs-wred-queue
  - hs-wrr-weight
  - mbs
  - packet-byte-offset
  - parent
  - percent-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos sap-egress queue port-parent

- port-parent
- rate
- sched-class
- wred-queue
- sched-class-elevation
- scope
- sub-insert-shared-pccrule

sap-ingress
- default-fc
- default-priority
- description
- dot1p
- dscp
- dynamic-policer
  - cbs
  - mbs
  - packet-byte-offset
  - parent
  - range
  - stat-mode
- fc
  - broadcast-policer
  - broadcast-queue
  - de-1-out-profile
  - egress-fc
  - in-remark
  - multicast-policer
  - multicast-queue
  - out-remark
  - policer
  - profile
  - queue
  - unknown-policer
  - unknown-queue
- ip-criteria
  - entry
    - action
    - description
    - match
      - dscp
      - dst-ip
      - dst-port
      - fragment
      - src-ip
      - src-port
      - vxlan-vni
    - tag
  - renum
  - type
- ipv6-criteria
  - entry
    - action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos sap-ingress ipv6-criteria entry description

- description
- match
  - dscp
  - dst-ip
  - dst-port
  - fragment
  - src-ip
  - src-port
  - vxlan-vni
- tag
- renum
- type

- lsp-exp
- mac-criteria
  - entry
    - action
    - description
    - match
      - atm-vci
      - dot1p
      - dsap
      - dst-mac
      - etype
      - inner-tag
      - outer-tag
      - snap-oui
      - snap-pid
      - src-mac
      - ssap
  - renum
  - type
- policer
  - adaptation-rule
  - adv-config-policy
  - cbs
  - description
  - high-prio-only
  - mbs
  - packet-byte-offset
  - parent
  - percent-rate
  - profile-capped
  - rate
  - scheduler-parent
  - stat-mode
- policers-hqos-manageable
- prec
- queue
  - adaptation-rule
  - adv-config-policy
  - burst-limit
  - cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos sap-ingress queue cir-non-profiling

- cir-non-profiling
- drop-tail
  - low
    - percent-reduction-from-mbs
- mbs
- packet-byte-offset
- parent
- percent-rate
- rate

- scope
- sub-insert-shared-pccrule

- scheduler-policy
  - description
  - frame-based-accounting
  - tier
    - parent-location
    - scheduler
      - description
      - limit-unused-bandwidth
      - parent
      - percent-rate
      - port-parent
      - rate

- shared-queue
  - description
  - fc
    - broadcast-queue
    - multicast-queue
    - queue
    - unknown-queue
  - queue
    - cbs
    - drop-tail
      - low
        - percent-reduction-from-mbs
    - mbs
    - rate

- slope-policy
  - description
  - exceed-slope
    - max-avg
    - max-prob
    - shutdown
    - start-avg
  - high-slope
    - max-avg
    - max-prob
    - shutdown
    - start-avg
  - highplus-slope
    - max-avg
    - max-prob

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos slope-policy highplus-slope shutdown

- **shutdown**
- **start-avg**

low-slope

- **max-avg**
- **max-prob**
- **shutdown**
- **start-avg**

time-average-factor

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.36 configure redundancy Commands

- redundancy
  - bgp-evpn-multi-homing
    - boot-timer
    - es-activation-timer
    - site-activation-timer
  - bgp-multi-homing
    - boot-timer
    - site-activation-timer
    - site-min-down-timer
  - cert-sync
  - mgmt-ethernet
  - multi-chassis
    - options
      - sub-mgmt
        - dhcp-leasetime-threshold
    - peer
      - authentication-key
      - description
      - mc-endpoint
        - bfd-enable
        - boot-timer
        - hold-on-neighbor-failure
        - keep-alive-interval
        - passive-mode
        - shutdown
        - system-priority
      - mc-ipsec
        - bfd-enable
        - discovery-interval
        - hold-on-neighbor-failure
        - keep-alive-interval
        - tunnel-group
          - peer-group
          - priority
          - shutdown
      - mc-lag
        - hold-on-neighbor-failure
        - keep-alive-interval
        - lag
        - shutdown
      - mc-ring
        - l3-ring
          - in-band-control-path
            - debounce
            - dst-ip
            - interface
            - max-debounce-time
            - service-id
            - service-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure redundancy multi-chassis peer mc-ring l3-ring ring-node

- ring-node
  - connectivity-verify
    - dst-ip
    - interval
    - service-id
    - service-name
    - shutdown
    - src-ip
    - src-mac
    - vlan
  - shutdown
  - srrp-instance
- ring
  - in-band-control-path
    - debounce
    - dst-ip
    - interface
    - max-debounce-time
    - service-id
    - service-name
  - path-b
    - range
  - path-excl
    - range
  - ring-node
    - connectivity-verify
      - dst-ip
      - interval
      - service-id
      - service-name
      - shutdown
      - src-ip
      - src-mac
      - vlan
    - shutdown
  - shutdown
    - connectivity-verify
      - src-ip
      - src-mac
      - interval
      - service-name
    - in-band-control-path
      - debounce
      - dst-ip
      - interface
      - max-debounce-time
    - srrp-instance
- peer-name
- shutdown
- source-address
- sync
  - diameter-node

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure redundancy multi-chassis peer sync diameter-node node

- **node**
- diameter-proxy
- igmp
- igmp-snooping
- ipsec
- l2tp
- local-dhcp-server
- mc-ring
- mld
- mld-snooping
- nat
  - nat-group
- pim-snooping
- port
  - range
- python
- sdp
  - range
- shutdown
- srrp
- sub-host-trk
- sub-mgmt
- track-srrp-instances
  - track-srrp
    - l2tp-tunnel-id-range
- transport-encryption
  - application
- tunnel-group
- warm-standby
- rollback-sync
- srrp
  - auto-srrp-id-range
- synchronize

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37 configure router Commands

— router

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.1 configure router admin-tags Commands

- admin-tags
  - admin-tag
  - route-admin-tag-policy
    - exclude
    - include

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.2 configure router aggregate Commands

— aggregate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.3 configure router allow-icmp-redirect Commands

— **allow-icmp-redirect**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router allow-icmp6-redirect

3.4.37.4 configure router allow-icmp6-redirect Commands

— **allow-icmp6-redirect**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router autonomous-system

3.4.37.5 configure router autonomous-system Commands

— **autonomous-system**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bfd

3.4.37.6 configure router bfd Commands

- **bfd**
  - **abort**
  - **begin**
  - **bfd-template**
    - **echo-receive**
    - **multiplier**
    - **receive-interval**
    - **transmit-interval**
    - **type**
  - **commit**
  - **seamless-bfd**
    - **peer**
      - **discriminator**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.7 configure router bgp Commands

- bgp
  - add-paths
    - evpn
    - ipv4
    - ipv6
    - label-ipv4
    - label-ipv6
    - mcast-vpn-ipv4
    - mcast-vpn-ipv6
    - mvpn-ipv4
    - mvpn-ipv6
    - vpn-ipv4
    - vpn-ipv6
  - advertise-external
  - advertise-inactive
  - advertise-ipv6-next-hops
  - aggregator-id-zero
  - auth-keychain
  - authentication-key
  - backup-path
  - best-path-selection
    - always-compare-med
    - as-path-ignore
    - compare-origin-validation-state
    - d-path-length-ignore
    - deterministic-med
    - ebgp-ibgp-equal
    - ignore-nh-metric
    - ignore-router-id
    - origin-invalid-unusable
  - bfd-enable
  - bgp-tunnel-metric
  - bgp-tunnel-preference
  - block-prefix-sid
  - cluster
  - connect-retry
  - convergence
    - family
      - max-wait-to-advertise
    - min-wait-to-advertise
  - damp-peer-oscillations
  - damping
  - def-recv-evpn-encap
  - default-label-preference
  - default-preference
  - description
  - disable-4byte-asn
  - disable-client-reflect
  - disable-communities

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp disable-fast-external-failover

- disable-fast-external-failover
- disable-route-table-install
- dynamic-neighbor-limit
- ebgp-default-reject-policy
- egress-peer-engineering
  - shutdown
- enable-inter-as-vpn
- enable-peer-tracking
- enable-rr-vpn-forwarding
- enable-subconfed-vpn-forwarding
- enforce-first-as
- error-handling
  - update-fault-tolerance
- export
- extended-nh-encoding
- family
- flowspec
  - validate-dest-prefix
  - validate-redirect-ip
- graceful-restart
  - enable-notification
  - long-lived
    - advertise-stale-to-all-neighbors
    - advertised-stale-time
    - family
      - advertised-stale-time
      - helper-override-stale-time
    - forwarding-bits-set
    - helper-override-restart-time
    - helper-override-stale-time
  - restart-time
  - stale-routes-time
- group
  - add-paths
    - evpn
    - ipv4
    - ipv6
    - label-ipv4
    - label-ipv6
    - mcast-vpn-ipv4
    - mcast-vpn-ipv6
    - mvpn-ipv4
    - mvpn-ipv6
    - vpn-ipv4
    - vpn-ipv6
  - advertise-inactive
  - advertise-ipv6-next-hops
  - aggregator-id-zero
  - aigp
  - as-override
  - auth-keychain
  - authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group bfd-enable

- bfd-enable
- block-prefix-sid
- cluster
- connect-retry
- damp-peer-oscillations
- damping
- def-recv-evpn-encap
- default-label-preference
- default-preference
- default-route-target
- description
- disable-4byte-asn
- disable-capability-negotiation
- disable-client-reflect
- disable-communities
- disable-fast-external-failover
- dynamic-neighbor
  - match
    - prefix
      - allowed-peer-as
- dynamic-neighbor-limit
- ebgp-default-reject-policy
- egress-engineering
  - shutdown
- egress-peer-engineering-label-unicast
- enable-origin-validation
- enable-peer-tracking
- enforce-first-as
- error-handling
  - update-fault-tolerance
- export
- extended-nh-encoding
- family
- graceful-restart
  - enable-notification
  - long-lived
    - advertise-stale-to-all-neighbors
    - advertised-stale-time
    - family
      - advertised-stale-time
      - helper-override-stale-time
    - forwarding-bits-set
    - helper-override-restart-time
    - helper-override-stale-time
  - restart-time
  - stale-routes-time
- hold-time
- import
- initial-send-delay-zero
- keepalive
- label-preference
- link-bandwidth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group link-bandwidth accept-from-ebgp

- accept-from-ebgp
- add-to-received-ebgp
- aggregate-used-paths
- send-to-ebgp
- local-address
- local-as
- local-preference
- loop-detect
- loop-detect-threshold
- med-out
- min-route-advertisement
- monitor
  - route-monitoring
  - shutdown
  - station
- multihop
- multipath-eligible
- neighbor
  - add-paths
    - evpn
    - ipv4
    - ipv6
    - label-ipv4
    - label-ipv6
    - mcast-vpn-ipv4
    - mcast-vpn-ipv6
    - mvpn-ipv4
    - mvpn-ipv6
    - vpn-ipv4
    - vpn-ipv6
  - advertise-inactive
  - advertise-ipv6-next-hops
  - advertise-ldp-prefix
  - aggregator-id-zero
  - aigp
  - as-override
  - auth-keychain
  - authentication-key
  - bfd-enable
  - block-prefix-sid
  - cluster
  - connect-retry
  - damp-peer-oscillations
  - damping
  - def-recv-evpn-encap
  - default-label-preference
  - default-preference
  - default-route-target
  - description
  - disable-4byte-asn
  - disable-capability-negotiation
  - disable-client-reflect

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group neighbor disable-communities

- disable-communities
- disable-fast-external-failover
- ebgp-default-reject-policy
- egress-engineering
  - shutdown
- egress-peer-engineering-label-unicast
- enable-origin-validation
- enable-peer-tracking
- enforce-first-as
- error-handling
  - update-fault-tolerance
- export
- extended-nh-encoding
- family
- graceful-restart
  - enable-notification
  - long-lived
    - advertise-stale-to-all-neighbors
    - advertised-stale-time
    - family
      - advertised-stale-time
      - helper-override-stale-time
    - forwarding-bits-set
    - helper-override-restart-time
    - helper-override-stale-time
  - restart-time
  - stale-routes-time
- hold-time
- import
- initial-send-delay-zero
- keepalive
- l2vpn-cisco-interop
- label-preference
- link-bandwidth
  - accept-from-ebgp
  - add-to-received-ebgp
  - aggregate-used-paths
  - send-to-ebgp
- local-address
- local-as
- local-preference
- loop-detect
- loop-detect-threshold
- med-out
- min-route-advertisement
- monitor
  - route-monitoring
  - shutdown
  - station
- multihop
- multipath-eligible
- next-hop-self

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group neighbor next-hop-unchanged

- next-hop-unchanged
- outbound-route-filtering
  - extended-community
    - accept-orf
    - send-orf
- passive
- path-mtu-discovery
- peer-as
- preference
- prefix-limit
- remove-private
- segment-routing-v6
  - route-advertisement
    - drop-routes-with-srv6-tlvs
    - family
      - strip-srv6-tlvs
- selective-label-ipv4-install
- send-default
- shutdown
- split-horizon
- tcp-mss
- third-party-nexthop
- ttl-security
- type
- vpn-apply-export
- vpn-apply-import

- next-hop-self
- next-hop-unchanged
- outbound-route-filtering
  - extended-community
    - accept-orf
    - send-orf
- passive
- path-mtu-discovery
- peer-as
- preference
- prefix-limit
- remove-private
- segment-routing-v6
  - route-advertisement
    - drop-routes-with-srv6-tlvs
    - family
      - strip-srv6-tlvs
- selective-label-ipv4-install
- send-default
- shutdown
- split-horizon
- tcp-mss
- third-party-nexthop
- ttl-security
- type
- vpn-apply-export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group vpn-apply-import

- vpn-apply-import
- hold-time
- ibgp-multipath
- import
- initial-send-delay-zero
- keepalive
- label-allocation
  - label-ipv6
    - disable-explicit-null
- label-preference
- link-state-export-enable
- link-state-import-enable
- local-as
- local-preference
- loop-detect
- loop-detect-threshold
- med-out
- min-route-advertisement
- monitor
  - route-monitoring
  - shutdown
  - station
- mp-bgp-keep
- multi-path
  - ipv4
  - ipv6
  - label-ipv4
  - label-ipv6
  - maximum-paths
- multihop
- mvpn-vrf-import-subtype-new
- neighbor-trust
- next-hop-resolution
  - allow-unresolved-leaking
  - labeled-routes
    - allow-static
    - rr-use-route-table
    - transport-tunnel
      - family
        - allow-flex-algo-fallback
        - enforce-strict-tunnel-tagging
        - resolution
        - resolution-filter
          - bgp
          - ldp
          - mpls-fwd-policy
          - rib-api
          - rsvp
          - sr-isis
          - sr-ospf
          - sr-ospf3
          - sr-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter sr-te

- sr-te
- udp
- use-bgp-routes
- label-ipv6-explicit-null
- policy
- shortcut-tunnel
- family
- allow-flex-algo-fallback
- disallow-igp
- enforce-strict-tunnel-tagging
- resolution
- resolution-filter
- bgp
- ldp
- mpls-fwd-policy
- rib-api
- rsvp
- sr-isis
- sr-ospf
- sr-ospf3
- sr-policy
- sr-te
- use-bgp-routes
- vpn-family-policy
- weighted-ecmp
- optimal-route-reflection
- location
- primary-ip-address
- primary-ipv6-address
- secondary-ip-address
- secondary-ipv6-address
- tertiary-ip-address
- tertiary-ipv6-address
- spf-wait
- outbound-route-filtering
- extended-community
- accept-orf
- send-orf
- override-tunnel-elc
- path-mtu-discovery
- peer-tracking-policy
- preference
- purge-timer
- rapid-update
- rapid-withdrawal
- remove-private
- rib-management
- ipv4
- leak-import
- route-table-import
- ipv6
- leak-import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp rib-management ipv6 route-table-import

- route-table-import
- label-ipv4
  - leak-import
  - route-table-import
- label-ipv6
  - route-table-import
- route-target-list
- router-id
- segment-routing
  - prefix-sid-range
  - shutdown
- segment-routing-v6
  - family
    - add-srv6-tlvs
    - ignore-received-srv6-tlvs
  - source-address
- selective-label-ip-prioritization
- selective-label-ipv4-install
- send-default
- shutdown
- split-horizon
- sr-policy-import
- tcp-mss
- third-party-nexthop
- vpn-apply-export
- vpn-apply-import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bier

3.4.37.8 configure router bier Commands

- bier
  - bfd-enable
  - fast-reroute
  - shutdown
  - template
    - shutdown
    - sub-domain
      - bfr-id
      - mt
      - prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router class-forwarding

3.4.37.9 configure router class-forwarding Commands

— class-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.10 configure router confederation Commands

— confederation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router description

3.4.37.11 configure router description Commands

— description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.12 configure router dhcp Commands

- dhcp
  - local-dhcp-server
    - description
    - failover
      - ignore-mclt-on-takeover
      - maximum-client-lead-time
      - partner-down-delay
      - peer
      - shutdown
      - startup-wait-time
    - force-renews
    - lease-hold-time
    - lease-hold-time-for
      - internal-lease-ipsec
      - solicited-release
    - pool
      - description
      - failover
        - ignore-mclt-on-takeover
        - maximum-client-lead-time
        - partner-down-delay
        - peer
        - shutdown
        - startup-wait-time
      - max-lease-time
      - min-lease-time
      - minimum-free
      - nak-non-matching-subnet
      - offer-time
      - options
        - custom-option
        - dns-server
        - domain-name
        - lease-rebind-time
        - lease-renew-time
        - lease-time
        - netbios-name-server
        - netbios-node-type
      - subnet
        - address-range
        - drain
        - exclude-addresses
        - maximum-declined
        - minimum-free
        - options
          - custom-option
          - default-router
          - subnet-mask
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router dhcp local-dhcp-server use-gi-address

- use-gi-address
- use-pool-from-client
- user-db
- user-ident
  - ignore-mclt-on-takeover
  - maximum-client-lead-time
  - peer
  - startup-wait-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.13 configure router dhcp6 Commands

- dhcp6
  - local-dhcp-server
    - allow-lease-query
    - defaults
      - options
        - custom-option
        - dns-server
        - domain-name
      - preferred-lifetime
      - rebind-timer
      - renew-timer
      - valid-lifetime
    - description
    - failover
      - ignore-mclt-on-takeover
      - maximum-client-lead-time
      - partner-down-delay
      - peer
      - shutdown
      - startup-wait-time
    - ignore-rapid-commit
    - interface-id-mapping
    - lease-hold-time
    - lease-hold-time-for
      - internal-lease-ipsec
      - solicited-release
    - pool
      - delegated-prefix-length
      - description
      - exclude-prefix
      - failover
        - ignore-mclt-on-takeover
        - maximum-client-lead-time
        - partner-down-delay
        - peer
        - shutdown
        - startup-wait-time
      - options
        - custom-option
        - dns-server
        - domain-name
      - prefix
        - drain
        - options
          - custom-option
          - dns-server
          - domain-name
        - preferred-lifetime
        - rebind-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router dhcp6 local-dhcp-server pool prefix renew-timer

- renew-timer
- thresholds
  - minimum-free
    - depleted-event
    - minimum
  - valid-lifetime
- thresholds
  - minimum-free
    - depleted-event
    - minimum
- server-id
- shutdown
- use-link-address
- use-pool-from-client
- user-ident
  - ignore-mclt-on-takeover
  - maximum-client-lead-time
  - peer
  - startup-wait-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router disable-selective-fib

3.4.37.14 configure router disable-selective-fib Commands

— disable-selective-fib

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.15 configure router dns Commands

— dns
  — redirect-vprn
    — service

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.16 configure router ecmp Commands

— ecmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.17 configure router entropy-label Commands

— **entropy-label**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router fib-priority

3.4.37.18 configure router fib-priority Commands

— **fib-priority**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.19 configure router fib-telemetry Commands

— **fib-telemetry**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.20 configure router firewall Commands

- firewall
  - domain
    - dhcp6-server
    - prefix
      - description
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.21 configure router flexible-algorithm-definitions Commands

- flexible-algorithm-definitions
  - flex-algo
    - description
    - exclude
      - admin-group
    - flags-tlv
    - include-all
      - admin-group
    - include-any
      - admin-group
    - metric-type
    - priority
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.22 configure router flowspec Commands

- flowspec
  - filter-cam-type
  - ip-filter-max-size
  - ipv6-filter-max-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.23 configure router gmpls Commands

- gmpls
  - gr-helper-time
  - keep-multiplier
  - lsp
    - e2e-protection-type
    - encoding-type
    - generalized-pid
    - protect-path
      - bandwidth
      - exclude-srlg
      - peer
      - segment-protection-type
      - shutdown
    - retry-limit
    - retry-timer
    - revert-timer
    - shutdown
    - switching-type
    - to
    - working-path
      - bandwidth
      - exclude-srlg
      - peer
      - segment-protection-type
      - shutdown
  - lsp-init-retry-timeout
  - path
    - hop
    - shutdown
  - peer
    - hello-interval
    - lsp-hold-timer
    - shutdown
  - rapid-retransmit-time
  - rapid-retry-limit
  - refresh-time
  - shutdown
  - te-link
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router gtm

3.4.37.24 configure router gtm Commands

- gtm
  - mvpn
  - provider-tunnel
    - inclusive
      - rsvp
        - lsp-template
        - shutdown
    - selective
      - data-delay-interval
      - data-threshold
      - maximum-p2mp-spmsi
      - rsvp
        - lsp-template
        - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.25 configure router gtp Commands

- gtp
  - s11
    - interface
      - apn-policy
    - peer-profile-map
      - address
  - upf-data-endpoint
  - uplink
    - apn
    - pdn-type
    - peer-profile-map
      - address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.26 configure router icmp-tunneling Commands

— icmp-tunneling

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.27 configure router if-attribute Commands

- if-attribute
  - admin-group
  - srlg-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.28 configure router igmp Commands

- igmp
  - group-interface
    - disable-router-alert-check
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - shutdown
      - policy
      - unconstrained-bw
    - query-interval
    - query-last-member-interval
    - query-response-interval
    - query-src-ip
    - shutdown
    - sub-hosts-only
    - subnet-check
    - version
  - grp-if-query-src-ip
  - interface
    - disable-router-alert-check
    - group-interface
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - level
        - number-down
        - shutdown
        - use-lag-port-weight
      - policy
      - unconstrained-bw
    - query-interval
    - query-last-member-interval
    - query-response-interval
    - redundant-multicast
    - shutdown
    - ssm-translate
      - grp-range
        - source
    - static
      - group
        - source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router igmp interface static group starg

— starg
— subnet-check
— version
— query-interval
— query-last-member-interval
— query-response-interval
— robust-count
— shutdown
— ssm-translate
— grp-range
— source
— tunnel-interface
— shutdown
— static
— group
— source
— starg

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.29 configure router interface Commands

- interface
  - address
  - allow-directed-broadcasts
  - arp-learn-unsolicited
  - arp-limit
  - arp-proactive-refresh
  - arp-retry-timer
  - arp-timeout
  - bfd
  - cflowd-parameters
    - sampling
  - cpu-protection
  - description
  - dhcp
    - description
    - gi-address
    - option
      - action
      - circuit-id
      - client-mac-address
      - remote-id
      - vendor-specific-option
        - client-mac-address
        - pool-name
        - port-id
        - service-id
        - string
        - system-id
    - python-policy
    - relay-plain-bootp
    - release-include-gi-address
    - server
    - shutdown
    - trusted
  - dist-cpu-protection
  - egress
    - filter
  - enable-ingress-stats
  - enable-mac-accounting
  - eth-cfm
    - mep
      - alarm-notification
        - fng-alarm-time
        - fng-reset-time
      - ccm-enable
      - ccm-ltm-priority
      - ccm-padding-size
      - ccm-tlv-ignore
      - collect-lmm-fc-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface eth-cfm mep collect-lmm-fc-stats fc

- fc
- fc-in-profile
- collect-lmm-stats
- description
- eth-test-enable
  - bit-error-threshold
  - test-pattern
  - test-pattern
- facility-fault
- fng-alarm-time
- fng-reset-time
- grace
  - eth-ed
    - max-rx-defect-window
    - priority
    - rx-eth-ed
    - tx-eth-ed
  - eth-vsm-grace
    - rx-eth-vsm-grace
    - tx-eth-vsm-grace
- lbm-svc-act-responder
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown

- gre-termination
- group-encryption
  - encryption-keygroup
  - ip-exception
- hold-time
  - down
  - up
- icmp
  - mask-reply
  - param-problem
  - redirects
  - ttl-expired
  - unreachables
- if-attribute
  - admin-group
  - delay
    - delay-selection
    - dynamic
      - measurement-template
      - twamp-light
      - twamp-light
        - ipv4
          - destination
          - shutdown
          - source
        - ipv6
          - destination

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface if-attribute delay dynamic twamp-light ipv6 shutdown

- shutdown
- source
- static
- srlg-group
- ingress
- destination-class-lookup
- filter
- policy-accounting
- ip-helper-address
- ip-mtu
- ip-tunnel
- remote-ip
- ipsec
- ip-exception
- ipsec-tunnel
- bfd-designate
- bfd-enable
- clear-df-bit
- copy-traffic-class-upon-decapsulation
- description
- icmp6-generation
- dynamic-keying
- auto-establish
- cert
- cert-profile
- status-verify
- default-result
- primary
- trust-anchor-profile
- ike-policy
- local-id
- pre-shared-key
- transform
- encapsulated-ip-mtu
- icmp-generation
- frag-required
- interval
- message-count
- icmp6-generation
- pkt-too-big
- interval
- message-count
- ip-mtu
- local-gateway-address
- manual-keying
- max-history-ike-key-records
- security-association
- max-history-esp-key-records
- max-history-ike-key-records
- pmtu-discovery-aging
- private-tcp-mss-adjust
- propagate-pmtu-v4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface ipsec ipsec-tunnel propagate-pmtu-v6

- propagate-pmtu-v6
- public-tcp-mss-adjust
- remote-gateway-address
- replay-window
- security-policy
- shutdown
- ipv6-exception
- shutdown
- pkt-too-big
- interval
- message-count

- ipv6
- address
- bfd
- dad-disable
- forward-ipv4-packets
- icmp6
- packet-too-big
- param-problem
- redirects
- time-exceeded
- unreachables
- link-local-address
- local-dhcp-server
- local-proxy-nd
- nd-learn-unsolicited
- nd-proactive-refresh
- neighbor
- neighbor-limit
- proxy-nd-policy
- qos-route-lookup
- reachable-time
- secure-nd
- allow-unsecured-msgs
- link-local-modifier
- public-key-min-bits
- security-parameter
- shutdown
- stale-time
- tcp-mss
- urpf-check
- ignore-default
- mode
- vrrp
- backup
- bfd-enable
- init-delay
- mac
- master-int-inherit
- message-interval
- ntp-reply
- oper-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface ipv6 vrrp ping-reply

- ping-reply
- policy
- preempt
- priority
- shutdown
- standby-forwarding
- telnet-reply
- traceroute-reply

- lag-link-map-profile
- lag-per-link-hash
- ldp-sync-timer
- load-balancing
  - egr-ip-load-balancing
  - flow-label-load-balancing
  - lsr-load-balancing
  - spi-load-balancing
  - teid-load-balancing
- local-dhcp-server
- local-proxy-arp
- loopback
- mac
- network-domain
- port
- proxy-arp-policy
- ptp-hw-assist
- qos
- qos-route-lookup
- remote-proxy-arp
- secondary
- shutdown
- static-arp
- strip-label
- tcp-mss
- tos-marking-state
- unnumbered
- untrusted
- urpf-check
  - ignore-default
  - mode
- urpf-selected-vprns
- vas-if-type
- vrrp
  - authentication-key
  - backup
  - bfd-enable
  - description
  - init-delay
  - mac
  - master-int-inherit
  - message-interval
  - ntp-reply
  - oper-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface vrrp ping-reply

- **ping-reply**
- **policy**
- **preempt**
- **priority**
- **shutdown**
- **ssh-reply**
- **standby-forwarding**
- **telnet-reply**
- **traceroute-reply**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.30 configure router ip-fast-reroute Commands

— ip-fast-reroute

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.31 configure router ipsec Commands

- **ipsec**
  - **security-policy**
    - **entry**
      - **local-ip**
      - **local-v6-ip**
      - **remote-ip**
      - **remote-v6-ip**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ipv6

3.4.37.32 configure router ipv6 Commands

— ipv6
  — reachable-time
  — stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.33 configure router ipv6-te-router-id Commands

— ipv6-te-router-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.34 configure router isa-service-chaining Commands

— isa-service-chaining
  — nat-group
  — vxlan-vtep-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.35 configure router isis Commands

- isis
  - advertise-passive-only
  - advertise-router-capability
  - advertise-tunnel-link
  - all-l1isis
  - all-l2isis
  - area-id
  - auth-keychain
  - authentication-check
  - authentication-key
  - authentication-type
  - csnp-authentication
  - database-export
  - default-route-tag
  - disable-ldp-sync
  - entropy-label
    - override-tunnel-elc
  - export
  - export-limit
  - flexible-algorithms
    - flex-algo
      - advertise
      - loopfree-alternates
      - micro-loop-avoidance
      - participate
    - shutdown
  - graceful-restart
    - helper-disable
  - hello-auth-keychain
  - hello-authentication
  - hello-padding
  - ignore-attached-bit
  - ignore-lsp-errors
  - ignore-narrow-metric
  - igp-shortcut
    - shutdown
    - tunnel-next-hop
      - family
        - resolution
        - resolution-filter
          - rsvp
          - **sr-te**
        - sr-te
  - iid-tlv-enable
  - import
  - interface
    - adjacency-set
    - bfd-enable
    - csnp-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router isis interface default-instance

- default-instance
- flex-algo
  - ipv4-node-sid
  - ipv6-node-sid
- hello-auth-keychain
- hello-authentication
- hello-authentication-key
- hello-authentication-type
- hello-padding
- interface-type
- ipv4-adjacency-sid
- ipv4-multicast-disable
- ipv4-node-sid
- ipv6-adjacency-sid
- ipv6-multicast-disable
- ipv6-node-sid
- ipv6-unicast-disable
- level
  - hello-auth-keychain
  - hello-authentication-key
  - hello-authentication-type
  - hello-interval
  - hello-multiplier
  - hello-padding
  - ipv4-multicast-metric
  - ipv6-multicast-metric
  - ipv6-unicast-metric
    - hello-multiplier
  - metric
  - passive
  - priority
  - sd-offset
  - sf-offset
  - shutdown
- level-capability
- lfa-policy-map
- load-balancing-weight
- loopfree-alternate-exclude
- lsp-pacing-interval
- mesh-group
- passive
- retransmit-interval
- shutdown
- sid-protection
- tag
- tag
- ipv4-multicast-routing
- ipv4-routing
- ipv6-multicast-routing
- ipv6-routing
- ldp-over-rsvp
- level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router isis level advertise-router-capability

- advertise-router-capability
- auth-keychain
- authentication-key
- authentication-type
- bier
  - shutdown
  - template
- csnp-authentication
- database-export-exclude
- default-ipv4-multicast-metric
- default-ipv6-multicast-metric
- default-ipv6-unicast-metric
- default-metric
- external-preference
- hello-auth-keychain
- hello-authentication
- hello-padding
- loopfree-alternate-exclude
- lsp-mtu-size
- preference
- psnp-authentication
- wide-metrics-only

- level-capability
- link-group
  - description
  - level
    - ipv4-multicast-metric-offset
    - ipv4-unicast-metric-offset
    - ipv6-multicast-metric-offset
    - ipv6-unicast-metric-offset
    - member
    - oper-members
    - revert-members
- loopfree-alternates
  - augment-route-table
  - exclude
    - prefix-policy
  - remote-lfa
    - node-protect
  - ti-lfa
    - node-protect
- lsp-lifetime
- lsp-minimum-remaining-lifetime
- lsp-mtu-size
- lsp-refresh-interval
- mru-mismatch-detection
- multi-topology
  - ipv4-multicast
  - ipv6-multicast
  - ipv6-unicast
- multicast-import
- overload

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router isis overload-export-external

- overload-export-external
- overload-export-interlevel
- overload-on-boot
- poi-tlv-enable
- prefix-attributes-tlv
- prefix-limit
- psnp-authentication
- reference-bandwidth
- rib-priority
- router-id
- segment-routing
  - adj-sid-hold
  - adjacency-set
    - family
    - parallel
    - sid
  - class-forwarding
  - egress-statistics
    - adj-set
    - adj-sid
    - node-sid
  - entropy-label
  - export-tunnel-table
  - ingress-statistics
    - adj-set
    - adj-sid
    - node-sid
  - mapping-server
    - shutdown
    - sid-map
  - maximum-sid-depth
    - override-bmi
    - override-erld
  - micro-loop-avoidance
  - prefix-sid-range
  - shutdown
  - srlb
  - tunnel-mtu
  - tunnel-table-pref
- segment-routing-v6
  - adj-sid-hold
  - locator
    - level
      - metric
    - level-capability
    - tag
  - shutdown
- shutdown
- standard-multi-instance
- strict-adjacency-check
- summary-address
- suppress-attached-bit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router isis system-id

- system-id
- timers
  - lsp-wait
  - spf-wait
- traffic-engineering
- traffic-engineering-options
  - application-link-attributes
    - legacy
  - ipv6
- unicast-import-disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.36 configure router l2tp Commands

- l2tp
  - avp-hiding
  - calling-number-format
  - challenge
  - cisco-nas-port
  - destruct-timeout
  - df-bit-lac
  - eth-tunnel
    - reconnect-timeout
  - exclude-avps
  - failover
    - recovery-max-session-lifetime
    - recovery-method
    - recovery-time
    - track-srrp
  - group
    - avp-hiding
    - challenge
    - description
    - destruct-timeout
    - df-bit-lac
    - eth-tunnel
      - reconnect-timeout
    - failover
      - recovery-method
      - recovery-time
    - hello-interval
    - idle-timeout
    - l2tpv3
      - cookie-length
      - digest-type
      - nonce-length
      - password
      - private-tcp-mss-adjust
      - public-tcp-mss-adjust
      - pw-cap-list
      - rem-router-id
      - track-password-change
    - lns-group
    - load-balance-method
    - local-address
    - local-name
    - max-retries-estab
    - max-retries-not-estab
    - mlppp
      - endpoint
      - interleave
      - max-fragment-delay
      - max-links

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router l2tp group mlppp reassembly-timeout

- reassembly-timeout
- short-sequence-numbers
- shutdown
- password
- ppp
  - authentication
  - authentication-policy
  - chap-challenge-length
  - default-group-interface
  - ipcp-subnet-negotiation
  - keepalive
  - lcp-force-ack-accm
  - lcp-ignore-magic-numbers
  - mtu
  - proxy-authentication
  - proxy-lcp
  - reject-disabled-ncp
  - user-db
- radius-accounting-policy
- receive-window-size
- session-assign-method
- session-limit
- shutdown
- tunnel
  - auto-establish
  - avp-hiding
  - challenge
  - description
  - destruct-timeout
  - df-bit-lac
  - failover
    - recovery-method
    - recovery-time
  - hello-interval
  - idle-timeout
  - l2tpv3
    - private-tcp-mss-adjust
    - public-tcp-mss-adjust
  - lns-group
  - load-balance-method
  - local-address
  - local-name
  - max-retries-estab
  - max-retries-not-estab
  - mlppp
    - admin-state
    - endpoint
    - interleave
    - max-fragment-delay
    - max-links
    - reassembly-timeout
    - short-sequence-numbers

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router l2tp group tunnel password

- password
- peer
- ppp
  - authentication
  - authentication-policy
  - chap-challenge-length
  - default-group-interface
  - ipcp-subnet-negotiation
  - keepalive
  - lcp-force-ack-accm
  - lcp-ignore-magic-numbers
  - mtu
  - proxy-authentication
  - proxy-lcp
  - reject-disabled-ncp
  - user-db
- preference
- radius-accounting-policy
- receive-window-size
- remote-name
- session-limit
- shutdown

- group-session-limit
- hello-interval
- idle-timeout
- ignore-avps
- l2tpv3
  - cookie-length
  - digest-type
  - nonce-length
  - password
  - private-tcp-mss-adjust
  - public-tcp-mss-adjust
  - transport-type
- local-address
- local-name
- max-retries-estab
- max-retries-not-estab
- next-attempt
- password
- peer-address-change-policy
- radius-accounting-policy
- receive-window-size
- replace-result-code
- rtm-debounce-time
- session-assign-method
- session-limit
- shutdown
- tunnel-selection-blacklist
  - add-tunnel
  - max-list-length
  - max-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router l2tp tunnel-selection-blacklist timeout-action

— **timeout-action**
— **tunnel-session-limit**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.37 configure router ldp Commands

- ldp
  - aggregate-prefix-match
    - prefix-exclude
    - shutdown
  - class-forwarding
  - consider-system-ip-in-gep
    - accounting-policy
    - collect-stats
  - egress-statistics
    - fec-prefix
      - accounting-policy
      - collect-stats
      - shutdown
  - entropy-label-capability
  - export
  - export-tunnel-table
  - fast-reroute
  - fec-originate
  - generate-basic-fec-only
  - graceful-restart
    - maximum-recovery-time
    - neighbor-liveness-time
  - implicit-null-label
  - import
  - import-mcast-policy
  - import-pmsi-routes
    - evpn
    - mvpn
    - mvpn-no-export
    - mvpn-no-export-community
  - import-tunnel-table
  - interface-parameters
    - interface
      - bfd-enable
      - ipv4
        - fec-type-capability
          - p2mp-ipv4
          - p2mp-ipv6
          - prefix-ipv4
          - prefix-ipv6
        - hello
        - keepalive
        - local-lsr-id
        - shutdown
        - transport-address
      - ipv6
        - fec-type-capability
          - p2mp-ipv4
          - p2mp-ipv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ldp interface-parameters interface ipv6 fec-type-capability prefix-ipv4

- prefix-ipv4
- prefix-ipv6
- hello
- keepalive
- local-lsr-id
- shutdown
- transport-address
- load-balancing-weight
- shutdown
- ipv4
- hello
- keepalive
- transport-address
- ipv6
- hello
- keepalive
- transport-address
- label-withdrawal-delay
- legacy-ipv4-lsr-interop
- lsp-bfd
- bfd-enable
- bfd-template
- failure-action
- lsp-ping-interval
- priority
- source-address
- max-ecmp-routes
- mcast-upstream-asbr-frr
- mcast-upstream-frr
- mp-mbb-time
- prefer-mcast-tunnel-in-tunnel
- prefer-protocol-stitching
- prefer-tunnel-in-tunnel
- resolve-root-using
- session-parameters
- peer
- adv-adj-addr-only
- adv-local-lsr-id
- community
- dod-label-distribution
- export-addresses
- export-prefixes
- fec-limit
- fec-type-capability
- p2mp
- p2mp-ipv4
- p2mp-ipv6
- prefix-ipv4
- prefix-ipv6
- fec129-cisco-interop
- import-prefixes
- pe-id-mac-flush-interop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ldp shortcut-local-ttl-propagate

- shortcut-local-ttl-propagate
- shortcut-transit-ttl-propagate
- shutdown
- targeted-session
  - auto-rx
    - ipv4
      - shutdown
      - tunneling
  - auto-tx
    - ipv4
      - shutdown
      - tunneling
  - disable-targeted-session
  - export-prefixes
  - import-prefixes
  - ipv4
    - hello
    - hello-reduction
    - keepalive
  - ipv6
    - hello
    - hello-reduction
    - keepalive
  - peer
    - bfd-enable
    - hello
    - hello-reduction
    - keepalive
    - local-lsr-id
    - mcast-tunneling
      - lsp
    - shutdown
    - tunneling
      - lsp
  - peer-template
    - adv-local-lsr-id
    - bfd-enable
    - community
    - hello
    - hello-reduction
    - keepalive
    - local-lsr-id
    - mcast-tunneling
    - shutdown
    - tunneling
  - peer-template-map
- tcp-session-parameters
  - auth-keychain
  - authentication-key
  - peer-transport
    - auth-keychain
    - authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ldp tcp-session-parameters peer-transport path-mtu-discovery

- **path-mtu-discovery**
- **ttl-security**

- **tunnel-down-damp-time**
- **tunnel-table-pref**
- **weighted-ecmp**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.38 configure router ldp-shortcut Commands

— ldp-shortcut

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.39 configure router leak-export Commands

— leak-export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.40 configure router leak-export-limit Commands

— leak-export-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.41 configure router lmp Commands

- lmp
  - gmpls-loopback-address
  - peer
    - control-channel
      - hello
      - peer-interface-address
      - setup-role
      - shutdown
      - ttl
    - control-channel-router
      - gmpls-loopback-address
    - peer-loopback-address
    - retransmission-interval
    - retry-limit
    - shutdown
    - te-link
  - shutdown
  - te-link
    - data-bearer
      - port
      - remote-id
      - shutdown
    - link-name
    - remote-id
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.42 configure router lsp-bfd Commands

- **lsp-bfd**
  - **bfd-sessions**
  - **tail-end**
    - **multiplier**
    - **receive-interval**
    - **transmit-interval**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.43 configure router mc-maximum-routes Commands

— **mc-maximum-routes**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.44 configure router mcac Commands

- mcac
  - if-policy
    - description
    - shutdown
    - unconstrained-bw
  - policy
    - bundle
      - bandwidth
      - channel
      - description
      - mc-constraints
        - lag-port-down
        - level
        - use-lag-port-weight
      - shutdown
    - default-action
    - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.45 configure router mld Commands

- mld
  - group-interface
    - disable-router-alert-check
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - shutdown
      - policy
      - unconstrained-bw
    - policy
    - query-interval
    - query-last-listener-interval
    - query-response-interval
    - query-src-ip
    - shutdown
    - sub-hosts-only
    - subnet-check
    - version
  - grp-if-query-src-ip
  - interface
    - disable-router-alert-check
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - level
        - number-down
        - shutdown
        - use-lag-port-weight
      - policy
      - unconstrained-bw
    - policy
    - query-interval
    - query-last-listener-interval
    - query-response-interval
    - shutdown
    - ssm-translate
      - grp-range
        - source
    - static
      - group
        - source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mld interface static group starg

— starg
— version
— query-interval
— query-last-listener-interval
— query-response-interval
— robust-count
— shutdown
— ssm-translate
— grp-range
— source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.46 configure router mpls Commands

- mpls
  - admin-group-frr
  - auto-bandwidth-multipliers
  - auto-lsp
  - aux-stats
  - bypass-resignal-timer
  - class-forwarding-policy
    - default-set
    - fc
  - cspf-on-loose-hop
  - dynamic-bypass
  - entropy-label
  - exponential-backoff-retry
  - forwarding-policies
    - forwarding-policy
      - binding-label
      - egress-statistics
        - shutdown
      - endpoint
      - ingress-statistics
        - shutdown
      - metric
      - next-hop-group
        - backup-next-hop
          - next-hop
          - pushed-labels
        - load-balancing-weight
        - primary-next-hop
          - next-hop
          - pushed-labels
        - shutdown
      - preference
      - revert-timer
      - shutdown
      - tunnel-table-pref
    - reserved-label-block
    - shutdown
  - frr-object
  - hold-timer
  - ingress-statistics
    - lsp
      - accounting-policy
      - collect-stats
      - shutdown
      - stat-mode
    - p2mp-template-lsp
      - accounting-policy
      - collect-stats
      - max-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls ingress-statistics p2mp-template-lsp shutdown

- shutdown
- stat-mode
- p2p-template-lsp
  - accounting-policy
  - collect-stats
  - max-stats
  - shutdown
  - stat-mode
- interface
  - admin-group
  - label-map
    - pop
    - shutdown
    - swap
  - mpls-tp-mep
    - ais-enable
    - if-num
    - if-num-validation
  - shutdown
  - srlg-group
  - te-metric
- least-fill-min-thd
- least-fill-reoptim-thd
- logger-event-bundling
- lsp
  - adaptive
  - admin-tag
  - adspec
  - auto-bandwidth
    - adjust-down
    - adjust-up
    - fc
    - max-bandwidth
    - min-bandwidth
    - monitor-bandwidth
    - multipliers
    - overflow-limit
    - underflow-limit
    - use-last-adj-bw
      - secondary-retry-limit
  - bfd
    - bfd-enable
    - bfd-template
    - failure-action
    - lsp-ping-interval
    - return-path-label
    - wait-for-up-timer
  - bgp-shortcut
  - bgp-transport-tunnel
  - class-forwarding
    - forwarding-set
  - forwarding-set

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls lsp class-type

- class-type
  - class-forwarding
- dest-global-id
- dest-tunnel-number
  - max-stats
- egress-statistics
  - accounting-policy
  - collect-stats
  - shutdown
  - stat-mode
- entropy-label
- exclude
- exclude-node
- fallback-path-computation-method
- fast-reroute
  - hop-limit
  - node-protect
  - propagate-admin-group
- from
- hop-limit
- igp-shortcut
- include
- ingress-statistics
  - accounting-policy
  - collect-stats
  - shutdown
  - stat-mode
- label-stack-reduction
- ldp-over-rsvp
- least-fill
- load-balancing-weight
- local-sr-protection
- lsp-self-ping
- main-ct-retry-limit
- max-sr-labels
- metric
- metric-type
- override-tunnel-elc
- p2mp-id
- path-computation-method
- path-profile
- pce-control
- pce-report
- primary
  - adaptive
  - backup-class-type
  - bandwidth
  - bfd
    - bfd-enable
    - bfd-template
    - lsp-ping-interval
    - return-path-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls lsp primary bfd wait-for-up-timer

- wait-for-up-timer
- class-type
- exclude
- hop-limit
- include
- priority
- record
- record-label
- shutdown

- primary-p2mp-instance
  - adaptive
  - bandwidth
  - exclude
  - hop-limit
  - include
  - priority
  - record
  - record-label
  - s2l-path
    - shutdown
  - shutdown
- propagate-admin-group
- protect-tp-path
  - in-label
  - lsp-num
  - mep
    - bfd-enable
    - bfd-trap-suppression
    - dsmap
    - oam-template
    - protection-template
    - shutdown
  - out-label
  - shutdown
- retry-limit
- retry-timer
- revert-timer
- rsvp-resv-style
- secondary
  - adaptive
  - bandwidth
  - bfd
    - bfd-enable
    - bfd-template
    - lsp-ping-interval
    - return-path-label
    - wait-for-up-timer
  - class-type
  - exclude
  - hop-limit
  - include
  - path-preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls lsp secondary priority

- priority
- record
- record-label
- shutdown
- srlg
- standby
- shutdown
- soft-preemption
- to
  - dsmap
  - dsmap
- vprn-auto-bind
- working-tp-path
  - in-label
  - lsp-num
  - mep
    - bfd-enable
    - bfd-trap-suppression
    - dsmap
    - oam-template
    - shutdown
  - out-label
  - shutdown
- lsp-init-retry-timeout
- lsp-self-ping
  - interval
  - rsvp-te
  - timeout
  - timeout-action
- lsp-template
  - adaptive
  - admin-tag
  - adspec
  - auto-bandwidth
    - adjust-down
    - adjust-up
    - fc
    - max-bandwidth
    - min-bandwidth
    - monitor-bandwidth
    - multipliers
    - overflow-limit
    - underflow-limit
  - backup-class-type
  - bandwidth
  - bfd
    - bfd-enable
    - bfd-template
    - failure-action
    - lsp-ping-interval
    - return-path-label
    - wait-for-up-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls lsp-template bgp-shortcut

- bgp-shortcut
- bgp-transport-tunnel
- class-forwarding
  - forwarding-set
- class-type
- default-path
  - max-stats
- egress-statistics
  - accounting-policy
  - collect-stats
  - shutdown
  - stat-mode
- entropy-label
- exclude
- fallback-path-computation-method
- family
- fast-reroute
  - hop-limit
  - node-protect
  - propagate-admin-group
- from
- hop-limit
- igp-shortcut
- include
- label-stack-reduction
- ldp-over-rsvp
- least-fill
- load-balancing-weight
- local-sr-protection
- lsp-self-ping
- main-ct-retry-limit
- max-sr-labels
- metric
- metric-type
- override-tunnel-elc
- path-computation-method
- path-profile
- pce-control
- pce-report
- priority
- propagate-admin-group
- record
- record-label
- retry-limit
- retry-timer
- shutdown
- soft-preemption
- vprn-auto-bind
- max-bypass-associations
- max-bypass-plr-associations
- mbb-prefer-current-hops
- mpls-tp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls mpls-tp global-id

- global-id
- node-id
- oam-template
  - bfd-template
  - hold-time-down
  - hold-time-up
- protection-template
  - rapid-psc-timer
  - revertive
  - slow-psc-timer
  - wait-to-restore
- shutdown
- tp-tunnel-id-range
- transit-path
  - forward-path
    - in-label
    - mip
      - dsmap
  - path-id
  - reverse-path
    - in-label
    - mip
      - dsmap
  - shutdown
- p2mp-resignal-timer
- p2mp-s2l-fast-retry
- p2p-active-path-fast-retry
- path
  - hop
  - shutdown
- pce-initiated-lsp
  - sr-te
    - shutdown
- pce-report
- resignal-on-igp-overload
- resignal-timer
- retry-on-igp-overload
- secondary-fast-retry-timer
- shortcut-local-ttl-propagate
- shortcut-transit-ttl-propagate
- shutdown
- sr-te-resignal
  - resignal-on-igp-event
  - resignal-timer
- srlg-database
  - router-id
    - interface
    - shutdown
- srlg-frr
- static-lsp
  - metric
  - push

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls static-lsp shutdown

- shutdown
- to
- static-lsp-fast-retry
- tunnel-table-pref
  - rsvp-te
  - sr-te
- user-srlg-db

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.47 configure router mpls-labels Commands

- mpls-labels
  - bgp-labels-hold-timer
  - reserved-label-block
    - start-label
  - sr-labels
  - static-label-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.48 configure router msdp Commands

- msdp
  - active-source-limit
  - data-encapsulation
  - export
  - group
    - active-source-limit
    - export
    - import
    - local-address
    - mode
    - peer
      - active-source-limit
      - authentication-key
      - default-peer
      - export
      - import
      - local-address
      - receive-msdp-msg-rate
      - shutdown
    - receive-msdp-msg-rate
    - shutdown
  - import
  - local-address
  - peer
    - active-source-limit
    - authentication-key
    - default-peer
    - export
    - import
    - local-address
    - receive-msdp-msg-rate
    - shutdown
  - receive-msdp-msg-rate
  - rpf-table
  - sa-timeout
  - shutdown
  - source
    - active-source-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.49 configure router mss-adjust-group Commands

— **mss-adjust-group**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.50 configure router mtrace2 Commands

— mtrace2
  — shutdown
  — udp-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.51 configure router multicast-info-policy Commands

— **multicast-info-policy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router nat

3.4.37.52 configure router nat Commands

- nat
  - inside
    - address
    - classic-lsn-max-subscriber-limit
    - destination-prefix
    - deterministic
      - classic-lsn-max-subscriber-limit
      - prefix
        - map
        - shutdown
      - prefix-map
        - map
        - shutdown
    - dnat-only
      - source-prefix-list
      - dslite-max-subscriber-limit
    - dslite-max-subscriber-limit
      - reassembly
      - tunnel-mtu
    - dual-stack-lite
      - address
        - ip-fragmentation
        - min-first-fragment-size-rx
        - reassembly
        - tunnel-mtu
      - shutdown
      - subscriber-prefix-length
    - l2-aware
      - address
    - nat-import
    - nat-policy
    - nat64
      - drop-zero-ipv4-checksum
      - ignore-tos
      - insert-ipv6-fragment-header
      - ip-fragmentation
      - ipv6-mtu
      - prefix
      - set-tos
      - shutdown
      - subscriber-prefix-length
    - redundancy
      - peer
      - peer6
      - steering-route
        - shutdown
    - source-prefix-list
      - description
      - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router nat inside subscriber-identification

- subscriber-identification
  - attribute
  - description
  - drop-unidentified-traffic
  - radius-proxy-server
  - shutdown
- map
  - map-domain
- outside
  - dnat-only
    - route-limit
  - downstream-ip-filter
  - downstream-ipv6-filter
  - mtu
  - pool
    - address-range
      - description
      - drain
      - shutdown
    - description
    - deterministic
      - port-reservation
    - external-assignment
    - icmp-echo-reply
    - mode
    - port-block-extensions
      - ports
    - port-forwarding-dyn-block-reservation
    - port-forwarding-range
    - port-reservation
    - redundancy
      - export
      - follow
      - monitor
      - shutdown
    - shutdown
    - subscriber-limit
    - watermarks
  - upstream-ip-filter
  - upstream-ipv6-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router network-domains

3.4.37.53 configure router network-domains Commands

- network-domains
  - network-domain
    - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.54 configure router origin-validation Commands

- origin-validation
  - rpki-session
    - connect-retry
    - description
    - local-address
    - port
    - refresh-time
    - shutdown
    - stale-time
  - static-entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.55 configure router ospf Commands

- ospf
  - advertise-router-capability
  - advertise-tunnel-link
  - area
    - advertise-router-capability
    - area-range
    - bier
      - shutdown
      - template
    - blackhole-aggregate
    - database-export-exclude
    - export
    - import
    - interface
      - adjacency-set
      - adjacency-sid
      - advertise-router-capability
      - advertise-subnet
      - auth-keychain
      - authentication-key
      - authentication-type
      - bfd-enable
      - dead-interval
      - flex-algo
        - node-sid
        - node-sid
      - hello-interval
      - interface-type
      - lfa-policy-map
      - load-balancing-weight
      - loopfree-alternate-exclude
      - lsa-filter-out
      - message-digest-key
      - metric
      - mtu
      - neighbor
      - node-sid
      - passive
      - poll-interval
      - priority
      - retransmit-interval
      - rib-priority
      - shutdown
      - sid-protection
      - transit-delay
    - loopfree-alternate-exclude
    - nssa
      - area-range
      - originate-default-route

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf area nssa redistribute-external

- redistribute-external
- summaries
- stub
  - default-metric
  - summaries
- virtual-link
  - auth-keychain
  - authentication-key
  - authentication-type
  - dead-interval
  - hello-interval
  - message-digest-key
  - retransmit-interval
  - shutdown
  - transit-delay
- asbr
- compatible-rfc1583
- database-export
- disable-ldp-sync
- entropy-label
  - override-tunnel-elc
- export
- export-limit
- external-db-overflow
- external-preference
- flexible-algorithms
  - flex-algo
    - advertise
    - loopfree-alternates
    - participate
  - shutdown
- graceful-restart
  - helper-disable
  - strict-lsa-checking
- igp-shortcut
  - shutdown
  - tunnel-next-hop
    - family
      - resolution
      - resolution-filter
        - rsvp
        - **sr-te**
      - sr-te
- import
- ldp-over-rsvp
- loopfree-alternate-exclude
- loopfree-alternates
  - augment-route-table
  - exclude
    - prefix-policy
  - multi-homed-prefix
    - preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf loopfree-alternates remote-lfa

- remote-lfa
  - node-protect
- ti-lfa
  - node-protect
- multi-instance
- multicast-import
- overload
- overload-include-ext-1
- overload-include-ext-2
- overload-include-stub
- overload-on-boot
- preference
- reference-bandwidth
- rib-priority
- router-id
- rtr-adv-lsa-limit
- segment-routing
  - adj-sid-hold
  - adjacency-set
    - parallel
    - sid
  - backup-node-sid
  - class-forwarding
  - egress-statistics
    - adj-set
    - adj-sid
    - node-sid
  - entropy-label
  - export-tunnel-table
  - ingress-statistics
    - adj-set
    - adj-sid
    - node-sid
  - mapping-server
    - shutdown
    - sid-map
  - maximum-sid-depth
    - override-bmi
    - override-erld
  - prefix-sid-range
  - shutdown
  - srlb
  - tunnel-mtu
  - tunnel-table-pref
- shutdown
- timers
  - incremental-spf-wait
  - lsa-accumulate
  - lsa-arrival
  - lsa-generate
  - redistribute-delay
  - spf-wait

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf traffic-engineering

- **traffic-engineering**
- **traffic-engineering-options**
  - **sr-te**
- **unicast-import-disable**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf3

3.4.37.56 configure router ospf3 Commands

- ospf3
  - advertise-router-capability
  - area
    - advertise-router-capability
    - area-range
    - blackhole-aggregate
    - database-export-exclude
    - export
    - extended-lsa
    - import
    - interface
      - advertise-router-capability
      - authentication
      - bfd-enable
      - dead-interval
      - hello-interval
      - interface-type
      - lfa-policy-map
      - load-balancing-weight
      - loopfree-alternate-exclude
      - lsa-filter-out
      - metric
      - mtu
      - neighbor
      - node-sid
      - passive
      - poll-interval
      - priority
      - retransmit-interval
      - rib-priority
      - shutdown
      - sid-protection
      - transit-delay
    - key-rollover-interval
    - loopfree-alternate-exclude
    - nssa
      - area-range
      - originate-default-route
      - redistribute-external
      - summaries
    - stub
      - default-metric
      - summaries
    - virtual-link
      - authentication
      - dead-interval
      - hello-interval
      - retransmit-interval
      - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf3 area virtual-link transit-delay

- transit-delay
- asbr
- database-export
- disable-ldp-sync
- export
- export-limit
- extended-lsa
- external-db-overflow
- external-preference
- graceful-restart
  - helper-disable
  - strict-lsa-checking
- igp-shortcut
  - shutdown
  - tunnel-next-hop
    - family
      - resolution
      - resolution-filter
        - rsvp
        - sr-te
      - sr-te
- import
- loopfree-alternate-exclude
- loopfree-alternates
  - exclude
    - prefix-policy
  - remote-lfa
    - node-protect
  - ti-lfa
    - node-protect
- multicast-import
- overload
- overload-include-ext-1
- overload-include-ext-2
- overload-include-stub
- overload-on-boot
- preference
- reference-bandwidth
- rib-priority
- router-id
- rtr-adv-lsa-limit
- segment-routing
  - adj-sid-hold
  - egress-statistics
    - adj-sid
    - node-sid
  - ingress-statistics
    - adj-sid
    - node-sid
  - prefix-sid-range
  - shutdown
  - tunnel-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf3 segment-routing tunnel-table-pref

- — tunnel-table-pref
- — shutdown
- — timers
  - — incremental-spf-wait
  - — lsa-accumulate
  - — lsa-arrival
  - — lsa-generate
  - — redistribute-delay
  - — spf-wait
- — unicast-import-disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.57 configure router p2mp-sr-tree Commands

- p2mp-sr-tree
  - bfd-enable
  - p2mp-policy
    - p2mp-candidate-path
      - active-instance
      - instances
        - instance
      - preference
      - shutdown
    - root-address
    - root-tree-id
    - shutdown
  - replication-segment
    - incoming-sid
    - instance-id
    - next-hop-id
      - next-hop-address
      - next-hop-interface-name
      - protecting-nexthop-id
      - replication-sid
      - shutdown
    - root-address
    - root-tree-id
    - shutdown
    - sid-action
  - reserved-lbl-block
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router pcep

3.4.37.58 configure router pcep Commands

- pcep
  - pcc
    - dead-timer
    - keepalive
    - local-address
    - max-srte-pce-init-lsps
    - peer
      - route-preference
      - shutdown
      - tls-client-profile
      - tls-wait-timer
    - redelegation-timer
    - report-path-constraints
    - shutdown
    - state-timer
    - unknown-message-rate
    - dead-timer
    - keepalive
    - local-address
    - shutdown
    - tls-server-profile
    - unknown-message-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.59 configure router pcp-server Commands

- pcp-server
  - server
    - description
    - dual-stack-lite-address
    - fwd-inside-router
    - interface
    - pcp-server-policy
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.60 configure router pim Commands

- pim
  - apply-to
  - enable-mdt-spt
  - gtm
  - gtm
    - auto-discovery
  - import
  - interface
    - assert-period
    - bfd-enable
    - bier-signaling
    - bsm-check-rtr-alert
    - hello-interval
    - hello-multiplier
    - improved-assert
    - instant-prune-echo
    - ipv4-multicast-disable
    - ipv6-multicast-disable
    - max-groups
    - mcac
      - if-policy
      - mc-constraints
        - level
        - number-down
        - shutdown
        - use-lag-port-weight
      - policy
      - unconstrained-bw
    - monitor-oper-group
    - multicast-senders
    - p2mp-ldp-tree-join
    - policy
    - priority
    - shutdown
    - sticky-dr
    - three-way-hello
    - tracking-support
  - ipv4-multicast-disable
  - ipv6-multicast-disable
  - lag-usage-optimization
  - mc-ecmp-balance
  - mc-ecmp-balance-hold
  - mc-ecmp-hashing-enabled
  - multicast-fast-failover
  - multicast6-fast-failover
  - non-dr-attract-traffic
  - pim-ssm-scaling
  - rp
    - anycast

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router pim rp anycast rp-set-peer

- rp-set-peer
- auto-rp-discovery
- bootstrap-export
- bootstrap-import
- bsr-candidate
  - address
  - hash-mask-len
  - priority
  - shutdown
- ipv6
  - anycast
    - rp-set-peer
  - bsr-candidate
    - address
    - hash-mask-len
    - priority
    - shutdown
  - embedded-rp
    - group-range
    - shutdown
  - rp-candidate
    - address
    - group-range
    - holdtime
    - priority
    - shutdown
  - static
    - address
      - group-prefix
      - override
- rp-candidate
  - address
  - group-range
  - holdtime
  - priority
  - shutdown
- static
  - address
    - group-prefix
    - override
- rpf-table
- rpf6-table
- rpfv
- shutdown
- spt-switchover-threshold
- ssm-assert-compatible-mode
- ssm-default-range-disable
- ssm-groups
  - group-range
- tunnel-interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.61 configure router policy-acct-template Commands

- policy-acct-template
  - destination-class
    - policer
  - policer
    - max-burst-size
    - peak-rate
  - source-class

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.62 configure router policy-options Commands

- policy-options
  - abort
  - as-path
    - expression
  - as-path-group
    - entry
  - begin
  - commit
  - community
    - expression
    - members
  - damping
    - half-life
    - max-suppress
    - reuse
    - suppress
  - exclusive-lock-time
  - global-variables
    - name
  - policy-statement
    - default-action
      - add-paths-send-limit
      - admin-tag-policy
      - advertise-label
      - aigp-metric
      - as-path
      - as-path-prepend
      - bgp-high-priority
      - bgp-leak
      - bgp-med
      - bgp-tunnel-metric
      - community
      - create-mpls-tunnel
      - create-udp-tunnel
      - damping
      - dest-class
      - disable-route-table-install
      - egress-statistics
      - flex-algo
      - ingress-statistics
      - install-backup-path
      - local-preference
      - metric
      - multicast-redirection
      - nat-policy
      - next-hop
      - next-hop-self
      - origin
      - origin-validation-state

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router policy-options policy-statement default-action preference

- preference
- resolve-static
- source-class
- sr-label-index
- sr-maintenance-policy
- sticky-ecmp
- tag
- type

- description
- entry
  - action
    - add-paths-send-limit
    - admin-tag-policy
    - advertise-label
    - aigp-metric
    - as-path
    - as-path-prepend
    - bgp-high-priority
    - bgp-leak
    - bgp-med
    - bgp-tunnel-metric
    - community
    - create-mpls-tunnel
    - create-udp-tunnel
    - damping
    - dest-class
    - disable-route-table-install
    - egress-statistics
    - fc
    - flex-algo
    - ingress-statistics
    - install-backup-path
    - local-preference
    - metric
    - multicast-redirection
    - nat-policy
    - next-hop
    - next-hop-self
    - origin
    - origin-validation-state
    - policy
    - preference
    - resolve-static
    - source-class
    - sr-label-index
    - sr-maintenance-policy
    - sticky-ecmp
    - tag
    - type
  - add-paths-send-limit
  - conditional-expression
    - route-exists

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router policy-options policy-statement entry description

- description
- dest-class
- from
  - aggregate-contributor
    - aggregate-contributor
  - area
  - as-path
  - as-path-group
  - as-path-length
  - cluster-id
  - color
  - community
  - community-count
  - distinguisher
  - endpoint
  - evpn-type
  - external
  - family
  - flow-spec-dest
  - flow-spec-source
  - group-address
  - host-ip
  - interface
  - interface-subnets
  - level
  - local-preference
  - metric
  - mvpn-type
  - neighbor
  - next-hop
  - origin
  - origin-validation-state
  - path-type
  - policy
  - policy-variables
    - name
  - prefix-list
  - protocol
  - source-address
  - state
  - tag
  - type
- local-preference
- to
  - level
  - neighbor
  - prefix-list
  - protocol
  - preference
- renumber
- prefix-list
  - prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.63 configure router policy-reference-checks Commands

— **policy-reference-checks**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.64 configure router radius-proxy Commands

- radius-proxy
  - shutdown
  - server
    - attribute-matching
      - entry
      - type
    - cache
      - key
      - shutdown
      - timeout
      - track-accounting
      - track-authentication
      - track-delete-hold-time
    - default-accounting-server-policy
    - default-authentication-server-policy
    - description
    - interface
    - load-balance-key
    - python-policy
    - secret
    - send-accounting-response
    - shutdown
    - wlan-gw
      - address
      - ipv6-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.65 configure router radius-server Commands

— radius-server
  — server
    — accept-coa
    — acct-port
    — auth-port
    — coa-script-policy
    — description
    — pending-requests-limit
    — python-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.66 configure router reassembly-group Commands

— **reassembly-group**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.67 configure router rib-api Commands

- rib-api
  - mpls
    - reserved-label-block
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.68 configure router rip Commands

- rip
  - authentication-key
  - authentication-type
  - bfd-enable
  - check-zero
  - description
  - export
  - export-limit
  - group
    - authentication-key
    - authentication-type
    - bfd-enable
    - check-zero
    - description
    - export
    - import
    - message-size
    - metric-in
    - metric-out
    - neighbor
      - authentication-key
      - authentication-type
      - bfd-enable
      - check-zero
      - description
      - export
      - import
      - message-size
      - metric-in
      - metric-out
      - preference
      - receive
      - send
      - shutdown
      - split-horizon
      - timers
      - unicast-address
    - preference
    - receive
    - send
    - shutdown
    - split-horizon
    - timers
  - import
  - message-size
  - metric-in
  - metric-out
  - preference
  - receive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router rip send

- **send**
- **shutdown**
- **split-horizon**
- **timers**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.69 configure router ripng Commands

- ripng
  - bfd-enable
  - check-zero
  - description
  - export
  - export-limit
  - group
    - bfd-enable
    - check-zero
    - description
    - export
    - import
    - message-size
    - metric-in
    - metric-out
    - neighbor
      - bfd-enable
      - check-zero
      - description
      - export
      - import
      - message-size
      - metric-in
      - metric-out
      - preference
      - receive
      - send
      - shutdown
      - split-horizon
      - timers
      - unicast-address
    - preference
    - receive
    - send
    - shutdown
    - split-horizon
    - timers
  - import
  - message-size
  - metric-in
  - metric-out
  - preference
  - receive
  - send
  - shutdown
  - split-horizon
  - timers

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.70 configure router route-next-hop-policy Commands

- route-next-hop-policy
  - abort
  - begin
  - commit
  - template
    - description
    - exclude-group
    - include-group
    - nh-type
    - protection-type
    - srlg-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.71 configure router router-advertisement Commands

- router-advertisement
  - dns-options
    - rdnss-lifetime
    - server
  - interface
    - current-hop-limit
    - dns-options
      - include-dns
      - rdnss-lifetime
      - server
    - managed-configuration
    - max-advertisement-interval
    - min-advertisement-interval
    - mtu
    - other-stateful-configuration
    - prefix
      - autonomous
      - on-link
      - preferred-lifetime
      - valid-lifetime
    - reachable-time
    - retransmit-time
    - router-lifetime
    - shutdown
    - use-virtual-mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.72 configure router router-id Commands

— router-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.73 configure router rsvp Commands

- rsvp
  - dbw-accounting
    - dbw-multiplier
    - down-threshold
    - sample-interval
    - sample-multiplier
    - up-threshold
  - diffserv-te
    - class-type-bw
    - fc
    - te-class
  - entropy-label-capability
  - gr-helper-time
  - graceful-shutdown
  - implicit-null-label
  - interface
    - auth-keychain
    - authentication-key
    - bfd-enable
    - class-type-bw
    - dbw-down-threshold
    - dbw-multiplier
    - dbw-up-threshold
    - gr-helper
    - graceful-shutdown
    - hello-interval
    - implicit-null-label
    - refresh-reduction
      - reliable-delivery
    - shutdown
    - subscription
    - te-down-threshold
    - te-up-threshold
  - keep-multiplier
  - msg-pacing
    - max-burst
    - period
  - node-id-in-rro
  - p2mp-merge-point-abort-timer
  - p2mp-s2l-fast-retry
  - p2p-merge-point-abort-timer
  - preemption-timer
  - rapid-retransmit-time
  - rapid-retry-limit
  - refresh-reduction-over-bypass
  - refresh-time
  - shutdown
  - te-down-threshold
  - te-threshold-update

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router rsvp te-threshold-update on-cac-failure

- on-cac-failure
- update-timer
- te-up-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.74 configure router segment-routing Commands

- segment-routing
  - maintenance-policy
    - bfd-enable
    - bfd-template
    - hold-down-timer
    - mode
    - revert-timer
    - shutdown
    - threshold
  - segment-routing-v6
    - base-routing-instance
      - locator
        - function
          - end
            - srh-mode
          - end-dt4
          - end-dt46
          - end-dt6
          - end-x
            - interface
            - protection
            - srh-mode
          - end-x-auto-allocate
    - locator
      - algorithm
      - block-length
      - function-length
      - prefix
        - ip-prefix
      - shutdown
      - static-function
        - label-block
        - max-entries
      - termination-fpe
    - origination-fpe
    - source-address
  - sr-mpls
    - prefix-sids
      - ipv4-sid
      - ipv6-sid
      - node-sid
  - sr-policies
    - egress-statistics
      - shutdown
    - ingress-statistics
      - shutdown
    - reserved-label-block
    - segment-list
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router segment-routing sr-policies static-policy

- static-policy
  - binding-sid
  - color
  - distinguisher
  - endpoint
  - head-end
  - maintenance-policy
  - preference
  - segment-list
    - segment
      - mpls-label
    - shutdown
    - weight
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router sgt-qos

3.4.37.75 configure router sgt-qos Commands

- sgt-qos
  - application
    - grpc
      - dscp
  - dscp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.76 configure router shutdown Commands

— **shutdown**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.77 configure router single-sfm-overload Commands

— **single-sfm-overload**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router static-route-entry

3.4.37.78 configure router static-route-entry Commands

- static-route-entry
  - backup-tag
  - black-hole
    - community
    - description
    - dynamic-bgp
    - generate-icmp
    - metric
    - preference
    - prefix-list
    - shutdown
    - tag
  - community
  - indirect
    - community
    - cpe-check
      - drop-count
      - interval
      - log
      - padding-size
    - description
    - destination-class
    - forwarding-class
      - priority
    - metric
    - preference
    - prefix-list
    - shutdown
    - source-class
    - tag
    - tunnel-next-hop
      - disallow-igp
      - flex-algo
      - resolution
      - resolution-filter
        - ldp
        - mpls-fwd-policy
        - rib-api
        - rsvp-te
          - lsp
        - sr-isis
        - sr-ospf
        - sr-ospf3
        - sr-te
          - lsp
  - ipsec-tunnel
    - community
    - description
    - metric

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router static-route-entry ipsec-tunnel preference

- **preference**
- **shutdown**
- **tag**
- next-hop
  - backup-next-hop
    - address
  - bfd-enable
  - community
  - cpe-check
    - drop-count
    - interval
    - log
    - padding-size
  - description
  - destination-class
  - forwarding-class
    - priority
  - ldp-sync
  - load-balancing-weight
  - metric
  - preference
  - prefix-list
  - shutdown
  - source-class
  - tag
  - validate-next-hop
- tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router static-route-hold-down

3.4.37.79 configure router static-route-hold-down Commands

— **static-route-hold-down**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.80 configure router triggered-policy Commands

— **triggered-policy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.81 configure router ttl-propagate Commands

- ttl-propagate
  - label-route-local
  - label-route-transit
  - lsr-label-route
  - vprn-local
  - vprn-transit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.82 configure router tunnel-interface Commands

— **tunnel-interface**
  — **description**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.83 configure router twamp-light Commands

- twamp-light
  - reflector
    - allow-ipv6-udp-checksum-zero
    - description
    - prefix
      - description
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.84 configure router vrgw Commands

- vrgw
  - lanext
    - description
    - shutdown
    - vxlan-port
    - vxlan-vtep-range
    - wlan-gw-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.85 configure router weighted-ecmp Commands

— weighted-ecmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.86 configure router wlan-gw Commands

- wlan-gw
  - distributed-sub-mgmt
    - ipv6-tcp-mss-adjust
  - mobility-triggered-acct
    - interim-update
  - xconnect
    - shutdown
    - tunnel-source-ip
    - wlan-gw-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.37.87 configure router wpp Commands

- wpp
  - initial-sla-profile
  - portals
    - portal
      - ack-auth-retry-count
      - ntf-logout-retry-count
      - port-format
      - retry-interval
      - secret
      - shutdown
      - version
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.38 configure saa Commands

- saa
  - test
    - accounting-policy
    - continuous
    - description
    - jitter-event
    - latency-event
    - loss-event
    - probe-history
    - shutdown
    - trap-gen
      - probe-fail-enable
      - probe-fail-threshold
      - test-completion-enable
      - test-fail-enable
      - test-fail-threshold
    - type
      - cpe-ping
      - dns
      - eth-cfm-linktrace
      - eth-cfm-loopback
      - eth-cfm-two-way-delay
      - eth-cfm-two-way-slm
      - icmp-ping
      - icmp-trace
      - lsp-ping
      - lsp-trace
      - mac-ping
      - mac-trace
      - sdp-ping
      - vccv-ping
      - vccv-trace
      - vprn-ping
      - vprn-trace
    - type-multi-line
      - lsp-ping
        - sr-policy
          - fc
          - interval
          - path-destination
          - profile
          - segment-list
          - send-count
          - size
          - src-ip-address
          - timeout
          - ttl
      - lsp-trace
        - sr-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure saa test type-multi-line lsp-trace sr-policy downstream-map-tlv

- **downstream-map-tlv**
- **fc**
- **interval**
- **max-fail**
- **path-destination**
- **probe-count**
- **profile**
- **segment-list**
- **size**
- **src-ip-address**
- **timeout**
- **ttl**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39 configure service Commands

— service

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.1 configure service apipe Commands

- apipe
  - description
  - endpoint
    - active-hold-delay
    - description
    - revert-time
  - interworking
  - sap
    - accounting-policy
    - atm
      - egress
        - traffic-desc
      - ingress
        - traffic-desc
      - llf
      - oam
        - alarm-cells
        - terminate
    - bandwidth
    - collect-stats
    - description
    - dist-cpu-protection
    - egress
      - agg-rate
        - limit-unused-bandwidth
        - rate
      - policer-control-override
        - max-rate
        - priority-mbs-thresholds
          - min-thresh-separation
          - priority
            - mbs-contribution
      - policer-control-policy
      - policer-override
        - policer
          - cbs
          - mbs
          - packet-byte-offset
          - percent-rate
          - rate
          - stat-mode
      - qinq-mark-top-only
      - qos
      - queue-override
        - queue
          - adaptation-rule
          - avg-frame-overhead
          - burst-limit
          - cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service apipe sap egress queue-override queue drop-tail

- drop-tail
  - low
    - percent-reduction-from-mbs
  - mbs
  - monitor-queue-depth
  - parent
  - percent-rate
  - rate
- scheduler-override
  - scheduler
    - parent
    - rate
  - scheduler-policy
- frame-relay
  - scheduling-class
- ingress
  - criteria-overrides
    - ip-criteria
      - activate-entry-tag
    - ipv6-criteria
      - activate-entry-tag
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qos
  - queue-override
    - queue
      - adaptation-rule
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs
      - monitor-queue-depth
      - parent
      - percent-rate
      - rate
  - scheduler-override
    - scheduler
      - parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service apipe sap ingress scheduler-override scheduler rate

- rate
- scheduler-policy
- multi-service-site
- shutdown
- service-mtu
- shutdown
- signaled-vc-type-override
- spoke-sdp
  - bandwidth
  - bfd
    - bfd-enable
    - bfd-template
  - cell-concatenation
    - aal5-frame-aware
    - clp-change
    - max-cells
    - max-delay
  - control-channel-status
    - acknowledgment
    - refresh-timer
    - request-timer
    - shutdown
  - control-word
  - description
  - egress
    - qos
    - vc-label
  - ingress
    - qos
    - vc-label
  - precedence
  - pw-path-id
    - agi
    - saii-type2
    - taii-type2
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.2 configure service cpipe Commands

- cpipe
  - description
  - endpoint
    - active-hold-delay
    - description
    - revert-time
  - sap
    - accounting-policy
    - cem
      - packet
      - report-alarm
      - rtp-header
    - collect-stats
    - description
    - dist-cpu-protection
    - egress
      - agg-rate
        - limit-unused-bandwidth
        - rate
      - policer-control-override
        - max-rate
        - priority-mbs-thresholds
          - min-thresh-separation
          - priority
            - mbs-contribution
      - policer-control-policy
      - policer-override
        - policer
          - cbs
          - mbs
          - packet-byte-offset
          - percent-rate
          - rate
          - stat-mode
      - qos
      - queue-override
        - queue
          - adaptation-rule
          - avg-frame-overhead
          - burst-limit
          - cbs
          - drop-tail
            - low
              - percent-reduction-from-mbs
          - mbs
          - monitor-queue-depth
          - parent
          - percent-rate
          - rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service cpipe sap egress scheduler-override

- scheduler-override
  - scheduler
    - parent
    - rate
  - scheduler-policy
- ingress
  - criteria-overrides
    - ip-criteria
      - activate-entry-tag
    - ipv6-criteria
      - activate-entry-tag
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qos
  - queue-override
    - queue
      - adaptation-rule
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs
      - monitor-queue-depth
      - parent
      - percent-rate
      - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
- multi-service-site
- shutdown
- service-mtu
- shutdown
- spoke-sdp
  - bandwidth
  - bfd
    - bfd-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service cpipe spoke-sdp bfd bfd-template

- bfd-template
- control-channel-status
  - acknowledgment
  - refresh-timer
  - request-timer
  - shutdown
- control-word
- description
- egress
  - filter
  - qos
  - vc-label
- ingress
  - filter
  - qos
  - vc-label
- precedence
- pw-path-id
  - agi
  - saii-type2
  - taii-type2
- shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.3 configure service customer Commands

- customer
  - contact
  - description
  - multi-service-site
    - assignment
    - description
    - egress
      - agg-rate
        - limit-unused-bandwidth
        - queue-frame-based-accounting
        - rate
      - policer-control-policy
      - scheduler-override
        - scheduler
          - parent
          - rate
      - scheduler-policy
    - ingress
      - policer-control-policy
      - scheduler-override
        - scheduler
          - parent
          - rate
      - scheduler-policy
  - phone

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.4 configure service dynamic-services Commands

- dynamic-services
  - dynamic-services-policy
    - accounting-1
    - stats-type
      - server-policy
      - **stats-type**
      - update-interval
      - update-interval-jitter
    - accounting-2
      - server-policy
      - stats-type
      - update-interval
      - update-interval-jitter
    - authentication
      - local-auth-db
      - password
      - server-policy
    - cli-user
    - description
    - sap-limit
    - script-policy
  - local-auth-db
    - description
    - shutdown
    - user-name
      - description
      - index
        - accounting
          - stats-type
          - update-interval
        - dynamic-services-policy
        - sap-id
        - script-parameters-1
        - script-parameters-2
        - script-parameters-3
        - script-parameters-4
      - shutdown
  - service-range
  - timers
    - setup-timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.5 configure service epipe Commands

- epipe
  - bgp
    - adv-service-mtu
    - pw-template-binding
      - bfd-enable
      - bfd-template
    - route-distinguisher
    - route-target
    - vsi-export
    - vsi-import
  - bgp-evpn
    - evi
    - local-attachment-circuit
      - eth-tag
    - mpls
      - auto-bind-tunnel
        - allow-flex-algo-fallback
        - ecmp
        - enforce-strict-tunnel-tagging
        - resolution
        - resolution-filter
          - bgp
          - ldp
          - mpls-fwd-policy
          - rib-api
          - rsvp
          - sr-isis
          - sr-ospf
          - sr-ospf3
          - sr-policy
          - sr-te
          - udp
      - control-word
      - default-route-tag
      - dynamic-egress-label-limit
      - ecmp
      - entropy-label
      - evi-three-byte-auto-rt
      - force-qinq-vc-forwarding
      - force-vlan-vc-forwarding
      - oper-group
      - route-next-hop
      - send-tunnel-encap
      - shutdown
    - remote-attachment-circuit
      - eth-tag
    - segment-routing-v6
      - default-route-tag
      - ecmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe bgp-evpn segment-routing-v6 evi-three-byte-auto-rt

- evi-three-byte-auto-rt
- force-vlan-vc-forwarding
- oper-group
- route-next-hop
- shutdown
- source-address
- vxlan
  - default-route-tag
  - ecmp
  - evi-three-byte-auto-rt
  - send-tunnel-encap
  - shutdown
- bgp-vpws
  - remote-ve-name
    - ve-id
  - shutdown
  - ve-name
    - ve-id
- description
- endpoint
  - active-hold-delay
  - description
  - revert-time
  - standby-signaling-master
  - standby-signaling-slave
- eth-cfm
  - tunnel-fault
- ignore-l2vpn-mtu-mismatch
- load-balancing
  - lbl-eth-or-ip-l4-teid
  - per-service-hashing
- nat-outside
  - shutdown
- oper-group
- **pbb**
  - force-qtag-forwarding
  - local-switching-service-state
  - tunnel
- pw-port
- pw-port
  - down-on-peer-tldp-pw-status-faults
  - egress
    - shaper
      - int-dest-id
      - vport
  - monitor-oper-group
  - oper-up-on-mhstandby
  - shutdown
- sap
  - aarp
  - accounting-policy
  - app-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe sap atm

- atm
  - egress
    - traffic-desc
  - encapsulation
  - ingress
    - traffic-desc
  - oam
    - alarm-cells
- bandwidth
- cem
  - local-ecid
  - packet
  - remote-ecid
  - remote-mac
  - report-alarm
  - rtp-header
- cflowd
- collect-stats
- cpu-protection
- description
- dist-cpu-protection
- egress
  - agg-rate
    - limit-unused-bandwidth
    - queue-frame-based-accounting
    - rate
  - filter
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qinq-mark-top-only
  - qos
  - queue-override
    - hs-secondary-shaper
    - hs-wrr-group
      - class-weight
      - percent-rate
      - rate
    - queue
      - adaptation-rule

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe sap egress queue-override queue avg-frame-overhead

- avg-frame-overhead
- burst-limit
- cbs
- drop-tail
  - low
    - percent-reduction-from-mbs
- hs-class-weight
- hs-wred-queue
- hs-wrr-weight
- mbs
- monitor-queue-depth
- parent
- percent-rate
- rate

- scheduler-override
  - scheduler
    - parent
    - rate
  - scheduler-policy

- eth-cfm
  - ais-enable
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - client-meg-level
      - interface-support-enable
      - interval
      - low-priority-defect
      - priority
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - cfm-vlan-tag
    - client-meg-level
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe sap eth-cfm mep grace eth-ed tx-eth-ed

- tx-eth-ed
- eth-vsm-grace
  - rx-eth-vsm-grace
  - tx-eth-vsm-grace
- lbm-svc-act-responder
- low-priority-defect
- mac-address
- one-way-delay-threshold
- priority
- shutdown
- mip
- squelch-ingress-ctag-levels
- squelch-ingress-levels
- tunnel-fault

- eth-tunnel
  - path
- ethernet
  - llf
- frame-relay
  - frf-12
    - ete-fragment-threshold
    - interleave
    - interleave
  - scheduling-class
- ignore-oper-down
- ingress
  - criteria-overrides
    - ip-criteria
      - activate-entry-tag
    - ipv6-criteria
      - activate-entry-tag
  - filter
  - match-qinq-dot1p
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qinq-vlan-translation
  - qos
  - queue-override
    - queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe sap ingress queue-override queue adaptation-rule

- adaptation-rule
- cbs
- drop-tail
  - low
    - percent-reduction-from-mbs
- mbs
- monitor-queue-depth
- parent
- percent-rate
- rate

- scheduler-override
  - scheduler
    - parent
    - rate
- scheduler-policy
- vlan-translation

- l2tpv3-session
  - pw-type
  - router
  - shutdown
  - vc-id
- lag-link-map-profile
- lag-per-link-hash
- monitor-oper-group
- multi-service-site
- oper-group
- ring-node
- shutdown
- transit-policy

- segment-routing-v6
  - locator
    - function
      - end-dx2
- service-mtu
- shutdown
- site
  - boot-timer
  - sap
  - shutdown
  - site-activation-timer
  - site-id
  - site-min-down-timer
  - site-preference
- spoke-sdp
  - aarp
  - accounting-policy
  - adv-service-mtu
  - app-profile
  - bandwidth
  - bfd
    - bfd-enable
    - bfd-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe spoke-sdp bfd failure-action

- failure-action
- wait-for-up-timer
- block-on-peer-fault
- collect-stats
- control-channel-status
  - acknowledgment
  - refresh-timer
  - request-timer
  - shutdown
- control-word
- cpu-protection
- description
- egress
  - filter
  - l2tpv3
    - cookie
  - qos
  - vc-label
- entropy-label
- eth-cfm
    - priority
    - client-meg-level
    - interval
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - client-meg-level
      - interface-support-enable
      - interval
      - low-priority-defect
      - priority
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - cfm-vlan-tag
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed

- rx-eth-ed
- tx-eth-ed
- eth-vsm-grace
- rx-eth-vsm-grace
- tx-eth-vsm-grace
- lbm-svc-act-responder
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown
- mip
- squelch-ingress-ctag-levels
- squelch-ingress-levels
- force-qinq-vc-forwarding
- force-vlan-vc-forwarding
- hash-label
- ingress
- filter
- l2tpv3
- cookie
- qos
- vc-label
- monitor-oper-group
- oper-group
- precedence
- pw-path-id
- agi
- saii-type2
- taii-type2
- pw-status-signaling
- shutdown
- standby-signaling-slave
- transit-policy
- use-sdp-bmac
- vlan-vc-tag
- spoke-sdp-fec
- auto-config
- path
- precedence
- pw-template-bind
- retry-count
- retry-timer
- saii-type2
- shutdown
- signaling
- standby-signaling-slave
- taii-type2
- vxlan
- egr-vtep
- oper-group
- vxlan-src-vtep

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.6 configure service fpipe Commands

- fpipe
  - description
  - endpoint
    - active-hold-delay
    - description
    - revert-time
  - sap
    - accounting-policy
    - bandwidth
    - collect-stats
    - description
    - dist-cpu-protection
    - egress
      - agg-rate
        - limit-unused-bandwidth
        - rate
      - filter
      - policer-control-override
        - max-rate
        - priority-mbs-thresholds
          - min-thresh-separation
          - priority
            - mbs-contribution
      - policer-control-policy
      - policer-override
        - policer
          - cbs
          - mbs
          - packet-byte-offset
          - percent-rate
          - rate
          - stat-mode
      - qinq-mark-top-only
      - qos
      - queue-override
        - queue
          - adaptation-rule
          - avg-frame-overhead
          - burst-limit
          - cbs
          - drop-tail
            - low
              - percent-reduction-from-mbs
          - mbs
          - monitor-queue-depth
          - parent
          - percent-rate
          - rate
      - scheduler-override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service fpipe sap egress scheduler-override scheduler

- scheduler
  - parent
  - rate
- scheduler-policy
- frame-relay
- scheduling-class
- ingress
- criteria-overrides
- ip-criteria
  - activate-entry-tag
- ipv6-criteria
  - activate-entry-tag
- filter
- policer-control-override
- max-rate
- priority-mbs-thresholds
  - min-thresh-separation
  - priority
    - mbs-contribution
- policer-control-policy
- policer-override
- policer
  - cbs
  - mbs
  - packet-byte-offset
  - percent-rate
  - rate
  - stat-mode
- qos
- queue-override
- queue
  - adaptation-rule
  - cbs
  - drop-tail
    - low
      - percent-reduction-from-mbs
  - mbs
  - monitor-queue-depth
  - parent
  - percent-rate
  - rate
- scheduler-override
- scheduler
  - parent
  - rate
- scheduler-policy
- multi-service-site
- shutdown
- service-mtu
- shutdown
- spoke-sdp
- bandwidth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service fpipe spoke-sdp bfd

- **bfd**
  - **bfd-enable**
  - **bfd-template**
- **control-word**
- **description**
- **egress**
  - **filter**
  - **qos**
  - **vc-label**
- **entropy-label**
- **hash-label**
- **ingress**
  - **filter**
  - **qos**
  - **vc-label**
- **precedence**
- **shutdown**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.7 configure service ies Commands

- ies
  - aa-interface
    - address
    - description
    - ip-mtu
    - sap
      - description
      - egress
        - filter
        - qos
      - ingress
        - qos
      - shutdown
    - shutdown
  - aarp-interface
    - description
    - ip-mtu
    - shutdown
    - spoke-sdp
      - aarp
      - description
      - egress
        - filter
        - vc-label
      - ingress
        - filter
        - vc-label
      - shutdown
  - description
  - eth-cfm
    - tunnel-fault
  - igmp-host-tracking
    - expiry-time
    - shutdown
      - propagate-pmtu-v4
  - interface
    - address
    - allow-directed-broadcasts
    - arp-host-route
      - populate
    - arp-learn-unsolicited
    - arp-limit
    - arp-populate
    - arp-populate-host-route
    - arp-proactive-refresh
    - arp-retry-timer
    - arp-route-tag
    - arp-timeout
    - authentication-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface bfd

- bfd
- cflowd-parameters
  - sampling
- cpu-protection
- description
- dhcp
  - description
  - gi-address
  - lease-populate
  - option
    - action
    - circuit-id
    - remote-id
    - vendor-specific-option
      - client-mac-address
      - pool-name
      - sap-id
      - service-id
      - string
      - system-id
  - proxy-server
    - emulated-server
    - lease-time
    - shutdown
  - python-policy
  - relay-plain-bootp
  - relay-proxy
  - release-include-gi-address
  - server
  - shutdown
  - trusted
  - use-arp
- dhcp6
- dynamic-tunnel-redundant-next-hop
- enable-ingress-stats
- enable-mac-accounting
- hold-time
  - down
  - up
- host-connectivity-verify
- icmp
  - mask-reply
  - param-problem
  - redirects
  - ttl-expired
  - unreachables
- if-attribute
  - admin-group
  - srlg-group
- ignore-default
- ingress
  - destination-class-lookup

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface ingress policy-accounting

- policy-accounting
- ip-helper-address
- ip-mtu
- ipcp
  - dns
  - peer-ip-address
- ipsec
  - ip-exception
  - ipsec-tunnel
    - bfd-designate
    - bfd-enable
    - clear-df-bit
    - copy-traffic-class-upon-decapsulation
    - description
    - dynamic-keying
      - auto-establish
      - cert
        - cert-profile
        - status-verify
          - default-result
          - primary
        - trust-anchor-profile
      - ike-policy
      - local-id
      - pre-shared-key
      - transform
    - encapsulated-ip-mtu
    - icmp-generation
      - frag-required
        - interval
        - message-count
    - icmp6-generation
      - pkt-too-big
        - interval
        - interval
        - message-count
    - ip-mtu
    - local-gateway-address
    - manual-keying
      - security-association
    - max-history-esp-key-records
    - max-history-ike-key-records
    - pmtu-discovery-aging
    - private-tcp-mss-adjust
    - propagate-pmtu-v4
    - propagate-pmtu-v6
    - public-tcp-mss-adjust
    - remote-gateway-address
    - replay-window
    - security-policy
    - shutdown
  - ipv6-exception

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface ipsec shutdown

- shutdown
- ipv6
  - address
  - bfd
  - dad-disable
    - lease-populate
    - server
  - dhcp6-relay
    - description
    - lease-populate
    - link-address
    - neighbor-resolution
    - option
      - interface-id
      - remote-id
    - python-policy
    - server
    - shutdown
    - source-address
    - user-db
  - dhcp6-server
    - max-nbr-of-leases
    - prefix-delegation
      - prefix
        - duid
        - preferred-lifetime
        - valid-lifetime
      - shutdown
  - forward-ipv4-packets
  - icmp6
    - packet-too-big
    - param-problem
    - redirects
    - time-exceeded
    - unreachables
  - ignore-default
  - link-local-address
  - local-dhcp-server
  - local-proxy-nd
  - nd-host-route
    - populate
  - nd-learn-unsolicited
  - nd-populate-host-route
  - nd-proactive-refresh
  - nd-route-tag
  - neighbor
  - neighbor-limit
  - proxy-nd-policy
  - qos-route-lookup
  - reachable-time
  - secure-nd
    - allow-unsecured-msgs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface ipv6 secure-nd link-local-modifier

- link-local-modifier
- public-key-min-bits
- security-parameter
- shutdown
- stale-time
- tcp-mss
- urpf-check
  - ignore-default
  - mode
- vrrp
  - backup
  - bfd-enable
  - init-delay
  - mac
  - master-int-inherit
  - message-interval
  - ntp-reply
  - oper-group
  - ping-reply
  - policy
  - preempt
  - priority
  - shutdown
  - standby-forwarding
  - telnet-reply
  - traceroute-reply
- load-balancing
  - egr-ip-load-balancing
  - flow-label-load-balancing
  - spi-load-balancing
  - teid-load-balancing
- local-dhcp-server
- local-proxy-arp
- loopback
- mac
- monitor-oper-group
- multicast-network-domain
- ping-template
  - destination-address
  - shutdown
- proxy-arp-policy
- ptp-hw-assist
- qos-route-lookup
- remote-proxy-arp
- sap
  - aarp
  - accounting-policy
  - anti-spoof
  - app-profile
  - atm
    - egress
      - traffic-desc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap atm encapsulation

- encapsulation
- ingress
  - traffic-desc
- oam
  - alarm-cells
  - periodic-loopback
- bandwidth
- calling-station-id
- collect-stats
- cpu-protection
- description
- dist-cpu-protection
- egress
  - agg-rate
    - limit-unused-bandwidth
    - queue-frame-based-accounting
    - rate
  - filter
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qinq-mark-top-only
  - qos
  - queue-group-redirect-list
  - queue-override
    - hs-secondary-shaper
    - hs-wrr-group
      - class-weight
      - percent-rate
      - rate
    - queue
      - adaptation-rule
      - avg-frame-overhead
      - burst-limit
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - hs-class-weight
      - hs-wred-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap egress queue-override queue hs-wrr-weight

- hs-wrr-weight
- mbs
- monitor-queue-depth
- parent
- percent-rate
- rate
- scheduler-override
  - scheduler
    - parent
    - rate
  - scheduler-policy
- eth-cfm
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - interface-support-enable
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed
        - tx-eth-ed
      - eth-vsm-grace
        - rx-eth-vsm-grace
        - tx-eth-vsm-grace
    - low-priority-defect
    - mac-address
    - one-way-delay-threshold
    - shutdown
  - shutdown
  - squelch-ingress-levels
  - tunnel-fault
- frame-relay
  - frf-12
    - ete-fragment-threshold
    - interleave

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap frame-relay scheduling-class

- scheduling-class
- fwd-wholesale
  - pppoe
  - reassembly
- host-lockout-policy
- host-shutdown
- ingress
  - criteria-overrides
    - ip-criteria
      - activate-entry-tag
    - ipv6-criteria
      - activate-entry-tag
  - filter
  - flowspec
  - match-qinq-dot1p
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qos
  - queue-group-redirect-list
  - queue-override
    - queue
      - adaptation-rule
      - avg-frame-overhead
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs
      - monitor-queue-depth
      - parent
      - percent-rate
      - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
- ip-tunnel
  - backup-remote-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap ip-tunnel clear-df-bit

- clear-df-bit
- delivery-service
- description
- dest-ip
- dscp
- encapsulated-ip-mtu
- gre-header
- icmp-generation
  - frag-required
    - interval
    - message-count
- icmp6-generation
  - packet-too-big
- ip-mtu
- ipsec-transport-mode-profile
- pmtu-discovery-aging
- private-tcp-mss-adjust
- propagate-pmtu-v4
- propagate-pmtu-v4
- propagate-pmtu-v6
- public-tcp-mss-adjust
- reassembly
- remote-ip
- shutdown
- source
- default-secure-service
- default-tunnel-template
- dhcp
- dhcp6

- ipsec-gw
  - cert
    - cert-profile
    - status-verify
      - default-result
      - primary
    - trust-anchor-profile
  - client-db
  - default-secure-service
  - default-tunnel-template
  - dhcp
    - gi-address
    - send-release
    - server
    - shutdown
  - dhcp6
    - link-address
    - send-release
    - server
    - shutdown
  - ike-policy
  - local-address-assignment
    - ipv4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap ipsec-gw local-address-assignment ipv4 address-source

- address-source
- ipv6
  - address-source
- shutdown
- local-gateway-address
- local-id
- max-history-esp-key-records
- max-history-ike-key-records
- pre-shared-key
- radius-accounting-policy
- radius-authentication-policy
- shutdown
- transform
- ts-negotiation
- l2tpv3-session
  - pw-type
  - router
  - shutdown
  - vc-id
- lag-link-map-profile
- lag-per-link-hash
  - one-way-delay-threshold
- multi-service-site
- shutdown
- static-host
  - ancp-string
  - app-profile
  - inter-dest-id
  - shutdown
  - sla-profile
  - sub-profile
  - subscriber
  - subscriber-sap-id
- sub-sla-mgmt
  - def-sub-profile
    - profiled-traffic-only
  - single-sub-parameters
- transit-policy
- secondary
- shcv-policy-ipv4
- shcv-policy-ipv6
- shutdown
- spoke-sdp
  - aarp
  - accounting-policy
  - app-profile
  - bfd
    - bfd-enable
    - bfd-template
    - failure-action
    - wait-for-up-timer
  - collect-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface spoke-sdp control-channel-status

- control-channel-status
  - acknowledgment
  - refresh-timer
  - request-timer
  - shutdown
- control-word
- cpu-protection
- description
- egress
  - filter
  - qos
  - vc-label
- entropy-label
- eth-cfm
  - ais-enable
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - interface-support-enable
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed
        - tx-eth-ed
      - eth-vsm-grace
        - rx-eth-vsm-grace
        - tx-eth-vsm-grace
    - low-priority-defect
    - mac-address
    - one-way-delay-threshold
    - shutdown
  - squelch-ingress-levels
- hash-label
- ingress
  - filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface spoke-sdp ingress flowspec

- flowspec
- qos
- vc-label
- pw-path-id
- agi
- saii-type2
- taii-type2
- shutdown
- transit-policy
- static-arp
- static-tunnel-redundant-next-hop
- tcp-mss
- tos-marking-state
- unnumbered
- unnumbered
- urpf-check
- ignore-default
- mode
- vas-if-type
- vpls
- egress
- reclassify-using-qos
- v4-routed-override-filter
- v6-routed-override-filter
- evpn
- arp
- advertise
- flood-garp-and-unknown-req
- learn-dynamic
- nd
- advertise
- learn-dynamic
- ingress
- v4-routed-override-filter
- v6-routed-override-filter
- vrrp
- authentication-key
- backup
- bfd-enable
- init-delay
- mac
- master-int-inherit
- message-interval
- ntp-reply
- oper-group
- ping-reply
- policy
- preempt
- priority
- shutdown
- ssh-reply
- standby-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface vrrp telnet-reply

- telnet-reply
- traceroute-reply
- ipsec
  - stale-time
- multicast-info-policy
  - filter
  - filter
    - ingress
- redundant-interface
  - address
  - description
  - hold-time
    - down
    - up
  - ip-mtu
  - shutdown
  - spoke-sdp
    - control-channel-status
      - acknowledgment
      - refresh-timer
      - request-timer
      - shutdown
    - control-word
    - description
    - egress
      - filter
      - vc-label
    - ingress
      - filter
      - vc-label
    - pw-path-id
      - agi
      - saii-type2
      - taii-type2
    - shutdown
- rip
  - group
- sap
  - anti-spoof
  - scheduler-policy
    - interface-support-enable
  - scheduler-policy
  - multi-service-site
- shutdown
  - interface-support-enable
- subscriber-interface
  - address
  - allow-unmatching-subnets
  - default-dns
  - description
  - dhcp
    - client-applications

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface dhcp description

- description
- gi-address
  - client-mac-address
- python-policy
- relay-proxy
- release-include-gi-address
- server
- shutdown
- vendor-specific-option
- virtual-subnet

- dhcp6
- export-host-routes
- group-interface
  - arp-host
    - host-limit
    - min-auth-interval
    - sap-host-limit
    - shutdown
  - arp-populate
  - arp-timeout
  - authentication-policy
  - bonding-parameters
    - connection
      - service
    - fpe
      - connection
    - multicast
    - shutdown
  - brg
    - authenticated-brg-only
    - default-brg-profile
    - shutdown
  - cflowd-parameters
    - sampling
  - data-trigger
    - shutdown
  - description
  - dhcp
    - client-applications
    - description
    - filter
    - gi-address
    - lease-populate
    - match-circuit-id
    - offer-selection
      - client-mac
        - discover-delay
      - discover-delay
      - server
        - discover-delay
    - option
      - action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface dhcp option circuit-id

- circuit-id
- remote-id
- vendor-specific-option
  - client-mac-address
  - pool-name
  - sap-id
  - service-id
  - string
  - system-id
- proxy-server
  - emulated-server
  - lease-time
  - shutdown
- python-policy
- relay-proxy
- release-include-gi-address
- server
- shutdown
- trusted
- user-db

- dhcp6
  - filter
  - user-db
- diameter-application-policy
- diameter-auth-policy
- diameter-peer-policy
- enable-ingress-stats
- gtp-parameters
  - fpe
  - shutdown
- host-connectivity-verify
- host-limit
- icmp
  - mask-reply
  - param-problem
  - redirects
  - ttl-expired
  - unreachables
- ignore-default
- ignore-df-bit
- ingress
  - policy-accounting
- ip-mtu
- ipoe-linking
  - gratuitous-rtr-adv
  - shared-circuit-id
  - shutdown
- ipoe-session
  - description
  - force-auth
  - ipoe-session-policy
  - min-auth-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface ipoe-session radius-session-timeout

- radius-session-timeout
- sap-session-limit
- session-limit
- shutdown
- stateless-redundancy
- user-db
  - python-policy
- ipv6
  - allow-multiple-wan-addresses
  - auto-reply
    - neighbor-solicitation
    - router-solicitation
  - dhcp6
    - filter
    - option
      - interface-id
      - remote-id
    - override-slaac
    - pd-managed-route
    - proxy-server
      - client-applications
      - preferred-lifetime
      - rebind-timer
      - renew-timer
      - server-id
      - shutdown
      - valid-lifetime
    - python-policy
    - relay
      - advertise-selection
        - client-mac
          - preference-option
            - value
          - solicit-delay
        - preference-option
          - value
        - server
          - preference-option
            - value
          - solicit-delay
        - solicit-delay
      - client-applications
      - description
      - lease-split
        - shutdown
        - valid-lifetime
      - link-address
      - server
      - shutdown
      - source-address
    - snooping
      - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface ipv6 dhcp6 user-db

- user-db
- user-ident
- force-mcast
- ignore-default
- include-dns
- ipoe-bridged-mode
- managed-configuration
- max-advertisement
- min-advertisement
- mtu
- nd
  - dad-snooping
  - neighbor-limit
- other-stateful-configuration
- prefix-options
- qos-route-lookup
- rdnss-lifetime
  - reachable-time
- router-advertisements
  - current-hop-limit
  - dns-options
    - include-dns
    - rdnss-lifetime
  - force-mcast
  - managed-configuration
  - max-advertisement
  - min-advertisement
  - mtu
  - other-stateful-configuration
  - prefix-options
    - autonomous
    - on-link
    - preferred-lifetime
    - valid-lifetime
  - reachable-time
  - retransmit-time
  - router-lifetime
  - shutdown
- router-solicit
  - inactivity-timer
  - min-auth-interval
  - shutdown
  - user-db
- urpf-check
  - mode
- local-address-assignment
  - client-application
  - default-pool
  - ipv6
    - client-application
    - server
  - server

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface local-address-assignment shutdown

- shutdown
- local-proxy-arp
- mac
- mask-reply
- min-auth-interval
- oper-up-while-empty
- policy-control
- ppp
  - description
  - policy
  - session-limit
  - shutdown
  - user-db
- pppoe
  - anti-spoof
  - anti-spoof
  - description
  - dhcp-client
    - client-id
  - policy
  - python-policy
  - sap-session-limit
  - session-limit
  - shutdown
  - user-db
- proxy-arp-policy
- qos-route-lookup
- redundant-interface
- remote-proxy-arp
- sap
  - accounting-policy
  - anti-spoof
  - anti-spoof
  - app-profile
  - atm
    - egress
      - traffic-desc
    - encapsulation
    - ingress
      - traffic-desc
    - oam
      - alarm-cells
      - periodic-loopback
  - calling-station-id
  - collect-stats
  - cpu-protection
  - default-host
  - description
  - dist-cpu-protection
  - egress
    - agg-rate
      - limit-unused-bandwidth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface sap egress agg-rate queue-frame-based-accounting

- queue-frame-based-accounting
- rate
- filter
- policer-control-policy
- qinq-mark-top-only
- qos
- queue-override
  - queue
    - adaptation-rule
    - avg-frame-overhead
    - burst-limit
- scheduler-policy

- eth-cfm
  - collect-lmm-fc-stats
  - collect-lmm-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - csf-enable
    - multiplier
  - mep
    - ais-enable
      - interface-support-enable
      - interval
      - priority
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed
        - tx-eth-ed
      - eth-vsm-grace
        - rx-eth-vsm-grace
        - tx-eth-vsm-grace
    - low-priority-defect
    - mac-address
    - multiplier
    - one-way-delay-threshold
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface sap eth-cfm squelch-ingress-levels

- squelch-ingress-levels
- tunnel-fault
- fwd-wholesale
- pppoe
- host-lockout-policy
- host-shutdown
- igmp-host-tracking
- disable-router-alert-check
- expiry-time
- import
- max-num-groups
- max-num-grp-sources
- max-num-sources
- ingress
- filter
- match-qinq-dot1p
- policer-control-policy
- qos
- scheduler-policy
- lag-link-map-profile
- lag-per-link-hash
- monitor-oper-group
- multi-service-site
- oper-group
- shutdown
- static-host
- ancp-string
- app-profile
- inter-dest-id
- mac-linking
- managed-routes
- route-entry
- metric
- preference
- tag
- retail-svc-id
- rip-policy
- shutdown
- sla-profile
- sub-profile
- subscriber
- subscriber-sap-id
- static-host-mgmt
- mac-learning-options
- data-triggered
- single-mac
- sub-sla-mgmt
- def-app-profile
- def-inter-dest-id
- def-sla-profile
- def-sub-id
- def-sub-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface sap sub-sla-mgmt multi-sub-sap

- multi-sub-sap
- shutdown
- single-sub-parameters
  - non-sub-traffic
  - profiled-traffic-only
- sub-ident-policy

- sap-parameters
  - anti-spoof
  - description
  - sub-sla-mgmt
    - def-app-profile
    - def-sla-profile
    - def-sub-id
    - def-sub-profile
    - sub-ident-policy
- shared-circuit-id
- shcv-policy
- shcv-policy-ipv4
- shcv-policy-ipv6
- shutdown
- srrp
  - bfd-enable
  - description
  - gw-mac
  - keep-alive-interval
  - message-path
  - monitor-oper-group
  - one-garp-per-sap
  - policy
  - preempt
  - priority
  - send-fib-population-packets
  - shutdown
- srrp-enabled-routing
- suppress-aa-sub
- tos-marking-state
- urpf-check
  - mode
- wlan-gw
  - address
  - description
    - active-lease-time
    - initial-lease-time
  - egress
    - rate
    - agg-rate-limit
    - hold-time
    - qos
    - scheduler-policy
    - shape-multi-client-only
    - shaping
  - group-encryption

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface wlan-gw group-encryption encryption-keygroup

- encryption-keygroup
- gw-addresses
  - address
- l2-access-points
  - l2-ap
    - encap-type
    - epipe-sap-template
    - shutdown
- l2-ap-auto-sub-id-fmt
- l2-ap-encap-type
- learn-ap-mac
- learn-l2tp-cookie
- max-lanext-bd
- mobility
  - hold-time
  - inter-vlan
  - multi-tunnel-type
  - trigger
- oper-down-on-group-degrade
  - default-retail-svc-id
  - dhcp
  - dhcp6
    - brg
      - authenticated-brg-only
      - default-brg-profile
      - shutdown
        - description
          - description
          - max-mac
          - policer
  - vlan
- router
- shutdown
- tcp-mss-adjust
- tunnel-encaps
  - learn-l2tp-cookie
    - vrgw
      - authenticated-brg-only
      - default-brg-profile
      - shutdown
- vlan-tag-ranges
  - default-retail-svc-id
  - range
    - authenticate-on-dhcp
    - authentication
      - authentication-policy
      - hold-time
      - local
        - coa-policy
        - default-ue-state
      - vlan-mismatch-timeout
    - data-triggered-ue-creation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp

- dhcp
  - active-lease-time
  - initial-lease-time
  - l2-aware-ip-address
  - primary-dns
  - primary-nbns
  - secondary-dns
  - secondary-nbns
  - shutdown
- dhcp6
  - active-preferred-lifetime
  - active-valid-lifetime
  - initial-preferred-lifetime
  - initial-valid-lifetime
  - shutdown
- distributed-sub-mgmt
  - aa-url-parameter
  - accounting-policy
  - accounting-update-interval
  - collect-aa-acct-stats
  - def-app-profile
  - dsm-ip-filter
  - egress-policer
  - ingress-policer
  - one-time-redirect
  - shutdown
  - soft-quota-exhausted-filter
  - volume-quota-direction
- extensions
  - extension
- http-redirect-policy
- idle-timeout
- l2-service
  - description
  - shutdown
- nat-policy
- retail-svc-id
- slaac
  - active-preferred-lifetime
  - active-valid-lifetime
  - initial-preferred-lifetime
  - initial-valid-lifetime
  - shutdown
- track-mobility
  - mac-format
  - radius-proxy-cache
- vrgw
  - brg
    - authenticated-brg-only
    - default-brg-profile
    - shutdown
  - lanext

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect

- access
  - max-mac
  - multi-access
  - policer
- assistive-address-resolution
- bd-mac-prefix
- mac-translation
- network
  - max-mac
  - policer
  - shutdown
- shutdown

- xconnect
  - accounting-policy
  - accounting-update-interval
  - mobility-acct-updates
  - shutdown

- wlan-gw-group

- wpp
  - enable-triggered-hosts
  - initial-app-profile
  - initial-sla-profile
  - initial-sub-profile
  - lease-time
  - portal
  - portal-group
  - restore-disconnected
  - shutdown
  - user-db

- hold-time
  - down
  - up
- ip-mtu
- ipoe-linking
  - gratuitous-rtr-adv
- ipoe-session
  - session-limit
- ipv6
  - address
  - allow-multiple-wan-addresses
  - allow-unmatching-prefixes
  - allow-unmatching-subnets
  - default-dns
  - delegated-prefix-length
  - dhcp6
    - override-slaac
    - pd-managed-route
    - proxy-server
      - client-applications
      - preferred-lifetime
      - rebind-timer
      - renew-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface ipv6 dhcp6 proxy-server server-id

- server-id
- shutdown
- valid-lifetime
- python-policy
- relay
  - client-applications
  - description
  - lease-split
    - shutdown
    - valid-lifetime
  - link-address
  - server
  - shutdown
  - source-address
- ipoe-bridged-mode
- link-local-address
- router-advertisements
  - current-hop-limit
  - dns-options
    - include-dns
    - rdnss-lifetime
  - force-mcast
  - managed-configuration
  - max-advertisement
  - min-advertisement
  - mtu
  - other-stateful-configuration
  - prefix-options
    - autonomous
    - on-link
    - preferred-lifetime
    - valid-lifetime
  - reachable-time
  - retransmit-time
  - router-lifetime
  - shutdown
- router-solicit
  - inactivity-timer
  - include-dns
  - rdnss-lifetime
- subscriber-prefixes
  - prefix
- local-address-assignment
  - client-application
  - default-pool
  - ipv6
    - client-application
    - server
  - server
  - shutdown
- pppoe
  - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface pppoe session-limit

- session-limit
- shutdown
- unnumbered
- unnumbered
- wlan-gw
  - pool-manager
    - dhcpv6-client
      - dhcpv4-nat
        - link-addr
        - pool-name
        - shutdown
      - ia-na
        - link-addr
        - pool-name
        - shutdown
      - lease-query
      - server
      - slaac
        - link-addr
        - pool-name
        - shutdown
      - source-ip
    - watermarks
    - wlan-gw-group
      - shutdown
      - shutdown
      - shutdown
  - redundancy
    - export
    - monitor
    - shutdown
- subscriber-mgmt
  - multi-chassis-shunt-id
  - up-resiliency
    - monitor-oper-group
- video-interface
  - accounting-policy
  - address
  - adi
    - scte30
      - ad-server
      - local-address
  - channel
    - description
    - scte35-action
    - zone-channel
  - cpu-protection
  - description
  - multicast-service
  - output-format
  - rt-client-src-address
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies video-interface video-sap

- video-sap
  - egress
    - filter
    - qos
  - ingress
    - filter
    - qos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.8 configure service ipfix Commands

- ipfix
  - ipfix-export-policy
    - collector
      - mtu
      - shutdown
      - source-address
      - template-refresh-timeout
    - description
    - template-format

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.9 configure service ipipe Commands

- ipipe
  - ce-address-discovery
  - description
  - endpoint
    - active-hold-delay
    - description
    - revert-time
    - standby-signaling-master
  - eth-cfm
    - tunnel-fault
  - eth-legacy-fault-notification
    - recovery-timer
    - shutdown
  - sap
    - accounting-policy
    - app-profile
    - atm
      - egress
        - traffic-desc
      - encapsulation
      - ingress
        - traffic-desc
      - oam
        - alarm-cells
    - bandwidth
    - ce-address
    - collect-stats
    - cpu-protection
    - description
    - dist-cpu-protection
    - egress
      - agg-rate
        - limit-unused-bandwidth
        - rate
      - filter
      - policer-control-override
        - max-rate
        - priority-mbs-thresholds
          - min-thresh-separation
          - priority
            - mbs-contribution
      - policer-control-policy
      - policer-override
        - policer
          - cbs
          - mbs
          - packet-byte-offset
          - percent-rate
          - rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ipipe sap egress policer-override policer stat-mode

- stat-mode
- qinq-mark-top-only
- qos
- queue-override
  - hs-secondary-shaper
  - hs-wrr-group
    - class-weight
    - percent-rate
    - rate
  - queue
    - adaptation-rule
    - avg-frame-overhead
    - burst-limit
    - cbs
    - drop-tail
      - low
        - percent-reduction-from-mbs
    - hs-class-weight
    - hs-wred-queue
    - hs-wrr-weight
    - mbs
    - monitor-queue-depth
    - parent
    - percent-rate
    - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
- eth-cfm
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ipipe sap eth-cfm mep grace eth-ed tx-eth-ed

- tx-eth-ed
- eth-vsm-grace
  - rx-eth-vsm-grace
  - tx-eth-vsm-grace
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown
- squelch-ingress-levels
- tunnel-fault

- eth-tunnel
  - path
- frame-relay
  - frf-12
    - ete-fragment-threshold
    - interleave
    - interleave
  - scheduling-class
- ingress
  - criteria-overrides
    - ip-criteria
      - activate-entry-tag
    - ipv6-criteria
      - activate-entry-tag
  - filter
  - match-qinq-dot1p
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qos
  - queue-override
    - queue
      - adaptation-rule
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs
      - monitor-queue-depth
      - parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ipipe sap ingress queue-override queue percent-rate

- percent-rate
- rate
- scheduler-override
- scheduler
- parent
- rate
- scheduler-policy
- lag-link-map-profile
- lag-per-link-hash
- mac
- mac-refresh
- multi-service-site
- shutdown
- transit-policy
- use-broadcast-mac
- service-mtu
- shutdown
- spoke-sdp
- aarp
- app-profile
- bandwidth
- bfd
- bfd-enable
- bfd-template
- ce-address
- control-word
- description
- egress
- filter
- qos
- vc-label
- entropy-label
- hash-label
- ingress
- filter
- qos
- vc-label
- precedence
- shutdown
- transit-policy
- stack-capability-signaling

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.10 configure service mac-list Commands

- mac-list
  - description
  - mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service mac-notification

3.4.39.11 configure service mac-notification Commands

- mac-notification
  - count
  - interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.12 configure service md-auto-id Commands

- md-auto-id
  - customer-id-range
  - pw-template-id-range
  - service-id-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.13 configure service mrp Commands

- mrp
  - copy
  - mrp-policy
    - default-action
    - description
    - entry
      - action
      - description
      - match
        - isid
    - renum
    - scope

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.14 configure service nat Commands

- **nat**
  - deterministic-script
    - location
  - firewall-policy
    - alg
      - ftp
      - rtsp
      - sip
    - description
    - domain
    - filtering
    - l2-outside
    - port-forwarding-range
    - port-limits
      - forwarding
    - priority-sessions
      - fc
    - session-limits
      - max
      - reserved
      - watermarks
    - tcp-mss-adjust
    - timeouts
      - icmp6-query
      - sip
      - tcp-established
      - tcp-rst
      - tcp-syn
      - tcp-time-wait
      - tcp-transitory
      - udp
      - udp-dns
      - udp-initial
      - unknown-protocol
    - udp-inbound-refresh
    - unknown-protocols
      - protocol
  - map-domain
    - **description**
    - dmr-prefix
    - **ip-fragmentation**
      - v6-frag-header
    - mapping-rule
      - description
      - ea-length
      - ipv4-prefix
      - psid-offset
      - rule-prefix
      - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service nat map-domain mtu

- mtu
- shutdown
- tcp-mss-adjust
- nat-classifier
  - default-action
  - default-dnat-ip-address
  - description
  - entry
    - action
    - description
    - match
      - dst-port-range
      - foreign-ip
- nat-policy
  - alg
    - ftp
    - pptp
    - rtsp
    - sip
  - block-limit
  - description
  - dnat
    - dnat-only
    - nat-classifier
  - filtering
  - ipfix-export-policy
  - l2-outside
  - pool
  - port-forwarding-range
  - port-limits
    - forwarding
    - reserved
    - watermarks
  - priority-sessions
    - fc
  - reset-unknown-tcp
  - session-limits
    - max
    - reserved
    - watermarks
  - syslog-export-policy
  - tcp-mss-adjust
  - timeouts
    - icmp-query
    - sip
    - subscriber-retention
    - tcp-established
    - tcp-rst
    - tcp-syn
    - tcp-time-wait
    - tcp-transitory
    - udp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service nat nat-policy timeouts udp-dns

- udp-dns
- udp-initial
- udp-inbound-refresh
- nat-prefix-list
  - prefix
- pcp-server-policy
  - description
  - lifetime
  - max-description-size
  - opcode
    - announce
    - get
    - map
  - option
    - description
    - next
    - port-reservation
    - port-set
    - prefer-failure
    - third-party
  - reuse-ext-ip
  - version
- port-forwarding
  - l2-aware
  - lsn
- syslog
  - syslog-export-policy
    - collector
      - destination-port
      - ipv4-source-address
      - **shutdown**
    - **description**
    - facility
    - include
      - destination-ip
      - foreign-ip
      - foreign-port
      - nat-policy-name
      - sub-id
    - log-prefix
    - max-tx-delay
    - mtu
    - rate-limit
    - severity-level
- up-nat-policy
  - alg
    - ftp
    - pptp
    - rtsp
    - sip
  - **block-limit**
  - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service nat up-nat-policy filtering

- filtering
- icmp-echo-reply
- ipfix-export-policy
- port-limits
  - reserved
  - watermarks
- priority-sessions
  - fc
- reset-unknown-tcp
- session-limits
  - max
  - reserved
  - watermarks
- tcp-mss-adjust
- timeouts
  - icmp-query
  - sip
  - subscriber-retention
  - tcp-established
  - tcp-rst
  - tcp-syn
  - tcp-time-wait
  - tcp-transitory
  - udp
  - udp-dns
  - udp-initial
- udp-inbound-refresh
- watermarks

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.15 configure service oper-group Commands

- oper-group
  - bfd-enable
  - hold-time
    - group
      - group down
      - group up

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.16 configure service pbb Commands

— **pbb**
  — **leaf-source-bmac**
  — **mac-name**
  — **source-bmac**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.17 configure service proxy-arp-nd Commands

- proxy-arp-nd
  - mac-list
    - mac
  - port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.18 configure service pw-routing Commands

- pw-routing
  - boot-timer
    - shutdown
  - local-prefix
    - advertise-bgp
  - path
    - hop
    - **shutdown**
  - retry-count
  - retry-timer
  - spe-address
  - static-route

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.19 configure service pw-template Commands

- pw-template
  - accounting-policy
  - allow-fragmentation
  - auto-learn-mac-protect
  - block-on-peer-fault
  - collect-stats
  - controlword
  - description
  - disable-aging
  - disable-learning
  - discard-unknown-source
  - egress
    - filter
    - filter-name
      - ip
      - ipv6
      - mac
    - mfib-allowed-mda-destinations
      - mda
    - qos
  - encryption-keygroup
  - entropy-label
  - force-qinq-vc-forwarding
  - force-vlan-vc-forwarding
  - hash-label
  - igmp-snooping
    - fast-leave
    - import
    - last-member-query-interval
    - max-num-groups
    - mcac
      - policy
    - query-interval
    - query-response-interval
    - robust-count
    - send-queries
    - version
  - ingress
    - filter
    - filter-name
      - ip
      - ipv6
      - mac
    - qos
  - l2pt-termination
  - limit-mac-move
  - mac-pinning
  - max-nbr-mac-addr
  - restrict-protected-src

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service pw-template sdp-exclude

- sdp-exclude
- sdp-include
- split-horizon-group
  - auto-learn-mac-protect
  - description
  - restrict-protected-src
  - restrict-unprotected-dst
- stp
  - auto-edge
  - edge-port
  - link-type
  - path-cost
  - priority
  - root-guard
  - shutdown
- vc-type
- vlan-vc-tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.20 configure service sdp Commands

- sdp
  - accounting-policy
  - adv-mtu-override
  - allow-fragmentation
  - bgp-tunnel
  - binding
    - port
    - pw-port
      - adv-service-mtu
      - control-word
      - description
      - egress
        - shaper
          - int-dest-id
          - pw-sap-secondary-shaper
          - vport
        - vc-label
      - entropy-label
      - ingress
        - vc-label
      - monitor-oper-group
      - shutdown
      - vc-type
      - vlan-vc-tag
  - booking-factor
  - class-forwarding
    - enforce-diffserv-lsp-fc
    - fc
    - multicast-lsp
    - shutdown
  - collect-stats
  - description
  - encryption-keygroup
  - far-end
  - keep-alive
    - hello-time
    - hold-down-time
    - max-drop-count
    - message-length
    - shutdown
    - timeout
  - ldp
  - local-end
  - lsp
  - metric
  - mixed-lsp-mode
    - revert-time
  - network-domain
  - path-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service sdp pbb-etype

- pbb-etype
- **sdp-group**
- shutdown
- signaling
- source-bmac-lsb
- sr-isis
- sr-ospf
- sr-te-lsp
- tunnel-far-end
- vlan-vc-etype
- weighted-ecmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.21 configure service sdp-group Commands

- sdp-group
  - group-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.22 configure service system Commands

- **system**
  - bgp-auto-rd-range
  - bgp-evpn
    - ad-per-es-route-target
    - ethernet-segment
      - ac-df-capability
      - auto-esi
      - dot1q
        - q-tag-range
      - es-activation-timer
      - es-orig-ip
      - esi
      - lag
      - multi-homing
      - network-interconnect-vxlan
      - oper-group
      - port
      - pw-port
      - qinq
        - s-tag
        - s-tag-range
      - route-next-hop
      - sdp
      - service-carving
        - manual
          - evi
          - isid
          - preference
            - value
        - mode
      - service-id
        - service-range
      - shutdown
      - source-bmac-lsb
      - vc-id-range
    - evpn-etree-leaf-label
    - ip-prefix-routes
      - iff-attribute-uniform-propagation
      - iff-bgp-path-selection
    - multicast-leave-sync-propagation
    - route-distinguisher
  - fdb-table-size
  - gre-eth-bridged
    - tunnel-termination
  - pw-port-list
    - **port**
  - vpn-gre-source-ip
  - vxlan
    - assisted-replication-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service system vxlan tunnel-termination

— **tunnel-termination**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.23 configure service template Commands

- template
  - epipe-sap-template
    - egress
      - filter
        - ip
        - ipv6
        - mac
      - filter-name
        - ip
        - ipv6
        - mac
      - qos
    - ingress
      - filter
        - ip
        - ipv6
        - mac
      - filter-name
        - ip
        - ipv6
        - mac
      - qos
  - vpls-sap-template
    - bpdu-translation
    - collect-stats
    - cpu-protection
    - disable-aging
    - disable-learning
    - discard-unknown-source
    - dist-cpu-protection
    - egress
      - agg-rate
        - limit-unused-bandwidth
        - queue-frame-based-accounting
        - rate
      - filter
      - filter-name
        - ip
        - ipv6
        - mac
      - policer-control-policy
      - qinq-mark-top-only
      - qos
      - scheduler-policy
    - eth-cfm
      - mip
      - squelch-ingress-ctag-levels
      - squelch-ingress-levels
    - ingress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service template vpls-sap-template ingress filter

- filter
- filter-name
  - ip
  - ipv6
  - mac
- match-qinq-dot1p
- policer-control-policy
- qos
- scheduler-policy

- l2pt-termination
- limit-mac-move
- mac-move-level
- max-nbr-mac-addr
- stp
  - auto-edge
  - edge-port
  - link-type
  - path-cost
  - priority
  - root-guard
  - shutdown

- vpls-template
  - customer
  - disable-aging
  - disable-learning
  - discard-unknown
  - discard-unknown-source
  - fdb-table-high-wmark
  - fdb-table-low-wmark
  - fdb-table-size
  - load-balancing
    - per-service-hashing
    - spi-load-balancing
    - teid-load-balancing
  - local-age
  - mac-move
    - move-frequency
    - number-retries
    - primary-ports
      - cumulative-factor
    - retry-timeout
    - secondary-ports
      - cumulative-factor
    - shutdown
  - remote-age
  - service-mtu
  - stp
    - forward-delay
    - hello-time
    - hold-count
    - max-age
    - mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service template vpls-template stp priority

— **priority**
— **shutdown**
— **temp-flooding**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.24 configure service upnp Commands

- upnp
  - upnp-policy
    - description
    - http-listening-port
    - mapping-limit
    - strict-mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.25 configure service vpls Commands

- vpls
  - allow-ip-int-bind
    - evpn-mcast-gateway
      - advertise
      - dr-activation-timer
      - non-dr-attract-traffic
      - shutdown
    - evpn-mpls-ecmp
    - forward-ipv4-multicast-to-ip-int
    - forward-ipv6-multicast-to-ip-int
    - igmp-snooping
      - mrouter-port
    - ip-multicast-ecmp
    - mld-snooping
      - mrouter-port
    - vxlan-ipv4-tep-ecmp
      - spf-wait
    - spbm-control-vpls
    - stp
  - bgp
    - adv-service-mtu
    - pw-template-binding
      - bfd-enable
      - bfd-template
      - monitor-oper-group
      - oper-group
    - route-distinguisher
    - route-target
    - vsi-export
    - vsi-import
  - bgp-ad
    - pw-template-binding
      - bfd-enable
      - bfd-template
    - route-target
    - shutdown
    - vpls-id
    - vsi-export
    - vsi-id
      - prefix
      - vsi-import
  - bgp-evpn
    - accept-ivpls-evpn-flush
    - cfm-mac-advertisement
    - evi
    - incl-mcast-orig-ip
    - ingress-repl-inc-mcast-advertisement
    - ip-route-advertisement
    - isid-route-target

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls bgp-evpn isid-route-target isid-range

- isid-range
- mac-advertisement
- mac-duplication
  - black-hole-dup-mac
  - detect
  - retry
- mpls
  - auto-bind-tunnel
    - allow-flex-algo-fallback
    - ecmp
    - enforce-strict-tunnel-tagging
    - resolution
    - resolution-filter
      - bgp
      - ldp
      - mpls-fwd-policy
      - rib-api
      - rsvp
      - sr-isis
      - sr-ospf
      - sr-ospf3
      - sr-policy
      - sr-te
      - udp
  - control-word
  - default-route-tag
  - dynamic-egress-label-limit
  - ecmp
  - entropy-label
  - evi-three-byte-auto-rt
  - force-vlan-vc-forwarding
  - incl-mcast-orig-ip
  - ingress-replication-bum-label
  - mh-mode
  - oper-group
  - restrict-protected-src
  - route-next-hop
  - send-tunnel-encap
  - shutdown
  - split-horizon-group
- sel-mcast-advertisement
- unknown-mac-route
- vxlan
  - auto-disc-route-advertisement
  - default-route-tag
  - ecmp
  - evi-three-byte-auto-rt
  - mh-mode
  - oper-group
  - send-imet-ir-on-ndf
  - send-tunnel-encap
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls bgp-vpls

- bgp-vpls
  - max-ve-id
  - shutdown
  - ve-name
    - ve-id
      - load-balancing
- description
- disable-aging
- disable-learning
- discard-unknown
- endpoint
  - auto-learn-mac-protect
  - block-on-mesh-failure
  - description
  - ignore-standby-signaling
  - mac-pinning
  - max-nbr-mac-addr
  - mc-endpoint
    - mc-ep-peer
  - restrict-protected-src
  - revert-time
  - static-mac
  - suppress-standby-signaling
- eth-cfm
  - mep
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - cfm-vlan-tag
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed
        - tx-eth-ed
      - eth-vsm-grace
        - rx-eth-vsm-grace
        - tx-eth-vsm-grace
    - low-priority-defect
    - mac-address
    - one-way-delay-threshold
    - shutdown
    - vmep-filter
    - vmep-filter
    - vmep-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls eth-cfm tunnel-fault

- tunnel-fault
- eth-ring
- eth-tunnel
- fdb-table-high-wmark
- fdb-table-low-wmark
- fdb-table-size
- gsmp
  - group
    - ancp
      - dynamic-topology-discover
      - oam
    - description
    - hold-multiplier
    - idle-filter
    - keepalive
    - neighbor
      - description
      - local-address
      - priority-marking
      - shutdown
    - persistency-database
    - shutdown
  - hold-multiplier
  - idle-filter
  - persistency-database
  - shutdown
- host-connectivity-verify
- igmp-host-tracking
  - expiry-time
  - shutdown
- igmp-snooping
  - evpn-proxy
  - mvr
    - description
    - group-policy
    - shutdown
  - query-interval
  - query-src-ip
  - report-src-ip
  - robust-count
  - shutdown
    - group
- ignore-l2vpn-mtu-mismatch
- interface
  - address
  - arp-timeout
  - description
  - hold-time
    - down
    - up
  - mac
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls interface static-arp

- static-arp
- static-mac
- unnumbered
- unnumbered
- isid-policy
  - entry
    - advertise-local
    - range
    - use-def-mcast
- load-balancing
  - spi-load-balancing
  - lbl-eth-or-ip-l4-teid
  - per-service-hashing
  - spi-load-balancing
  - teid-load-balancing
- local-age
- mac-move
  - move-frequency
  - number-retries
  - primary-ports
    - cumulative-factor
    - sap
    - spoke-sdp
  - retry-timeout
  - secondary-ports
    - cumulative-factor
    - sap
    - spoke-sdp
  - shutdown
- mac-notification
  - count
  - interval
  - renotify
  - shutdown
- mac-protect
  - mac
- mac-subnet-length
- mcast-ipv6-snooping-scope
- mcr-default-gtw
  - ip
  - mac
- mesh-sdp
  - accounting-policy
  - auto-learn-mac-protect
  - bfd
    - bfd-enable
    - bfd-template
  - collect-stats
  - control-word
  - cpu-protection
  - description
  - dhcp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp dhcp description

- description
- snoop
- dhcp6
- egress
  - filter
  - mfib-allowed-mda-destinations
    - mda
  - qos
  - vc-label
- entropy-label
- eth-cfm
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - client-meg-level
      - interface-support-enable
      - interval
      - low-priority-defect
      - priority
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - cfm-vlan-tag
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed
        - tx-eth-ed
      - eth-vsm-grace
        - rx-eth-vsm-grace
        - tx-eth-vsm-grace
    - lbm-svc-act-responder
    - low-priority-defect
    - mac-address
    - one-way-delay-threshold
    - shutdown
  - mip
  - squelch-ingress-ctag-levels

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp eth-cfm squelch-ingress-levels

- squelch-ingress-levels
- vmep-filter
- fault-propagation-bmac
- force-qinq-vc-forwarding
- force-vlan-vc-forwarding
- hash-label
- igmp-snooping
  - disable-router-alert-check
  - fast-leave
  - import
  - last-member-query-interval
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
  - mcac
    - if-policy
    - policy
    - unconstrained-bw
  - mrouter-port
  - query-interval
  - query-response-interval
  - robust-count
  - send-queries
  - static
    - group
      - source
      - starg
  - version
- ingress
  - filter
  - qos
  - vc-label
- mac-pinning
  - ccm-enable
  - ccm-ltm-priority
- mld-snooping
  - disable-router-alert-check
  - fast-leave
  - import
  - last-member-query-interval
  - max-num-groups
  - mcac
    - if-policy
    - policy
    - unconstrained-bw
  - mrouter-port
  - query-interval
  - query-response-interval
  - robust-count
  - send-queries
  - static
    - group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp mld-snooping static group source

- source
- starg
- version
- mrp
  - join-time
  - leave-all-time
  - leave-time
  - mrp-policy
  - periodic-time
  - periodic-timer
- restrict-protected-src
- shutdown
  - mcac
- static-mac
- vlan-vc-tag
- mfib-table-high-wmark
- mfib-table-low-wmark
- mfib-table-size
- mld-snooping
  - evpn-proxy
  - mvr
    - description
    - group-policy
    - shutdown
  - query-interval
  - query-src-ip
  - report-src-ip
  - robust-count
  - shutdown
- mrp
  - flood-time
  - mmrp
    - attribute-table-high-wmark
    - attribute-table-low-wmark
    - attribute-table-size
    - end-station-only
    - flood-time
    - shutdown
  - mvrp
    - attribute-table-high-wmark
    - attribute-table-low-wmark
    - attribute-table-size
    - endstation-vid-group
    - hold-time
    - shutdown
  - shutdown
- multicast-info-policy
- pbb
  - backbone-vpls
    - igmp-snooping
      - mrouter-dest
    - mld-snooping

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls pbb backbone-vpls mld-snooping mrouter-dest

- mrouter-dest
- restrict-protected-src
- sap
  - igmp-snooping
    - mrouter-port
  - mld-snooping
    - mrouter-port
- sdp
  - igmp-snooping
    - mrouter-port
  - mld-snooping
    - mrouter-port
- stp

- force-qtag-forwarding
- propagate-mac-flush-from-bvpls
- send-bvpls-evpn-flush
- send-bvpls-flush
- send-flush-on-bvpls-failure
- source-bmac
- use-es-bmac
- use-sap-bmac

- pim-snooping
  - group-policy
  - hold-time
  - ipv4-multicast-disable
  - ipv6-multicast-disable
  - mode
- ppp-user-db
- pppoe-user-db
- propagate-mac-flush
- provider-tunnel
  - inclusive
    - data-delay-interval
    - mldp
    - owner
    - root-and-leaf
    - rsvp
      - lsp-template
    - shutdown
- proxy-arp
  - age-time
  - dup-detect
  - dynamic
    - mac-list
    - resolve
  - dynamic-arp-populate
  - evpn-route-tag
  - garp-flood-evpn
  - send-refresh
  - shutdown
  - static
  - table-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls proxy-arp unknown-arp-request-flood-evpn

- unknown-arp-request-flood-evpn
- proxy-nd
  - age-time
  - dup-detect
  - dynamic
    - mac-list
    - resolve
  - dynamic-nd-populate
  - evpn-nd-advertise
  - evpn-route-tag
  - host-unsolicited-na-flood-evpn
  - router-unsolicited-na-flood-evpn
  - send-refresh
  - shutdown
  - static
  - table-size
  - unknown-ns-flood-evpn
- remote-age
- restrict-unprotected-dst
- sap
  - accounting-policy
  - allow-dot1q-msaps
  - anti-spoof
  - anti-spoof
  - app-profile
  - arp-host
    - host-limit
    - min-auth-interval
    - shutdown
  - arp-reply-agent
  - atm
  - atm
    - alarm-cells
    - egress
      - traffic-desc
    - encapsulation
    - ingress
      - traffic-desc
    - oam
      - alarm-cells
    - vc-range
  - authentication-policy
  - auto-learn-mac-protect
  - bandwidth
  - bgp-vpls-mh-ve-id
  - bpdu-translation
  - calling-station-id
  - cflowd
  - collect-stats
  - cpu-protection
  - cpu-protection
  - default-msap-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap description

- description
- dhcp
  - description
  - lease-populate
  - option
    - action
    - circuit-id
    - remote-id
    - vendor-specific-option
      - client-mac-address
      - sap-id
      - service-id
      - string
      - system-id
  - proxy-server
    - emulated-server
    - lease-time
    - shutdown
  - shutdown
  - snoop
- dhcp-python-policy
- dhcp-user-db
- dhcp6
- dhcp6-python-policy
- dhcp6-user-db
- diameter-application-policy
- diameter-auth-policy
- disable-aging
- disable-learning
- disable-send-bvpls-evpn-flush
- discard-unknown-source
- dist-cpu-protection
- dynamic-services
  - dynamic-services-policy
  - shutdown
- egress
- egress
  - agg-rate
    - limit-unused-bandwidth
    - queue-frame-based-accounting
    - rate
  - dest-mac-rewrite
  - encap-defined-qos
    - encap-group
      - agg-rate
        - limit-unused-bandwidth
        - queue-frame-based-accounting
        - rate
      - member
      - qos
      - scheduler-policy
  - filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap egress policer-control-override

- policer-control-override
  - max-rate
  - priority-mbs-thresholds
    - min-thresh-separation
    - priority
      - mbs-contribution
  - policer-control-policy
  - policer-override
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - percent-rate
      - rate
      - stat-mode
  - qinq-mark-top-only
  - qos
  - qos
  - queue-override
    - hs-secondary-shaper
    - hs-wrr-group
      - class-weight
      - percent-rate
      - rate
    - queue
      - adaptation-rule
      - avg-frame-overhead
      - burst-limit
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - hs-class-weight
      - hs-wred-queue
      - hs-wrr-weight
      - mbs
      - monitor-queue-depth
      - parent
      - percent-rate
      - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
- eth-cfm
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap eth-cfm mep ais-enable client-meg-level

- client-meg-level
- interface-support-enable
- interval
- low-priority-defect
- priority
- alarm-notification
  - fng-alarm-time
  - fng-reset-time
- ccm-enable
- ccm-ltm-priority
- ccm-padding-size
- cfm-vlan-tag
- csf-enable
  - multiplier
- description
- eth-test-enable
  - bit-error-threshold
  - test-pattern
- fault-propagation-enable
- grace
  - eth-ed
    - max-rx-defect-window
    - priority
    - rx-eth-ed
    - tx-eth-ed
  - eth-vsm-grace
    - rx-eth-vsm-grace
    - tx-eth-vsm-grace
- lbm-svc-act-responder
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown
- mip
- squelch-ingress-ctag-levels
- squelch-ingress-levels
- tunnel-fault
- vmep-filter
- eth-tunnel
  - path
- fault-propagation-bmac
- force-l2pt-boundary
- frame-relay
  - frf-12
    - ete-fragment-threshold
    - interleave
    - interleave
  - scheduling-class
- host-connectivity-verify
- host-lockout-policy
- host-shutdown
- igmp-host-tracking

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap igmp-host-tracking disable-router-alert-check

- disable-router-alert-check
- expiry-time
- import
- max-num-groups
- max-num-grp-sources
- max-num-sources
- igmp-snooping
  - disable-router-alert-check
  - fast-leave
  - import
  - last-member-query-interval
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
  - mcac
    - if-policy
    - mc-constraints
      - level
      - number-down
      - shutdown
      - use-lag-port-weight
    - policy
    - unconstrained-bw
  - mrouter-port
  - mvr
    - from-vpls
    - group-policy
    - to-sap
  - query-interval
  - query-response-interval
  - robust-count
  - send-queries
  - static
    - group
      - source
      - starg
  - version
- ingress
  - criteria-overrides
    - ip-criteria
      - activate-entry-tag
    - ipv6-criteria
      - activate-entry-tag
  - filter
  - match-qinq-dot1p
  - policer-control-override
    - max-rate
    - priority-mbs-thresholds
      - min-thresh-separation
      - priority
        - mbs-contribution
  - policer-control-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap ingress policer-override

- policer-override
  - policer
    - cbs
    - mbs
    - packet-byte-offset
    - percent-rate
    - rate
    - stat-mode
  - qos
  - queue-override
    - queue
      - adaptation-rule
      - avg-frame-overhead
      - cbs
      - drop-tail
        - low
          - percent-reduction-from-mbs
      - mbs
      - monitor-queue-depth
      - parent
      - percent-rate
      - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
  - vlan-translation
- ipoe-session
  - description
  - ipoe-session-policy
  - shutdown
  - user-db
- l2pt-termination
- l2tpv3-session
  - pw-type
  - router
  - shutdown
  - vc-id
- lag-link-map-profile
- lag-per-link-hash
- limit-mac-move
- mac-pinning
- managed-vlan-list
  - default-sap
  - range
- max-nbr-mac-addr
- mld-snooping
  - disable-router-alert-check
  - fast-leave
  - import
  - last-member-query-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap mld-snooping max-num-groups

- max-num-groups
- mcac
  - if-policy
  - mc-constraints
    - level
    - number-down
    - shutdown
    - use-lag-port-weight
  - policy
  - unconstrained-bw
- mrouter-port
- mvr
  - from-vpls
  - to-sap
- query-interval
- query-response-interval
- robust-count
- send-queries
- static
  - group
    - source
    - starg
- version

- monitor-oper-group
- mrp
  - join-time
  - leave-all-time
  - leave-time
  - mrp-policy
  - mvrp
    - endstation-vid-group
    - shutdown
  - periodic-time
  - periodic-timer
- msap-defaults
  - group-interface
  - policy
  - service
- multi-service-site
- oper-group
- pfcp
  - association
  - l2-access-id-alias
  - up-resiliency
    - monitor-oper-group
- pim-snooping
  - max-num-groups
- ppp-policy
- ppp-user-db
- pppoe-policy
- pppoe-python-policy
- pppoe-user-db

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap process-cpm-traffic-on-sap-down

- process-cpm-traffic-on-sap-down
- restrict-protected-src
- restrict-unprotected-dst
- ring-node
- rtr-solicit-user-db
- shcv-policy-ipv4
- shutdown
  - to-sap
- spb
  - level
    - hello-interval
    - hello-multiplier
    - metric
  - lsp-pacing-interval
  - retransmit-interval
  - retransmit-interval
  - shutdown
- static-host
  - ancp-string
  - app-profile
  - inter-dest-id
  - shutdown
  - sla-profile
  - sub-profile
  - subscriber
  - subscriber-sap-id
- static-isid
  - range
- static-mac
- stp
  - auto-edge
  - edge-port
  - link-type
  - mst-instance
    - mst-path-cost
    - mst-port-priority
  - path-cost
  - port-num
  - priority
  - root-guard
  - shutdown
- sub-sla-mgmt
  - def-app-profile
  - def-inter-dest-id
  - def-sla-profile
  - def-sub-id
  - def-sub-profile
  - mac-da-hashing
  - multi-sub-sap
  - shutdown
  - single-sub-parameters
    - non-sub-traffic

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap sub-sla-mgmt single-sub-parameters profiled-traffic-only

- profiled-traffic-only
- sub-ident-policy
- track-srrp
- transit-policy
- trigger-packet
- selective-learned-fdb
- send-flush-on-failure
- service-mtu
- shcv-policy-ipv4
- shutdown
- site
- boot-timer
- failed-threshold
- mesh-sdp-binding
- monitor-oper-group
- sap
- shutdown
- site-activation-timer
- site-id
- site-min-down-timer
- split-horizon-group
- spoke-sdp
- spb
- level
- level
- bridge-priority
- ect-algorithm
- forwarding-tree-topology
- shutdown
- lsp-lifetime
- lsp-refresh-interval
- overload
- overload-on-boot
- shutdown
- timers
- lsp-wait
- spf-wait
- spbm-control-vpls
- split-horizon-group
- auto-learn-mac-protect
- description
- restrict-protected-src
- restrict-unprotected-dst
- spoke-sdp
- spoke-sdp
- spoke-sdp
- spoke-sdp
- accounting-policy
- app-profile
- auto-learn-mac-protect
- bfd
- bfd-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls spoke-sdp bfd bfd-template

- bfd-template
- failure-action
- wait-for-up-timer
- block-on-mesh-failure
- bpdu-translation
- collect-stats
- control-channel-status
  - acknowledgment
  - refresh-timer
  - request-timer
  - request-timer
  - shutdown
- control-word
- control-word
- cpu-protection
- description
- dhcp
  - description
  - snoop
- dhcp6
- disable-aging
- disable-learning
- disable-send-bvpls-evpn-flush
- discard-unknown-source
- egress
  - filter
  - mfib-allowed-mda-destinations
    - mda
  - qos
  - vc-label
- entropy-label
- eth-cfm
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - client-meg-level
      - interface-support-enable
      - interval
      - low-priority-defect
      - priority
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - cfm-vlan-tag
    - csf-enable
      - multiplier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls spoke-sdp eth-cfm mep description

- **description**
- eth-test-enable
  - bit-error-threshold
  - test-pattern
- fault-propagation-enable
- grace
  - eth-ed
    - max-rx-defect-window
    - priority
    - rx-eth-ed
    - tx-eth-ed
  - eth-vsm-grace
    - rx-eth-vsm-grace
    - tx-eth-vsm-grace
- lbm-svc-act-responder
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown

- mip
- squelch-ingress-ctag-levels
- squelch-ingress-levels
- **vmep-filter**

- fault-propagation-bmac
- force-qinq-vc-forwarding
- force-vlan-vc-forwarding
- hash-label
- igmp-snooping
  - disable-router-alert-check
  - fast-leave
  - import
  - last-member-query-interval
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
  - mcac
    - if-policy
    - policy
    - unconstrained-bw
  - mrouter-port
  - query-interval
  - query-response-interval
  - robust-count
  - send-queries
  - static
    - group
      - source
      - starg
  - version
- ignore-standby-signaling
- ingress
  - filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls spoke-sdp ingress qos

- qos
- vc-label
- l2pt-termination
- limit-mac-move
- mac-pinning
- max-nbr-mac-addr
- mld-snooping
  - disable-router-alert-check
  - fast-leave
  - import
  - last-member-query-interval
  - max-num-groups
  - mcac
    - if-policy
    - policy
    - unconstrained-bw
  - mrouter-port
  - query-interval
  - query-response-interval
  - robust-count
  - send-queries
  - static
    - group
      - source
      - starg
  - version
- monitor-oper-group
- mrp
  - join-time
  - leave-all-time
  - leave-time
  - mrp-policy
  - periodic-time
  - periodic-timer
- oper-group
- pim-snooping
  - max-num-groups
- precedence
- priority
- pw-path-id
  - agi
  - saii-type2
  - taii-type2
- pw-status-signaling
- restrict-protected-src
- shutdown
- shutdown
- spb
  - level
    - hello-interval
    - hello-multiplier
    - metric

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls spoke-sdp spb lsp-pacing-interval

- lsp-pacing-interval
- retransmit-interval
- retransmit-interval
- shutdown
- shutdown
- static-isid
  - range
- static-mac
- stp
  - auto-edge
  - edge-port
  - link-type
  - path-cost
  - port-num
  - priority
  - root-guard
  - shutdown
- transit-policy
- vlan-vc-tag
- static-mac
  - mac
- stp
  - forward-delay
  - hello-time
  - hold-count
  - max-age
  - mode
  - mst-instance
    - mst-priority
    - vlan-range
  - mst-max-hops
  - mst-name
  - mst-revision
  - priority
  - shutdown
- temp-flooding
- video-interface
  - accounting-policy
  - address
  - cpu-protection
  - description
  - gateway-ip
  - multicast-service
  - rt-client-src-address
  - shutdown
  - video-sap
    - egress
      - filter
      - qos
    - ingress
      - filter
      - qos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls vpls-group

- vpls-group
  - mvrp-control
  - sap-template-binding
  - service-range
  - shutdown
  - vpls-template-binding
- vsd-domain
- vxlan
  - assisted-replication
  - disable-aging
  - disable-learning
  - discard-unknown-source
  - egr-vtep
  - igmp-snooping
    - mrouter-port
  - max-nbr-mac-addr
  - mld-snooping
    - mrouter-port
  - network
    - ingress
      - qos
  - restrict-protected-src
  - rx-discard-on-ndf
  - source-vtep-security
- vxlan-src-vtep
- wlan-gw
  - description
  - sap-template
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.26 configure service vprn Commands

- vprn
  - aa-interface
    - address
    - description
    - ip-mtu
    - sap
    - sap
      - description
      - egress
        - filter
        - qos
      - ingress
        - qos
      - shutdown
    - shutdown
  - aaa
    - remote-servers
      - radius
        - access-algorithm
        - accounting
        - accounting-port
        - authorization
        - interactive-authentication
        - port
        - retry
        - server
        - shutdown
        - timeout
        - use-default-template
      - tacplus
        - accounting
        - authorization
        - interactive-authentication
        - priv-lvl-map
          - priv-lvl
        - request-format
          - access-operation-cmd
        - server
        - shutdown
        - timeout
        - use-default-template
  - aarp-interface
    - description
    - ip-mtu
    - shutdown
    - spoke-sdp
      - aarp
      - description
      - egress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn aarp-interface spoke-sdp egress filter

- filter
- vc-label
- ingress
  - filter
  - vc-label
- shutdown
- aggregate
- allow-export-bgp-vpn
  - resolution
- autonomous-system
- bgp
  - advertise-inactive
  - advertise-ipv6-next-hops
  - aggregator-id-zero
  - auth-keychain
  - authentication-key
  - backup-path
  - best-path-selection
    - always-compare-med
    - as-path-ignore
    - compare-origin-validation-state
    - d-path-length-ignore
    - deterministic-med
    - ebgp-ibgp-equal
    - ignore-nh-metric
    - ignore-router-id
    - origin-invalid-unusable
  - bfd-enable
  - cluster
  - connect-retry
  - convergence
    - family
      - max-wait-to-advertise
    - min-wait-to-advertise
  - damp-peer-oscillations
  - damping
  - default-label-preference
  - default-preference
  - description
  - disable-4byte-asn
  - disable-client-reflect
  - disable-communities
  - disable-fast-external-failover
  - domain-id
  - dynamic-neighbor-limit
  - ebgp-default-reject-policy
  - eibgp-loadbalance
  - enable-peer-tracking
  - enforce-first-as
  - error-handling
    - update-fault-tolerance
  - export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp extended-nh-encoding

- extended-nh-encoding
- family
- flowspec
  - validate-dest-prefix
  - validate-redirect-ip
- graceful-restart
  - enable-notification
  - long-lived
    - advertise-stale-to-all-neighbors
    - advertised-stale-time
    - family
      - advertised-stale-time
      - helper-override-stale-time
    - forwarding-bits-set
    - helper-override-restart-time
    - helper-override-stale-time
  - restart-time
  - stale-routes-time
- group
  - advertise-inactive
  - advertise-ipv6-next-hops
  - aggregator-id-zero
  - as-override
  - auth-keychain
  - authentication-key
  - bfd-enable
  - cluster
  - connect-retry
  - damp-peer-oscillations
  - damping
  - default-label-preference
  - default-preference
  - description
  - disable-4byte-asn
  - disable-capability-negotiation
  - disable-client-reflect
  - disable-communities
  - disable-fast-external-failover
  - dynamic-neighbor
    - match
      - prefix
        - allowed-peer-as
  - dynamic-neighbor-limit
  - ebgp-default-reject-policy
  - enable-origin-validation
  - enable-peer-tracking
  - enforce-first-as
  - error-handling
    - update-fault-tolerance
  - export
  - extended-nh-encoding
  - family

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group graceful-restart

- graceful-restart
  - enable-notification
  - long-lived
    - advertise-stale-to-all-neighbors
    - advertised-stale-time
    - family
      - advertised-stale-time
      - helper-override-stale-time
    - forwarding-bits-set
    - helper-override-restart-time
    - helper-override-stale-time
  - restart-time
  - stale-routes-time
- hold-time
- import
- initial-send-delay-zero
- keepalive
- label-preference
- link-bandwidth
  - accept-from-ebgp
  - add-to-received-ebgp
  - aggregate-used-paths
  - send-to-ebgp
- local-address
- local-as
- local-preference
- loop-detect
- loop-detect-threshold
- med-out
- min-route-advertisement
- monitor
  - route-monitoring
  - shutdown
  - station
- multihop
- multipath-eligible
- neighbor
  - advertise-inactive
  - advertise-ipv6-next-hops
  - aggregator-id-zero
  - as-override
  - auth-keychain
  - authentication-key
  - bfd-enable
  - cluster
  - connect-retry
  - damp-peer-oscillations
  - damping
  - default-label-preference
  - default-preference
  - description
  - disable-4byte-asn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group neighbor disable-capability-negotiation

- disable-capability-negotiation
- disable-client-reflect
- disable-communities
- disable-fast-external-failover
- ebgp-default-reject-policy
- enable-origin-validation
- enable-peer-tracking
- enforce-first-as
- error-handling
  - update-fault-tolerance
- export
- extended-nh-encoding
- family
- graceful-restart
  - enable-notification
  - long-lived
    - advertise-stale-to-all-neighbors
    - advertised-stale-time
    - family
      - advertised-stale-time
      - helper-override-stale-time
    - forwarding-bits-set
    - helper-override-restart-time
    - helper-override-stale-time
  - restart-time
  - stale-routes-time
- hold-time
- import
- initial-send-delay-zero
- keepalive
- label-preference
- link-bandwidth
  - accept-from-ebgp
  - add-to-received-ebgp
  - aggregate-used-paths
  - send-to-ebgp
- local-address
- local-as
- local-preference
- loop-detect
- loop-detect-threshold
- med-out
- min-route-advertisement
- monitor
  - route-monitoring
  - shutdown
  - station
- multihop
- multipath-eligible
- next-hop-self
- passive
- path-mtu-discovery

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group neighbor peer-as

- peer-as
- preference
- prefix-limit
- remove-private
- send-default
- shutdown
- split-horizon
- tcp-mss
- third-party-nexthop
- ttl-security
- type
- updated-error-handling

- next-hop-self
- passive
- path-mtu-discovery
- peer-as
- preference
- prefix-limit
- remove-private
- send-default
- shutdown
- split-horizon
- tcp-mss
- third-party-nexthop
- ttl-security
- type
- updated-error-handling

- hold-time
- ibgp-multipath
- import
- initial-send-delay-zero
- keepalive
- label-preference
- local-as
- local-preference
- loop-detect
- loop-detect-threshold
- med-out
- min-route-advertisement
- monitor
  - route-monitoring
  - shutdown
  - station
- multi-path
  - ipv4
  - ipv6
  - label-ipv4
  - label-ipv6
  - maximum-paths
- multihop
  - multipath-eligible
- next-hop-resolution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp next-hop-resolution policy

- policy
- use-bgp-routes
- path-mtu-discovery
- peer-tracking-policy
- preference
- rapid-withdrawal
- remove-private
- rib-management
  - ipv4
    - leak-import
    - route-table-import
  - ipv6
    - leak-import
    - route-table-import
  - label-ipv4
    - leak-import
    - route-table-import
  - label-ipv6
    - leak-import
- router-id
- send-default
- shutdown
- split-horizon
- tcp-mss
- third-party-nexthop

- bgp-evpn
  - mpls
    - auto-bind-tunnel
      - allow-flex-algo-fallback
      - ecmp
      - enforce-strict-tunnel-tagging
      - resolution
      - resolution-filter
        - bgp
        - ldp
        - mpls-fwd-policy
        - rib-api
        - rsvp
        - sr-isis
        - sr-ospf
        - sr-ospf3
        - sr-policy
        - sr-te
        - udp
    - default-route-tag
    - domain-id
    - dynamic-egress-label-limit
    - route-distinguisher
    - send-tunnel-encap
    - shutdown
    - vrf-export
    - vrf-import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp-evpn mpls vrf-target

- vrf-target
- domain-id
- bgp-ipvpn
  - mpls
    - auto-bind-tunnel
      - allow-flex-algo-fallback
      - ecmp
      - enforce-strict-tunnel-tagging
      - resolution
      - resolution-filter
        - bgp
        - gre
        - ldp
        - mpls-fwd-policy
        - rib-api
        - rsvp
        - sr-isis
        - sr-ospf
        - sr-ospf3
        - sr-policy
        - sr-te
        - udp
      - weighted-ecmp
    - domain-id
    - dynamic-egress-label-limit
    - route-distinguisher
    - shutdown
    - vrf-export
    - vrf-import
    - vrf-target
  - segment-routing-v6
    - default-route-tag
    - domain-id
    - route-distinguisher
    - shutdown
    - source-address
    - srv6-instance
    - vrf-export
    - vrf-import
    - vrf-target
    - default-route-tag
- bgp-shared-queue
- carrier-carrier-vpn
- class-forwarding
- confederation
- d-path-length-ignore
- description
- dhcp
  - interface
  - local-dhcp-server
    - description
    - failover

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn dhcp local-dhcp-server failover ignore-mclt-on-takeover

- ignore-mclt-on-takeover
- maximum-client-lead-time
- partner-down-delay
- peer
- shutdown
- startup-wait-time

- force-renews
- lease-hold-time
- lease-hold-time-for
  - internal-lease-ipsec
  - solicited-release
- pool
  - description
  - failover
    - ignore-mclt-on-takeover
    - maximum-client-lead-time
    - partner-down-delay
    - peer
    - shutdown
    - startup-wait-time
  - max-lease-time
  - min-lease-time
  - minimum-free
  - nak-non-matching-subnet
  - offer-time
  - options
    - custom-option
    - dns-server
    - domain-name
    - lease-rebind-time
    - lease-renew-time
    - lease-time
    - netbios-name-server
    - netbios-node-type
  - subnet
    - address-range
    - drain
    - exclude-addresses
    - maximum-declined
    - minimum-free
    - options
      - custom-option
      - default-router
      - subnet-mask
  - shutdown
  - use-gi-address
  - use-pool-from-client
  - user-db
  - user-ident
  - peer
    - address-range
    - peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn dhcp6

- dhcp6
  - rebind-timer
  - interface
  - local-dhcp-server
    - allow-lease-query
    - defaults
      - options
        - custom-option
        - dns-server
        - domain-name
      - preferred-lifetime
      - rebind-timer
      - renew-timer
      - valid-lifetime
    - description
    - failover
      - ignore-mclt-on-takeover
      - maximum-client-lead-time
      - partner-down-delay
      - peer
      - shutdown
      - startup-wait-time
    - ignore-rapid-commit
    - interface-id-mapping
    - lease-hold-time
    - lease-hold-time-for
      - internal-lease-ipsec
      - solicited-release
    - pool
      - delegated-prefix-length
      - description
      - exclude-prefix
      - failover
        - ignore-mclt-on-takeover
        - maximum-client-lead-time
        - partner-down-delay
        - peer
        - shutdown
        - startup-wait-time
      - options
        - custom-option
        - dns-server
        - domain-name
      - prefix
        - drain
        - options
          - custom-option
          - dns-server
          - domain-name
        - preferred-lifetime
        - rebind-timer
        - renew-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn dhcp6 local-dhcp-server pool prefix thresholds

```
                    — thresholds
                        — minimum-free
                            — depleted-event
                            — minimum
                        — valid-lifetime
                    — thresholds
                        — minimum-free
                            — depleted-event
                            — minimum
                — server-id
                — shutdown
                — use-link-address
                — use-pool-from-client
                — user-ident
                — peer
                    — peer
                        — default-router
        — disable-selective-fib
        — dns
            — default-domain
            — ipv4-source-address
            — ipv6-source-address
            — primary-dns
            — secondary-dns
            — shutdown
            — tertiary-dns
        — ecmp
        — ecmp-unequal-cost
        — enable-bgp-vpn-backup
        — encryption-keygroup
        — entropy-label
        — eth-cfm
            — tunnel-fault
        — export-inactive-bgp
        — fib-priority
        — firewall
            — domain
                — dhcp6-server
                — prefix
                    — description
                — shutdown
        — flowspec
            — filter-cam-type
            — ip-filter-max-size
            — ipv6-filter-max-size
        — grt-lookup
            — enable-grt
                — allow-local-management
            — export-grt
            — export-limit
            — export-v6-limit
            — import-grt
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn gsmp

- gsmp
  - group
    - ancp
    - ancp
      - dynamic-topology-discover
      - oam
    - description
    - hold-multiplier
    - idle-filter
    - keepalive
    - neighbor
    - neighbor
      - description
      - local-address
      - priority-marking
      - shutdown
    - persistency-database
    - shutdown
  - hold-multiplier
  - idle-filter
  - persistency-database
  - shutdown
- gtp
  - s11
    - interface
      - apn-policy
    - peer-profile-map
      - address
  - upf-data-endpoint
  - uplink
    - apn
    - pdn-type
    - peer-profile-map
      - address
- hash-label
- igmp
  - group-interface
    - disable-router-alert-check
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - shutdown
      - policy
      - unconstrained-bw
    - query-interval
    - query-last-member-interval
    - query-response-interval
    - query-src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn igmp group-interface shutdown

- shutdown
- sub-hosts-only
- subnet-check
- version
- grp-if-query-src-ip
- interface
  - disable-router-alert-check
  - import
  - max-groups
  - max-grp-sources
  - max-sources
  - mcac
    - if-policy
    - mc-constraints
      - level
      - number-down
      - shutdown
      - use-lag-port-weight
    - policy
    - shutdown
    - unconstrained-bw
  - query-interval
  - query-last-member-interval
  - query-response-interval
  - redundant-multicast
  - shutdown
  - ssm-translate
    - grp-range
      - source
  - static
    - group
      - source
      - starg
  - subnet-check
  - version
- query-interval
- query-last-member-interval
- query-response-interval
- robust-count
- shutdown
- ssm-translate
  - grp-range
    - source
- igmp-host-tracking
  - expiry-time
  - shutdown
- ignore-nh-metric
  - nat64
    - drop-zero-ipv4-checksum
    - ignore-tos
    - insert-ipv6-fragment-header
- interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface active-cpm-protocols

- active-cpm-protocols
- address
- allow-directed-broadcasts
- arp-host-route
  - populate
- arp-learn-unsolicited
- arp-limit
- arp-populate
- arp-proactive-refresh
- arp-retry-timer
- arp-timeout
- authentication-policy
- bfd
- cflowd-parameters
  - sampling
- clear-df-bit
- cpu-protection
- description
- dhcp
  - description
  - gi-address
  - lease-populate
  - option
    - action
    - circuit-id
    - remote-id
    - snoop
    - vendor-specific-option
      - client-mac-address
      - pool-name
      - sap-id
      - service-id
      - string
      - system-id
  - proxy-server
    - emulated-server
    - lease-time
    - shutdown
  - python-policy
  - relay-plain-bootp
  - relay-proxy
  - release-include-gi-address
  - server
  - shutdown
  - trusted
  - use-arp
- dhcp6
- dynamic-tunnel-redundant-next-hop
- enable-ingress-stats
- enable-mac-accounting
- hold-time
  - down

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface hold-time up

- up
- host-connectivity-verify
- icmp
  - mask-reply
  - param-problem
  - redirects
  - ttl-expired
  - unreachables
- if-attribute
  - admin-group
  - srlg-group
- ingress
  - destination-class-lookup
  - policy-accounting
- ip-helper-address
- ip-mtu
  - public-tcp-mss-adjust
- ipcp
  - dns
  - peer-ip-address
- ipsec
  - ip-exception
    - clear-df-bit
  - ipsec-tunnel
    - bfd-designate
    - bfd-enable
    - clear-df-bit
    - copy-traffic-class-upon-decapsulation
    - description
    - dynamic-keying
      - auto-establish
      - cert
        - cert-profile
        - status-verify
          - default-result
          - primary
        - trust-anchor-profile
      - ike-policy
      - local-id
      - pre-shared-key
      - transform
    - encapsulated-ip-mtu
    - icmp-generation
      - frag-required
        - interval
        - message-count
    - icmp6-generation
      - pkt-too-big
        - interval
        - message-count
    - ip-mtu
    - local-gateway-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface ipsec ipsec-tunnel manual-keying

- manual-keying
  - security-association
- max-history-esp-key-records
- max-history-ike-key-records
- pmtu-discovery-aging
- private-tcp-mss-adjust
- propagate-pmtu-v4
- propagate-pmtu-v6
- public-tcp-mss-adjust
- remote-gateway-address
- replay-window
- security-policy
- shutdown

- ipv6-exception
- shutdown

- ipv6
  - address
  - bfd
  - dad-disable
  - dhcp6-relay
    - description
    - lease-populate
    - link-address
    - neighbor-resolution
    - option
      - interface-id
      - remote-id
    - python-policy
    - server
    - shutdown
    - source-address
    - user-db
  - dhcp6-server
    - max-nbr-of-leases
    - prefix-delegation
      - prefix
        - duid
        - preferred-lifetime
        - valid-lifetime
      - shutdown
  - forward-ipv4-packets
  - icmp6
    - packet-too-big
    - param-problem
    - redirects
    - time-exceeded
    - unreachables
  - link-local-address
  - local-dhcp-server
  - local-proxy-nd
  - nd-host-route
    - populate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface ipv6 nd-learn-unsolicited

- nd-learn-unsolicited
- nd-proactive-refresh
- neighbor
- neighbor-limit
- proxy-nd-policy
- python-policy
- qos-route-lookup
- reachable-time
- secure-nd
  - allow-unsecured-msgs
  - link-local-modifier
  - public-key-min-bits
  - security-parameter
  - shutdown
- stale-time
- tcp-mss
- urpf-check
  - ignore-default
  - mode
- vrrp
  - backup
  - bfd-enable
  - init-delay
  - mac
  - master-int-inherit
  - message-interval
  - ntp-reply
  - oper-group
  - ping-reply
  - policy
  - preempt
  - priority
  - shutdown
  - standby-forwarding
  - telnet-reply
  - traceroute-reply
- load-balancing
  - egr-ip-load-balancing
  - flow-label-load-balancing
  - spi-load-balancing
  - teid-load-balancing
- local-dhcp-server
- local-proxy-arp
- loopback
- mac
- mask-reply
- message-interval
- monitor-oper-group
  - egr-ip-load-balancing
- ping-template
  - destination-address
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface preempt

- preempt
- proxy-arp-policy
- ptp-hw-assist
- qos-route-lookup
- redirects
- remote-proxy-arp
- sap
- sap
  - aarp
  - accounting-policy
  - anti-spoof
  - anti-spoof
  - app-profile
  - atm
    - egress
      - traffic-desc
    - encapsulation
    - ingress
      - traffic-desc
    - oam
      - alarm-cells
      - periodic-loopback
  - bandwidth
  - calling-station-id
  - collect-stats
  - cpu-protection
  - description
  - dist-cpu-protection
  - egress
    - agg-rate
      - limit-unused-bandwidth
      - queue-frame-based-accounting
      - rate
    - filter
    - policer-control-override
      - max-rate
      - priority-mbs-thresholds
        - min-thresh-separation
        - priority
          - mbs-contribution
    - policer-control-policy
      - min-thresh-separation
    - policer-override
      - policer
        - cbs
        - mbs
        - packet-byte-offset
        - percent-rate
        - rate
        - stat-mode
    - qinq-mark-top-only
    - qos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap egress queue-group-redirect-list

- queue-group-redirect-list
- queue-override
  - burst-limit
  - hs-secondary-shaper
  - hs-wrr-group
    - class-weight
    - percent-rate
    - rate
  - queue
    - adaptation-rule
    - avg-frame-overhead
    - burst-limit
    - cbs
    - drop-tail
      - low
        - percent-reduction-from-mbs
    - hs-class-weight
    - hs-wred-queue
    - hs-wrr-weight
    - mbs
    - monitor-queue-depth
    - parent
    - percent-rate
    - rate
  - scheduler-override
    - scheduler
      - parent
      - rate
  - scheduler-policy
- eth-cfm
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - mep
    - ais-enable
      - interface-support-enable
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - bit-error-threshold
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap eth-cfm mep grace eth-ed

- eth-ed
  - max-rx-defect-window
  - priority
  - rx-eth-ed
  - tx-eth-ed
- eth-vsm-grace
  - rx-eth-vsm-grace
  - tx-eth-vsm-grace
- low-priority-defect
- mac
- mac-address
- one-way-delay-threshold
- shutdown
- one-way-delay-threshold
- squelch-ingress-levels
- tunnel-fault
- frame-relay
- frf-12
- ete-fragment-threshold
- interleave
- interleave
- scheduling-class
- frf-12
- ete-fragment-threshold
- fwd-wholesale
- pppoe
- reassembly
- host-lockout-policy
- host-shutdown
- ingress
- criteria-overrides
- ip-criteria
- activate-entry-tag
- ipv6-criteria
- activate-entry-tag
- filter
- flowspec
- match-qinq-dot1p
- policer-control-override
- max-rate
- priority-mbs-thresholds
- min-thresh-separation
- priority
- mbs-contribution
- policer-control-policy
- min-thresh-separation
- policer-override
- policer
- cbs
- mbs
- packet-byte-offset
- percent-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ingress policer-override policer rate

- rate
- stat-mode
- qos
- queue-group-redirect-list
- queue-override
  - queue
    - adaptation-rule
    - cbs
    - drop-tail
      - low
        - percent-reduction-from-mbs
    - mbs
    - monitor-queue-depth
    - parent
    - percent-rate
    - rate
- scheduler-override
  - scheduler
    - parent
    - rate
- scheduler-policy

- ip-tunnel
  - backup-remote-ip
  - clear-df-bit
  - delivery-service
  - description
  - description
  - dest-ip
  - dscp
  - encapsulated-ip-mtu
  - gre-header
  - icmp-generation
    - frag-required
      - interval
      - message-count
  - icmp6-generation
    - packet-too-big
  - ip-mtu
  - ipsec-transport-mode-profile
  - pmtu-discovery-aging
  - private-tcp-mss-adjust
  - propagate-pmtu-v4
  - propagate-pmtu-v6
  - public-tcp-mss-adjust
  - reassembly
  - remote-ip
  - shutdown
  - source
  - default-secure-service
  - default-tunnel-template
  - dhcp
  - dhcp6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ipsec-gw

- ipsec-gw
  - cert
    - cert-profile
    - status-verify
      - default-result
      - primary
    - trust-anchor-profile
  - client-db
  - default-secure-service
  - default-tunnel-template
  - dhcp
    - gi-address
    - send-release
    - server
    - shutdown
  - dhcp6
    - link-address
    - send-release
    - server
    - shutdown
  - ike-policy
  - local-address-assignment
    - ipv4
      - address-source
    - ipv6
      - address-source
    - shutdown
  - local-gateway-address
  - local-id
  - max-history-esp-key-records
  - max-history-ike-key-records
  - pre-shared-key
  - radius-accounting-policy
  - radius-authentication-policy
  - shutdown
  - transform
  - ts-negotiation
- ipsec-tunnel
  - bfd-designate
  - bfd-enable
    - trust-anchor-profile
  - clear-df-bit
  - copy-traffic-class-upon-decapsulation
  - description
  - dest-ip
  - dynamic-keying
    - auto-establish
    - cert
      - cert-profile
      - status-verify
        - default-result
        - primary

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ipsec-tunnel dynamic-keying cert trust-anchor-profile

- trust-anchor-profile
- ike-policy
- local-id
- pre-shared-key
- transform
- encapsulated-ip-mtu
- icmp-generation
  - frag-required
    - interval
    - message-count
- icmp6-generation
  - pkt-too-big
    - interval
    - message-count
- ip-mtu
- local-gateway-address
- manual-keying
  - security-association
- max-history-esp-key-records
- max-history-ike-key-records
- pmtu-discovery-aging
- private-tcp-mss-adjust
- propagate-pmtu-v4
- propagate-pmtu-v6
- public-tcp-mss-adjust
- replay-window
- security-policy
- shutdown
- transform
- l2tpv3-session
  - pw-type
  - router
  - shutdown
  - vc-id
- lag-link-map-profile
- lag-per-link-hash
- multi-service-site
- multi-service-site
- scheduling-class
- shutdown
- static-host
  - ancp-string
  - app-profile
  - inter-dest-id
  - shutdown
  - sla-profile
  - sub-profile
  - subscriber
  - subscriber-sap-id
- sub-sla-mgmt
  - profiled-traffic-only
- transit-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface secondary

- secondary
  - allow-unsecured-msgs
  - link-local-modifier
  - public-key-min-bits
  - security-parameter
  - shutdown
- shcv-policy-ipv4
- shcv-policy-ipv6
- shutdown
- spoke-sdp
  - aarp
  - accounting-policy
  - app-profile
  - bfd
    - bfd-enable
    - bfd-template
    - failure-action
    - wait-for-up-timer
  - collect-stats
  - control-channel-status
    - acknowledgment
    - refresh-timer
    - request-timer
    - shutdown
  - control-word
  - cpu-protection
  - description
  - egress
    - filter
    - qos
    - vc-label
  - entropy-label
  - eth-cfm
    - ais-enable
    - collect-lmm-fc-stats
      - fc
      - fc-in-profile
    - collect-lmm-stats
    - mep
      - ais-enable
        - interface-support-enable
      - alarm-notification
        - fng-alarm-time
        - fng-reset-time
      - bit-error-threshold
      - ccm-enable
      - ccm-ltm-priority
      - ccm-padding-size
      - csf-enable
        - multiplier
      - description
      - eth-test-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface spoke-sdp eth-cfm mep eth-test-enable bit-error-threshold

- bit-error-threshold
- test-pattern
- fault-propagation-enable
- grace
- eth-ed
- max-rx-defect-window
- priority
- rx-eth-ed
- tx-eth-ed
- eth-vsm-grace
- rx-eth-vsm-grace
- tx-eth-vsm-grace
- low-priority-defect
- mac-address
- one-way-delay-threshold
- shutdown
- one-way-delay-threshold
- squelch-ingress-levels
- hash-label
- ingress
- filter
- flowspec
- qos
- vc-label
- pw-path-id
- agi
- saii-type2
- taii-type2
- shutdown
- transit-policy
- static-arp
- static-tunnel-redundant-next-hop
- tcp-mss
- tos-marking-state
- unnumbered
- unnumbered
- urpf-check
- ignore-default
- mode
- vas-if-type
- vpls
- egress
- reclassify-using-qos
- v4-routed-override-filter
- v6-routed-override-filter
- evpn
- arp
- advertise
- flood-garp-and-unknown-req
- learn-dynamic
- nd
- advertise

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface vpls evpn nd learn-dynamic

- learn-dynamic
- evpn-tunnel
- ingress
  - v4-routed-override-filter
  - v6-routed-override-filter
- vrrp
- vrrp
  - authentication-key
  - backup
  - bfd-enable
  - init-delay
  - mac
  - master-int-inherit
  - message-interval
  - ntp-reply
  - oper-group
  - ping-reply
  - policy
  - preempt
  - priority
  - shutdown
  - ssh-reply
  - standby-forwarding
  - telnet-reply
  - traceroute-reply
- ip-mirror-interface
  - description
  - shutdown
  - spoke-sdp
    - description
    - ingress
      - filter
      - vc-label
    - shutdown
    - filter
    - vc-label
- ipsec
  - allow-reverse-route-override
  - security-policy
    - entry
      - local-ip
      - local-v6-ip
      - remote-ip
      - remote-v6-ip
- ipv6
  - reachable-time
  - stale-time
- isis
  - advertise-passive-only
  - advertise-router-capability
  - all-l1isis
  - all-l2isis

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn isis area-id

- area-id
- auth-keychain
- authentication-check
- authentication-key
- authentication-type
- csnp-authentication
- default-route-tag
- export
- export-limit
- graceful-restart
  - helper-disable
- hello-authentication
- hello-padding
- ignore-attached-bit
- ignore-lsp-errors
- ignore-narrow-metric
- iid-tlv-enable
- import
- interface
  - bfd-enable
  - csnp-interval
  - default-instance
  - hello-auth-keychain
  - hello-authentication
  - hello-authentication-key
  - hello-authentication-type
  - hello-padding
  - interface-type
  - ipv4-multicast-disable
  - ipv6-unicast-disable
  - level
    - hello-auth-keychain
    - hello-authentication-key
    - hello-authentication-type
    - hello-interval
    - hello-multiplier
    - hello-padding
    - ipv4-multicast-metric
    - ipv6-unicast-metric
    - metric
    - passive
    - priority
    - sd-offset
    - sf-offset
  - level-capability
  - lfa-policy-map
  - load-balancing-weight
  - loopfree-alternate-exclude
  - lsp-pacing-interval
  - mesh-group
  - passive
  - retransmit-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn isis interface shutdown

- shutdown
- tag
- ipv4-multicast-routing
- ipv4-routing
- ipv6-routing
- level
  - advertise-router-capability
  - auth-keychain
  - authentication-key
  - authentication-type
  - csnp-authentication
  - default-ipv4-multicast-metric
  - default-ipv6-multicast-metric
  - default-ipv6-unicast-metric
  - default-metric
  - external-preference
  - hello-authentication
  - hello-padding
  - loopfree-alternate-exclude
  - lsp-mtu-size
  - preference
  - psnp-authentication
  - wide-metrics-only
- level-capability
- link-group
  - description
  - level
    - ipv4-multicast-metric-offset
    - ipv4-unicast-metric-offset
    - ipv6-unicast-metric-offset
    - member
    - oper-members
    - revert-members
- loopfree-alternates
  - exclude
    - prefix-policy
- lsp-lifetime
- lsp-minimum-remaining-lifetime
- lsp-mtu-size
- lsp-refresh-interval
- mru-mismatch-detection
- multi-topology
  - ipv4-multicast
  - ipv6-unicast
- multicast-import
- overload
- overload-export-external
- overload-export-interlevel
- overload-on-boot
- poi-tlv-enable
- prefix-attributes-tlv
- prefix-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn isis psnp-authentication

- psnp-authentication
- reference-bandwidth
- rib-priority
- router-id
- shutdown
- standard-multi-instance
- strict-adjacency-check
- summary-address
- suppress-attached-bit
- system-id
- timers
  - lsp-wait
  - spf-wait
- unicast-import-disable

— l2tp
- avp-hiding
- calling-number-format
- challenge
- cisco-nas-port
- cisco-nas-port
- description
- destruct-timeout
- df-bit-lac
- eth-tunnel
  - reconnect-timeout
- exclude-avps
- failover
  - recovery-max-session-lifetime
  - recovery-method
  - recovery-time
  - track-srrp
- group
  - avp-hiding
  - challenge
  - **description**
  - destruct-timeout
  - df-bit-lac
  - eth-tunnel
    - reconnect-timeout
  - failover
    - recovery-method
    - recovery-time
  - hello-interval
  - idle-timeout
  - l2tpv3
    - cookie-length
    - digest-type
    - nonce-length
    - password
    - private-tcp-mss-adjust
    - public-tcp-mss-adjust
    - pw-cap-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn l2tp group l2tpv3 rem-router-id

- rem-router-id
- track-password-change
- lns-group
- load-balance-method
- local-address
- local-name
- max-retries-estab
- max-retries-not-estab
- mlppp
  - endpoint
  - interleave
  - max-fragment-delay
  - max-links
  - reassembly-timeout
  - short-sequence-numbers
  - shutdown
- password
- ppp
  - authentication
  - authentication-policy
  - chap-challenge-length
  - default-group-interface
  - ipcp-subnet-negotiation
  - keepalive
  - lcp-force-ack-accm
  - lcp-ignore-magic-numbers
  - mtu
  - proxy-authentication
  - proxy-lcp
  - reject-disabled-ncp
  - user-db
- radius-accounting-policy
- receive-window-size
- reconnect-timeout
- session-assign-method
- session-limit
- shutdown
- tunnel
  - auto-establish
  - avp-hiding
  - challenge
  - chap-challenge-length
  - description
  - destruct-timeout
  - df-bit-lac
  - failover
    - recovery-method
    - recovery-time
  - hello-interval
  - idle-timeout
  - l2tpv3
    - private-tcp-mss-adjust

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn l2tp group tunnel l2tpv3 public-tcp-mss-adjust

- public-tcp-mss-adjust
- lns-group
- load-balance-method
- local-address
- local-name
- max-retries-estab
- max-retries-not-estab
- mlppp
  - admin-state
  - endpoint
  - interleave
  - max-fragment-delay
  - max-links
  - reassembly-timeout
  - short-sequence-numbers
- password
- peer
- ppp
  - authentication
  - authentication-policy
  - chap-challenge-length
  - default-group-interface
  - ipcp-subnet-negotiation
  - keepalive
  - lcp-force-ack-accm
  - lcp-ignore-magic-numbers
  - mtu
  - proxy-authentication
  - proxy-lcp
  - reject-disabled-ncp
  - user-db
- preference
- radius-accounting-policy
- receive-window-size
- remote-name
- session-limit
- shutdown

- group-session-limit
- hello-interval
- idle-timeout
- ignore-avps
- l2tpv3
  - cookie-length
  - digest-type
  - nonce-length
  - password
  - private-tcp-mss-adjust
  - public-tcp-mss-adjust
  - transport-type
- local-address
- local-name
- max-retries-estab

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn l2tp max-retries-not-estab

- max-retries-not-estab
- next-attempt
- password
- peer-address-change-policy
- radius-accounting-policy
- receive-window-size
- reconnect-timeout
- replace-result-code
- rtm-debounce-time
- session-assign-method
- session-limit
- shutdown
  - shutdown
- tunnel-selection-blacklist
  - add-tunnel
  - max-list-length
  - max-time
  - timeout-action
- tunnel-session-limit
- shutdown

- label-mode
- local-routes-domain-id
- log
  - filter
    - default-action
    - description
    - entry
      - action
      - description
      - match
        - application
        - message
        - number
        - severity
        - subject
  - log-id
    - description
    - filter
    - from
    - netconf-stream
    - python-policy
    - shutdown
    - time-format
    - to
  - snmp-trap-group
    - description
    - trap-target
  - syslog
    - address
    - description
    - facility
    - level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn log syslog log-prefix

- log-prefix
- port
- tls-client-profile
- log
- management
  - allow-ftp
  - allow-grpc
  - allow-netconf
  - allow-ssh
  - allow-telnet
  - allow-telnet6
- maximum-ipv6-routes
- maximum-routes
- mc-maximum-routes
- mld
  - group-interface
    - disable-router-alert-check
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - shutdown
      - policy
      - unconstrained-bw
    - query-interval
    - query-last-listener-interval
    - query-response-interval
    - query-src-ip
    - shutdown
    - sub-hosts-only
    - subnet-check
    - version
  - grp-if-query-src-ip
  - interface
    - disable-router-alert-check
    - import
    - max-groups
    - max-grp-sources
    - max-sources
    - mcac
      - if-policy
      - mc-constraints
        - level
        - number-down
        - shutdown
        - use-lag-port-weight
      - policy
      - unconstrained-bw
    - query-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn mld interface query-last-listener-interval

- query-last-listener-interval
- query-last-member-interval
- query-response-interval
- shutdown
- ssm-translate
  - grp-range
    - source
- static
  - group
    - source
    - starg
- version
- query-interval
- query-last-listener-interval
- query-last-member-interval
- query-response-interval
- robust-count
- shutdown
- ssm-translate
  - grp-range
    - source

- msdp
  - active-source-limit
  - data-encapsulation
  - export
  - group
    - active-source-limit
    - export
    - import
    - local-address
    - mode
    - peer
      - active-source-limit
      - authentication-key
      - default-peer
      - export
      - import
      - local-address
      - receive-msdp-msg-rate
      - shutdown
    - receive-msdp-msg-rate
    - shutdown
  - import
  - local-address
  - peer
    - active-source-limit
    - authentication-key
    - default-peer
    - export
    - import
    - local-address
    - receive-msdp-msg-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn msdp peer shutdown

- shutdown
- receive-msdp-msg-rate
- rpf-table
- sa-timeout
- shutdown
- source
  - active-source-limit
- mss-adjust-group
- mtrace2
  - shutdown
  - udp-port
- multicast-info-policy
- mvpn
  - auto-discovery
  - c-mcast-signaling
  - intersite-shared
  - mdt-type
  - provider-tunnel
    - inclusive
      - bier
        - shutdown
        - sub-domain
      - bsr
      - mldp
        - shutdown
      - p2mp-sr
        - enable-bfd-leaf
        - enable-bfd-root
        - p2mp-policy
        - shutdown
        - static-policy
      - pim
        - hello-interval
        - hello-multiplier
        - improved-assert
        - shutdown
        - three-way-hello
        - tracking-support
      - rsvp
        - enable-bfd-leaf
        - enable-bfd-root
        - lsp-template
        - shutdown
      - umh-rate-monitoring
        - revertive-timer
        - traffic-rate-delta
      - wildcard-spmsi
    - selective
      - auto-discovery-disable
      - bier
        - shutdown
        - sub-domain

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn mvpn provider-tunnel selective data-delay-interval

- data-delay-interval
- data-threshold
- enable-asm-mdt
- join-tlv-packing-disable
- maximum-p2mp-spmsi
- mldp
  - shutdown
- multistream-spmsi
  - group
    - source
  - lsp-template
  - mdt-pim
  - p2mp-policy
  - shutdown
  - shutdown
  - static-policy
- p2mp-sr
  - p2mp-policy
  - shutdown
  - static-policy
- pim-asm
- pim-ssm
- rsvp
  - lsp-template
  - shutdown
- umh-rate-monitoring
  - group
    - source
      - revertive-timer
      - traffic-rate-delta
  - lsp-template
    - shutdown

- red-source-list
  - ipv6
    - src-prefix
  - src-prefix
- rpf-select
  - core-mvpn
    - group-prefix
- umh-pe-backup
  - umh-pe
- umh-selection
- vrf-export
- vrf-import
- vrf-target
  - export
  - import

- nat
  - dual-stack-lite
  - inside
    - classic-lsn-max-subscriber-limit
    - destination-prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn nat inside deterministic

- deterministic
  - classic-lsn-max-subscriber-limit
  - prefix
    - map
    - shutdown
  - prefix-map
    - map
    - shutdown
- dnat-only
  - source-prefix-list
- downstream-ip-filter
    - ip-fragmentation
- dslite-max-subscriber-limit
- dual-stack-lite
  - address
    - ip-fragmentation
    - min-first-fragment-size-rx
    - reassembly
    - tunnel-mtu
  - shutdown
  - subscriber-prefix-length
- l2-aware
  - address
- nat-import
- nat-policy
- nat64
  - drop-zero-ipv4-checksum
  - ignore-tos
  - insert-ipv6-fragment-header
  - ip-fragmentation
  - ipv6-mtu
  - prefix
  - set-tos
  - shutdown
  - subscriber-prefix-length
- redundancy
  - peer
  - peer6
  - steering-route
- source-prefix-list
- subscriber-identification
  - attribute
  - description
  - drop-unidentified-traffic
  - radius-proxy-server
  - shutdown

- map
  - map-domain
- outside
  - dnat-only
    - route-limit
  - downstream-ip-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn nat outside downstream-ipv6-filter

- downstream-ipv6-filter
- mtu
- pool
  - address-range
    - description
    - drain
    - shutdown
  - description
  - deterministic
    - port-reservation
  - external-assignment
  - icmp-echo-reply
  - mode
  - port-block-extensions
    - ports
  - port-forwarding-dyn-block-reservation
  - port-forwarding-range
  - port-reservation
  - redundancy
    - export
    - follow
    - monitor
    - shutdown
  - shutdown
  - subscriber-limit
  - watermarks
- upstream-ip-filter
- upstream-ipv6-filter

- network
  - ingress
    - filter
    - qos
    - urpf-check

- network-interface
  - address
  - allow-directed-broadcasts
  - arp-retry-timer
  - arp-timeout
  - bfd
  - cflowd-parameters
    - sampling
  - cpu-protection
  - description
  - dist-cpu-protection
  - egress
  - egress
    - filter
  - enable-ingress-stats
  - hold-time
    - down
    - up
  - icmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn network-interface icmp mask-reply

- mask-reply
- param-problem
- redirects
- ttl-expired
- unreachables

- ingress
  - filter
- ip-mtu
- lag
- lag-link-map-profile
- lag-per-link-hash
- load-balancing
  - egr-ip-load-balancing
  - flow-label-load-balancing
  - lsr-load-balancing
  - spi-load-balancing
  - teid-load-balancing
- loopback
- mac
- port
- qos
- secondary
- shutdown
- static-arp
- tcp-mss
- tos-marking-state
- urpf-check
  - ignore-default
  - mode

- ntp
  - authenticate
  - authentication-check
  - authentication-key
  - broadcast
  - shutdown
    - snoop
      - shutdown
  - proxy-arp
  - remote-proxy-arp
  - unnumbered
  - unnumbered
- ospf
  - advertise-router-capability
  - area
    - advertise-ne-profile
    - advertise-router-capability
    - area-range
    - blackhole-aggregate
    - export
    - import
    - interface
      - advertise-router-capability

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ospf area interface advertise-subnet

- advertise-subnet
- auth-keychain
- authentication-key
- authentication-type
- **bfd-enable**
- dead-interval
- hello-interval
- interface-type
- lfa-policy-map
- load-balancing-weight
- loopfree-alternate-exclude
- lsa-filter-out
- message-digest-key
- metric
- mtu
- neighbor
- passive
- poll-interval
- priority
- retransmit-interval
- rib-priority
- shutdown
- transit-delay

- loopfree-alternate-exclude
- nssa
  - area-range
  - originate-default-route
  - redistribute-external
  - summaries
- sham-link
  - auth-keychain
  - authentication-key
  - authentication-type
  - dead-interval
  - hello-interval
  - message-digest-key
  - metric
  - retransmit-interval
  - shutdown
  - transit-delay
- stub
  - default-metric
  - summaries
- virtual-link
  - auth-keychain
  - authentication-key
  - authentication-type
  - dead-interval
  - hello-interval
  - message-digest-key
  - retransmit-interval
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ospf area virtual-link transit-delay

- transit-delay
- compatible-rfc1583
- export
- export-limit
- external-db-overflow
- external-preference
- graceful-restart
  - helper-disable
  - strict-lsa-checking
- ignore-dn-bit
- import
  - bfd-enable
- loopfree-alternates
  - exclude
    - prefix-policy
- multicast-import
- overload
- overload-include-ext-1
- overload-include-ext-2
- overload-include-stub
- overload-on-boot
- preference
- reference-bandwidth
- rib-priority
- router-id
- rtr-adv-lsa-limit
- shutdown
- super-backbone
- suppress-dn-bit
- timers
  - incremental-spf-wait
  - lsa-accumulate
  - lsa-arrival
  - lsa-generate
  - redistribute-delay
  - spf-wait
- unicast-import-disable
- vpn-domain
- vpn-tag

- ospf3
  - advertise-router-capability
  - area
    - advertise-router-capability
    - area-range
    - blackhole-aggregate
    - export
    - import
    - interface
      - advertise-router-capability
      - authentication
      - bfd-enable
      - dead-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ospf3 area interface hello-interval

- hello-interval
- interface-type
- lfa-policy-map
- load-balancing-weight
- loopfree-alternate-exclude
- lsa-filter-out
- metric
- mtu
- neighbor
- passive
- poll-interval
- priority
- retransmit-interval
- rib-priority
- shutdown
- transit-delay

- key-rollover-interval
- loopfree-alternate-exclude
- nssa
  - area-range
  - originate-default-route
  - redistribute-external
  - summaries
- stub
  - default-metric
  - summaries
- virtual-link
  - authentication
  - dead-interval
  - hello-interval
  - retransmit-interval
  - shutdown
  - transit-delay

- export
- export-limit
- external-db-overflow
- external-preference
- graceful-restart
  - helper-disable
  - strict-lsa-checking
- ignore-dn-bit
- import
- loopfree-alternates
  - exclude
    - prefix-policy
- multicast-import
- overload
- overload-include-ext-1
- overload-include-ext-2
- overload-include-stub
- overload-on-boot
- preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ospf3 reference-bandwidth

- reference-bandwidth
- rib-priority
- router-id
- rtr-adv-lsa-limit
- shutdown
- suppress-dn-bit
- timers
  - incremental-spf-wait
  - lsa-accumulate
  - lsa-arrival
  - lsa-generate
  - redistribute-delay
  - spf-wait
- unicast-import-disable

- pcp-server
  - server
    - description
    - dual-stack-lite-address
    - fwd-inside-router
    - interface
    - pcp-server-policy
    - shutdown

- pim
  - apply-bgp-nh-override
  - apply-to
  - grt-extranet
    - group-prefix
  - import
  - interface
    - assert-period
    - bfd-enable
    - bsm-check-rtr-alert
    - hello-interval
    - hello-multiplier
    - improved-assert
    - instant-prune-echo
    - ipv4-multicast-disable
    - ipv6-multicast-disable
    - max-groups
    - mcac
      - if-policy
      - mc-constraints
        - level
        - number-down
        - shutdown
        - use-lag-port-weight
      - policy
      - unconstrained-bw
    - monitor-oper-group
    - multicast-senders
    - p2mp-ldp-tree-join
    - priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn pim interface shutdown

- shutdown
- sticky-dr
- three-way-hello
- tracking-support
- ipv4-multicast-disable
- ipv6-multicast-disable
- mc-ecmp-balance
- mc-ecmp-balance-hold
- mc-ecmp-hashing-enabled
- mtu-over-head
- non-dr-attract-traffic
- rp
  - anycast
    - rp-set-peer
  - auto-rp-discovery
  - bootstrap-export
  - bootstrap-import
  - bsr-candidate
    - address
    - hash-mask-len
    - priority
    - shutdown
  - ipv6
    - anycast
      - rp-set-peer
    - bsr-candidate
      - address
      - hash-mask-len
      - priority
      - shutdown
    - embedded-rp
      - group-range
      - shutdown
    - rp-candidate
      - address
      - group-range
      - holdtime
      - priority
      - shutdown
    - static
      - address
        - group-prefix
        - override
      - group-prefix
  - rp-candidate
    - address
    - group-range
    - holdtime
    - priority
    - shutdown
  - static
    - address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn pim rp static address group-prefix

- group-prefix
- override
- group-prefix
- override
- group-prefix
- rpf-table
- rpf6-table
- shutdown
- spt-switchover-threshold
- ssm-assert-compatible-mode
- ssm-default-range-disable
- ssm-groups
- group-range
- ptp
- peer
- local-priority
- log-sync-interval
- shutdown
- peer-limit
- shutdown
- radius-proxy
- server
- attribute-matching
- entry
- type
- cache
- key
- shutdown
- timeout
- track-accounting
- track-authentication
- track-delete-hold-time
- default-accounting-server-policy
- default-authentication-server-policy
- description
- interface
- load-balance-key
- python-policy
- secret
- send-accounting-response
- shutdown
- wlan-gw
- address
- ipv6-address
- radius-server
- server
- accept-coa
- acct-port
- auth-port
- coa-script-policy
- description
- pending-requests-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn radius-server server python-policy

- **python-policy**
- reassembly-group
- redundant-interface
  - address
  - address
  - description
  - hold-time
    - down
    - up
  - ip-mtu
  - shutdown
  - shutdown
  - spoke-sdp
    - control-channel-status
      - acknowledgment
      - refresh-timer
      - request-timer
      - shutdown
    - control-word
    - description
    - egress
      - filter
      - vc-label
    - ingress
      - filter
      - vc-label
    - pw-path-id
      - agi
      - saii-type2
      - taii-type2
    - shutdown
    - shutdown
- rip
  - authentication-key
  - authentication-type
  - bfd-enable
  - check-zero
  - description
  - export
  - export-limit
  - group
    - authentication-key
    - authentication-type
    - bfd-enable
    - check-zero
    - description
    - export
    - import
    - message-size
    - metric-in
    - metric-out
    - neighbor

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn rip group neighbor authentication-key

- — authentication-key
- — authentication-type
- — bfd-enable
- — check-zero
- — description
- — export
- — import
- — message-size
- — metric-in
- — metric-out
- — preference
- — receive
- — send
- — shutdown
- — split-horizon
- — timers
- — unicast-address
- — preference
- — receive
- — send
- — shutdown
- — split-horizon
- — timers
- — import
- — message-size
- — metric-in
- — metric-out
- — preference
- — propagate-metric
- — receive
- — send
- — shutdown
- — split-horizon
- — timers
- — ripng
- — bfd-enable
- — check-zero
- — description
- — export
- — export-limit
- — group
- — bfd-enable
- — check-zero
- — description
- — export
- — import
- — message-size
- — metric-in
- — metric-out
- — neighbor
- — bfd-enable
- — check-zero

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ripng group neighbor description

- description
- export
- import
- message-size
- metric-in
- metric-out
- preference
- receive
- send
- shutdown
- split-horizon
- timers
- unicast-address
- preference
- receive
- send
- shutdown
- split-horizon
- timers
- import
- message-size
- metric-in
- metric-out
- preference
- receive
- send
- shutdown
- split-horizon
- timers
- max-advertisement
- min-advertisement
- on-link
- valid-lifetime
- router-advertisement
- dns-options
- dns-options
- rdnss-lifetime
- server
- interface
- current-hop-limit
- dns-options
- include-dns
- rdnss-lifetime
- server
- managed-configuration
- max-advertisement-interval
- min-advertisement-interval
- mtu
- other-stateful-configuration
- prefix
- autonomous
- on-link

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn router-advertisement interface prefix preferred-lifetime

- preferred-lifetime
- valid-lifetime
- reachable-time
- retransmit-time
- router-lifetime
- shutdown
- use-virtual-mac

- router-id
- sap
  - mbs
  - ais-enable
    - interface-support-enable
  - alarm-notification
    - fng-alarm-time
    - fng-reset-time
- igmp-host-tracking
  - expiry-time
  - import
    - mbs
  - encapsulated-ip-mtu
  - dest-ip
  - hs-secondary-shaper
- segment-routing-v6
  - locator
  - function
    - end-dt4
    - end-dt46
    - end-dt6
  - force-renews
- sgt-qos
  - application
  - dscp
- shutdown
- shutdown
- single-sfm-overload
- snmp
  - access
  - community
- source-address
  - application
  - application6
- spoke-sdp
  - description
    - interface-support-enable
  - hash-label
- ssm-groups
- static-route-entry
  - backup-tag
  - black-hole
    - community
    - description
    - generate-icmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn static-route-entry black-hole metric

- metric
- preference
- prefix-list
- shutdown
- tag
- community
- grt
  - description
  - metric
  - preference
  - shutdown
- indirect
  - community
  - cpe-check
    - drop-count
    - interval
    - log
    - padding-size
  - description
  - destination-class
  - forwarding-class
    - priority
  - ldp-sync
  - metric
  - preference
  - prefix-list
  - shutdown
  - source-class
  - tag
  - community
- ipsec-tunnel
  - community
  - description
  - destination-class
  - forwarding-class
    - priority
  - metric
  - preference
  - shutdown
  - source-class
  - tag
- next-hop
  - backup-next-hop
    - address
  - bfd-enable
  - community
  - cpe-check
    - drop-count
    - interval
    - log
    - padding-size
  - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn static-route-entry next-hop destination-class

- destination-class
- forwarding-class
  - priority
- load-balancing-weight
- metric
- preference
- prefix-list
- shutdown
- source-class
- tag
- validate-next-hop
- tag

- static-route-hold-down
- subscriber-interface
  - address
  - allow-unmatching-subnets
  - arp-host
    - host-limit
    - shutdown
  - bfd
  - default-dns
  - description
  - dhcp
    - client-applications
    - description
    - gi-address
    - lease-populate
    - match-circuit-id
    - offer-selection
      - client-mac
        - discover-delay
      - discover-delay
      - server
        - discover-delay
    - option
      - vendor-specific-option
        - client-mac-address
        - sap-id
        - service-id
        - string
        - system-id
    - proxy-server
      - emulated-server
      - lease-time
      - shutdown
    - python-policy
    - relay-proxy
    - release-include-gi-address
    - server
    - shutdown
    - virtual-subnet
  - dhcp6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface export-host-routes

- export-host-routes
- group-interface
  - arp-host
    - description
    - host-limit
    - min-auth-interval
    - sap-host-limit
    - shutdown
  - arp-populate
  - arp-timeout
  - authentication-policy
  - bfd
  - bonding-parameters
    - connection
      - service
    - fpe
      - connection
    - multicast
    - shutdown
  - brg
    - authenticated-brg-only
    - default-brg-profile
    - shutdown
  - cflowd-parameters
    - sampling
  - data-trigger
    - shutdown
  - description
  - dhcp
    - client-applications
    - description
    - filter
    - gi-address
    - lease-populate
    - match-circuit-id
    - offer-selection
      - client-mac
        - discover-delay
      - discover-delay
      - server
        - discover-delay
    - option
      - action
      - circuit-id
      - remote-id
      - vendor-specific-option
        - client-mac-address
        - pool-name
        - sap-id
        - service-id
        - string
        - system-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface dhcp proxy-server

- proxy-server
  - emulated-server
  - lease-time
  - shutdown
- python-policy
- relay-proxy
- release-include-gi-address
- server
- shutdown
- trusted
- user-db

- dhcp6
  - filter
  - user-db
- diameter-application-policy
- diameter-auth-policy
- enable-ingress-stats
- gtp-parameters
  - fpe
  - shutdown
- host-connectivity-verify
- icmp
  - mask-reply
  - param-problem
  - redirects
  - ttl-expired
  - unreachables
- ignore-default
- ignore-df-bit
- ingress
  - policy-accounting
- ip-mtu
- ipoe-linking
  - gratuitous-rtr-adv
  - shared-circuit-id
  - shutdown
- ipoe-session
  - description
  - force-auth
  - ipoe-session-policy
  - min-auth-interval
  - radius-session-timeout
  - sap-session-limit
  - session-limit
  - shutdown
  - stateless-redundancy
  - user-db
    - python-policy
- ipv6
  - allow-multiple-wan-addresses
  - auto-reply
    - neighbor-solicitation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface ipv6 auto-reply router-solicitation

- router-solicitation
- bfd
- dhcp6
  - filter
  - option
    - interface-id
    - remote-id
  - override-slaac
  - pd-managed-route
  - proxy-server
    - client-applications
    - emulated-server
    - preferred-lifetime
    - python-policy
    - rebind-timer
    - renew-timer
    - server-id
    - shutdown
    - valid-lifetime
  - python-policy
  - relay
    - advertise-selection
      - client-mac
        - preference-option
          - value
        - solicit-delay
      - preference-option
        - value
      - server
        - preference-option
          - value
        - solicit-delay
      - solicit-delay
    - client-applications
    - description
    - lease-split
      - shutdown
      - valid-lifetime
    - link-address
    - server
    - shutdown
    - source-address
  - snooping
    - shutdown
  - user-db
  - user-ident
- force-mcast
- include-dns
- ipoe-bridged-mode
- managed-configuration
- max-advertisement
- min-advertisement

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface ipv6 mtu

- mtu
- nd
  - dad-snooping
  - neighbor-limit
- option
- other-stateful-configuration
- prefix-options
- qos-route-lookup
- rdnss-lifetime
- router-advertisements
  - current-hop-limit
  - dns-options
    - include-dns
    - rdnss-lifetime
  - force-mcast
  - managed-configuration
  - max-advertisement
  - min-advertisement
  - mtu
  - other-stateful-configuration
  - prefix-options
    - autonomous
    - on-link
    - preferred-lifetime
    - valid-lifetime
  - reachable-time
  - retransmit-time
  - router-lifetime
  - shutdown
- router-solicit
  - inactivity-timer
  - min-auth-interval
  - shutdown
  - user-db
- urpf-check
  - mode
- local-address-assignment
  - client-application
  - default-pool
  - ipv6
    - client-application
    - server
  - server
  - shutdown
- local-proxy-arp
- mac
- oper-up-while-empty
- policy-control
- ppp
  - description
  - policy
  - session-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface ppp shutdown

- shutdown
- user-db
- pppoe
  - anti-spoof
  - anti-spoof
  - description
  - dhcp-client
    - client-id
  - policy
  - python-policy
  - sap-session-limit
  - session-limit
  - shutdown
  - user-db
- proxy-arp-policy
- qos-route-lookup
- redundant-interface
- remote-proxy-arp
- sap
- sap
  - accounting-policy
  - anti-spoof
  - anti-spoof
  - app-profile
  - atm
    - egress
      - traffic-desc
    - encapsulation
    - ingress
      - traffic-desc
    - oam
      - alarm-cells
      - periodic-loopback
    - periodic-loopback
  - calling-station-id
  - collect-stats
  - cpu-protection
  - default-host
  - description
  - dist-cpu-protection
  - egress
    - agg-rate
      - limit-unused-bandwidth
      - queue-frame-based-accounting
      - rate
    - filter
    - limit-unused-bandwidth
    - policer-control-policy
    - qinq-mark-top-only
    - qos
      - burst-limit
    - scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap eth-cfm

- eth-cfm
  - ais-enable
  - bit-error-threshold
  - ccm-enable
  - ccm-ltm-priority
  - collect-lmm-fc-stats
    - fc
    - fc-in-profile
  - collect-lmm-stats
  - eth-test-enable
    - test-pattern
  - fault-propagation-enable
  - low-priority-defect
  - mac-address
  - mep
    - ais-enable
      - interface-support-enable
      - interval
      - priority
    - alarm-notification
      - fng-alarm-time
      - fng-reset-time
    - ccm-enable
    - ccm-ltm-priority
    - ccm-padding-size
    - csf-enable
      - multiplier
    - description
    - eth-test-enable
      - bit-error-threshold
      - test-pattern
    - fault-propagation-enable
    - grace
      - eth-ed
        - max-rx-defect-window
        - priority
        - rx-eth-ed
        - tx-eth-ed
      - eth-vsm-grace
        - rx-eth-vsm-grace
        - tx-eth-vsm-grace
    - low-priority-defect
    - mac-address
    - one-way-delay-threshold
    - shutdown
  - one-way-delay-threshold
  - squelch-ingress-levels
  - tunnel-fault
- fwd-wholesale
  - pppoe
- host-lockout-policy
- host-shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap igmp-host-tracking

- igmp-host-tracking
  - disable-router-alert-check
  - expiry-time
  - import
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
  - expiry-time
  - import
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
- ingress
  - filter
  - match-qinq-dot1p
  - policer-control-policy
  - qos
  - scheduler-policy
- lag-link-map-profile
- lag-per-link-hash
- monitor-oper-group
- multi-service-site
- oper-group
- shutdown
- static-host
  - ancp-string
  - app-profile
  - inter-dest-id
  - mac-linking
  - managed-routes
    - route-entry
      - metric
      - preference
      - tag
  - retail-svc-id
  - rip-policy
  - shutdown
  - sla-profile
  - sub-profile
  - subscriber
  - subscriber-sap-id
- static-host-mgmt
  - mac-learning-options
    - data-triggered
    - single-mac
- sub-sla-mgmt
  - def-app-profile
  - def-inter-dest-id
  - def-sla-profile
  - def-sub-id
  - def-sub-profile
  - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap sub-sla-mgmt multi-sub-sap

- multi-sub-sap
- shutdown
- single-sub-parameters
  - non-sub-traffic
  - profiled-traffic-only
- sub-ident-policy

- sap-parameters
  - anti-spoof
  - description
  - sub-sla-mgmt
    - def-app-profile
    - def-sla-profile
    - def-sub-id
    - def-sub-profile
    - sub-ident-policy
- shared-circuit-id
- shcv-policy
- shcv-policy-ipv4
- shcv-policy-ipv6
- shutdown
- srrp
  - bfd-enable
  - description
  - gw-mac
  - keep-alive-interval
  - message-path
  - monitor-oper-group
  - one-garp-per-sap
  - policy
  - preempt
  - priority
  - send-fib-population-packets
  - shutdown
- srrp-enabled-routing
- suppress-aa-sub
- tos-marking-state
- urpf-check
  - mode
- wlan-gw
  - address
  - description
    - active-lease-time
    - initial-lease-time
  - egress
    - rate
    - agg-rate-limit
    - hold-time
    - qos
    - scheduler-policy
    - shape-multi-client-only
    - shaping
  - group-encryption

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface wlan-gw group-encryption encryption-keygroup

- encryption-keygroup
- gw-addresses
  - address
- l2-access-points
  - l2-ap
    - encap-type
    - epipe-sap-template
    - shutdown
- l2-ap-auto-sub-id-fmt
- l2-ap-encap-type
- learn-ap-mac
- learn-l2tp-cookie
- max-lanext-bd
- mobility
  - hold-time
  - inter-vlan
  - multi-tunnel-type
  - trigger
- oper-down-on-group-degrade
  - default-retail-svc-id
  - dhcp
  - dhcp6
    - brg
      - authenticated-brg-only
      - default-brg-profile
      - shutdown
        - description
        - filter
          - description
          - filter
          - filter
          - max-mac
          - policer
  - vlan
- router
- shutdown
- tcp-mss-adjust
- tunnel-encaps
  - learn-l2tp-cookie
    - authenticated-brg-only
    - default-brg-profile
    - shutdown
- vlan-tag-ranges
  - default-retail-svc-id
  - range
    - authenticate-on-dhcp
    - authentication
      - authentication-policy
      - hold-time
      - local
        - coa-policy
        - default-ue-state

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range data-triggered-ue-creation

- vlan-mismatch-timeout
- data-triggered-ue-creation
- dhcp
  - active-lease-time
  - initial-lease-time
  - l2-aware-ip-address
  - primary-dns
  - primary-nbns
  - secondary-dns
  - secondary-nbns
  - shutdown
- dhcp6
  - active-preferred-lifetime
  - active-valid-lifetime
  - initial-preferred-lifetime
  - initial-valid-lifetime
  - shutdown
- distributed-sub-mgmt
  - aa-url-parameter
  - accounting-policy
  - accounting-update-interval
  - collect-aa-acct-stats
  - def-app-profile
  - dsm-ip-filter
  - egress-policer
  - ingress-policer
  - one-time-redirect
  - shutdown
  - soft-quota-exhausted-filter
  - volume-quota-direction
- extensions
  - extension
- http-redirect-policy
- idle-timeout
- l2-service
  - description
  - shutdown
- nat-policy
- retail-svc-id
- slaac
  - active-preferred-lifetime
  - active-valid-lifetime
  - initial-preferred-lifetime
  - initial-valid-lifetime
  - shutdown
- track-mobility
  - mac-format
  - radius-proxy-cache
- vrgw
  - brg
    - authenticated-brg-only
    - default-brg-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect

- shutdown
- lanext
  - access
    - max-mac
    - multi-access
    - policer
  - assistive-address-resolution
  - bd-mac-prefix
  - mac-translation
  - network
    - max-mac
    - policer
    - shutdown
  - shutdown
- xconnect
  - accounting-policy
  - accounting-update-interval
  - mobility-acct-updates
  - shutdown
- wlan-gw-group
- wpp
  - description
  - enable-triggered-hosts
  - initial-app-profile
  - initial-sla-profile
  - initial-sub-profile
  - lease-time
  - portal
  - portal-group
    - shutdown
  - restore-disconnected
  - shutdown
  - user-db
- hold-time
  - down
  - up
- ip-mtu
- ipoe-linking
  - gratuitous-rtr-adv
- ipoe-session
  - session-limit
- ipv6
  - address
  - allow-multiple-wan-addresses
  - allow-unmatching-prefixes
  - allow-unmatching-subnets
  - bfd
  - default-dns
  - delegated-prefix-length
  - dhcp6
    - override-slaac
    - pd-managed-route

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface ipv6 dhcp6 proxy emulated-server

- emulated-server
- python-policy
- proxy-server
  - client-applications
  - preferred-lifetime
  - rebind-timer
  - renew-timer
  - server-id
  - shutdown
  - valid-lifetime
- python-policy
- relay
  - advertise-selection
    - client-mac
      - preference-option
        - value
      - solicit-delay
    - preference-option
      - value
    - server
      - preference-option
        - value
      - solicit-delay
    - solicit-delay
  - client-applications
  - description
  - lease-split
    - shutdown
    - valid-lifetime
  - link-address
  - server
  - shutdown
  - source-address
- ipoe-bridged-mode
- link-local-address
- router-advertisements
  - current-hop-limit
  - dns-options
    - include-dns
    - rdnss-lifetime
  - force-mcast
  - managed-configuration
  - max-advertisement
  - min-advertisement
  - mtu
  - other-stateful-configuration
  - prefix-options
    - autonomous
    - on-link
    - preferred-lifetime
    - valid-lifetime
  - reachable-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface ipv6 router-advertisements retransmit-time

- retransmit-time
- router-lifetime
- shutdown
- router-solicit
- inactivity-timer
- include-dns
- autonomous
- rdnss-lifetime
- subscriber-prefixes
- prefix
- local-address-assignment
- client-application
- default-pool
- ipv6
- client-application
- server
- server
- shutdown
- pppoe
- description
- session-limit
- shutdown
- private-retail-subnets
- python-policy
- shutdown
- unnumbered
- unnumbered
- wlan-gw
- pool-manager
- dhcpv6-client
- dhcpv4-nat
- link-addr
- pool-name
- shutdown
- ia-na
- link-addr
- pool-name
- shutdown
- lease-query
- server
- slaac
- link-addr
- pool-name
- shutdown
- source-ip
- watermarks
- wlan-gw-group
- shutdown
- shutdown
- shutdown
- redundancy
- export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface wlan-gw redundancy monitor

```
            — monitor
            — shutdown
      — subscriber-mgmt
         — multi-chassis-shunt-id
         — up-resiliency
            — monitor-oper-group
      — ttl-propagate
         — local
         — transit
      — twamp-light
         — reflector
            — allow-ipv6-udp-checksum-zero
            — description
            — prefix
               — description
            — shutdown
      — type
      — video-interface
         — accounting-policy
         — address
         — adi
            — scte30
               — ad-server
               — local-address
         — channel
            — description
            — scte35-action
            — zone-channel
         — cpu-protection
         — description
         — multicast-service
         — output-format
         — rt-client-src-address
         — shutdown
         — video-sap
            — egress
               — filter
               — qos
            — ingress
               — filter
               — qos
      — vrgw
         — lanext
            — shutdown
            — wlan-gw-group
      — vsd-domain
      — vxlan
         — tunnel-termination
      — weighted-ecmp
      — wlan-gw
         — distributed-sub-mgmt
         — distributed-sub-mgmt
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn wlan-gw distributed-sub-mgmt ipv6-tcp-mss-adjust

- ipv6-tcp-mss-adjust
- gtp-peer-clear-timeout
- gtp
  - source-ip-address-ranges
    - source-address-range
  - mobility-triggered-acct
    - interim-update
  - xconnect
    - shutdown
    - tunnel-source-ip
    - wlan-gw-group
- wpp
  - portals
    - portal
      - ack-auth-retry-count
      - ntf-logout-retry-count
      - port-format
      - retry-interval
      - secret
      - shutdown
      - version
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.39.27 configure service vsd Commands

- vsd
  - domain
    - description
    - shutdown
  - service-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.40 configure sflow Commands

- sflow
  - egress-counter-map
  - ingress-counter-map
  - receiver
    - ip-addr-backup
    - ip-addr-primary
    - max-data-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.41 configure sfm Commands

- sfm
  - sfm-type
  - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.42 configure subscriber-mgmt Commands

- subscriber-mgmt
  - accu-stats-policy
    - description
    - entry
  - ancp
    - ancp-policy
      - egress
        - rate-adjustment
        - rate-modify
        - rate-monitor
        - rate-reduction
      - ingress
        - rate-adjustment
        - rate-modify
        - rate-monitor
        - rate-reduction
      - port-down
        - disable-shcv
    - ancp-static-map
      - entry
  - authentication-origin
    - priority
  - authentication-policy
    - accept-authorization-change
    - accept-script-policy
    - coa-script-policy
    - description
    - fallback-action
    - gtp-user-name
    - include-radius-attribute
      - access-loop-options
      - acct-session-id
      - apn
      - called-station-id
      - calling-station-id
      - circuit-id
      - dhcp-options
      - dhcp-vendor-class-id
      - dhcp6-options
      - gprs-negotiated-qos-profile
      - imei
      - imsi
      - mac-address
      - msisdn
      - nas-identifier
      - nas-port
      - nas-port-id
      - nas-port-type
      - pppoe-service-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt authentication-policy include-radius-attribute rat-type

- rat-type
- remote-id
- sap-session-index
- tunnel-server-attrs
- uli
- wifi-num-attached-ues
- wifi-ssid-vlan
- xconnect-tunnel-home-address

- password
- ppp-user-name
- pppoe-access-method
- radius-authentication-server
  - access-algorithm
  - hold-down-time
  - retry
  - router
  - server
  - source-address
  - timeout
- radius-server-policy
- re-authentication
- request-script-policy
- send-acct-stop-on-fail
- user-name-format

- auto-sub-id-key
  - implicit-generation
  - ipoe-sub-id-key
  - ppp-sub-id-key
- bgp-peering-policy
  - advertise-inactive
  - aggregator-id-zero
  - as-override
  - auth-keychain
  - authentication-key
  - bfd-enable
  - cluster
  - connect-retry
  - damping
  - description
  - disable-4byte-asn
  - disable-client-reflect
  - disable-communities
  - disable-fast-external-failover
  - export
  - hold-time
  - import
  - keepalive
  - local-address
  - local-as
  - local-preference
  - loop-detect
  - med-out

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt bgp-peering-policy min-route-advertisement

- min-route-advertisement
- multihop
- next-hop-self
- passive
- peer-as
- preference
- prefix-limit
- remove-private
- ttl-security
- type
- category-map
  - activity-threshold
  - category
    - credit-type-override
    - default-credit
    - description
    - exhausted-credit-service-level
      - egress-ip-filter-entries
        - entry
          - action
          - description
          - match
            - dscp
            - dst-port
            - fragment
            - icmp-code
            - icmp-type
            - ip-option
            - multiple-option
            - option-present
            - src-ip
            - src-port
            - tcp-ack
            - tcp-syn
      - egress-ipv6-filter-entries
        - entry
          - action
          - description
          - match
            - dscp
            - dst-port
            - icmp-code
            - icmp-type
            - src-ip
            - src-port
            - tcp-ack
            - tcp-syn
      - ingress-ip-filter-entries
        - entry
          - action
          - **description**
          - match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match dscp

- dscp
- dst-ip
- dst-port
- fragment
- icmp-code
- icmp-type
- ip-option
- multiple-option
- option-present
- src-port
- tcp-ack
- tcp-syn

- ingress-ipv6-filter-entries
  - entry
    - action
    - description
    - match
      - dscp
      - dst-ip
      - dst-port
      - icmp-code
      - icmp-type
      - src-port
      - tcp-ack
      - tcp-syn
    - pir
  - out-of-credit-action-override
  - policer
  - queue
  - rating-group
- credit-exhaust-threshold
- credit-type
- description
- gx-session-level-usage

- credit-control-policy
  - credit-control-server
  - default-category-map
  - description
  - error-handling-action
  - out-of-credit-action
- diameter-application-policy
  - application
  - description
  - diameter-node
  - diameter-peer-policy
  - gx
    - 3gpp-qos-mapping
      - apn-ambr-dl
      - apn-ambr-ul
    - avp-subscription-id
    - ccrt-replay
      - interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt diameter-application-policy gx ccrt-replay interval

- interval
- max-lifetime
- shutdown
- credit-mcs-interval
- dest-realm-learning
- features
  - extended-bw
- include-avp
  - an-gw-address
  - apn-ambr
  - called-station-id
  - calling-station-id
  - ip-can-type
  - logical-access-id
  - nas-port
  - nas-port-id
  - nas-port-type
  - pdn-connection-id
  - physical-access-id
  - rai
  - rat-type
  - sgsn-mcc-mnc
  - supported-features
  - user-equipment-info
  - user-location-info
- mac-format
- report-ip-address-event

- gy
  - avp-subscription-id
  - ccrt-replay
    - interval
    - interval
    - max-lifetime
    - shutdown
  - dest-realm-learning
  - extended-failure-handling
    - interim-credit
      - max-attempts
      - reporting
      - validity-time
      - volume
    - new-session-id
    - shutdown
  - include-avp
    - 3gpp-charging-characteristics
    - 3gpp-charging-id
    - 3gpp-ggsn-address
    - 3gpp-ggsn-ipv6-address
    - 3gpp-gprs-negotiated-qos-profile
    - 3gpp-imsi
    - 3gpp-nsapi
    - 3gpp-rat-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-selection-mode

- 3gpp-selection-mode
- 3gpp-session-stop-indicator
- 3gpp-user-location-info
- address-avp
- called-station-id
- charging-rule-base-name
- ggsn-address
- pdp-context-type
- ps-information
- radius-user-name
- service-context-id
- user-equipment-info
- mac-format
- out-of-credit-reporting
- vendor-support

- nasreq
  - include-avp
    - called-station-id
    - calling-station-id
    - circuit-id
    - imei
    - nas-port
    - nas-port-id
    - nas-port-type
    - rat-type
    - remote-id
    - user-location-info
  - mac-format
  - password
  - user-name-format
  - user-name-operation
- on-failure
- on-failure
- tx-timer

- explicit-subscriber-map
  - entry
- group-interface-statistics
  - shutdown
- group-interface-template
  - description
  - ip-mtu
  - ipv4
    - icmp
      - mask-reply
      - param-problem
      - redirects
      - ttl-expired
      - unreachables
    - proxy-arp-policy
    - remote-proxy-arp
    - urpf-check
      - mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt group-interface-template ipv6

- **ipv6**
  - **urpf-check**
    - **mode**
- gtp
  - apn-policy
    - apn
      - ambr-qos-mapping
        - downlink
        - uplink
      - defaults
        - group-interface
      - diameter-auth-policy
      - radius-auth-policy
      - skip-gtp-ipv4-alloc
      - user-db
  - max-held-sessions
  - peer-profile
    - change-reporting-action
    - charging-characteristics
      - home
      - roaming
    - description
    - end-marker-count
    - ggsn
      - qos
        - ambr
        - arp
        - down-link
        - up-link
    - interface-type
    - ip-ttl
    - ipv4-mtu
    - keep-alive
    - message-retransmit
    - mme
      - qos
        - ambr
        - arp
        - down-link
        - qci
        - up-link
    - pgw
      - qos
        - ambr
        - arp
        - down-link
        - qci
        - up-link
    - protocol-configuration-options
    - python-policy
    - rat-type
    - report-wlan-location

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt gtp peer-profile session-hold-time

- session-hold-time
- serving-network
- host-lockout-policy
  - description
  - host-key
  - lockout-reset-time
  - lockout-time
  - max-lockout-hosts
  - description
- host-tracking-policy
  - description
  - egress-rate-modify
- http-redirect-policy
  - aa-url-parameter
  - application-assurance
  - description
  - dst-port
  - forward-entries
    - dst-ip
  - ignore-app-profile
  - portal-hold-time
  - url
- igmp-policy
  - description
  - disable-router-alert-check
  - egress-rate-modify
  - fast-leave
  - import
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
  - mcast-reporting
    - mcast-reporting-dest
    - opt-reporting-fields
    - shutdown
  - per-host-replication
  - per-spi-replication
  - query-interval
  - query-last-member-interval
  - query-response-interval
  - redirection-policy
  - source
  - starg
  - static
    - group
      - source
      - starg
  - version
- ipoe-session-policy
  - circuit-id-from-auth
  - description
  - session-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt ipoe-session-policy session-timeout

- session-timeout
- isa-filter
  - default-action
  - description
  - entry
    - action
    - description
    - match
      - dst-ip
      - dst-port
      - src-ip
      - src-port
  - ipv6
    - default-action
    - entry
      - action
      - description
      - match
        - dst-ip
        - dst-port
        - src-ip
        - src-port
- isa-policer
  - action
  - adaptation-rule
  - cbs
  - description
  - mbs
  - rate
- isa-service-chaining
  - evpn
    - bgp
      - route-distinguisher
      - route-target
    - description
    - export
      - gw-address-range
      - ip-advertise-routes
        - pool
        - shutdown
      - vxlan
    - shutdown
  - mac-prefix
  - vas-filter
    - description
    - entry
      - action
        - fail-action
        - forward
        - insert-nsh
          - meta-data
            - insert-subscriber-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt isa-service-chaining vas-filter entry action insert-nsh meta-data opaque-data

- opaque-data
- svc-path
- description
- match
  - foreign-ip
  - foreign-port
  - protocol
- shutdown
- shutdown

- local-user-db
  - description
  - ipoe
    - host
      - acct-policy
      - address
      - auth-domain-name
      - auth-policy
      - diameter-application-policy
      - diameter-auth-policy
      - gi-address
      - host-identification
        - circuit-id
        - derived-id
        - encap-tag-range
        - encap-tag-separate-range
        - ip-prefix
        - mac
        - option60
        - remote-id
        - sap-id
        - service-id
        - string
        - system-id
      - identification-strings
        - ancp-string
        - app-profile-string
        - category-map-name
        - inter-dest-id
        - sla-profile-string
        - spi-sharing-group-id
        - sub-profile-string
        - subscriber-id
      - interface
      - ipv6-address
      - ipv6-delegated-prefix
      - ipv6-delegated-prefix-length
      - ipv6-delegated-prefix-pool
      - ipv6-lease-times
        - preferred-lifetime
        - rebind-timer
        - renew-timer
        - valid-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt local-user-db ipoe host ipv6-slaac-prefix

- ipv6-slaac-prefix
- ipv6-slaac-prefix-pool
- ipv6-wan-address-pool
- link-address
- match-radius-proxy-cache
  - fail-action
  - mac-format
  - match
  - server
- mld-parameters
  - import
- msap-defaults
  - group-interface
  - policy
  - service
- options
  - custom-option
  - default-router
  - dns-server
  - domain-name
  - lease-rebind-time
  - lease-renew-time
  - lease-time
  - netbios-name-server
  - netbios-node-type
  - subnet-mask
- options6
  - dns-server
- retail-service-id
- rip-policy
- router-advertisement-policy
- server
- server6
- shutdown
- to-client-options
  - ipv4
    - option
  - ipv6
    - option
- to-server-options
  - ipv6
    - option
- wpp
  - initial-app-profile
  - initial-sla-profile
  - initial-sub-profile
  - portal
  - portal-group
  - restore-disconnected
- mask
- match-list
- ppp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt local-user-db ppp host

- host
  - access-loop-encapsulation
    - encap-offset
    - rate-down
  - access-loop-information
    - circuit-id
    - remote-id
  - acct-policy
  - address
  - auth-policy
  - diameter-application-policy
  - diameter-auth-policy
  - force-ipv6cp
  - host-identification
    - circuit-id
    - derived-id
    - encap-tag-range
    - encap-tag-separate-range
    - mac
    - remote-id
    - sap-id
    - service-name
    - username
  - identification-strings
    - ancp-string
    - app-profile-string
    - category-map-name
    - inter-dest-id
    - sla-profile-string
    - spi-sharing-group-id
    - sub-profile-string
    - subscriber-id
  - ignore-df-bit
  - interface
  - ipv6-address
  - ipv6-delegated-prefix
  - ipv6-delegated-prefix-length
  - ipv6-delegated-prefix-pool
  - ipv6-lease-times
    - preferred-lifetime
    - rebind-timer
    - renew-timer
    - valid-lifetime
  - ipv6-slaac-prefix
  - ipv6-slaac-prefix-pool
  - ipv6-wan-address-pool
  - l2tp
    - group
  - mld-parameters
    - import
  - msap-defaults
    - group-interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt local-user-db ppp host msap-defaults policy

- policy
- service
- options
  - custom-option
  - dns-server
  - netbios-name-server
- options6
  - dns-server
- padi-auth-policy
- pado-delay
- password
- pre-auth-policy
- retail-service-id
- rip-policy
- router-advertisement-policy
- shutdown
- steering-profile
- to-client-options
  - ipv6
    - option
- user-db
- mask
- match-list
- shutdown
- mld-policy
- description
- disable-router-alert-check
- egress-rate-modify
- fast-leave
- import
- max-num-groups
- max-num-grp-sources
- max-num-sources
- per-host-replication
- per-spi-replication
- query-interval
- query-last-listener-interval
- query-response-interval
- redirection-policy
- static
  - group
    - source
    - starg
- version
- msap-policy
- atm
  - egress
    - traffic-desc
  - ingress
    - traffic-desc
  - oam
    - alarm-cells

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt msap-policy atm oam periodic-loopback

- periodic-loopback
- cpu-protection
- description
- dist-cpu-protection
- ies-vprn-only-sap-parameters
  - anti-spoof
  - egress
    - qos
  - ingress
    - qos
- igmp-host-tracking
  - expiry-time
  - import
  - max-num-groups
  - max-num-grp-sources
  - max-num-sources
- lag-link-map-profile
- sticky-msaps
- sub-sla-mgmt
  - def-app-profile
  - def-inter-dest-id
  - def-sla-profile
  - def-sub-id
  - def-sub-profile
  - multi-sub-sap
  - single-sub-parameters
    - non-sub-traffic
    - profiled-traffic-only
  - sub-ident-policy
- vpls-only-sap-parameters
  - arp-host
    - host-limit
    - min-auth-interval
  - arp-reply-agent
  - dhcp
    - lease-populate
    - option
      - action
      - circuit-id
      - remote-id
      - vendor-specific-option
        - client-mac-address
        - sap-id
        - service-id
        - string
        - system-id
    - proxy-server
      - emulated-server
      - lease-time
      - shutdown
  - egress
    - qos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping

- igmp-snooping
  - fast-leave
  - import
  - last-member-query-interval
  - max-num-groups
  - mcac
    - if-policy
    - mc-constraints
      - level
      - number-down
      - use-lag-port-weight
    - policy
    - unconstrained-bw
  - mvr
    - from-vpls
  - query-interval
  - query-response-interval
  - robust-count
  - send-queries
  - version
- ingress
  - qos
- mac-da-hashing
- split-horizon-group

- pfcp-association
  - association-setup-retry
  - description
  - heartbeat
    - interval
    - retries
    - timeout
  - interface
  - nat
    - nat-group
  - node-id
  - path-restoration-time
  - peer
  - release-timeout
  - shutdown
  - tx
    - retries
    - timeout
    - ttl
- pim-policy
  - description
- ppp-policy
  - default-pap-password
  - default-user-name
  - description
  - disable-cookies
  - force-ppp-mtu-gt-1492
  - ipcp-subnet-negotiation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt ppp-policy keepalive

- keepalive
- lcp-ignore-identifier
- lcp-ignore-magic-numbers
- max-sessions-per-cid
- max-sessions-per-mac
- mlppp
  - accept-mrru
  - endpoint
  - short-sequence-numbers
- ncp-renegotiation
- pado-ac-name
- pado-delay
- ppp-authentication
- ppp-chap-challenge-length
- ppp-initial-delay
- ppp-mtu
- ppp-options
  - custom-option
- re-establish-session
- reject-disabled-ncp
- reply-on-padt
- session-timeout
- sid-allocation
- unique-sid-per-sap

- pppoe-client-policy
  - description
  - keepalive
  - mru
  - mtu
  - python-policy
  - restart-backoff
  - stack
- radius-accounting-policy
  - acct-request-script-policy
  - acct-tunnel-connection-fmt
  - custom-record
    - queue
      - e-counters
        - all
        - in-profile-octets-discarded-count
        - in-profile-octets-forwarded-count
        - in-profile-packets-discarded-count
        - in-profile-packets-forwarded-count
        - out-profile-octets-discarded-count
        - out-profile-octets-forwarded-count
        - out-profile-packets-discarded-count
        - out-profile-packets-forwarded-count
      - i-counters
        - all
        - all-octets-offered-count
        - all-packets-offered-count
        - high-octets-discarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters high-octets-offered-count

- high-octets-offered-count
- high-packets-discarded-count
- high-packets-offered-count
- in-profile-octets-forwarded-count
- in-profile-packets-forwarded-count
- low-octets-discarded-count
- low-octets-offered-count
- low-packets-discarded-count
- low-packets-offered-count
- out-profile-octets-forwarded-count
- out-profile-packets-forwarded-count
- uncoloured-octets-offered-count
- uncoloured-packets-offered-count

- ref-queue
  - e-counters
    - all
    - in-profile-octets-discarded-count
    - in-profile-octets-forwarded-count
    - in-profile-packets-discarded-count
    - in-profile-packets-forwarded-count
    - out-profile-octets-discarded-count
    - out-profile-octets-forwarded-count
    - out-profile-packets-discarded-count
    - out-profile-packets-forwarded-count
  - i-counters
    - all
    - all-octets-offered-count
    - all-packets-offered-count
    - high-octets-discarded-count
    - high-octets-offered-count
    - high-packets-discarded-count
    - high-packets-offered-count
    - in-profile-octets-forwarded-count
    - in-profile-packets-forwarded-count
    - low-octets-discarded-count
    - low-octets-offered-count
    - low-packets-discarded-count
    - low-packets-offered-count
    - out-profile-octets-forwarded-count
    - out-profile-packets-forwarded-count
    - uncoloured-octets-offered-count
    - uncoloured-packets-offered-count
  - significant-change
- delay-start-time
- description
- host-accounting
- include-radius-attribute
  - access-loop-options
  - acct-authentic
  - acct-delay-time
  - alc-acct-triggered-reason
  - alc-error-code

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt radius-accounting-policy include-radius-attribute all-authorized-session-addresses

- all-authorized-session-addresses
- apn
- bearer-fteid
- bonding-active-connections
- bonding-id
- brg-num-active-sessions
- called-station-id
- calling-station-id
- circuit-id
- delegated-ipv6-prefix
- detailed-acct-attributes
- dhcp-vendor-class-id
- firewall-info
- framed-interface-id
- framed-ip-addr
- framed-ip-netmask
- framed-ipv6-prefix
- framed-ipv6-route
- framed-route
- imei
- imsi
- ipv6-address
- lanext-bridge-id
- lanext-device-type
- lanext-route-distinguisher
- lanext-route-target
- lanext-vni
- mac-address
- msisdn
- nas-identifier
- nas-port
- nas-port-id
- nas-port-type
- nat-port-range
- remote-id
- sla-profile
- spi-sharing-id
- std-acct-attributes
- steering-profile
- sub-profile
- subscriber-id
- tunnel-client-attrs
- tunnel-server-attrs
- uli
- user-name
- v6-aggregate-stats
- wifi-num-attached-ues
- wifi-rssi
- wifi-ssid-vlan
- xconnect-tunnel-home-address

- mcs-interval
- queue-instance-accounting

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt radius-accounting-policy radius-accounting-server

- **radius-accounting-server**
  - access-algorithm
  - retry
  - router
  - server
  - source-address
  - timeout
- radius-server-policy
- session-accounting
- session-id-format
- triggered-updates
  - gtp-mobility
- update-interval
- update-interval-jitter

- rip-policy
  - authentication-key
  - authentication-type
  - description
- router-advertisement-policy
  - current-hop-limit
  - dns-options
    - include-dns
    - rdnss-lifetime
  - force-mcast
  - managed-configuration
  - max-advertisement
  - min-advertisement
  - mtu
  - other-stateful-configuration
  - prefix-options
    - stateful
      - auto-lifetimes
      - on-link
      - preferred-lifetime
      - valid-lifetime
    - stateless
      - on-link
      - preferred-lifetime
      - valid-lifetime
  - reachable-time
  - retransmit-time
  - router-lifetime
- sap-template
  - cpu-protection
  - description
  - dist-cpu-protection
  - hold-time
- shcv-policy
  - **description**
  - layer-3
    - source-ip-origin
    - unnumbered-source-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt shcv-policy periodic

- periodic
  - action
  - interval
  - retry-count
  - shutdown
  - timeout
- trigger
  - retry-count
  - shutdown
  - timeout
- vpls
  - source-ip
  - source-mac

- sla-profile
- category-map
  - category
    - idle-timeout
    - idle-timeout-action
- control
  - cups
  - local
- credit-control-policy
- def-instance-sharing
- description
- egress
  - bonding-selection
    - rate-thresholds
    - weight
  - hs-agg-rate-limit
  - ip-filter
  - ipv6-filter
  - qos
    - hs-queue-stat-mode
    - hs-wrr-group
      - hs-class-weight
      - rate
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - rate
      - stat-mode
    - queue
      - avg-frame-overhead
      - cbs
      - high-prio-only
      - hs-class-weight
      - hs-wred-queue-policy
      - hs-wrr-weight
      - mbs
      - rate
      - stat-mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt sla-profile egress qos-marking-from-sap

- qos-marking-from-sap
- report-rate
- scheduler-policy
  - scheduler
- use-ingress-l2tp-dscp

- host-limits
  - ipv4-arp
  - ipv4-dhcp
  - ipv4-overall
  - ipv4-ppp
  - ipv6-overall
  - ipv6-pd-ipoe-dhcp
  - ipv6-pd-overall
  - ipv6-pd-ppp-dhcp
  - ipv6-wan-ipoe-dhcp
  - ipv6-wan-ipoe-slaac
  - ipv6-wan-overall
  - ipv6-wan-ppp-dhcp
  - ipv6-wan-ppp-slaac
  - lac-overall
  - overall
  - remove-oldest
- ingress
  - ip-filter
  - ipv6-filter
  - qos
    - policer
      - cbs
      - mbs
      - packet-byte-offset
      - rate
      - stat-mode
    - queue
      - cbs
      - high-prio-only
      - mbs
      - rate
      - stat-mode
  - report-rate
- one-time-http-redirection
- pfcp-mappings
  - session-qer
    - downlink-mbr-gbr
    - uplink-mbr-gbr
- session-limits
  - ipoe
  - l2tp-lns
  - l2tp-lts
  - l2tp-overall
  - overall
  - pppoe-lac
  - pppoe-local

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt sla-profile session-limits pppoe-overall

- pppoe-overall
- steering-profile
  - access
  - description
  - network
- sub-ident-policy
  - app-profile-map
    - entry
    - use-direct-map-as-default
  - description
  - primary
    - script-url
    - shutdown
  - secondary
    - script-url
    - shutdown
  - sla-profile-map
    - entry
    - use-direct-map-as-default
  - strings-from-option
  - sub-profile-map
    - entry
    - use-direct-map-as-default
  - tertiary
    - script-url
    - shutdown
- sub-mcac-policy
  - description
  - shutdown
  - unconstrained-bw
- sub-profile
  - accounting-policy
  - accu-stats-policy
  - ancp
    - ancp-policy
  - collect-stats
  - control
    - cups
    - local
  - description
  - egress
    - agg-rate-limit
    - agg-rate-limit
    - encap-offset
    - hs-agg-rate-limit
    - hs-low-burst-max-class
    - lag-per-link-hash
    - policer-control-policy
      - max-rate
      - priority-mbs-thresholds
        - min-thresh-separation
        - priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt sub-profile egress policer-control-policy priority-mbs-thresholds priority mbs-contribution

— mbs-contribution
— scheduler-policy
— scheduler
— firewall-policy
— host-limits
— ipv4-arp
— ipv4-dhcp
— ipv4-overall
— ipv4-ppp
— ipv6-overall
— ipv6-pd-ipoe-dhcp
— ipv6-pd-overall
— ipv6-pd-ppp-dhcp
— ipv6-wan-ipoe-dhcp
— ipv6-wan-ipoe-slaac
— ipv6-wan-overall
— ipv6-wan-ppp-dhcp
— ipv6-wan-ppp-slaac
— lac-overall
— overall
— host-tracking-policy
— hs-sla-mode
— igmp-policy
— ingress
— policer-control-policy
— max-rate
— priority-mbs-thresholds
— min-thresh-separation
— priority
— mbs-contribution
— scheduler-policy
— scheduler
— mld-policy
— nat-access-mode
— nat-allow-bypass
— nat-policy
— nat-prefix-list
— pim-policy
— preference
— radius-accounting
— policy
— session-optimized-stop
— secondary-shaper-hashing
— session-limits
— ipoe
— l2tp-lns
— l2tp-lts
— l2tp-overall
— overall
— pppoe-lac
— pppoe-local
— pppoe-overall

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt sub-profile sla-profile-map

- sla-profile-map
  - entry
  - use-direct-map-as-default
- sub-mcac-policy
- upnp-policy
- volume-stats-type
- vport-hashing
- subscriber-interface-statistics
  - shutdown
- svlan-statistics
  - shutdown
- system-behavior
  - legacy-dns-nbns
- up-resiliency
  - fate-sharing-group-template
    - description
    - gratuitous-arp
    - redundant-interface
    - uplink-forwarding-while-standby
- vrgw
  - brg
    - brg-profile
      - connectivity-verification
      - description
      - dhcp-pool
        - lease-time
        - options
          - custom-option
        - standby-ip-lifetime
        - subnet
      - hold-time
      - initial-hold-time
      - radius-authentication
        - password
        - radius-server-policy
      - radius-proxy-server
      - radius-server-policy
      - sla-profile-string
      - sub-profile-string
      - uplink-initial-wait
  - lanext
    - router-target-as-number
- wlan-gw
  - distributed-sub-mgmt
  - tunnel-query
    - address-type
    - ap-mac-learn-failed
    - calculate-counts
    - l2-inner-vlan
    - l2-outer-vlan
    - l2-sap
    - local-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt wlan-gw tunnel-query max-num-ue

- max-num-ue
- min-num-ue
- remote-address
- router
- type
  - gre
  - l2
  - l2tp
  - vxlan
- ue-state
  - dsm
  - esm
  - l2w
  - migrant
  - xcon

- ue-query
  - address-type
  - bd
  - dhcp6-address
  - ipv4-address
  - mac-address
  - slaac-prefix
  - soft-quota-exhausted
  - state
    - already-signed-in
    - authorized-only
    - cross-connect
    - data-triggered
    - delete-pending
    - dhcp-triggered
    - dsm
    - esm
    - gtp-authorized
    - ip-assigned
    - ip-assigned-authorized
    - l2
    - portal
  - tunnel-local-address
  - tunnel-remote-address
  - tunnel-router
  - tunnel-type
  - vlan
  - wlan-gw-group
- virtual-chassis-identifier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.43 configure system Commands

- **system**
  - alarm-contact-in-power
  - alarm-contact-input
    - clear-alarm-msg
    - description
    - normal-state
    - shutdown
    - trigger-alarm-msg
  - alarms
    - max-cleared
    - shutdown
  - allow-boot-license-violations
  - atm
    - atm-location-id
    - oam
      - loopback-period
      - retry-down
      - retry-up
  - bluetooth
    - advertising-timeout
    - device
      - description
    - module
      - identifier
    - pairing-button
    - passkey
    - power
  - boot-bad-exec
  - boot-good-exec
  - chassis-mode
  - clli-code
  - config-backup
  - **congestion-management**
  - contact
  - coordinates
  - cpm-http-redirect
    - optimized-mode
      - cbs
  - cron
    - schedule
      - count
      - day-of-month
      - description
      - end-time
      - hour
      - interval
      - minute
      - month
      - script-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system cron schedule shutdown

- shutdown
- type
- weekday

- dhcp6
  - adv-noaddrs-global
- dns
  - address-pref
  - dnssec
    - ad-validation
- enable-icmp-vse
- ethernet
  - efm-oam
    - dying-gasp-tx-on-reset
    - grace-tx-enable
  - new-qinq-untagged-sap
- file-transmission-profile
  - ipv4-source-address
  - ipv6-source-address
  - redirection
  - retry
  - router
  - timeout
- grpc
  - allow-unsecure-connection
  - gnmi
    - auto-config-save
    - shutdown
  - gnoi
    - cert-mgmt
      - shutdown
    - file
      - shutdown
    - system
      - shutdown
  - max-msg-size
  - md-cli
    - shutdown
  - rib-api
    - purge-timeout
    - shutdown
  - shutdown
  - tcp-keepalive
    - idle-time
    - interval
    - retries
    - shutdown
  - tls-server-profile
- grpc-tunnel
  - destination-group
    - allow-unsecure-connection
    - description
    - destination

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system grpc-tunnel destination-group destination local-source-address

- local-source-address
- originated-qos-marking
- router-instance
- tcp-keepalive
  - idle-time
  - interval
  - retries
  - shutdown
- tls-client-profile
- tunnel
  - description
  - destination-group
  - handler
    - port
    - shutdown
    - target-type
  - shutdown
  - target-name
- ip
  - allow-qinq-network-interface
  - enforce-unique-if-index
  - forward-6in4
  - forward-ip-over-gre
  - ipv6-eh
  - mpls
    - label-stack-statistics-count
- l2tp
  - non-multi-chassis-tunnel-id-range
- lacp-system-priority
- lldp
  - message-fast-tx
  - message-fast-tx-init
  - notification-interval
  - reinit-delay
  - shutdown
  - tx-credit-max
  - tx-hold-multiplier
  - tx-interval
- load-balancing
  - l2tp-load-balancing
  - l4-load-balancing
  - lsr-load-balancing
  - mc-enh-load-balancing
  - service-id-lag-hashing
  - system-ip-load-balancing
- location
- login-control
  - exponential-backoff
  - ftp
    - inbound-max-sessions
  - idle-timeout
  - login-banner

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system login-control login-scripts

- login-scripts
  - global
  - per-user
- motd
- pre-login-message
- ssh
  - disable-graceful-shutdown
  - inbound-max-sessions
  - outbound-max-sessions
  - ttl-security
- telnet
  - enable-graceful-shutdown
  - inbound-max-sessions
  - outbound-max-sessions
  - ttl-security

- management-interface
- cli
  - classic-cli
    - allow-immediate
  - cli-engine
  - md-cli
    - auto-config-save
    - environment
      - command-completion
        - enter
        - space
        - tab
      - console
        - length
        - width
      - message-severity-level
        - cli
      - more
      - progress-indicator
        - delay
        - shutdown
        - type
      - prompt
        - context
        - newline
        - timestamp
        - uncommitted-changes-indicator
      - time-display
      - **time-format**
- configuration-mode
- operations
  - global-timeouts
    - asynchronous-execution
    - asynchronous-retention
    - synchronous-execution
- remote-management
  - allow-unsecure-connection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system management-interface remote-management client-tls-profile

- client-tls-profile
- connection-timeout
- device-label
- device-name
- hello-interval
- manager
  - allow-unsecure-connection
  - client-tls-profile
  - connection-timeout
  - description
  - device-label
  - device-name
  - manager-address
  - manager-port
  - router
  - shutdown
  - source-address
  - source-port
- router
- shutdown
- source-address
- source-port
- schema-path
- yang-modules
  - base-r13-modules
  - nmda
    - nmda-support
  - nokia-combined-modules
  - nokia-submodules
- monitor-filter-door
- name
- netconf
  - auto-config-save
  - capabilities
    - candidate
    - writable-running
  - port
  - shutdown
- network-element-discovery
  - generate-traps
  - profile
    - neid
    - neip
      - ipv4
      - ipv6
    - platform-type
    - system-mac
    - vendor-id
- ospf-dynamic-hostnames
- persistence
  - ancp
    - description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system persistence ancp location

- location
- application-assurance
  - description
  - location
  - shutdown
- dhcp-server
  - description
  - location
  - shutdown
  - shutdown
- nat-port-forwarding
  - description
  - location
- options
  - dhcp-leasetime-threshold
- python-policy-cache
  - description
  - location
  - shutdown
- subscriber-mgmt
  - description
  - location
  - shutdown
- port-topology
  - port
- power-management
  - mode
  - pcm
  - peq
    - input-power-mode
    - peq-type
    - shutdown
  - power-safety-alert
  - power-safety-level
- power-shelf
  - description
  - power-module
    - power-module-type
    - shutdown
  - power-shelf-type
  - shutdown
- power-supply
- ptp
  - anno-rx-timeout
  - clock-type
  - domain
  - local-priority
  - log-anno-interval
  - network-type
  - peer
    - local-priority
    - log-sync-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system ptp peer shutdown

- shutdown
- peer-limit
- port
  - address
  - local-priority
  - log-delay-interval
  - log-sync-interval
  - master-only
  - shutdown
- priority1
- priority2
- profile
- ptsf
  - monitor-ptsf-unusable
    - shutdown
- shutdown
- tx-while-sync-uncertain

- rollback
  - local-max-checkpoints
  - remote-max-checkpoints
  - rescue-location
  - rollback-location

- satellite
  - eth-sat
    - client-down-delay
    - description
    - enable-console-access
    - feature
    - mac-address
    - port-map
    - ptp-tc
    - sat-type
    - shutdown
    - software-repository
    - sync-e
  - file-transfer
  - local-forward
    - description
    - sap
      - description
      - shutdown
    - shutdown
  - port-template
    - description
    - port
      - role
      - uplink
    - shutdown
  - tdm-sat
    - description
    - mac-address
    - sat-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system satellite tdm-sat shutdown

- shutdown
- software-repository
- sync-e

- script-control
  - script
    - description
    - location
    - shutdown
  - script-policy
    - expire-time
    - lifetime
    - lock-override
    - max-completed
    - results
    - script
    - shutdown
- security
  - cli-script
    - authorization
      - cron
        - cli-user
      - event-handler
        - cli-user
      - vsd
        - cli-user
    - cli-session-group
      - combined-max-sessions
      - description
      - ssh-max-sessions
      - telnet-max-sessions
    - copy
    - cpm-filter
      - default-action
      - ip-filter
        - entry
          - action
          - description
          - log
          - match
            - dscp
            - dst-ip
            - dst-port
            - fragment
            - icmp-code
            - icmp-type
            - ip-option
            - multiple-option
            - option-present
            - port
            - router
            - src-ip
            - src-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security cpm-filter ip-filter entry match tcp-ack

- tcp-ack
- tcp-syn
- renum
- shutdown
- ipv6-filter
  - entry
    - action
    - description
    - log
    - match
      - dscp
      - dst-ip
      - dst-port
      - flow-label
      - fragment
      - hop-by-hop-opt
      - icmp-code
      - icmp-type
      - port
      - router
      - src-ip
      - src-port
      - tcp-ack
      - tcp-syn
    - renum
    - shutdown
- mac-filter
  - entry
    - action
    - description
    - log
    - match
      - cfm-opcode
      - dsap
      - dst-mac
      - etype
      - src-mac
      - ssap
      - svc-id
    - shutdown
  - renum
  - shutdown
- cpm-queue
  - queue
    - cbs
    - mbs
    - rate
- cpu-protection
  - ip-src-monitoring
    - included-protocols
      - dhcp
      - gtp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security cpu-protection ip-src-monitoring included-protocols icmp

- icmp
- igmp
- link-specific-rate
- policy
  - alarm
  - description
  - eth-cfm
    - entry
  - out-profile-rate
  - overall-rate
  - per-source-parameters
    - ip-src-monitoring
      - limit-dhcp-ci-addr-zero
  - per-source-rate
- port-overall-rate
- protocol-protection

- dist-cpu-protection
  - policy
    - description
    - local-monitoring-policer
      - description
      - exceed-action
      - log-events
      - rate
    - protocol
      - dynamic-parameters
        - detection-time
        - exceed-action
        - log-events
        - rate
      - enforcement
    - static-policer
      - description
      - detection-time
      - exceed-action
      - log-events
      - rate

- dot1x
  - radius-plcy
    - retry
    - server
    - shutdown
    - source-address
    - timeout
  - shutdown

- ftp-server

- keychain
  - description
  - direction
    - bi
      - entry
        - begin-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security keychain direction bi entry description

- description
- option
- shutdown
- tolerance
- uni
  - receive
    - entry
      - begin-time
      - description
      - end-time
      - shutdown
      - tolerance
  - send
    - entry
      - begin-time
      - description
      - shutdown
- shutdown
- tcp-option-number
  - receive
  - send
- ldap
  - public-key-authentication
  - retry
  - route-preference
  - server
    - address
    - bind-authentication
    - ldap-server
    - search
    - shutdown
    - tls-profile
  - shutdown
  - timeout
  - use-default-template
- management
  - allow-ftp
  - allow-grpc
  - allow-netconf
  - allow-ssh
  - allow-telnet
  - allow-telnet6
- management-access-filter
  - ip-filter
    - default-action
    - entry
      - action
      - description
      - dst-port
      - l4-src-port
      - log
      - protocol

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security management-access-filter ip-filter entry router

- router
- src-ip
- src-port
- renum
- shutdown

- ipv6-filter
  - default-action
  - entry
    - action
    - description
    - dst-port
    - flow-label
    - l4-src-port
    - log
    - next-header
    - router
    - src-ip
    - src-port
  - renum
  - shutdown

- mac-filter
  - default-action
  - entry
    - action
    - description
    - log
    - match
      - cfm-opcode
      - dot1p
      - dsap
      - dst-mac
      - etype
      - snap-oui
      - snap-pid
      - src-mac
      - ssap
      - svc-id
  - renum
  - shutdown

- management-interface
  - classic-cli
    - read-algorithm
    - write-algorithm
  - grpc
    - hash-algorithm
  - md-cli
    - command-accounting-during-load
    - hash-algorithm
  - netconf
    - hash-algorithm
  - output-authorization
    - md-interfaces

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security management-interface output-authorization telemetry-data

- telemetry-data
- password
  - admin-password
  - aging
  - attempts
  - authentication-order
  - complexity-rules
    - allow-user-name
    - credits
    - minimum-classes
    - minimum-length
    - repeated-characters
    - required
  - dynsvc-password
  - enable-admin-control
    - tacplus-map-to-priv-lvl
  - hashing
  - health-check
  - history-size
  - minimum-age
  - minimum-change
  - vsd-password
- per-peer-queuing
- pki
  - ca-profile
    - auto-crl-update
      - crl-urls
        - url-entry
          - file-transmission-profile
          - url
      - periodic-update-interval
      - pre-update-time
      - retry-interval
      - schedule-type
      - shutdown
    - cert-file
      - http-response-timeout
      - response-signing-cert
      - same-recipnonce-for-pollreq
      - url
    - cmpv2
      - accept-unprotected-errormsg
      - accept-unprotected-pkiconf
      - always-set-sender-for-ir
      - http-response-timeout
      - http-version
      - key-list
        - key
      - response-signing-cert
      - same-recipnonce-for-pollreq
      - url
    - crl-file

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security pki ca-profile description

- description
- ocsp
  - responder-url
  - service
  - transmission-profile
- revocation-check
- shutdown

certificate-display-format
certificate-expiration-warning
common-name-list
- cn
- common-name

crl-expiration-warning
est-profile
- check-id-kp-cmcra-only
- client-tls-profile
- http-auth
- server
- transmission-profile

imported-format
maximum-cert-chain-depth

profile
- cli-session-group
- combined-max-sessions
- default-action
- entry
  - action
  - description
  - match
- grpc
  - rpc-authorization
    - gnmi-capabilities
    - gnmi-get
    - gnmi-set
    - gnmi-subscribe
    - gnoi-cert-mgmt-cangenerate
    - gnoi-cert-mgmt-getcert
    - gnoi-cert-mgmt-install
    - gnoi-cert-mgmt-revoke
    - gnoi-cert-mgmt-rotate
    - gnoi-file-get
    - gnoi-file-put
    - gnoi-file-remove
    - gnoi-file-stat
    - gnoi-file-transfertoremote
    - gnoi-system-cancelreboot
    - gnoi-system-ping
    - gnoi-system-reboot
    - gnoi-system-rebootstatus
    - gnoi-system-setpackage
    - gnoi-system-switchcontrolprocessor
    - gnoi-system-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security profile grpc rpc-authorization gnoi-system-traceroute

- gnoi-system-traceroute
- md-cli-session
- rib-api-getversion
- rib-api-modify
- li
- netconf
  - base-op-authorization
    - action
    - cancel-commit
    - close-session
    - commit
    - copy-config
    - create-subscription
    - delete-config
    - discard-changes
    - edit-config
    - get
    - get-config
    - get-data
    - get-schema
    - kill-session
    - lock
    - validate
  - renum
  - ssh-max-sessions
  - telnet-max-sessions
- radius
  - access-algorithm
  - accounting
  - accounting-port
  - authorization
  - interactive-authentication
  - port
  - retry
  - route-preference
  - server
  - shutdown
  - timeout
  - use-default-template
- snmp
  - access
    - access group
  - attempts
  - community
  - src-access-list
    - src-host
  - usm-community
  - view
    - mask
      - mask
- source-address
  - application

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security source-address application6

- application6
- ssh
  - client-cipher-list
    - cipher
  - client-kex-list
    - kex
  - client-mac-list
    - mac
  - key-re-exchange
    - client
      - mbytes
      - minutes
      - shutdown
    - server
      - mbytes
      - minutes
      - shutdown
  - preserve-key
  - server-cipher-list
    - cipher
  - server-kex-list
    - kex
  - server-mac-list
    - mac
  - server-shutdown
  - version
- tacplus
  - accounting
  - authorization
  - interactive-authentication
  - priv-lvl-map
    - priv-lvl
  - request-format
    - access-operation-cmd
  - route-preference
  - server
  - shutdown
  - timeout
  - use-default-template
- tech-support
  - ts-location
- telnet-server
- telnet6-server
- tls
  - cert-profile
    - entry
      - cert
      - key
      - send-chain
        - ca-profile
    - shutdown
  - client-cipher-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security tls client-cipher-list cipher

- cipher
- client-tls-profile
  - cert-profile
  - cipher-list
  - shutdown
  - trust-anchor-profile
- server-cipher-list
  - cipher
- server-tls-profile
  - authenticate-client
    - cn-authentication
    - trust-anchor-profile
  - cert-profile
  - cipher-list
  - shutdown
  - tls-re-negotiate-timer
- trust-anchor-profile
  - trust-anchor

— user
- access
- cli-engine
- console
  - cannot-change-password
  - login-exec
  - member
  - new-password-at-login
- home-directory
- password
- public-keys
  - ecdsa
    - ecdsa-key
      - description
      - key-value
  - rsa
    - rsa-key
      - description
      - key-value
- restricted-to-home
- snmp
  - authentication
  - group

— user-template
- access
- console
  - login-exec
- home-directory
- profile
- restricted-to-home

— vprn-aaa-server
- inband
- outband
- vprn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security vprn-network-exceptions

- vprn-network-exceptions
- selective-fib
- snmp
  - engineID
  - general-port
  - packet-size
  - shutdown
  - streaming
    - shutdown
- software-repository
  - description
  - primary-location
  - secondary-location
  - tertiary-location
- switch-fabric
  - failure-recovery
    - shutdown
  - sfm-loss-threshold
- switchover-exec
- sync-if-timing
  - abort
  - begin
  - bits
    - input
      - shutdown
    - interface-type
    - output
      - line-length
      - ql-minimum
      - shutdown
      - source
      - squelch
    - ql-override
    - ssm-bit
  - commit
  - ptp
    - ql-override
    - shutdown
  - ql-minimum
  - ql-selection
  - ref-order
  - ref1
    - bits-interface-type
    - ql-override
    - shutdown
    - source-port
  - ref2
    - bits-interface-type
    - ql-override
    - shutdown
    - source-port
  - revert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system sync-if-timing synce

- synce
  - ql-override
  - shutdown
- wait-to-restore

- telemetry
  - destination-group
    - allow-unsecure-connection
    - description
    - destination
      - router-instance
    - tcp-keepalive
      - idle-time
      - interval
      - retries
      - shutdown
    - tls-client-profile
    - tls-client-profile
  - notification-bundling
    - max-msg-count
    - max-time-granularity
    - shutdown
  - persistent-subscriptions
    - subscription
      - description
      - destination-group
      - encoding
        - local-source-address
      - local-source-address
      - mode
      - originated-qos-marking
      - sample-interval
      - sensor-group
      - shutdown
  - sensor-groups
    - sensor-group
      - description
      - path
- thresholds
  - cflash-cap-alarm
  - cflash-cap-alarm-pct
  - cflash-cap-warn
  - cflash-cap-warn-pct
  - kb-memory-use-alarm
  - kb-memory-use-warn
  - memory-use-alarm
  - memory-use-warn
  - rmon
    - alarm
    - event
- time
  - dst-zone
    - end

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system time dst-zone offset

- offset
- start
- ntp
  - authentication-check
  - authentication-key
  - broadcast
  - broadcastclient
  - multicast
  - multicastclient
  - ntp-server
  - peer
  - server
  - shutdown
- prefer-local-time
- sntp
  - broadcast-client
  - server-address
  - shutdown
- zone
- vsd
  - system-id
- xmpp
  - server
    - shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.44 configure test-oam Commands

- test-oam
  - build-packet
    - header
      - control-word
      - dot1q
        - prio-code-point
        - tag-protocol-id
        - vlan-id
      - ethernet
        - dst-mac-address
        - src-mac-address
      - gre
      - gtp-user
        - tunnel-endpoint-id
      - ipsec-auth
        - security-param-index
      - ipv4
        - dscp
        - dst-ipv4-address
        - more-fragments
        - src-ipv4-address
      - ipv6
        - dscp
        - dst-ipv6-address
        - src-ipv6-address
      - ipv6-fragment
      - l2tp
        - session-id
        - tunnel-id
      - mpls
        - label
        - traffic-class
      - pbb
        - i-sid
        - tag-protocol-id
      - tcp
        - dst-tcp-port
        - src-tcp-port
      - udp
        - dst-udp-port
        - src-udp-port
  - icmp
    - ping-template
      - **description**
      - dot1p
      - dscp
      - failure-threshold
      - interval
      - reactivation-failure-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure test-oam icmp ping-template reactivation-interval

- reactivation-interval
- reactivation-threshold
- reactivation-timeout
- size
- timeout
- ttl

- ldp-treetrace
  - fc
  - path-discovery
    - interval
    - max-path
    - max-ttl
    - policy-statement
    - retry-count
    - timeout
  - path-probing
    - interval
    - retry-count
    - timeout
  - shutdown
- link-measurement
  - measurement-template
    - aggregate-sample-window
      - multiplier
      - threshold
        - absolute
        - relative
      - window-integrity
    - delay
    - description
    - interval
    - last-reported-delay-hold
    - sample-window
      - multiplier
      - threshold
        - absolute
        - relative
      - window-integrity
    - shutdown
    - twamp-light
      - allow-egress-remark-dscp
      - allow-ipv6-udp-checksum-zero
      - dest-udp-port
      - dscp
      - fc
      - profile
      - timestamp-format
      - ttl
    - unidirectional-measurement
- mpls-dm
  - shutdown
- mpls-echo-request-downstream-map

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure test-oam mpls-time-stamp-format

- mpls-time-stamp-format
- twamp
  - server
    - allow-ipv6-udp-checksum-zero
    - inactivity-timeout
    - max-conn-server
    - max-sess-server
    - prefix
      - description
      - max-conn-prefix
      - max-sess-prefix
      - shutdown
    - shutdown
  - twamp-light
    - inactivity-timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.4.45 configure vrrp Commands

- **vrrp**
  - policy
    - delta-in-use-limit
    - description
    - priority-event
      - host-unreachable
        - drop-count
        - hold-clear
        - hold-set
        - **interval**
        - **padding-size**
        - priority
        - **timeout**
      - lag-port-down
        - hold-clear
        - hold-set
        - number-down
          - priority
        - weight-down
          - priority
      - mc-ipsec-non-forwarding
        - hold-clear
        - hold-set
        - priority
      - port-down
        - hold-clear
        - hold-set
        - priority
      - route-unknown
        - hold-clear
        - hold-set
        - less-specific
        - next-hop
        - priority
        - protocol
    - shutdown
      - interval
      - padding-size
        - timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug

3.5 debug Commands

- debug
  - aaa
    - radius-script-policy
      - script-all-info
      - script-compile-error
      - script-export-variables
      - script-output
      - script-output-on-error
      - script-runtime-error
        - mirror-source
  - application-assurance
    - group
      - http-host-recorder
        - filter
          - default-filter-action
          - expression
          - record
        - rate
        - shutdown
      - port-recorder
        - application
        - rate
        - shutdown
      - traffic-capture
        - match
          - application
          - client-ip
          - client-port
          - dst-ip
          - dst-port
          - ip-addr1
          - ip-addr2
          - ip-protocol-num
          - port1
          - port2
          - server-ip
          - server-port
          - src-ip
          - src-port
        - record
          - cut-through-packets
          - limit
          - start
        - shutdown
  - atm
    - ilmi
  - call-trace
    - ipoe

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug call-trace ipoe trace

- trace
- ppp
  - pppoe-trace
- wlan-gw
  - ue
- certificate
  - auto-crl-update
    - ca-profile
  - cmpv2
    - ca-profile
  - est-profile
  - ocsp
    - ca-profile
- cisco-hdlc
  - on-error
- diameter
  - application
    - on-error
    - policy
      - on-error
      - session-messages
  - dest-realm
  - detail-level
  - diameter-peer
  - diameter-peer-policy
    - avp-match
      - avp
      - message-type
      - shutdown
    - diameter-peer
    - message-type
  - message-type
  - node
    - on-error
    - peer
      - on-error
      - peer-to-peer
    - relayed-messages
  - origin-realm
- dynamic-services
  - data-triggers
    - capture-sap
  - scripts
    - event
      - cli
      - errors
      - executed-cmd
      - state-change
      - warnings
    - instance
      - event
        - cli

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug dynamic-services scripts instance event errors

```
                    — errors
                    — executed-cmd
                    — state-change
                    — warnings
                — script
                    — event
                    — cli
                    — errors
                    — executed-cmd
                    — state-change
                    — warnings
— eth-cfm
    — mep
        — packet
    — mip
        — packet
— ethernet
    — elmi
— frame-relay
    — frf16
    — lmi
— gtp
    — event
    — imsi
    — packet
        — detail-level
        — mode
    — peer
— ipsec
    — certificate
    — client-db
    — gateway
    — transport-mode
    — tunnel
— l2tp
    — predictable-id-assignment
— lag
— macsec
— mcast-management
    — mcast-reporting-dest
        — detail-level
        — igmp
        — mode
— mirror-source
    — ingress-label
    — ip-filter
    — ipv6-filter
    — isa-aa-group
    — mac-filter
    — port
    — sap
    — shutdown
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug mirror-source subscriber

- subscriber
- subscriber
- nat
  - classic-lsn-sub
  - dslite-lsn-sub
  - l2-aware-sub
  - nat-import
  - nat64-lsn-sub
- oam
  - build-packet
    - field-override
    - packet
      - field-override
        - header
          - dot1q
            - prio-code-point
            - tag-protocol-id
            - vlan-id
          - ethernet
            - dst-mac-address
            - src-mac-address
          - gtp-user
            - tunnel-endpoint-id
          - ipsec-auth
            - security-param-index
          - ipv4
            - dscp
            - dst-ipv4-address
            - more-fragments
            - src-ipv4-address
          - ipv6
            - dscp
            - dst-ipv6-address
            - src-ipv6-address
          - l2tp
            - session-id
            - tunnel-id
          - mpls
            - label
            - traffic-class
          - pbb
            - i-sid
            - tag-protocol-id
          - tcp
            - dst-tcp-port
            - src-tcp-port
          - udp
            - dst-udp-port
            - src-udp-port
        - header-sequence
  - ldp-treetrace
  - lsp-ping-trace

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug open-flow

- open-flow
  - all
  - error
  - msg
  - of-switch
    - all
    - channel
    - error
    - filter
    - flowtable
    - msg
    - packet
    - port
    - red
  - port
  - red
- pcap
  - capture
- ppp
- python
  - python-script
    - script-all-info
    - script-compile-error
    - script-export-variables
    - script-output
    - script-output-on-error
    - script-runtime-error
- radius
- router
  - bgp
    - events
    - graceful-restart
    - keepalive
    - notification
    - open
    - outbound-route-filtering
    - packets
    - route-refresh
    - rtm
    - socket
    - timers
    - update
  - bier
    - db
    - fib
    - management
    - red
    - rtm
    - template
    - tunnel
  - bmp
    - events

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router bmp packets

- packets
- gmpls
  - event
    - all
    - lsp-setup
    - misc
    - path
    - peer
    - resv
    - rr
  - packet
    - ack
    - all
    - bundle
    - hello
    - notify
    - path
    - patherr
    - pathtear
    - resv
    - resverr
    - resvtear
    - srefresh
- igmp
  - group-interface
  - host
  - interface
  - mcs
  - misc
  - packet
  - packet
- ip
  - arp
  - dhcp
    - detail-level
    - mode
  - dhcp6
    - detail-level
    - mode
  - event
    - ipv6-error
  - icmp
  - icmp6
  - interface
  - neighbor
  - packet
  - route-table
  - tunnel-table
- isis
  - adjacency
  - cspf
  - graceful-restart

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router isis interface

- interface
- leak
- lsdb
- misc
- packet
- rtm
- spf
- summary
- tunnel-endpoint

- l2tp
  - assignment-id
    - event
      - call-disconnect-notification
      - finite-state-machine
      - ppp
      - recovery
      - recovery-failed
      - stop-control-connection-notification
    - packet
      - detail-level
      - dhcp-client
      - direction
      - l2tp
      - ppp
  - event
    - call-disconnect-notification
    - finite-state-machine
    - lac-session-setup
    - ppp
    - recovery
    - recovery-failed
    - skipped-lns
    - stop-control-connection-notification
  - group
    - event
      - call-disconnect-notification
      - finite-state-machine
      - lac-session-setup
      - ppp
      - recovery
      - recovery-failed
      - skipped-lns
      - stop-control-connection-notification
    - packet
      - detail-level
      - dhcp-client
      - direction
      - l2tp
      - ppp
  - packet
    - detail-level
    - dhcp-client

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router l2tp packet direction

```
            — direction
            — l2tp
            — ppp
         — peer
            — event
               — call-disconnect-notification
               — finite-state-machine
               — ppp
               — recovery
               — recovery-failed
               — stop-control-connection-notification
            — packet
               — detail-level
               — dhcp-client
               — direction
               — l2tp
               — ppp
         — tunnel
            — event
               — call-disconnect-notification
               — finite-state-machine
               — ppp
               — recovery
               — recovery-failed
               — stop-control-connection-notification
            — packet
               — detail-level
               — dhcp-client
               — direction
               — l2tp
               — ppp
      — ldp
         — interface
            — event
               — messages
            — packet
               — hello
         — peer
            — event
               — bindings
               — messages
            — packet
               — hello
               — init
               — keepalive
               — label
      — lmp
         — peer
            — control-channel
               — packet-type
                  — all
                  — ipcc-config
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router lmp peer control-channel packet-type ipcc-hello

- ipcc-hello
- link-summary
- te-link
- packet-type
- link-summary
- local-dhcp-server
- detail-level
- mode
- mld
- group-interface
- host
- interface
- ipsec-interface
- mcs
- misc
- packet
- mpls
- event
- all
- frr
- iom
- lsp-setup
- mbb
- misc
- pcc
- te
- xc
- forwarding-policies
- binding-label
- endpoint
- msdp
- packet
- pim
- rtm
- sa-db
- mtrace
- misc
- packet
- mtrace2
- misc
- packet
- ospf
- area
- area-range
- cspf
- graceful-restart
- interface
- leak
- lsdb
- misc
- neighbor
- nssa-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router ospf packet

- packet
- rsvp-shortcut
- rtm
- sham-neighbor
- spf
- tunnel-endpoint
- virtual-neighbor

— ospf3
- area
- area-range
- graceful-restart
- interface
- leak
- lsdb
- misc
- neighbor
- nssa-range
- packet
- rtm
- spf
- tunnel-endpoint
- virtual-neighbor

— p2mp-sr-tree
- db
- iom
- mgmt
- p2mp-policy
  - candidate-path
- pcep
- replication-policy
  - next-hop
- tunnel

— pcep
- pcc
  - all
  - connection
  - cspf-te
  - db
  - error
  - msg
  - packet
  - red
  - task

— pcp
- pcp-server
  - packet
    - detail-level
    - direction

— pim
- adjacency
- all
- assert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router pim auto-rp

- auto-rp
- bgp
- bier-inband
- bier-signaling
- bsr
- data
- db
- dynmldp
- extranet
- graft
- grafts
- interface
- jp
- mofrr
- mrib
- msg
- mvpn-rtcache
- packet
- red
- register
- rpfv
- rtm
- s-pmsi
- tunnel-interface

- radius
  - detail-level
  - packet-type
  - radius-attr
  - server-address
- radius-proxy
  - server
    - client-address
    - detail-level
    - direction
    - dropped-only
    - packet-type
- rib-api
  - label
  - tunnel
- rip
  - auth
  - error
  - events
  - holddown
  - packets
  - requests
  - trigger
  - updates
- ripng
  - error
  - events
  - holddown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router ripng packets

- packets
- requests
- trigger
- updates

- rpki-session
  - packet
    - all
    - cache-reset
    - cache-response
    - end-of-data
    - error-report
    - ipv4-prefix
    - ipv6-prefix
    - reset-query
    - serial-notify
    - serial-query
- rsvp
  - event
    - all
    - auth
    - misc
    - nbr
    - path
    - resv
    - rr
    - te-threshold-update
      - te-threshold-update
  - packet
    - ack
    - all
    - bundle
    - hello
    - path
    - patherr
    - pathtear
    - resv
    - resverr
    - resvtear
    - srefresh
- srrp
  - events
  - packets
- vrrp
  - events
  - packets
- wpp
  - detail-level
  - packet
    - detail-level
  - portal
    - packet
      - detail-level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug service

- service
  - id
  - id
    - arp-host
      - ip
      - mac
      - mode
      - sap
    - dhcp
      - detail-level
      - mac
      - mode
      - sap
      - sdp
    - dhcp6
      - detail-level
      - mac
      - mode
      - sap
    - event-type
    - host-connectivity-verify
      - ip
      - mac
      - sap
    - igmp-host-tracking
      - detail-level
      - host
      - mode
      - sap
    - igmp-snooping
      - detail-level
      - evpn-mpls
      - mac
      - mode
      - sap
      - sdp
      - vxlan
    - mld-snooping
      - detail-level
      - evpn-mpls
      - mac
      - mode
      - sap
      - sdp
      - vxlan
    - mrp
      - all-events
      - applicant-sm
      - leave-all-sm
      - mmrp-mac
      - mrpdu
      - mvrp-vlan

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug service id mrp periodic-sm

- periodic-sm
- registrant-sm
- sap
- sdp
- one-time-http-redirection
  - ip
  - mac
  - sap
- pim-snooping
  - adjacency
  - all
  - database
  - jp
  - mcs
  - packet
  - port
  - red
- ppp
  - circuit-id
  - event
    - dhcp-client
    - l2tp
    - local-address-assignment
    - ppp
  - mac
  - msap
  - packet
    - detail-level
    - dhcp-client
    - discovery
    - mode
    - ppp
  - remote-id
  - sap
  - username
- proxy-arp
- proxy-nd
- rtr-solicit
  - mac
  - mode
  - sap
- sap
  - event-type
- sdp
  - event-type
- spb
  - adjacency
  - interface
  - l2db
  - lsdb
  - packet
  - spf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug service id stp

- stp
  - all-events
  - bpdu
  - bpdu
  - core-connectivity
  - exception
  - fsm-state-changes
  - fsm-timers
  - port-role
  - port-state
  - sap
  - sdp
- video-interface
  - adi
  - adi-packet
  - fcc-server
  - packet-rx
  - packet-tx
  - rt-client
  - rt-server
  - sg
- sdp
  - event-type
- snmp
- subscriber-mgmt
  - authentication
  - local-user-db
    - detail
  - pfcp
    - packet
  - sub-ident-policy
    - script-all-info
    - script-compile-error
    - script-export-variables
    - script-output
    - script-output-on-error
    - script-runtime-error
  - vrgw
    - brg
      - pppoe-client
        - brg-id
          - detail-level
          - direction
          - discovery
          - dropped-only
          - ppp
- sync-if-timing
  - force-reference
- system
  - grpc
    - client
    - type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug system http-connections

- http-connections
- management-interface
  - remote-management
- netconf
  - info
- ntp
- persistence
- satellite
  - eth-sat
    - boot
    - sync-if-timing
      - force-reference
  - tdm-sat
    - boot
    - sync-if-timing
      - force-reference
- xmpp

upnp
- l2-aware-sub
  - event
  - packet

vsd
- scripts
  - event
    - cli
    - errors
    - executed-cmd
    - state-change
    - warnings
  - instance
    - cli
    - errors
    - event
      - cli
      - errors
      - executed-cmd
      - state-change
      - warnings
    - executed-cmd
    - state-change

wlan-gw
- group
  - learn-ap-mac
  - statistic
  - ue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.6 environment Commands

- environment
  - alias
  - create
  - kernel
  - more
  - reduced-prompt
  - saved-ind-prompt
  - shell
  - suggest-internal-objects
  - terminal
    - length
    - width
  - time-display
  - time-stamp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

file

3.7 file Commands

— file
  — attrib
  — cd
  — checksum
  — copy
  — delete
  — dir
  — format
  — md
  — move
  — rd
  — repair
  — scp
  — shutdown
  — type
  — unzip
  — version
  — vi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

global alias

3.8 Global Commands

- alias
- back
- compare
- echo
- enable-admin
- enable-dynamic-services-config
- enable-vsd-config
- exec
- exit
- help
- history
- logout
- mrinfo
- mstat
- mstat2
- mtrace
- mtrace2
- password
- ping
- pwc
- sleep
- ssh
- telnet
- traceroute
- tree
- write

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3.9 oam Commands

- oam
  - ancp
  - atm-ping
  - bier-ping
  - bier-trace
  - cpe-ping
  - dns
  - efm
  - eth-cfm
    - eth-test
    - linktrace
    - loopback
    - one-way-delay-test
    - two-way-delay-test
    - two-way-slm-test
  - find-egress
  - gtp-ping
  - host-connectivity-verify
  - ldp-treetrace
  - lsp-ping
    - bgp-label
    - ldp
    - prefix
    - rsvp-te
    - sr-isis
    - sr-ospf
    - sr-ospf3
    - sr-policy
    - sr-te
    - static
  - lsp-trace
    - bgp-label
    - ldp
    - prefix
    - rsvp-te
    - sr-isis
    - sr-ospf
    - sr-ospf3
    - sr-policy
    - sr-te
    - static
  - mac-ping
  - mac-populate
  - mac-purge
  - mac-trace
  - mfib-ping
  - oam-pm
  - p2mp-lsp-ping

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

oam p2mp-lsp-trace

- **p2mp-lsp-trace**
- **saa**
- **sdp-mtu**
- **sdp-ping**
- **svc-ping**
- **vccv-ping**
- **vccv-trace**
- **vprn-ping**
- **vprn-trace**
- **vxlan-ping**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

4 3 Commands

4.1 3gpp-charging-characteristics

3gpp-charging-characteristics

Syntax [**no**] **3gpp-charging-characteristics**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-charging-characteristics)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-charging-characteristics

Description This command includes the 3GPP-Charging-Characteristics AVP in all Diameter DCCA CCR messages.

The **no** form of this command removes the 3GPP-Charging-Characteristics AVP from the Diameter DCCA CCR messages.

Default 3gpp-charging-characteristics

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.2 3gpp-charging-id

3gpp-charging-id

Syntax **3gpp-charging-id** {**auto** | **esm-info** | **id**}
no 3gpp-charging-id

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-charging-id)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-charging-id

Description This command includes the 3GPP-Charging-Id AVP in all Diameter DCCA CCR messages. The value can be configured to contain a unique 32-bit identifier or ESM information.

The **no** form of this command removes the 3GPP-Charging-Id AVP from the Diameter DCCA CCR messages.

Default 3gpp-charging-id auto

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **auto** — When the vendor support is 3GPP, this parameter specifies the AVP value for the *subscriber-id*, *sap-id*, and *sla-profile*. The default parameter value selected is **auto**.

esm-info — Specifies the AVP value to *subscriber-id*, *sap-id*, and *sla-profile*.

id — Specifies the AVP value as a unique 32-bit identifier per Diameter Gy session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.3 3gpp-ggsn-address

3gpp-ggsn-address

Syntax [**no**] **3gpp-ggsn-address**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>include-avp 3gpp-ggsn-address)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-ggsn-address

Description This command includes the 3GPP GGSN Address AVP in the Diameter Gy messages. The value is set to the source IPv4 address that is used for outgoing diameter messages.

The **no** form of this command disables the command.

Default 3gpp-ggsn-address

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.4 3gpp-ggsn-ipv6-address

3gpp-ggsn-ipv6-address

Syntax **3gpp-ggsn-ipv6-address**
no 3gpp-ggsn-ipv6-address

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>include-avp 3gpp-ggsn-ipv6-address)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-ggsn-ipv6-address

Description This command includes the 3GPP GGSN IPv6 Address AVP in the Diameter Gy messages. The value is set to the source IPv6 address that is used for outgoing diameter messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.5 3gpp-gprs-negotiated-qos-profile

3gpp-gprs-negotiated-qos-profile

Syntax [**no**] **3gpp-gprs-negotiated-qos-profile**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-gprs-negotiated-qos-profile)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-gprs-negotiated-qos-profile

Description This command includes the 3GPP-GPRS-QoS-Negotiated-Profile AVP in all Diameter DCCA CCR messages. The value is the active SLA profile.

The **no** form of this command removes the 3GPP-GPRS-QoS-Negotiated-Profile AVP from the Diameter DCCA CCR messages.

Default 3gpp-gprs-negotiated-qos-profile

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.6 3gpp-imsi

3gpp-imsi

Syntax **3gpp-imsi** {**circuit-id** | **imsi** | **subscriber-id**}
no 3gpp-imsi

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-imsi)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-imsi

Description This command includes the 3GPP-IMSI AVP in all Diameter DCCA CCR messages.

The **no** form of this command removes the 3GPP-IMSI AVP from the Diameter DCCA CCR messages.

Default 3gpp-imsi subscriber-id

Parameters **circuit-id** — Specifies the circuit-id as DCCA IMSI AVP value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

subscriber-id — Specifies the subscriber-id as DCCA IMSI AVP value.

imsi — Specifies the IMSI as DCCA IMSI AVP value.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.7 3gpp-nsapi

3gpp-nsapi

Syntax [**no**] **3gpp-nsapi**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-nsapi)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-nsapi

Description This command includes the 3GPP-NSAPI AVP in all Diameter DCCA CCR messages. The **3gpp-nsapi** avp value is created from a semi-colon separated concatenation of the system name, service ID, and SAP ID of the subscriber host or session.

The **no** form of this command removes the 3GPP-NSAPI AVP from the Diameter DCCA CCR messages.

Default 3gpp-nsapi

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.8 3gpp-qos-mapping

3gpp-qos-mapping

Syntax **3gpp-qos-mapping**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx 3gpp-qos-mapping)

Full Context configure subscriber-mgmt diameter-application-policy gx 3gpp-qos-mapping

Description This command enables the configuration of mapping certain 3GPP-specific QoS attributes to SR OS objects.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

4.9 3gpp-rat-type

3gpp-rat-type

Syntax **3gpp-rat-type** *value*
no 3gpp-rat-type

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-rat-type)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-rat-type

Description This command includes the 3GPP-RAT-Type AVP with the specified value in all Diameter DCCA CCR messages.

The **no** form of this command removes the 3GPP-RAT-Type AVP from the Diameter DCCA CCR messages.

Parameters *value* — Specifies the 3GPP-RAT-Type AVP value to be included in Diameter DCCA CCR messages.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.10 3gpp-selection-mode

3gpp-selection-mode

Syntax [**no**] **3gpp-selection-mode**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-selection-mode)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-selection-mode

Description This command includes the 3GPP-Selection-Mode AVP in all Diameter DCCA CCR messages.

The **no** form of this command removes the 3GPP-Selection-Mode AVP from the Diameter DCCA CCR messages.

Default 3gpp-selection-mode

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

4.11 3gpp-session-stop-indicator

3gpp-session-stop-indicator

Syntax [**no**] **3gpp-session-stop-indicator**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-session-stop-indicator)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-session-stop-indicator

Description This command includes the 3GPP-Session-Stop-Indicator AVP in all Diameter DCCA CCR-Terminate messages.

The **no** form of this command removes the 3GPP-Session-Stop-Indicator AVP from the Diameter DCCA CCR-Terminate messages.

Default 3gpp-session-stop-indicator

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

4.12 3gpp-user-location-info

3gpp-user-location-info

Syntax [**no**] **3gpp-user-location-info**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp 3gpp-user-location-info)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-user-location-info

Description This command, in case of ESM over GTP access, includes the 3GPP-User-Location-Info attribute. If **ps-information** is also enabled this is grouped within the PS information AVP.

The **no** version of this command disables inclusion of the ULI AVP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5 a Commands

5.1 aa-admit-deny

aa-admit-deny

Syntax **aa-admit-deny**

Context **[Tree]** (config>app-assure>group>statistics aa-admit-deny)

Full Context configure application-assurance group statistics aa-admit-deny

Description Commands in this context configure admit-deny statistics generation.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.2 aa-interface

aa-interface

Syntax **aa-interface** *aa-if-name* [**create**]
no aa-interface *aa-if-name*

Context **[Tree]** (config>service>ies aa-interface)
[Tree] (config>service>vprn aa-interface)

Full Context configure service ies aa-interface
configure service vprn aa-interface

Description This commands creates a new AA interface within an IES or VPRN service. It is used by the aa-isa to send/receive IPv4 traffic. In the context of ICAP url-filtering this interface is used by the ISA to establish ICAP TCP connections to the ICAP servers.

This interface supports /31 subnet only, and uses by default .1q encapsulation.

The system will automatically configure the ISA IP address based on the address configured by the operator under the aa-interface object (which represents the ISA sap facing interface on the ISA).

Parameters *aa-if-name* — specifies the name of the AA Interface.

create — Keyword that specifies to create the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.3 aa-specific

aa-specific

Syntax [**no**] **aa-specific**

Context **[Tree]** (config>log>acct-policy>cr aa-specific)

Full Context configure log accounting-policy custom-record aa-specific

Description Commands in this context configure information for this custom record.

The **no** form of this command excludes aa-specific attributes in the AA subscriber's custom record.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.4 aa-sub

aa-sub

Syntax **aa-sub esm** {**eq** | **neq**} *sub-ident-string*
aa-sub esm-mac {**eq** | **neq**} *esm-mac-name*
aa-sub sap {**eq** | **neq**} *sap-id*
aa-sub spoke-sdp {**eq** | **neq**} *sdp-id:vc-id*
aa-sub transit {**eq** | **neq**} *transit-aasub-name*
no aa-sub

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match aa-sub)

Full Context configure application-assurance group policy app-qos-policy entry match aa-sub

Description This command specifies a Service Access Point (SAP) or an ESM subscriber as matching criteria.

The **no** form of this command removes the SAP or ESM matching criteria.

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-ident-string — Specifies the name of an existing application assurance subscriber.

esm-mac-name — Specifies the name of an ESM-MAC subscriber.

sap-id — Specifies the SAP ID.

sap *sap-id* — Specifies the physical port identifier portion of the SAP definition.

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 to 32767
1 to 4294967295

transit-aasub-name — Specifies the name of a transit AA subscriber.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aa-sub

Syntax **aa-sub**

Context **[Tree]** (config>app-assure>group>statistics aa-sub)

Full Context configure application-assurance group statistics aa-sub

Description Commands in this context configure accounting and statistics collection parameters per application assurance subscribers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aa-sub

Syntax [**no**] **aa-sub {esm** *sub-ident-string* **| sap** *sap-id* **| spoke-sdp** *sdp-id:vc-id* **| transit** *transit-aasub-name* **| esm-mac** *esm-mac-name***}**

Context **[Tree]** (config>app-assure>group>statistics>aa-sub-study aa-sub)

Full Context configure application-assurance group statistics aa-sub-study aa-sub

Description This command adds an existing subscriber identification to a group of special study subscribers (for example, subscribers for which per subscriber statistics and accounting records can be collected for protocols and applications of application assurance).

The **no** form of this command removes the subscriber from the special study subscribers.

Up to 100 subscribers can be configured into the special study group for protocols and up to a 100 potentially different subscribers can be configured into the special study group for applications.

When adding a subscriber to the special study group, accounting records and statistics generation will commence immediately. When removing a subscriber from the group, special study statistics and accounting records for that subscriber in the current interval will be lost.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sub-ident-string* — Specifies the name of a subscriber ID. The subscriber does not need to be currently active. Any sub-ident-string will be accepted. When the subscriber becomes active, statistics generation will start automatically at that time.

sap-id — Specifies the physical port identifier portion of the SAP definition.

spoke-id sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 to 32767
1 to 4294967295

transit-aasub-name — Specifies an existing transit subscriber name string, up to 32 characters in length.

esm-mac-name — Specifies an existing ESM-MAC subscriber name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aa-sub

Syntax **aa-sub** *transit-aasub-name*
no aa-sub

Context **[Tree]** (config>app-assure>group>transit-prefix-policy>entry aa-sub)

Full Context configure application-assurance group transit-prefix-policy entry aa-sub

Description This command configures a transit prefix policy entry subscriber.

The **no** form of this command removes the transit subscriber name from the transit prefix policy configuration.

Parameters *transit-aasub-name* — specifies the name of the transit prefix AA subscriber up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.5 aa-sub-attributes

aa-sub-attributes

Syntax **aa-sub-attributes** [**all**]
no aa-sub-attributes

Context **[Tree]** (config>log>acct-policy>cr>aa aa-sub-attributes)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-attributes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure aa-specific attributes such as aa-sub-attributes and counters that will be available in the AA subscriber's custom record.

The **no** form of this command excludes aa specific attributes from the AA subscriber's custom record.

Parameters **all** — Specifies all counters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.6 aa-sub-congestion-detection

aa-sub-congestion-detection

Syntax **aa-sub-congestion-detection**

Context **[Tree]** (config>app-assure>group aa-sub-congestion-detection)

Full Context configure application-assurance group aa-sub-congestion-detection

Description Commands in this context configure Non-Location Based DEM (NLB-DEM) parameters.

Note: NLB-DEM and Access-Network Location (ANL) DEM mode are mutually exclusive, and cannot operate simultaneously.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.7 aa-sub-counters

aa-sub-counters

Syntax **aa-sub-counters** [**all**]
no aa-sub-counters

Context **[Tree]** (config>log>acct-policy>cr>aa aa-sub-counters)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-counters

Description Commands in this context configure subscriber counter information. This command only applies to the 7750 SR.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command excludes the aa-sub-counters attributes in the AA subscriber's custom record.

Parameters **all** — Specifies all counters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.8 aa-sub-ip

aa-sub-ip

Syntax **aa-sub-ip** *ip-address*[*/mask*]
no aa-sub-ip

Context **[Tree]** (config>app-assure>group>transit-prefix-policy>entry>match aa-sub-ip)

Full Context configure application-assurance group transit-prefix-policy entry match aa-sub-ip

Description This command configures a transit prefix subscriber ip address prefix. It is used when the site is on the local side, being the same side of the system as the parent SAP. The local aa-sub-ip addresses represent the src-IP in the from-SAP direction and dest-IP in the to-SAP direction.

The **no** form of this command deletes the aa-sub-ip address assigned from the entry configuration.

Default no aa-sub-ip

Parameters *ip-address[/mask]* — Specifies the address type of the subscriber address prefix associated with this transit prefix policy entry.

Values

ip-address[/*mask*]:	ipv4-address - a.b.c.d[/mask]
	mask - [1..32]
	ipv6-address - x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D
	prefix-length [1..128]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.9 aa-sub-remote

aa-sub-remote

Syntax [**no**] **aa-sub-remote**

Context **[Tree]** (config>app-assure>group aa-sub-remote)

Full Context configure application-assurance group aa-sub-remote

Description This command specifies whether or not the from subscriber and to subscriber traffic direction is reversed for this group-partition.

Default no aa-sub-remote

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.10 aa-sub-study

aa-sub-study

Syntax **aa-sub-study** *study-type*

Context **[Tree]** (config>app-assure>group>statistics aa-sub-study)

Full Context configure application-assurance group statistics aa-sub-study

Description Commands in this context configure accounting and statistics collection parameters per application assurance special study subscribers.

Parameters *study-type* — Specifies special study protocol subscriber stats.

Values application, protocol

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.11 aa-sub-suppressible

aa-sub-suppressible

Syntax **aa-sub-suppressible**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no aa-sub-suppressible

Context [Tree] (config>app-assure>group>policy>app-profile aa-sub-suppressible)

Full Context configure application-assurance group policy app-profile aa-sub-suppressible

Description This command configures an app-profile as “aa-sub-suppressible”, this function is used in the context of an SRRP group interface. If an SRRP group interface is configured as “suppress-aa-sub” then subscribers with an app-profile configured as “aa-sub-suppressible” will not be diverted to Application Assurance.

The **no** form of this command restores the default behavior.

Default no aa-sub-suppressible

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.12 aa-sub-tethering-state

aa-sub-tethering-state

Syntax **aa-sub-tethering-state** {**detected** | **not-detected**}
no aa-sub-tethering-state

Context [Tree] (config>app-assure>group>policy>aqp>entry>match aa-sub-tethering-state)

Full Context configure application-assurance group policy app-qos-policy entry match aa-sub-tethering-state

Description This command specifies the tethering state of the subscriber where the AQP match entry will be applied.

The tethering state match condition is meaningful when configured in non-default subscriber policy AQP. Default subscriber policy consists of those AQPs that include match criteria based on the subscriber’s configuration. Tethering state match condition is also applicable in those AQPs that include matching criteria that are derived from actual subscriber’s traffic.

The **no** form of this command removes detection of sub-tethering state from the configuration.

Default no aa-sub-tethering-state

Parameters **detected** — Specifies that the subscriber is in the tethering state.

not-detected — Specifies that the subscriber is not in the tethering state.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.13 aa-url-parameter

aa-url-parameter

Syntax **aa-url-parameter** *url-param-string*

Context **[Tree]** (config>subscr-mgmt>http-rdr-plcy aa-url-parameter)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm aa-url-parameter)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm aa-url-parameter)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt aa-url-parameter
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt aa-url-parameter
configure subscriber-mgmt http-redirect-policy aa-url-parameter

Description This command configures the AA URL parameter that is used for HTTP portal redirect.

Parameters *url-param-string* — Specifies an AA URL parameter, up to 247 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.14 aaa

aaa

Syntax **aaa**

Context **[Tree]** (config aaa)

Full Context configure aaa

Description Commands in this context configure authentication, authorization, and accounting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

aaa

Syntax **aaa**

Context **[Tree]** (config>service>vprn aaa)

Full Context configure service vprn aaa

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure AAA on the VPRN.

Platforms All

5.15 aal5-frame-aware

aal5-frame-aware

Syntax [**no**] **aal5-frame-aware**

Context **[Tree]** (config>service>apipe>spoke-sdp>cell-concat aal5-frame-aware)

Full Context configure service apipe spoke-sdp cell-concatenation aal5-frame-aware

Description This command enables the configuration of AAL5 end-of-message (EOM) to be an indication to complete the cell concatenation operation.

The **no** form of this command resets the configuration to ignore the AAL5 EOM as an indication to complete the cell concatenation.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

5.16 aarp

aarp

Syntax **aarp** *aarpId* **type** *type*
no aarp

Context **[Tree]** (config>service>epipe>sap aarp)
[Tree] (config>service>epipe>spoke-sdp aarp)

Full Context configure service epipe sap aarp
configure service epipe spoke-sdp aarp

Description This command associates an AARP instance with a multi-homed SAP or spoke SDP. This instance uses the same AARP ID in the same node to provide traffic flow and packet asymmetry removal for a multi-homed SAP or spoke SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The type specifies the role of this service point in the AARP: either, primary (dual-homed) or secondary (dual-homed-secondary). The AA service attributes (app-profile and transit-policy) of the primary are inherited by the secondary endpoints. All endpoints within an AARP must be of the same type (SAP or spoke), and all endpoints with an AARP must be within the same service.

The no form of this command removes the association between an AARP instance and a multi-homed SAP or spoke SDP.

Default no aarp

Parameters *aarpid* — Specifies the AARP instance associated with this SAP. If not configured, no AARP instance is associated with this SAP.

Values 1 to 65535

type — Specifies the role of the SAP referenced by the AARP instance.

Values **dual-homed** — The primary dual-homed AA subscriber side service-point of an AARP instance; only supported for Epipe, IES, and VPRN SAP and spoke SDP.

dual-homed-secondary — One of the secondary dual-homed AA subscriber side service-points of an AARP instance; only supported for Epipe, IES, and VPRN SAP and spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aarp

Syntax **aarp** *aarp-id* **type** {**subscriber-side-shunt** | **network-side-shunt**}
no aarp

Context **[Tree]** (config>service>ipipe>spoke-sdp aarp)

Full Context configure service ipipe spoke-sdp aarp

Description This command associates an AARP instance to an Ipipe spoke SDP. This instance is paired with the same *aarp-id* in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP. The **type** parameter specifies the role of this service point in the AARP instance.

The **no** form of this command removes the association.

Default no aarp

Parameters *aarp-id* — An integer that identifies an AARP instance.

Values 1 to 65535

subscriber-side-shunt — Specifies that the AARP type is an inter-chassis shunt service for subscriber-side traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

network-side-shunt — Specifies that the AARP type is an inter-chassis shunt service for network-side traffic.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aarp

Syntax **aarp** *aarp-id* **type** {**subscriber-side-shunt** | **network-side-shunt**}
no aarp

Context **[Tree]** (config>service>ies>aarp-interface>spoke-sdp aarp)

Full Context configure service ies aarp-interface spoke-sdp aarp

Description This command associates an AARP instance to an AARP interface spoke SDP. This instance is paired with the same *aarp-id* in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP. The **type** parameter specifies the role of this service point in the AARP instance.

The **no** form of this command removes the association.

Default no aarp

Parameters *aarp-id* — Specifies an integer that identifies an AARP instance.

Values 1 to 65535

subscriber-side-shunt — Specifies that the AARP type is an inter-chassis shunt service for subscriber-side traffic.

network-side-shunt — Specifies that the AARP type is an inter-chassis shunt service for network-side traffic.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aarp

Syntax **aarp** *aarpId* **type** *type*
no aarp

Context **[Tree]** (config>service>ies>if>sap aarp)
[Tree] (config>service>ies>if>spoke-sdp aarp)

Full Context configure service ies interface sap aarp
configure service ies interface spoke-sdp aarp

Description This command associates an AARP instance with a multi-homed SAP or spoke SDP. This instance uses the same AARP ID in the same node or in a peer node (pre-configured) to provide traffic flow and packet asymmetry removal for a multi-homed SAP or spoke SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The type specifies the role of this service point in the AARP: either, primary (dual-homed) or secondary (dual-homed-secondary). The AA service attributes (app-profile and transit-policy) of the primary are inherited by the secondary endpoints. All endpoints within an AARP must be of the same type (SAP or spoke), and all endpoints with an AARP must be within the same service.

The **no** form of this command removes the association between an AARP instance and a multi-homed SAP or spoke SDP.

Default no aarp

Parameters *aarpId* — Specifies the AARP instance associated with this SAP. If not configured, no AARP instance is associated with this SAP.

Values 1 to 65535

type — Specifies the role of the SAP referenced by the AARP instance.

Values **dual-homed** — The primary dual-homed AA subscriber side service-point of an AARP instance; only supported for Epipe, IES, and VPRN SAP and spoke SDP.

dual-homed-secondary — One of the secondary dual-homed AA subscriber side service-points of an AARP instance; only supported for Epipe, IES, and VPRN SAP and spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aarp

Syntax **aarp** *aarp-id* **type** {**subscriber-side-shunt** | **network-side-shunt**}
no aarp

Context **[Tree]** (config>service>vprn>aarp-interface>spoke-sdp aarp)

Full Context configure service vprn aarp-interface spoke-sdp aarp

Description This command associates an AARP instance to an AARP interface spoke SDP. This instance is paired with the same *aarp-id* in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP. The **type** parameter specifies the role of this service point in the AARP instance.

The **no** form of this command removes the association.

Default no aarp

Parameters *aarp-id* — An integer that identifies an AARP instance.

Values 1 to 65535

subscriber-side-shunt — Specifies that the AARP type is an inter-chassis shunt service for subscriber-side traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

network-side-shunt — Specifies that the AARP type is an inter-chassis shunt service for network-side traffic.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

aarp

Syntax **aarp** *aarpId* **type** *type*
no aarp

Context **[Tree]** (config>service>vprn>if>sap aarp)
[Tree] (config>service>vprn>if>spoke-sdp aarp)

Full Context configure service vprn interface sap aarp
configure service vprn interface spoke-sdp aarp

Description This command associates an AARP instance with a multi-homed SAP or spoke SDP. This instance uses the same AARP ID in the same node or in a peer node (pre-configured) to provide traffic flow and packet asymmetry removal for a multi-homed SAP or spoke SDP.

The type specifies the role of this service point in the AARP: either, primary (dual-homed) or secondary (dual-homed-secondary). The AA service attributes (app-profile and transit-policy) of the primary are inherited by the secondary endpoints. All endpoints within an AARP must be of the same type (SAP or spoke), and all endpoints with an AARP must be within the same service.

The **no** form of this command removes the association between an AARP instance and a multi-homed SAP or spoke SDP.

Default no aarp

Parameters *aarpId* — Specifies the AARP instance associated with this SAP. If not configured, no AARP instance is associated with this SAP.

Values 1 to 65535

type — Specifies the role of the SAP referenced by the AARP instance.

Values
dual-homed — The primary dual-homed AA subscriber side service-point of an AARP instance; only supported for Epipe, IES, and VPRN SAP and spoke SDP.

dual-homed-secondary — One of the secondary dual-homed AA subscriber side service-points of an AARP instance; only supported for Epipe, IES, and VPRN SAP and spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

aarp

Syntax **aarp** *aarpId* [**create**]
no aarp *aarpId*

Context **[Tree]** (config>application-assurance aarp)

Full Context configure application-assurance aarp

Description This command defines an Application Assurance Redundancy Protocol (AARP) instance. This instance is paired with the same *aarpId* in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP.

The **no** form of this command removes the instance from the configuration.

Parameters *aarpid* — An integer that identifies an AARP instance.

Values 1 to 65535

create — Keyword used to create the AARP instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.17 aarp-interface

aarp-interface

Syntax **aarp-interface** *aarp-interface-name* [**create**]
no aarp-interface *aarp-interface-name*

Context **[Tree]** (config>service>ies aarp-interface)

Full Context configure service ies aarp-interface

Description This command creates an AARP interface for connecting a service to a peer node AARP service. This instance is paired with the same AARP interface in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP.

The **no** form of this command deletes the interface.

Default no aarp-interface

Parameters *aarp-interface-name* — Specifies a string of up to 32 characters identifying the interface.

create — Keyword used to create the AARP interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

aarp-interface

Syntax **aarp-interface** *aarp-interface-name* [**create**]
no aarp-interface *aarp-interface-name*

Context **[Tree]** (config>service>vprn aarp-interface)

Full Context configure service vprn aarp-interface

Description This command creates an AARP interface for connecting a service to a peer node AARP service. This instance is paired with the same AARP interface in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke SDP.

The **no** form of this command deletes the interface.

Default no aarp-interface

Parameters *aarp-interface-name* — Specifies the AARP interface name.

create — Keyword used to create the AARP interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.18 abandon-tcp-optimization

abandon-tcp-optimization

Syntax [**no**] **abandon-tcp-optimization**

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action abandon-tcp-optimization)

Full Context configure application-assurance group policy app-qos-policy entry action abandon-tcp-optimization

Description This command causes TCPO to stop for flows matching this AQP entry. The flows are counted as TCPO abandoned by policy flows.

The **no** form of this command removes abandon TCPO from actions on flows matching this AQP entry.

Default no abandon-tcp-optimization

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.19 abort

abort

Syntax **abort**

Context **[Tree]** (config>app-assure>group>policy abort)

Full Context configure application-assurance group policy abort

Description This command ends the current editing session and aborts any changes entered during this policy editing session.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

abort

Syntax **abort**

Context **[Tree]** (config>router>bfd abort)

Full Context configure router bfd abort

Description This command discards the changes made to a BFD template during an active session.

Platforms All

abort

Syntax **abort**

Context **[Tree]** (config>router>route-next-hop-policy abort)

Full Context configure router route-next-hop-policy abort

Description This command discards the changes made to route next-hop templates during an active session.

Platforms All

abort

Syntax **abort**

Context **[Tree]** (config>system>sync-if-timing abort)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system sync-if-timing abort

Description This command is required to discard changes that have been made to the synchronous interface timing configuration during a session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

abort

Syntax **abort**

Context **[Tree]** (config>router>policy-options abort)

Full Context configure router policy-options abort

Description This command is required to discard changes made to a route policy.

Platforms All

5.20 above-offered-allowance

above-offered-allowance

Syntax [**no**] **above-offered-allowance**

Context **[Tree]** (config>qos>adv-config-policy>child-control>bandwidth-distribution above-offered-allowance)

Full Context configure qos adv-config-policy child-control bandwidth-distribution above-offered-allowance

Description Commands in this context edit the parameters that control the child's **above-offered-allowance** bandwidth. These parameters are only applicable when the port scheduler is configured to use the **above-offered-allowance-control** algorithm, otherwise they are ignored.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.21 above-offered-cap

above-offered-cap

Syntax **above-offered-cap** {**percent** *percent-of-admin-pir* | **rate** *rate-in-kilobits-per-second*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no above-offered-cap

Context [Tree] (config>qos>adv-config-policy>child-control>bandwidth-distribution above-offered-cap)

Full Context configure qos adv-config-policy child-control bandwidth-distribution above-offered-cap

Description This command is used to limit the operationally configured shaping or policing rate on the child associated with the policy. After the parent virtual scheduler or policer control policy determines the appropriate rate for a given child, a separate operation decides the actual PIR that should be configured for that child. When the parent determines that the distributed rate is equal to or less than the child's offered rate, the configured operational PIR will be equal to that determined rate. But when the parent determines that the child's offered rate is less than the available bandwidth the child could consume, the operational PIR may be set to a value larger than the distributed bandwidth. This extra rate is not currently used by the child since the offered rate is less. The system provides this extra bandwidth in case the child's offered rate increases before the next sampling interval is complete, in order to mitigate the periodic nature of the child's operational PIR adjustments. The increase in the offered rate is not subtracted from the parent's remaining distribution bandwidth for lower priority children, only the determined rate is considered consumed by the parent virtual scheduler or policer control policy instance. The actual operationally configured PIR will never be greater than the child's administratively defined PIR.

This 'fair share' PIR configuration behavior may result in the sum of the children's PIRs exceeding the aggregate rate of the parent. If this behavior violates the downstream QoS requirements, the **above-offered-cap** command may be used to minimize or eliminate the increase in the child's configured PIR.

If the **above-offered-cap** command is used with a percent-based value, the increase is a function of the configured PIR value on the policer or queue. In this case, care should be taken that the child is either configured with an explicit PIR rate (other than max) or the child's administrative PIR is defined using the percent-rate command with the local parameter enabled if an explicit value is not desired. When a maximum PIR is in use on the child, the system attempts to interpret the maximum child forwarding rate. This rate could be very large if the child is associated with multiple ingress or egress ports.

If the child's administrative PIR is modified while a percent based above-offered-cap is in effect, the system automatically uses the new relative limit value the next time the child's operational PIR is distributed.

When this command is not specified or removed, the child's operational 'fair share' operational PIR may be configured up to the child's administrative PIR, based on the actual parental bandwidth available at the child's priority level.

The **no** form of this command is used to remove a fair share operational PIR rate increase limit from all child policers and queues associated with the policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent-of-admin-pir* — When the percent qualifier is used, the following percent-of-admin-pir parameter specifies the percentage of the child's administrative PIR that is used as the fair share increase limit. The new operational PIR result is capped by the child's PIR. If a value of 0 or 0.00 is used, the system will disable the fair share increase function and only configure the actual distribution rate. If a value of 100 or 100.00 is used, the system will interpret this equivalent to executing the **no above-offered-cap** command and return the fair-share operation to the default behavior.

Values 0.00 to 100.00

rate-in-kilobits-per-second — When the rate qualifier is used, the rate-in-kilobits-per-second parameter specifies an explicit rate, in kb/s, that are used as the limit to the child's fair share increase to the operational PIR. The new operational PIR result is capped by the child's PIR. If a value of 0 is used, the system will disable the fair share increase function and only configure the actual distribution rate.

Values 0 to 100,000,000

Platforms All

5.22 absolute

absolute

Syntax **absolute** *microseconds*
no absolute

Context **[Tree]** (config>test-oam>link-meas>template>asw>thr absolute)
[Tree] (config>test-oam>link-meas>template>sw>thr absolute)

Full Context configure test-oam link-measurement measurement-template aggregate-sample-window threshold absolute
configure test-oam link-measurement measurement-template sample-window threshold absolute

Description This command specifies the delta, in microseconds, that a new delay measurement must differ from the previously reported measurement to be reported directly to the routing engine.

The **no** form of this command reverts to the default value.

Default absolute 0

Parameters *microseconds* — Specifies the difference, in microseconds.
A value of 0 (zero) indicates that the absolute threshold is not used for reporting.

Values 0 to 100000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.23 ac-df-capability

ac-df-capability

Syntax **ac-df-capability** {**include** | **exclude**}

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg ac-df-capability)

Full Context configure service system bgp-evpn ethernet-segment ac-df-capability

Description This command configures the inclusion or exclusion of the Attachment Circuit-influenced (AC-Influenced) designated forwarder (DF) election capability (AC-DF) capability into the DF Election for the Ethernet Segment.

The SR OS supports the AC-DF capability, in accordance with RFC8584. The **include** option is the default command setting. The AC-DF capability is enabled by default to support the EVPN auto-discovery per EVI/ES (AD per EVI/ES) routes for a specific PE, which ensures that the PE is included in the candidate DF election list.

Configuring the **exclude** option disables the AC-DF capability. When **ac-df-capability exclude** is configured on a specific Ethernet Segment (ES), the presence or absence of the AD per EVI/ES routes from the ES peers do not modify the candidate DF Election list for the ES. The **exclude** option is recommended in ESs that use an **oper-group** monitored by the access LAG to signal standby lacp or power-off.

All PE routers attached to the same ES must be configured consistently for the AC-DF capability.

Default ac-df-capability include

Parameters **include** — Specifies that AC-DF capability is enabled.

exclude — Specifies that AC-DF capability is disabled.

Platforms All

5.24 accept-authorization-change

accept-authorization-change

Syntax [**no**] **accept-authorization-change**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>auth-policy accept-authorization-change)

Full Context configure subscriber-mgmt authentication-policy accept-authorization-change

Description This command specifies whether or not the system should handle the CoA messages initiated by the RADIUS server, and provide for mid-session interval changes of policies applicable to subscriber hosts.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.25 accept-coa

accept-coa

Syntax [**no**] **accept-coa**

Context [Tree] (config>router>radius-server>server accept-coa)
[Tree] (config>service>vprn>radius-server>server accept-coa)

Full Context configure router radius-server server accept-coa
configure service vprn radius-server server accept-coa

Description This command configures this server for Change of Authorization messages. The system will process the CoA request from the external server if configured with this command; otherwise the CoA request is dropped.

The **no** form of this command disables the command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.26 accept-from-ebgp

accept-from-ebgp

Syntax **accept-from-ebgp** *family* [*family*]
no accept-from-ebgp

Context [Tree] (config>service>vprn>bgp>group>link-bandwidth accept-from-ebgp)
[Tree] (config>service>vprn>bgp>group>neighbor>link-bandwidth accept-from-ebgp)

Full Context configure service vprn bgp group link-bandwidth accept-from-ebgp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group neighbor link-bandwidth accept-from-ebgp

Description This command configures BGP to accept and use the link-bandwidth extended community attached to any route received from any EBGP peer in the scope of the command, as long as that route belongs to one of the listed address families.

The link-bandwidth extended community is encoded as a non-transitive type. This means that by default it should not be attached to any route advertised to an EBGP peer and it should be discarded when received in any route from an EBGP peer. This command overrides the standard behavior.

Up to three families may be configured.

The **no** form of this command restores the default behavior of discarding the link-bandwidth extended community in any route received from an EBGP peer.

Default no accept-from-ebgp

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

Platforms All

accept-from-ebgp

Syntax **accept-from-ebgp** *family* [*family*]
no accept-from-ebgp

Context **[Tree]** (config>router>bgp>group>link-bandwidth accept-from-ebgp)
[Tree] (config>router>bgp>group>neighbor>link-bandwidth accept-from-ebgp)

Full Context configure router bgp group link-bandwidth accept-from-ebgp
configure router bgp group neighbor link-bandwidth accept-from-ebgp

Description This command configures BGP to accept and use the link-bandwidth extended community attached to any route received from any EBGP peer in the scope of the command, as long as that route belongs to one of the listed address families.

The link-bandwidth extended community is encoded as a non-transitive type. This means that by default it should not be attached to any route advertised to an EBGP peer and it should be discarded when received in any route from an EBGP peer. This command overrides the standard behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Up to six families may be configured.

The **no** form of this command restores the default behavior of discarding the link-bandwidth extended community in any route received from an EBGP peer.

Default no accept-from-ebgp

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

vpn-ipv4 — Adds a link-bandwidth extended community to IPv4 VPN (SAFI 128) routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

label-ipv6 — Adds a link-bandwidth extended community to labeled-unicast IPv6 routes.

vpn-ipv6 — Adds a link-bandwidth extended community to IPv6 VPN (SAFI 128) routes.

Platforms All

5.27 accept-ivpls-evpn-flush

accept-ivpls-evpn-flush

Syntax [**no**] **accept-ivpls-evpn-flush**

Context **[Tree]** (config>service>vpls>bgp-evpn accept-ivpls-evpn-flush)

Full Context configure service vpls bgp-evpn accept-ivpls-evpn-flush

Description This command enables the system to accept non-zero Ethernet tag MAC routes and process them only for C-MAC flushing. This command can be changed on the fly without shutting down BGP-EVPN MPLS.

The **no** version of the command prevents the router from processing B-MAC/ISID routes for cmac-flush.

Default no accept-ivpls-evpn-flush

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.28 accept-mrru

accept-mrru

Syntax [**no**] **accept-mrru**

Context **[Tree]** (config>subscr-mgmt>ppp-policy>mlppp accept-mrru)

Full Context configure subscriber-mgmt ppp-policy mlppp accept-mrru

Description This command is applicable only to LAC. MRRU option is an indication that the session is of MLPPPoX type. The 7750 SR LAC never initiates the MRRU option in LCP negotiation process. However, it responds to MRRU negotiation request by the client.

This command provides an option to specifically enable or disable negotiation of MLPPPoX on a capture SAP level or on a group interface level.

The **no** form of this command causes the MRRU option in LCP to not be negotiated by LAC.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

5.29 accept-orf

accept-orf

Syntax [**no**] **accept-orf**

Context **[Tree]** (config>router>bgp>outbound-route-filtering>extended-community accept-orf)
[Tree] (config>router>bgp>group>outbound-route-filtering>extended-community accept-orf)
[Tree] (config>router>bgp>group>neighbor>outbound-route-filtering>extended-community accept-orf)

Full Context configure router bgp group neighbor outbound-route-filtering extended-community accept-orf
configure router bgp group outbound-route-filtering extended-community accept-orf
configure router bgp outbound-route-filtering extended-community accept-orf

Description This command instructs the router to negotiate the receive capability in the BGP ORF negotiation with a peer, and to accept filters that the peer wishes to send.

The **no** form of this command causes the router to remove the accept capability in the BGP ORF negotiation with a peer, and to clear any existing ORF filters that are currently in place.

Default no accept-orf

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.30 accept-remote-loopback

accept-remote-loopback

Syntax [**no**] **accept-remote-loopback**

Context **[Tree]** (config>port>ethernet>efm-oam accept-remote-loopback)

Full Context configure port ethernet efm-oam accept-remote-loopback

Description This command enables reactions to loopback control OAM PDUs from peers.

The **no** form of this command disables reactions to loopback control OAM PDUs.

Default no accept-remote-loopback

Platforms All

5.31 accept-script-policy

accept-script-policy

Syntax **accept-script-policy** *policy-name*
no accept-script-policy

Context **[Tree]** (config>aaa>radius-srv-plcy accept-script-policy)

Full Context configure aaa radius-server-policy accept-script-policy

Description This command specifies the RADIUS script policy used to change the RADIUS attributes of the incoming Access-Accept messages.

Parameters *policy-name* — Specifies the name of the Python script to modify Access-Accept messages, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

accept-script-policy

Syntax **accept-script-policy** *policy-name*
no accept-script-policy

Context **[Tree]** (config>subscr-mgmt>auth-policy accept-script-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt authentication-policy accept-script-policy

Description This command specifies the RADIUS script policy used to change the RADIUS attributes of the incoming Access-Accept messages.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the name of the Python script to modify Access-Accept messages, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.32 accept-unprotected-errormsg

accept-unprotected-errormsg

Syntax [**no**] **accept-unprotected-errormsg**

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 accept-unprotected-errormsg)

Full Context configure system security pki ca-profile cmpv2 accept-unprotected-errormsg

Description This command enables the system to accept both protected and unprotected CMPv2 error message. Without this command, system will only accept protected error messages.

The **no** form of this command causes the system to only accept protected PKI confirmation message.

Default no accept-unprotected-errormsg

Platforms All

5.33 accept-unprotected-pkiconf

accept-unprotected-pkiconf

Syntax [**no**] **accept-unprotected-pkiconf**

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 accept-unprotected-pkiconf)

Full Context configure system security pki ca-profile cmpv2 accept-unprotected-pkiconf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the system to accept both protected and unprotected CMPv2 PKI confirmation messages. Without this command, the system will only accept protected PKI confirmation message.

The **no** form of this command causes the system to only accept protected PKI confirmation message.

Default no accept-unprotected-pkiconf

Platforms All

5.34 access

access

Syntax **access router** *router-instance*
access service *service-name*
no access

Context **[Tree]** (config>subscr-mgmt>steering-profile access)

Full Context configure subscriber-mgmt steering-profile access

Description This command specifies a routing instance to be used as a network VAS router in the steering profile.

The **no** form of this command removes the router instance.

Parameters *router-instance* — Specifies the router instance to be used as an access VAS router.

Values

router-instance:	*router-name* | *vprn-svc-id*
router-name:	"Base"
vprn-svc-id:	1 to 2147483647

service-name — Specifies the service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

access

Syntax **access**

Context **[Tree]** (config>port>ethernet access)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet access

Description This command configures Ethernet access port parameters.

Platforms All

access

Syntax [**no**] **access**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext access)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext access)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access

Description Commands in this context configure the access side of HLE for the VLAN range.

The **no** form of this command disables the vRGW parameters enabled in this context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

access

Syntax **access**

Context **[Tree]** (config>card>mda access)
[Tree] (config>port access)

Full Context configure card mda access
configure port access

Description This command enables the access context to configure egress and ingress pool policy parameters.

On the MDA level, access egress and ingress pools are only allocated on channelized MDAs.

Platforms All

access

Syntax **access**

Context **[Tree]** (config>card>fp>ingress access)

Full Context configure card fp ingress access

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This CLI node contains the access forwarding-plane parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

access

Syntax **access**

Context **[Tree]** (config>lag access)

Full Context configure lag access

Description Commands in this context configure access parameters.

Platforms All

access

Syntax **access**

Context **[Tree]** (config>eth-tunnel>lag-emulation access)

Full Context configure eth-tunnel lag-emulation access

Description Commands in this context configure eth-tunnel loadsharing access parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

access

Syntax [**no**] **access**

Context **[Tree]** (config>service>vprn>snmp access)

Full Context configure service vprn snmp access

Description This command enables SNMP access using VPRN interface addresses. This command allows SNMP messages destined to the VPRN interface IP addresses for this VPRN (including VPRN interfaces that are bound to R-VPLS services) to be processed by the SNMP agent on the router. SNMP messages that arrive on VPRN interfaces but are destined to IP addresses in the Base routing context that can be accessed in the VPRN (for example, the router system address via grt leaking) do not require **snmp access** to be enabled but do require **allow-local-management** to be enabled.

Using an SNMP community defined inside the VPRN context (**configure service vprn snmp community**) allows access to a subset of the full SNMP data model. This subset can be seen in the output of **show system security view "vprn-view"**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Using an SNMP community defined in the system context (**configure system security snmp community**) allows access to the full SNMP data model (unless otherwise restricted used SNMP views).

Alternatively, grt leaking and a Base routing IP address can be used (along with an SNMP community defined at the system context) to get access to the entire SNMP data model (see the **allow-local-management** command).

The Nokia NSP cannot discover or fully manage an SR OS router using an SNMP community defined inside the VPRN context. Full SNMP access requires using one of the approaches described above.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide* for detailed information about SNMP.

Platforms All

access

Syntax [**no**] **access** [**ftp**] [**snmp**] [**console**] [**li**] [**netconf**] [**grpc**]

Context **[Tree]** (config>system>security>user access)
[Tree] (config>system>security>user-template access)

Full Context configure system security user access
configure system security user-template access

Description This command grants a user permission for FTP, SNMP, console, lawful intercept (LI), NETCONF, or gRPC access.

If a user requires access to more than one application, then multiple applications can be specified in a single command. Multiple commands are treated additively.

The **no** form of this command removes access for a specific application, and denies permission for all management access methods.

To deny a single access method, enter the **no** form of this command followed by the method to be denied, for example, **no access FTP** denies FTP access.

Default no access

Parameters **ftp** — Specifies FTP permission.

snmp — Specifies SNMP permission. This keyword is only configurable in the **config>system>security>user** context.

console — Specifies console access (serial port or Telnet) permission.

li — Specifies CLI command access in the lawful intercept (LI) context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

netconf — Specifies NETCONF session access for the user defined in the specified user context. Because of the Base-R13 SR OS YANG data models, **console** access is also necessary in both classic and mixed configuration modes. **console** access is not required for the Nokia SR OS YANG data models in model-driven mode.

grpc — Specifies gRPC access.

Platforms All

5.35 access group

access group

Syntax [**no**] **access group** *group-name* **security-model** *security-model* **security-level** *security-level* [**context** *context-name* [**prefix-match**]] [**read** *view-name-1*] [**write** *view-name-2*] [**notify** *view-name-3*]

Context **[Tree]** (config>system>security>snmp access group)

Full Context configure system security snmp access group

Description This command creates an association between a user group, a security model, and the views that the user group can access. Access parameters must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.

Access groups are used by the usm-community command.

Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings. See the **community** command.

Default access group configurations cannot be modified or deleted.

To remove the user group with associated, security model(s), and security level(s), use:

no access group *group-name*

To remove a security model and security level combination from a group, use:

no access group *group-name* **security-model** {**snmpv1** | **snmpv2c** | **usm**} **security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}

Parameters *group-name* — Specify a unique group name up to 32 characters.

security-model {**snmpv1** | **snmpv2c** | **usm**} — Specifies the security model required to access the views configured in this node. A group can have multiple security models. For example, one view may only require SNMPv1/ SNMPv2c access while another view may require USM (SNMPv3) access rights.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

security-level {**no-auth-no-priv** | **auth-no-priv** | **privacy**} — Specifies the required authentication and privacy levels to access the views configured in this node.

security-level no-auth-no-privacy — Specifies that no authentication and no privacy (encryption) is required. When configuring the user's authentication, select the **none** option.

security-level auth-no-privacy — Specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the **group** and the **user** must be configured for authentication.

security-level privacy — Specifies that both authentication and privacy (encryption) is required. When this option is configured, both the **group** and the user must be configured for **authentication**. The user must also be configured for **privacy**.

context-name — Specifies a set of SNMP objects that are associated with the context-name.

The *context-name* is treated as either a full context-name string or a context name prefix depending on the keyword specified (**exact** or **prefix**).

prefix-match — Specifies the context name **prefix-match** keywords, **exact** or **prefix**. This parameter applies only to the 7750 SR.

The VPRN context names begin with a **vprn** prefix. The numerical value is associated with the service ID that the VPRN was created with and identifies the service in the service domain. For example, when a new VPRN service is created such as **config>service>vprn 2345 customer 1**, a VPRN with context name **vprn2345** is created.

The **exact** keyword specifies that an exact match between the context name and the prefix value is required. For example, when context **vprn2345 exact** is entered, matches for only **vprn2345** are considered.

The **prefix** keyword specifies that only a match between the prefix and the starting portion of context name is required. If only the **prefix** keyword is specified, simple wildcard processing is used. For example, when context **vprn prefix** is entered, all **vprn** contexts are matched.

Default **exact**

view-name-1 — Specifies the SNMP view used to control which MIB objects can be accessed using a read (get) operation.

view-name-2 — Specifies the SNMP view used to control which MIB objects can be accessed using a write (set) operation.

view-name-3 — Specifies the SNMP view used to control which MIB objects can be accessed for notifications.

Values none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.36 access-algorithm

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}
no access-algorithm

Context **[Tree]** (config>aaa>l2tp-acct-plcy>radius-acct-server access-algorithm)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server access-algorithm

Description This command configures the algorithm used to access the list of configured RADIUS servers.

The **no** form of this command reverts to the default.

Default access-algorithm direct

Parameters **direct** — Specifies that the first server is used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server is used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}

Context **[Tree]** (config>app-assure>rad-acct-plcy>server access-algorithm)

Full Context configure application-assurance radius-accounting-policy radius-accounting-server access-algorithm

Description This command configures the algorithm used to access the list of configured RADIUS servers.

Default access-algorithm direct

Parameters **direct** — Specifies that the first server is used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server is used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}
no access-algorithm

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server access-algorithm)
[Tree] (config>subscr-mgmt>acct-plcy>server access-algorithm)

Full Context configure subscriber-mgmt radius-accounting-policy radius-accounting-server access-algorithm
configure subscriber-mgmt authentication-policy radius-authentication-server access-algorithm

Description This command configures the algorithm used to access the list of configured RADIUS servers.

The **no** form of this command reverts to the default.

Parameters **direct** — Specifies that the first server is used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server is used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin** | **hash-based**}
no access-algorithm

Context **[Tree]** (config>aaa>radius-srv-plcy>servers access-algorithm)

Full Context configure aaa radius-server-policy servers access-algorithm

Description This command configures the algorithm used to select a RADIUS server from the pool of configured RADIUS servers.

Default access-algorithm direct

Parameters **direct** — Specifies that the first server is used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server is used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash-based — Select a RADIUS server based on the calculated hash result of the configured **load-balance-key** under the **radius-proxy server** hierarchy. This parameter is only applicable for radius-proxy server scenarios and results in an unpredictable RADIUS server selection if used in other scenarios.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}
no access-algorithm

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius access-algorithm)

Full Context configure service vprn aaa remote-servers radius access-algorithm

Description This command indicates the algorithm used to access the set of RADIUS servers.

Default access-algorithm direct

Parameters **direct** — The first server will be used as primary server for all requests, the second as secondary and so on.

round-robin — The first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

Platforms All

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin** | **hash-based** | **direct-priority**}
no access-algorithm

Context **[Tree]** (config>aaa>isa-radius-plcy>servers access-algorithm)

Full Context configure aaa isa-radius-policy servers access-algorithm

Description This command defines the algorithm used to access the list of available RADIUS servers. A RADIUS server is considered available initially and marked as unavailable if no response packets are received in a period equal to the configured packet **timeout** multiplied by the **retry** *count* after sending a request. A server is always marked as available when any valid RADIUS packet is received from that server. Some access algorithms periodically probe unavailable servers by sending a single request. If the server responds to the request, it is immediately marked as available.

Default access-algorithm direct

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **direct** — Specifies that the first server is used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server is used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

hashed-based — Specifies that the selection is based on the hash-based procedures.

direct-priority — Specifies that the first server is used for all requests. If that server is not available, the second server is used, and so on. This method periodically probes and falls back to higher-priority servers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

access-algorithm

Syntax **access-algorithm** {**direct** | **round-robin**}
no access-algorithm

Context **[Tree]** (config>system>security>radius access-algorithm)

Full Context configure system security radius access-algorithm

Description This command indicates the algorithm used to access the set of RADIUS servers.

Default access-algorithm direct

Parameters **direct** — Specifies that the first server is used as primary server for all requests, the second as secondary and so on.

round-robin — Specifies that the first server is used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

Platforms All

5.37 access-loop-encapsulation

access-loop-encapsulation

Syntax [**no**] **access-loop-encapsulation**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host access-loop-encapsulation)

Full Context configure subscriber-mgmt local-user-db ppp host access-loop-encapsulation

Description Commands in this context configure access loop information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

5.38 access-loop-information

access-loop-information

Syntax **access-loop-information**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host access-loop-information)

Full Context configure subscriber-mgmt local-user-db ppp host access-loop-information

Description Commands in this context configure access loop information in the local user database.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.39 access-loop-options

access-loop-options

Syntax [**no**] **access-loop-options**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute access-loop-options)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute access-loop-options)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute access-loop-options
configure subscriber-mgmt authentication-policy include-radius-attribute access-loop-options

Description This command enables inclusion of access loop information: Broadband Forum (BBF) access loop characteristics, DSL line state and DSL type. The BBF access loop characteristics are returned as BBF specific RADIUS attributes where DSL line state and DSL type are returned as Nokia-specific RADIUS VSAs.

Information obtained via the ANCP protocol has precedence over information received in PPPoE Vendor Specific BBF tags or DHCP Vendor Specific BBF Options.

If ANCP is utilized and interim accounting update is enabled, any Port Up event from GSMP will initiate in an interim update. Port Up messages can include information such as an update on the current subscriber actual-upstream-speed. The next interim accounting message is from port up triggering point.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.40 access-network-location

access-network-location

Syntax **access-network-location**

Context **[Tree]** (config>app-assure>group access-network-location)

Full Context configure application-assurance group access-network-location

Description Commands in this context configure parameters related to dynamic experience management, also known as Access Network Location (ANL).

These parameters include location source type congestion point and congestion detection parameters (such as roundtrip delay thresholds), if applicable.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.41 access-operation-cmd

access-operation-cmd

Syntax [**no**] **access-operation-cmd** *access-operation*

Context **[Tree]** (config>system>security>tacplus>request-format access-operation-cmd)

Full Context configure system security tacplus request-format access-operation-cmd

Description This command sends an operation argument in authorization requests.

In model-driven interfaces, this command configures the system to send the operation in the cmd argument, and the path in the cmd-args argument, in TACACS+ authorization requests. This command does not apply to authorization requests in classic interfaces.

The **no** form of this command removes the operation from the configuration.

Default no access-operation-cmd

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *access-operation* — Specifies that an operation in the authorization request is sent.

Values delete — Keyword that sends the operation "cmd=delete" and "cmd-args=path".

Platforms All

5.42 accounting

accounting

Syntax **accounting** {**1** | **2**} [**create**]
no accounting {**1** | **2**}

Context **[Tree]** (config>service>dynsvc>ladb>user>idx accounting)

Full Context configure service dynamic-services local-auth-db user-name index accounting

Description This command creates a context for one of the two accounting destinations specified in the dynamic services policy. In this context, overrides of RADIUS accounting parameters can be specified.

The **no** form of this command removes the RADIUS accounting overrides context from the configuration.

Parameters **{1 | 2}** — Indicates one of the two RADIUS accounting destinations.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

accounting

Syntax [**no**] **accounting**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius accounting)

Full Context configure service vprn aaa remote-servers radius accounting

Description This command enables RADIUS accounting.

The **no** form of this command disables RADIUS accounting.

Default no accounting

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

accounting

Syntax **accounting** [**record-type** {**start-stop** | **stop-only**}]
no accounting

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus accounting)

Full Context configure service vprn aaa remote-servers tacplus accounting

Description This command configures the type of accounting record packet that is to be sent to the TACACS+ server. The **record-type** parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent.

Default no accounting

Parameters **record-type start-stop** — Specifies that a TACACS+ start packet is sent whenever the user executes a command and a TACACS+ stop packet when command execution is complete.

record-type stop-only — Specifies that only a TACACS+ stop packet is sent whenever the command execution is complete.

Platforms All

accounting

Syntax **accounting** [**port** *udp-port*]
no accounting

Context **[Tree]** (config>aaa>isa-radius-plcy>servers>server accounting)

Full Context configure aaa isa-radius-policy servers server accounting

Description This command configures accounting for this server.

Parameters *udp-port* — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

accounting

Syntax [**no**] **accounting**

Context **[Tree]** (config>system>security>radius accounting)

Full Context configure system security radius accounting

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables RADIUS accounting.

The **no** form of this command disables RADIUS accounting.

Default no accounting

Platforms All

accounting

Syntax **accounting** [**record-type** {**start-stop** | **stop-only**}]
no accounting

Context **[Tree]** (config>system>security>tacplus accounting)

Full Context configure system security tacplus accounting

Description This command configures the type of accounting record packet that is to be sent to the TACACS+ server. The **record-type** parameter indicates whether TACACS+ accounting start and stop packets be sent or just stop packets be sent.

Default no accounting

Parameters **record-type start-stop** — Specifies that a TACACS+ start packet is sent whenever the user executes a command and a TACACS+ stop packet when command execution is complete.

record-type stop-only — Specifies that only a TACACS+ stop packet is sent whenever the command execution is complete.

Platforms All

5.43 accounting-1

accounting-1

Syntax **accounting-1**

Context **[Tree]** (config>service>dynsvc>policy accounting-1)

Full Context configure service dynamic-services dynamic-services-policy accounting-1

Description Commands in this context configure the first RADIUS accounting destination and corresponding RADIUS accounting parameters for dynamic data services.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.44 accounting-2

accounting-2

Syntax **accounting-2**

Context **[Tree]** (config>service>dynsvc>policy accounting-2)

Full Context configure service dynamic-services dynamic-services-policy accounting-2

Description Commands in this context configure the second RADIUS accounting destination and corresponding RADIUS accounting parameters for dynamic data services.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.45 accounting-policy

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>subscr-mgmt>sub-prof accounting-policy)
[Tree] (config>service>vpls>video-if accounting-policy)

Full Context configure service vpls video-interface accounting-policy
configure subscriber-mgmt sub-profile accounting-policy

Description This command specifies the policy to use to collect accounting statistics on this subscriber profile.

A maximum of one accounting policy can be associated with a profile at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association.

Parameters *acct-policy-id* — Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt sub-profile accounting-policy

7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls video-interface accounting-policy

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>service>ies>if>sap accounting-policy)
[Tree] (config>service>ies>sub-if>grp-if>sap accounting-policy)
[Tree] (config>service>vpls>sap accounting-policy)
[Tree] (config>service>vpls>spoke-sdp accounting-policy)
[Tree] (config>service>vpls>mesh-sdp accounting-policy)
[Tree] (config>service>vprn>if>sap accounting-policy)
[Tree] (config>service>vprn>if>spoke-sdp accounting-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap accounting-policy)

Full Context configure service ies interface sap accounting-policy
configure service ies subscriber-interface group-interface sap accounting-policy
configure service vpls mesh-sdp accounting-policy
configure service vpls sap accounting-policy
configure service vpls spoke-sdp accounting-policy
configure service vprn interface sap accounting-policy
configure service vprn interface spoke-sdp accounting-policy
configure service vprn subscriber-interface group-interface sap accounting-policy

Description This command creates the accounting policy context that can be applied to an interface SAP or interface SAP spoke SDP.

An accounting policy must be defined before it can be associated with a SAP or SDP.

If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP or SDP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP or SDP, and the accounting policy reverts to the default.

Default no accounting policy

Parameters *acct-policy-id* — Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap accounting-policy
- configure service ies subscriber-interface group-interface sap accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service vpls mesh-sdp accounting-policy
- configure service vprn interface sap accounting-policy
- configure service vprn interface spoke-sdp accounting-policy
- configure service ies interface sap accounting-policy
- configure service vpls spoke-sdp accounting-policy
- configure service vpls sap accounting-policy

accounting-policy

Syntax **accounting-policy** *isa-radius-policy-name*
no accounting-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range>xconnect accounting-policy)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range>xconnect accounting-policy)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect accounting-policy
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect accounting-policy

Description This command configures the ISA RADIUS accounting policy for the cross-connect.

The **no** form of this command removes the ISA RADIUS accounting policy from the cross-connect UE.

Parameters *isa-radius-policy-name* — Specifies the identifier of the ISA RADIUS policy name, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

accounting-policy

Syntax **accounting-policy** *policy-name*
no accounting-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm accounting-policy)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm accounting-policy)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt accounting-policy
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the **isa-radius-policy** used for accounting messages originated from the ISAs in the **wlan-gw** group. The policy can specify up to five accounting servers and configuration-specific to these accounting servers. It also specifies configuration specific to RADIUS client on ISAs and RADIUS attributes to be included in accounting messages.

Parameters *policy-name* — Specifies the name of the account policy up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>card>fp>ingress>access>queue-group accounting-policy)
[Tree] (config>card>fp>ingress>network>queue-group accounting-policy)

Full Context configure card fp ingress access queue-group accounting-policy
configure card fp ingress network queue-group accounting-policy

Description This command configures an accounting policy that can apply to a queue-group on the forwarding plane.

An accounting policy must be configured before it can be associated to an interface. If the accounting *policy-id* does not exist, an error is returned.

Accounting policies associated with service billing can only be applied to SAPs. The accounting policy can be associated with an interface at a time.

The **no** form of this command removes the accounting policy association from the queue-group.

Default No accounting policies are specified by default. You must explicitly specify a policy. If configured, the accounting policy configured as the default is used.

Parameters *acct-policy-id* — Specifies the name of the accounting policy to use for the queue-group.

Values 1 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

accounting-policy

Syntax **accounting-policy** *policy-id*
no accounting-policy

Context **[Tree]** (config>port>ethernet accounting-policy)
[Tree] (config>port>ethernet>access>egr>qgrp accounting-policy)
[Tree] (config>port>ethernet>access>ing>qgrp accounting-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>port>ethernet>network>egr>qgrp accounting-policy)
[Tree] (config>port>ethernet>network accounting-policy)
[Tree] (config>port>sonet-sdh>path>network accounting-policy)
[Tree] (config>port>tdm>ds1>channel-group>network accounting-policy)
[Tree] (config>port>tdm>ds3>network accounting-policy)
[Tree] (config>port>tdm>e1>channel-group>network accounting-policy)
[Tree] (config>port>tdm>e3>network accounting-policy)

Full Context

configure port ethernet access egress queue-group accounting-policy
configure port ethernet access ingress queue-group accounting-policy
configure port ethernet accounting-policy
configure port ethernet network accounting-policy
configure port ethernet network egress queue-group accounting-policy
configure port sonet-sdh path network accounting-policy
configure port tdm ds1 channel-group network accounting-policy
configure port tdm ds3 network accounting-policy
configure port tdm e1 channel-group network accounting-policy
configure port tdm e3 network accounting-policy

Description

This command configures an accounting policy that can apply to an interface.

An accounting policy must be configured before it can be associated to an interface. If the accounting *policy-id* does not exist, an error is returned.

Accounting policies associated with service billing can only be applied to SAPs. Accounting policies associated with network ports can only be associated with interfaces. Only one accounting policy can be associated with an interface at a time.

The **no** form of this command removes the accounting policy association from the network interface, and the accounting policy reverts to the default.

Default

No accounting policies are specified by default. You must explicitly specify a policy. If configured, the accounting policy configured as the default is used.

Parameters

policy-id — The accounting *policy-id* of an existing policy. Accounting policies record either service (access) or network information. A network accounting policy can only be associated with the network port configurations. Accounting policies are configured in the **config>log>accounting-policy** context.

Values 1 to 99

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path network accounting-policy

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 network accounting-policy
- configure port tdm e1 channel-group network accounting-policy
- configure port tdm ds3 network accounting-policy
- configure port tdm ds1 channel-group network accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure port ethernet network egress queue-group accounting-policy
- configure port ethernet access ingress queue-group accounting-policy
- configure port ethernet network accounting-policy
- configure port ethernet accounting-policy
- configure port ethernet access egress queue-group accounting-policy

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy [*acct-policy-id*]

Context **[Tree]** (config>service>apipe>sap accounting-policy)
[Tree] (config>service>cpipe>sap accounting-policy)
[Tree] (config>service>epipe>sap accounting-policy)
[Tree] (config>service>fpipe>sap accounting-policy)
[Tree] (config>service>ipipe>sap accounting-policy)
[Tree] (config>service>epipe>spoke-sdp accounting-policy)

Full Context configure service apipe sap accounting-policy
configure service cpipe sap accounting-policy
configure service epipe sap accounting-policy
configure service epipe spoke-sdp accounting-policy
configure service fpipe sap accounting-policy
configure service ipipe sap accounting-policy

Description This command creates the accounting policy context that can be applied to a SAP.

An accounting policy must be defined before it can be associated with a SAP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default.

Default no accounting policy

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap accounting-policy
- configure service cpipe sap accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap accounting-policy

All

- configure service epipe sap accounting-policy
- configure service ipipe sap accounting-policy
- configure service epipe spoke-sdp accounting-policy

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>service>ies>if>spoke-sdp accounting-policy)

Full Context configure service ies interface spoke-sdp accounting-policy

Description This command configures an accounting-policy.

Parameters *acct-policy-id* — Specifies an accounting policy ID.

Values 1 to 99

Platforms All

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>router>ldp>egr-stats accounting-policy)

Full Context configure router ldp egr-stats accounting-policy

Description This command associates an accounting policy to the MPLS instance.

An accounting policy must be defined before it can be associated else an error message is generated.

The **no** form of this command removes the accounting policy association.

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>router>mpls>ingr-stats>lsp accounting-policy)
[Tree] (config>router>mpls>ingr-stats>p2mp-template-lsp accounting-policy)
[Tree] (config>router>mpls>ingr-stats>p2p-template-lsp accounting-policy)
[Tree] (config>router>mpls>lsp>egr-stats accounting-policy)
[Tree] (config>router>mpls>lsp>ingr-stats accounting-policy)
[Tree] (config>router>mpls>lsp-template>egr-stats accounting-policy)

Full Context configure router mpls ingress-statistics lsp accounting-policy
configure router mpls ingress-statistics p2mp-template-lsp accounting-policy
configure router mpls ingress-statistics p2p-template-lsp accounting-policy
configure router mpls lsp egress-statistics accounting-policy
configure router mpls lsp ingress-statistics accounting-policy
configure router mpls lsp-template egress-statistics accounting-policy

Description This command associates an accounting policy to the MPLS instance.

The config>router>mpls>ingr-stats>p2mp-template-lsp>accounting-policy command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

An accounting policy must be defined before it can be associated else an error message is generated.

The **no** form of this command removes the accounting policy association.

Parameters *acct-policy-id* — Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router mpls lsp ingress-statistics accounting-policy

All

- configure router mpls ingress-statistics p2p-template-lsp accounting-policy
- configure router mpls ingress-statistics p2mp-template-lsp accounting-policy
- configure router mpls ingress-statistics lsp accounting-policy
- configure router mpls lsp egress-statistics accounting-policy
- configure router mpls lsp-template egress-statistics accounting-policy

accounting-policy

Syntax **accounting-policy** *acct-policy-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no accounting-policy

Context [Tree] (config>app-assure>group>statistics>aa-admit-deny accounting-policy)
[Tree] (config>app-assure>group>statistics>aa-partition accounting-policy)
[Tree] (config>app-assure>group>statistics>aa-sub accounting-policy)
[Tree] (config>app-assure>group>statistics>aa-sub-study accounting-policy)
[Tree] (config>app-assure>group>statistics>application accounting-policy)
[Tree] (config>app-assure>group>statistics>app-grp accounting-policy)
[Tree] (config>app-assure>group>statistics>protocol accounting-policy)
[Tree] (config>isa>aa-grp>statistics accounting-policy)

Full Context configure application-assurance group statistics aa-admit-deny accounting-policy
configure application-assurance group statistics aa-partition accounting-policy
configure application-assurance group statistics aa-sub accounting-policy
configure application-assurance group statistics aa-sub-study accounting-policy
configure application-assurance group statistics app-group accounting-policy
configure application-assurance group statistics application accounting-policy
configure application-assurance group statistics protocol accounting-policy
configure isa aa-group statistics accounting-policy

Description This command specifies the existing accounting policy to use for AA. Accounting policies are configured in the **config>log>accounting-policy** context.

Parameters *acct-policy-id* — Specifies the existing accounting policy to use for applications.

Values 1 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context [Tree] (config>saa>test accounting-policy)

Full Context configure saa test accounting-policy

Description This command associates an accounting policy to the SAA test. The accounting policy must already be defined before it can be associated otherwise an error message is generated.

A notification (trap) is issued whenever a test is completed or terminates.

The **no** form of this command removes the accounting policy association.

Parameters *acct-policy-id* — Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>oam-pm>session>meas-interval accounting-policy)

Full Context configure oam-pm session meas-interval accounting-policy

Description This optional command allows the operator to assign an accounting policy and the policy-id (configured under the **config>log>accounting-policy**) with a record-type of complete-pm. This runs the data collection process for completed measurement intervals in memory, file storage, and maintenance functions moving data from memory to flash. A single accounting policy can be applied to a measurement interval.

The **no** form of this command removes the accounting policy.

Parameters *acct-policy-id* — Specifies the accounting policy to be applied to the measurement interval.

Values 1 to 99

Platforms All

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context **[Tree]** (config>service>pw-template accounting-policy)
[Tree] (config>service>sdp accounting-policy)

Full Context configure service pw-template accounting-policy
configure service sdp accounting-policy

Description This command creates the accounting policy context that can be applied to an SDP. An accounting policy must be defined before it can be associated with a SDP. If the *acct-policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SDP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SDP, and the accounting policy reverts to the default.

Default no accounting-policy

Parameters *acct-policy-id* — Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

accounting-policy

Syntax **accounting-policy** *policy-id* [**interval** *minutes*]
no accounting-policy *policy-id*

Context **[Tree]** (config>log accounting-policy)

Full Context configure log accounting-policy

Description This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.

Access accounting policies are policies that can be applied to one or more SAPs. Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.

If an accounting policy is not specified on a SAP, then accounting records are produced in accordance with the access policy designated as the **default**. If a default access policy is not specified, then no accounting records are collected other than the records for the accounting policies that are explicitly configured.

Only one policy can be regarded as the default access policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new access default policy can be configured.

Network accounting policies are policies that can be applied to one or more network ports or SONET/SDH channels. Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports or SONET/SDH channels where this policy is applied.

If no accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy as designated with the **default** command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured. Default accounting policies cannot be explicitly applied. For example, for **accounting-policy 10**, if default is set, then that policy cannot be used:

```
*A:75>config>service>vpls>spoke-sdp# accounting-policy 10
```

Only one policy can be regarded as the default network policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new network default policy can be configured.

The **no** form of this command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs, network ports or channels where the policy is applied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-id* — Specifies the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 to 99

Platforms All

5.46 accounting-port

accounting-port

Syntax **accounting-port** *port*
no accounting-port

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius accounting-port)

Full Context configure service vprn aaa remote-servers radius accounting-port

Description This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.

Default accounting-port 1813

Parameters *port* — Specifies the UDP port number.

Values 1 to 65535

Default 1813

Platforms All

accounting-port

Syntax **accounting-port** *port*
no accounting-port

Context **[Tree]** (config>system>security>radius accounting-port)

Full Context configure system security radius accounting-port

Description This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.

Default accounting-port 1813

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port* — Specifies the UDP port number.

Values 1 to 65535

Default 1813

Platforms All

5.47 accounting-type

accounting-type

Syntax **accounting-type** [**session**] [**tunnel**]
no accounting-type

Context **[Tree]** (config>aaa>l2tp-acct-plcy accounting-type)

Full Context configure aaa l2tp-accounting-policy accounting-type

Description This command specifies the accounting type for the L2TP tunnel accounting policy.

The **no** form of this command reverts to the default.

Default accounting-type session tunnel

Parameters **session** — Enables tunnel level accounting, including:
Tunnel-Link-Start
Tunnel-Link-Stop
Tunnel-Link-Reject

tunnel — Enables link level accounting, including:
Tunnel-Start
Tunnel-Stop
Tunnel-Reject

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.48 accounting-update-interval

accounting-update-interval

Syntax **accounting-update-interval** [*interval*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no accounting-update-interval

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range>xconnect accounting-update-interval)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range>xconnect accounting-update-interval)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect accounting-update-interval
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect accounting-update-interval

Description This command configures the time interval between consecutive interim accounting update messages. If not configured, the system does not send interim accounting update messages.

The **no** form of this command removes the value from the cross-connect configuration.

Parameters *interval* — Specifies the time interval between consecutive interim accounting update messages in minutes.

Values 5 to 259200

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

accounting-update-interval

Syntax **accounting-update-interval** [*interval*]
no accounting-update-interval

Context [Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm accounting-update-interval)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm accounting-update-interval)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt accounting-update-interval
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt accounting-update-interval

Description This command enables the interim accounting and specifies the interim accounting interval.

Parameters *interval* — Specifies the interim accounting interval in seconds.

Values 5 to 259200

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.49 acct-authentic

acct-authentic

Syntax [**no**] **acct-authentic**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute acct-authentic)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute acct-authentic

Description This command enables the generation of the acct-authentic RADIUS attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.50 acct-delay-time

acct-delay-time

Syntax [**no**] **acct-delay-time**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute acct-delay-time)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute acct-delay-time

Description This command enables the generation of the **acct-delay-time** RADIUS attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

acct-delay-time

Syntax [**no**] **acct-delay-time**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes acct-delay-time)

Full Context configure aaa isa-radius-policy acct-include-attributes acct-delay-time

Description This command enables the acct-delay-time.

Default no acct-delay-time

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.51 acct-include-attributes

acct-include-attributes

Syntax [**no**] **acct-include-attributes**

Context **[Tree]** (config>aaa>isa-radius-plcy acct-include-attributes)

Full Context configure aaa isa-radius-policy acct-include-attributes

Description This command configures attributes to be included in RADIUS accounting messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.52 acct-interim

acct-interim

Syntax **acct-interim min** *min-val* **max** *max-val* **lifetime** *lifetime*
no acct-interim

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>buffering acct-interim)

Full Context configure aaa radius-server-policy servers buffering acct-interim

Description This command enables RADIUS accounting interim update message buffering.

1. The message is stored in the buffer, a lifetime timer is started and the message is sent to the RADIUS server
2. If after retry*timeout seconds no RADIUS accounting response is received for the interim update then a new attempt to send the message is started after minimum[(min-val*2n), max-val] seconds.
3. Repeat step 2 until for one of the following:
   a. a RADIUS accounting response is received.
   b. the lifetime of the buffered message expires.
   c. a new RADIUS accounting interim-update or a RADIUS accounting stop for the same accounting session-id and radius-server-policy is stored in the buffer.
   d. the message is manually purged from the message buffer via a clear command.
4. The message is purged from the buffer.

The **no** form of this command disables RADIUS accounting interim update message buffering.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *min-val* — Specifies the minimum interval in seconds between attempts to resend the RADIUS accounting interim update.

Values 1 to 3600

max-val — Specifies the maximum interval in seconds between attempts to resend the RADIUS accounting interim update.

Values 1 to 3600

lifetime — Specifies the lifetime in hours.

Values 1 to 25

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.53 acct-on-off

acct-on-off

Syntax **acct-on-off**
acct-on-off monitor-group *group-name*
acct-on-off oper-state-change [**group** *group-name*]

Context **[Tree]** (config>aaa>radius-srv-plcy acct-on-off)

Full Context configure aaa radius-server-policy acct-on-off

Description This command controls the sending of Accounting-On and Accounting-Off messages and the acct-on-off oper-state of the radius-server-policy:

acct-on-off: enables the sending of Accounting-On and Accounting-Off messages for this radius-server-policy. The acct-on-off oper-state is always not blocked.

acct-on-off oper-state-change [group *group-name*]: enables the sending of Accounting-On and Accounting-Off messages for this radius-server-policy. The acct-on-off oper-state is function of the Accounting-response received for the Accounting-On and Accounting-Off. Optionally, sets the acct-on-off oper-state of the acct-on-off-group.

acct-on-off monitor-group *group-name*: no Accounting-On and Accounting-Off messages are sent for this radius-server-policy. The acct-on-off oper-state is inherited from the acct-on-off-group.

The **no** form of this command disables the sending of Accounting-On and Accounting-Off messages.

Parameters *group-name* — Specifies the name of an acct-on-off group up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.54 acct-on-off-group

acct-on-off-group

Syntax **acct-on-off-group** *group-name* [**create**]
no acct-on-off-group *group-name*

Context **[Tree]** (config>aaa acct-on-off-group)

Full Context configure aaa acct-on-off-group

Description This command creates an acct-on-off-group.

An acct-on-off-group can be referenced by:

- A single radius-server-policy as controller — The acct-on-off oper-state of the acct-on-off-group is set to the acct-on-off oper-state of the radius-server-policy.
- Multiple radius-server-policies as monitor — The acct-on-off oper-state of the radius-server-policy is inherited from the acct-on-off oper-state of the acct-on-off group.

The **no** form of this command deletes the acct-on-off-group.

Parameters *group-name* — Specifies the name of an acct-on-off group up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.55 acct-policy

acct-policy

Syntax **acct-policy** *acct-policy-name* [**duplicate** *acct-policy-name*]
no acct-policy

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host acct-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host acct-policy)

Full Context configure subscriber-mgmt local-user-db ipoe host acct-policy
configure subscriber-mgmt local-user-db ppp host acct-policy

Description This command specifies the accounting policy used for sending an Accounting Stop message to report RADIUS authentication failures of PPPoE sessions. A duplicate policy can be specified if a copy of the Accounting Stop message must be sent to another destination.

Reporting RADIUS authentication failures with an Accounting Stop message must be enabled in the RADIUS authentication policy (“send-acct-stop-on-fail”).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A duplicate RADIUS accounting policy can be specified if the accounting stop resulting from a RADIUS authentication failure must also be sent to a second RADIUS destination.

The **no** form of this command reverts to the default.

Parameters *acct-policy-name* — Specifies the name of a RADIUS accounting policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.56 acct-port

acct-port

Syntax **acct-port** *port*
no acct-port

Context **[Tree]** (config>router>radius-server>server acct-port)
[Tree] (config>service>vprn>radius-server>server acct-port)

Full Context configure router radius-server server acct-port
configure service vprn radius-server server acct-port

Description This command specifies the UDP listening port for RADIUS accounting requests.

The **no** form of this commands resets the UDP port to its default value (1813)

Default acct-port 1813

Parameters *port* — Specifies the UDP listening port for accounting requests of the external RADIUS server.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.57 acct-request-script-policy

acct-request-script-policy

Syntax **acct-request-script-policy** *policy-name*
no acct-request-script-policy

Context **[Tree]** (config>subscr-mgmt>acct-plcy acct-request-script-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt radius-accounting-policy acct-request-script-policy

Description This command configures the Python script policy to modify Accounting-Request messages.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the Python script policy to modify Accounting-Request messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

acct-request-script-policy

Syntax **acct-request-script-policy** *policy-name*
no acct-request-script-policy

Context **[Tree]** (config>aaa>radius-srv-plcy acct-request-script-policy)

Full Context configure aaa radius-server-policy acct-request-script-policy

Description This command specifies the name of the RADIUS script policy used to change the RADIUS attributes of the Accounting-Request messages.

Parameters *policy-name* — Specifies the name of the Python script to modify Accounting-Request messages, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.58 acct-session-id

acct-session-id

Syntax **acct-session-id** [*session-id-type*]
no acct-session-id

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute acct-session-id)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute acct-session-id

Description The **acct-session-id** attribute for each subscriber host is generated at the very beginning of the session initiation. This command will enable or disable sending this attribute to the RADIUS server in the Access-Request messages regardless of whether the accounting is enabled or not. The **acct-session-id** attribute can be used to address the subscriber hosts from the RADIUS server in the CoA Request.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **acct-session-id** attribute is unique per subscriber host network wide. It is a 22 byte field comprised of the system MAC address along with the creation time and a sequence number in a hex format.

The **no** form of this command reverts to the default.

Default no acct-session-id

Parameters *session-id-type* — Specifies the format for the **acct-session-id** attribute used in RADIUS accounting requests.

Values host, session

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.59 acct-stats

acct-stats

Syntax [**no**] **acct-stats**

Context **[Tree]** (config>ipsec>rad-acct-plcy>include acct-stats)

Full Context configure ipsec radius-accounting-policy include-radius-attribute acct-stats

Description This command enables the system to include accounting attributes in RADIUS acct-stop and interim-update packets.

The **no** form of this command disables the system from including accounting attributes in RADIUS acct-stop and interim-update packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.60 acct-stop

acct-stop

Syntax **acct-stop min** *min-val* **max** *max-val* **lifetime** *lifetime*
no acct-stop

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>buffering acct-stop)

Full Context configure aaa radius-server-policy servers buffering acct-stop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables RADIUS accounting stop message buffering.

1. The message is stored in the buffer, a lifetime timer is started and the message is sent to the RADIUS server
2. If after retry*timeout seconds no RADIUS accounting response is received for the accounting stop, then a new attempt to send the message is started after minimum[(min-val*2n), max-val] seconds.
3. Repeat step 2 until
   a. a RADIUS accounting response is received, or
   b. the lifetime of the buffered message expires, or
   c. the message is manually purged from the message buffer via a clear command
4. The message is purged from the buffer.

The **no** form of this command disables RADIUS accounting stop message buffering.

Parameters *min-val* — Specifies the minimum interval in seconds between attempts to resend the RADIUS accounting stop.

Values 1 to 3600

max-val — Specifies the maximum interval in seconds between attempts to resend the RADIUS accounting stop.

Values 1 to 3600

lifetime — Specifies the lifetime in hours.

Values 1 – 25

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.61 acct-trigger-reason

acct-trigger-reason

Syntax [**no**] **acct-trigger-reason**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes acct-trigger-reason)

Full Context configure aaa isa-radius-policy acct-include-attributes acct-trigger-reason

Description This command enables the acct-trigger-reason.

Default no acct-trigger-reason

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.62 acct-tunnel-connection-fmt

acct-tunnel-connection-fmt

Syntax **acct-tunnel-connection-fmt** *ascii-spec*
no acct-tunnel-connection-fmt

Context **[Tree]** (config>aaa>l2tp-acct-plcy acct-tunnel-connection-fmt)

Full Context configure aaa l2tp-accounting-policy acct-tunnel-connection-fmt

Description This command configures the accounting tunnel connection ascii-specification.

Default no acct-tunnel-connection-fmt

Parameters *ascii-spec* — Specifies the ASCII specifications.

<ascii-spec>	<char-specification> <ascii-spec>	
char-specification	<ascii-char> | <char-origin>	
ascii-char	a printable ASCII character	
char-origin	%<origin>	
origin	n | s | S | t | T | c | C	
	n	Call Serial Number
	s | S	Local (s) or Remote (S) Session Id
	t | T	Local (t) or Remote (T) Tunnel Id
	c | C	Local (c) or Remote (C) Connection Id

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

acct-tunnel-connection-fmt

Syntax **acct-tunnel-connection-fmt** *ascii-spec*
no acct-tunnel-connection-fmt

Context **[Tree]** (config>subscr-mgmt>acct-plcy acct-tunnel-connection-fmt)

Full Context configure subscriber-mgmt radius-accounting-policy acct-tunnel-connection-fmt

Description This command specifies the string that is sent in the accounting message.

Default no acct-tunnel-connection-fmt

Parameters *ascii-spec* — Specifies the accounting tunnel connection ASCII specification.

Values

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

asci-spec	<*char-specification*> <*ascii-spec*>	
char-specification	<*ascii-char*> | <*char-origin*>	
ascii-char	A printable ASCII character	
char-origin	%<origin>	
origin	n | s | S | t | T | c | C	
	n	Call Serial Number
	s | S	Local (s) or Remote (S) Session Id
	t | T	Local (t) or Remote (T) Tunnel Id
	c | C	Local (c) or Remote (C) Connection Id

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.63 acct-update-triggers

acct-update-triggers

Syntax **acct-update-triggers**

Context **[Tree]** (config>aaa>isa-radius-plcy acct-update-triggers)

Full Context configure aaa isa-radius-policy acct-update-triggers

Description Commands in this context enable or disable the sending of triggered interim-updates, with the exception of the following:

- After an update interval change, an interim update is always sent to indicate the start of the new interval.
- Mobility-triggered updates are configured in the (**service vprn <svc-id> | router**) **wlan-gw mobility-triggered-acct** context.
- NAT port block allocation depends on the inclusion of NAT-related attributes (port-range, outside-service, outside-ip).

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.64 accu-stats-policy

accu-stats-policy

Syntax **accu-stats-policy** *policy-name* [**create**]
no accu-stats-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt accu-stats-policy)

Full Context configure subscriber-mgmt accu-stats-policy

Description This command creates a storage policy for cumulative statistics for subscribers. The policy defines the specific direction for the policer or the queue to be stored and performs the following functions.

- The policy stores subscriber statistics even if the subscriber session has ended. The subscriber statistics can be viewed even if the subscriber is offline.
- When the subscriber session ends, the statistics are added to the past statistics stored in memory so that all previous session statistics are accumulated. The accumulated statistics are not persistent; they are only stored in memory and reset to zero when the chassis reboots.

The **no** form of this command deletes the policy only when it is no longer referenced by a subscriber profile.

Parameters *policy-name* — Specifies the name for the policy, up to 32 characters.

create — Configures an entry for the policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

accu-stats-policy

Syntax **accu-stats-policy** *policy-name*
no accu-stats-policy

Context **[Tree]** (config>subscr-mgmt>sub-profile accu-stats-policy)

Full Context configure subscriber-mgmt sub-profile accu-stats-policy

Description This command associates an accumulated statistics policy with a subscriber profile.

The **no** form of this command removes the association of the accu-stats-policy from the subscriber profile. It is possible to remove the policy from the subscriber profile while the subscriber is still online, however, the statistics remain in memory and must be cleared manually, using the **clear subscriber-mgmt accu-stats active-subs no-accu-stats-policy** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the name of the accumulated statistics policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.65 ack

ack

Syntax **ack** [**detail**]
no ack

Context **[Tree]** (debug>router>gmpls>packet ack)

Full Context debug router gmpls packet ack

Description This command enables debugging for GMPLS Ack packets.

The **no** form of the command disables debugging for GMPLS Ack packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ack

Syntax **ack** [**detail**]
no ack

Context **[Tree]** (debug>router>rsvp>packet ack)

Full Context debug router rsvp packet ack

Description This command debugs ack events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about ack events.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.66 ack-auth-retry-count

ack-auth-retry-count

Syntax **ack-auth-retry-count** [*value*]
no ack-auth-retry-count

Context **[Tree]** (config>router>wpp>portals>portal ack-auth-retry-count)
[Tree] (config>service>vprn>wpp>portals>portal ack-auth-retry-count)

Full Context configure router wpp portals portal ack-auth-retry-count
configure service vprn wpp portals portal ack-auth-retry-count

Description This command configures the number of retransmissions of an ACK_OUT message.

The **no** form of this command reverts to the default.

Default ack-auth-retry-count 5

Parameters *value* — Specifies the number of retransmissions of an ACK_OUT message.

Values 0 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.67 ack-timeout

ack-timeout

Syntax **ack-timeout** *timer*
no ack-timeout

Context **[Tree]** (config>port>ml-bundle>mlfr ack-timeout)

Full Context configure port multilink-bundle mlfr ack-timeout

Description This command specifies the value of the MLFR bundle T_ACK timer.

This timer defines the maximum period to wait for a response to any message sent onto the bundle link before attempting to retransmit a message onto the bundle link.

Default ack-timeout 4

Parameters *timer* — Specifies the wait period in seconds.

Values 1 to 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e

5.68 acknowledgment

acknowledgment

Syntax [**no**] **acknowledgment**

Context **[Tree]** (config>service>apipe>spoke-sdp>control-channel-status acknowledgment)
[Tree] (config>service>cpipe>spoke-sdp>control-channel-status acknowledgment)
[Tree] (config>service>epipe>spoke-sdp>control-channel-status acknowledgment)
[Tree] (config>service>vpls>spoke-sdp>control-channel-status acknowledgment)

Full Context configure service apipe spoke-sdp control-channel-status acknowledgment
configure service cpipe spoke-sdp control-channel-status acknowledgment
configure service epipe spoke-sdp control-channel-status acknowledgment
configure service vpls spoke-sdp control-channel-status acknowledgment

Description This command enables the acknowledgment of control channel status messages. By default, no acknowledgment packets are sent.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp control-channel-status acknowledgment

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp control-channel-status acknowledgment

All

- configure service epipe spoke-sdp control-channel-status acknowledgment
- configure service vpls spoke-sdp control-channel-status acknowledgment

acknowledgment

Syntax [**no**] **acknowledgment**

Context **[Tree]** (config>service>ies>if>spoke-sdp>control-channel-status acknowledgment)
[Tree] (config>service>ies>red-if>spoke-sdp>control-channel-status acknowledgment)

Full Context configure service ies interface spoke-sdp control-channel-status acknowledgment
configure service ies redundant-interface spoke-sdp control-channel-status acknowledgment

Description This command enables the acknowledgment of control channel status messages. By default, no acknowledgment packets are sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no acknowledgment

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies redundant-interface spoke-sdp control-channel-status acknowledgment

All

- configure service ies interface spoke-sdp control-channel-status acknowledgment

acknowledgment

Syntax [**no**] **acknowledgment**

Context **[Tree]** (config>service>vprn>if>spoke-sdp>control-channel-status acknowledgment)
[Tree] (config>service>vprn>red-if>spoke-sdp>control-channel-status acknowledgment)

Full Context configure service vprn interface spoke-sdp control-channel-status acknowledgment
configure service vprn redundant-interface spoke-sdp control-channel-status acknowledgment

Description This command enables the acknowledgment of control channel status messages. By default, no acknowledgment packets are sent.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp control-channel-status acknowledgment

All

- configure service vprn interface spoke-sdp control-channel-status acknowledgment

acknowledgment

Syntax [**no**] **acknowledgment**

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp>control-channel-status acknowledgment)
[Tree] (config>mirror>mirror-dest>spoke-sdp>control-channel-status acknowledgment)

Full Context configure mirror mirror-dest remote-source spoke-sdp control-channel-status acknowledgment
configure mirror mirror-dest spoke-sdp control-channel-status acknowledgment

Description This command enables the acknowledgment of control channel status messages. By default, no acknowledgment packets are sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.69 action

action

Syntax **action bypass-host-creation**
action drop
no action

Context **[Tree]** (config>filter>dhcp-filter>entry action)

Full Context configure filter dhcp-filter entry action

Description This command specifies the action to take on DHCP host creation when the filter entry matches.

The **no** form of this command reverts to the default wherein the host creation proceeds as normal.

Parameters **bypass-host-creation** — Specifies that the host creation is bypassed.

drop — Specifies that the DHCP message is dropped.

Platforms All

action

Syntax **action bypass-host-creation** [**na**] [**pd**]
action drop
no action

Context **[Tree]** (config>filter>dhcp6-filter>entry action)

Full Context configure filter dhcp6-filter entry action

Description This command specifies the action to take on DHCP6 host creation when the filter entry matches.

The **no** form of this command reverts to the default wherein the host creation proceeds as normal.

Parameters **bypass-host-creation** — Specifies that the host creation is bypassed.

Values **na** — Bypasses the DHCP6 NA hosts creation.
pd — Bypasses the DHCP6 PD hosts creation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

drop — Specifies that the DHCP6 message is dropped.

Platforms All

action

Syntax **action** {**accept** | **next-entry** | **next-policy** | **drop** | **reject**}
no action

Context **[Tree]** (config>router>policy-options>policy-statement>entry action)

Full Context configure router policy-options policy-statement entry action

Description This command creates the context to configure actions to take for routes matching a route policy statement entry.

This command is required and must be entered for the entry to be active.

Any route policy entry without the **action** command will be considered incomplete and will be inactive.

The **no** form of this command deletes the action context from the entry.

Default no action

Parameters **accept** — Specifies that routes matching the entry match criteria will be accepted and propagated.

next-entry — Specifies that the actions specified would be made to the route attributes and then policy evaluation would continue with next policy entry (if any others are specified).

next-policy — Specifies that the actions specified would be made to the route attributes and then policy evaluation would continue with next route policy (if any others are specified).

drop — Specifies that routes matching the entry match criteria should be rejected. This parameter provides a context for modifying route properties.

reject — Specifies that routes matching the entry match criteria should be rejected. This parameter does not provide a context for modifying route properties.

Platforms All

action

Syntax **action** *dhcp-action*
no action

Context **[Tree]** (config>service>ies>if>dhcp>option action)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>dhcp>option action)
[Tree] (config>service>vpls>sap>dhcp>option action)
[Tree] (config>service>vprn>if>dhcp>option action)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option action)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option action)

Full Context

configure service ies interface dhcp option action
configure service ies subscriber-interface group-interface dhcp option action
configure service vpls sap dhcp option action
configure service vprn interface dhcp option action
configure service vprn subscriber-interface group-interface dhcp option action
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option action

Description

This command configures the processing required when the SR-Series receives a DHCP request that already has a Relay Agent Information Option (Option 82) field in the packet.

The **no** form of this command returns the system to the default value.

Default

action keep — Per RFC 3046, *DHCP Relay Agent Information Option*, section 2.1.1, *Reforwarded DHCP requests*. The default is to keep the existing information intact. The exception to this is if the giaddr of the received packet is the same as the ingress address on the router. In that case the packet is dropped and an error is logged.

Parameters

replace — In the upstream direction (from the user), the existing Option 82 field is replaced with the Option 82 field from the router. In the downstream direction (towards the user) the Option 82 field is stripped (in accordance with RFC 3046).

drop — Specifies that the packet is dropped, and an error is logged.

keep — Specifies that the existing information is kept in the packet and the router does not add any additional information. In the downstream direction the Option 82 field is not stripped and is sent on towards the client.

The behavior is slightly different in case of Vendor Specific Options (VSOs). When the keep parameter is specified, the router inserts its own VSO into the Option 82 field. This is only done when the incoming message has already an Option 82 field.

If no Option 82 field is present, the router will not create the Option 82 field. In this in that case, no VSO is added to the message.

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option action
- configure service ies subscriber-interface group-interface dhcp option action
- configure service vprn subscriber-interface group-interface dhcp option action

All

- configure service ies interface dhcp option action
- configure service vpls sap dhcp option action
- configure service vprn interface dhcp option action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

action

Syntax **action** {**drop** | **forward**}
no action

Context **[Tree]** (config>service>vprn>log>filter>entry action)
[Tree] (config>log>filter>entry action)

Full Context configure log filter entry action
configure service vprn log filter entry action

Description This command specifies a drop or forward action associated with the filter entry. If neither **drop** nor **forward** is specified, the default-action will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.

Multiple action statements entered will overwrite previous actions.

The **no** form of this command removes the specified action statement.

Default Action specified by the **default-action** command will apply.

Parameters **drop** — Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

Platforms All

action

Syntax **action** *direction* [**create**]
no action *direction*

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry action)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action

Description Commands in this context configure an action to be performed for traffic that matches a configured match criteria in the filter entry. The action can be configured as being applicable to upstream traffic, downstream traffic, or both.

The **no** form of this command removes the direction from the configuration.

Parameters *direction* — Specifies the direction for the action in a VAS filter entry.

Values upstream, downstream

create — Keyword used to create the action's direction. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

action

Syntax **action drop**
action forward
action http-redirect *url* [**allow-override**]
no action

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry action)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry action)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry action)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry action)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry action
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry action
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry action
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry action

Description This command configures the action for the filter entry.

The **no** form of this command reverts to the default.

Default action drop

Parameters **drop** — Specifies to drop the packets matching the IP filter entry.

forward — Specifies to forward the packets matching the IP filter entry.

http-redirect *url* [**allow-override**] — Specifies the HTTP web address, up to 255 characters, that is sent to the user's browser for redirection.

Note: This action is not supported for IPv6 filter entries.

The specified URL can be overridden by a Diameter Credit Control Server when the following conditions are met:

- a Final-Unit-Indication AVP is present in the Multiple-Services-Credit-Control AVP of a CCA message
- the Final-Unit-Action AVP is set to REDIRECT (1)
- a Redirect-Server AVP is included with the following:
  - the Redirect-Address-Type AVP set to URL (2)
  - the Redirect-Server-Address AVP containing the URL to use for this rating group (**category-map**)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- the out of credit action for the corresponding rating group is set to **change-service-level** using one of the following commands:
  - **configure>subscriber-mgmt>credit-control-policy** *policy-name***>out-of-credit-action change-service-level**
  - **configure>subscriber-mgmt>category-map** *category-map-name* **category** *category-name***>out-of-credit-action-override change-service-level**
- an IPv4 HTTP redirect action with **allow-override** is specified in the exhausted credit service level context for the corresponding rating group using the command **configure>subscriber-mgmt>category-map** *category-map-name* **category** *category-name*>**exhausted-credit-service-level>ingress-ip-filter-entries**>**entry** *entry-id*>**action http-redirect** *url* **allow-override**

In all other cases, the URL specified in the Redirect-Server-Address AVP is ignored and the configured URL is used. The URL received from the Credit Control Server is included in the output of **show>service>active-subscribers>credit-control**. The **allow-override** is ignored for RADIUS credit control.

The following variables can optionally be added in the configured URL (http-redirect url) and in the override URL from the Credit Control Server (Redirect-Server-Address AVP):

- $IP – Customer's IP address
- $MAC – Customer's MAC address
- $URL – Original requested URL
- $SAP – Customer's SAP
- $SUB – Customer's subscriber identification string
- $CID – string that represents the circuit-id or interface-id of the subscriber host (hexadecimal format)
- $RID – string that represents the remote-id of the subscriber host (hexadecimal format)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action** {**alarm** | **remove**}
no action

Context **[Tree]** (config>subscr-mgmt>shcv-policy>periodic action)

Full Context configure subscriber-mgmt shcv-policy periodic action

Description This command configures the action to take when the periodic connectivity verification failed.

The **no** form of this command reverts to the default.

Default action alarm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **alarm** — Raises an alarm indicating that the host is disconnected.

remove — Raises an alarm and releases all allocated resources (addresses, prefixes, queues, table entries, and so on). Static hosts are removed.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action** {**drop** | **forward** | **none**}
action http-redirect *rdr-url-string*
no action

Context **[Tree]** (config>subscr-mgmt>isa-filter>entry action)
[Tree] (config>subscr-mgmt>isa-filter>ipv6>entry action)

Full Context configure subscriber-mgmt isa-filter entry action
configure subscriber-mgmt isa-filter ipv6 entry action

Description This command specifies what should happen to packets that do match this entry.

The **no** form of this command reverts to the default value.

Default action none

Parameters **drop** — Specifies to drop the packet.

forward — Specifies to forward the packet.

none — Specifies to ignore the entry and continue processing with subsequent entries.

rdr-url-string — Specifies the URL to which matching HTTP flows are redirected, up to 255 characters. The URL can be overridden by AAA. Non-HTTP packets are dropped. The URL supports the $URL, $MAC, and $IP variables. For other macro substitutions, the string is not modified.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action** {**permit-deny** | **priority-mark**}
no action

Context **[Tree]** (config>subscr-mgmt>isa-policer action)

Full Context configure subscriber-mgmt isa-policer action

Description This command specifies what happens to packets that are in-profile and out-of-profile.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default action permit-deny

Parameters **permit-deny** — Drops all packets that are out of profile (they do not conform to the PIR).

priority-mark — Currently not supported. The policer will take no action.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action** {**log-only** | **reset-mda** | **fail-mda**}
no action

Context **[Tree]** (config>card>mda>event action)

Full Context configure card mda event action

Description This command defines the action to be taken when a specific hardware error event is raised against the target mda.

Only one action can be enabled at a time. Entering a new action will override a previously defined action.

The **no** form of this command sets the action to the default value.

Default action log-only

Parameters **log-only** — Specifies to pass the log event to log management. No other action is taken.

reset-mda — Specifies to reset the mda.

fail-mda — Specifies to set the operational state of the mda to Failed. This Failed state will persist until the clear mda command is issued (reset) or the mda is removed and re-inserted (re-seat).

Platforms All

action

Syntax [**no**] **action**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization action)

Full Context configure system security profile netconf base-op-authorization action

Description This command enables the NETCONF action operation.

The **no** form of this command disables the operation.

Default no action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

action

Syntax **action** {**priority-mark** | **permit-deny**}

Context **[Tree]** (config>app-assure>group>policer action)

Full Context configure application-assurance group policer action

Description This command configures the action to be performed by single-bucket bandwidth policers for non-conformant traffic.

Dual bucket bandwidth policers cannot have their action configured and always mark traffic below CIR in profile, between CIR and PIR out of profile, and drop traffic above PIR. Flow policers always discard non-conformant traffic.

When multiple application assurance policers are configured against a single flow (including policers at both subscriber and system), the final action done to the flow/packet will be a logical OR of all policers actions. For example, if only of the policers requires the packet to be discarded, the packet will be dropped regardless of the action of the other policers.

Default action permit-deny

Parameters **priority-mark** — Non-conformant traffic will be marked out of profile and the conformant traffic will be marked in profile. The new marking will overwrite any previous IOM QoS marking done to a packet.

permit-deny — Non-conformant traffic will be dropped.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action**

Context **[Tree]** (config>app-assure>group>policy>aqp>entry action)

Full Context configure application-assurance group policy app-qos-policy entry action

Description Commands in this context configure AQP actions to be performed on flows that match the AQP entry's match criteria.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

action

Syntax **action** {**permit** | **deny**} [**event-log** *event-log-name*]
action http-redirect *http-redirect-name* [**event-log** *event-log-name*]
action tcp-optimizer *tcp-optimizer-name*

Context **[Tree]** (config>app-assure>group>sess-fltr>entry action)

Full Context configure application-assurance group session-filter entry action

Description This command configures the action for this entry.

Parameters **deny** — Packets matching the criteria are denied.

permit — Packets matching the criteria are permitted.

event-log-name — Specifies the event log name, up to 32 characters.

http-redirect-name — Specifies the HTTP redirect name, up to 32 characters.

tcp-optimizer — Specifies to use TCP Optimization (TCPO) on the matching flows.The TCPO policy referenced within this session filter entry is configured under the AA group. If the TCPO action is removed from a session-filter entry, the existing flows are not affected. However, no new TCP flows are optimized.

tcp-optimizer-name — Specifies the name of the TCPO policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action** {**permit** | **deny**}

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>imsi-apn-fltr>entry action)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter entry action

Description This command configures an action for the IMSI-APN filter entry.

Default action permit

Parameters **permit** — Specifies to permit packets that do not match any message entries.

deny — Specifies to deny packets that do not match any message entries.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

action

Syntax **action** {**dnat** | **forward**} [**ip-address** *ip-address*]
no action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>nat>nat-classifier>entry action)

Full Context configure service nat nat-classifier entry action

Description This command specifies the action to take for packets that match this nat-classifier entry. The **no** form of the command removes the specified action statement. By default, the entry is ignored (skipped). Consequently, the action from another matching entry is applied. If there are no other matching entries found, the default-action is applied.

Default no action.

Parameters **dnat** — Performs the DNAT function. The destination IP address of the packet traversing the router in the direction from inside to outside is replaced by the configured IP address. Destination port is not translated. In the opposite direction (from outside to inside), the source address in the returning packet is restored to the original value.

forward — Specifies that the forward action ensures that the packet is transparently passed through the nat-classifier.

ip-address *ip-address* — Specifies that the destination IP address replaces the original IP address in the packet traveling from inside to outside.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

action

Syntax [**no**] **action** [**secondary**]

Context [Tree] (config>filter>ip-filter>entry action)
[Tree] (config>filter>ipv6-filter>entry action)
[Tree] (config>filter>mac-filter>entry action)

Full Context configure filter ip-filter entry action
configure filter ipv6-filter entry action
configure filter mac-filter entry action

Description Commands in this context configure a primary (no option specified) or secondary (**secondary** option specified) action to be performed on packets matching this filter entry. An ACL filter entry remains inactive (is not programmed in hardware) until a specific action is configured for that entry.

A primary action supports any filter entry action, a secondary action is used for redundancy and defines a redundant Layer 3 PBR action for an Layer 3 PBR primary action or a redundant L2 PBF action for a Layer 2 PBF primary action.

The **no** form of this command removes the specific action configured in the context of the action command. The primary action cannot be removed if a secondary action exists.

Default no action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **secondary** — Specifies a secondary action to be performed on packets matching this filter entry. A secondary action can only be configured if a primary action is configured.

Platforms All

action

Syntax **action** [**fc** *fc-name*] [**priority** {**high** | **low**}] [**policer** *policer-id*]
no action

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry action)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry action)
[Tree] (config>qos>sap-ingress>mac-criteria>entry action)

Full Context configure qos sap-ingress ip-criteria entry action
configure qos sap-ingress ipv6-criteria entry action
configure qos sap-ingress mac-criteria entry action

Description This mandatory command associates the forwarding class or enqueuing priority with specific IP, IPv6, or MAC criteria entry ID. The action command supports setting the forwarding class parameter to a subclass. Packets that meet all match criteria within the entry have their forwarding class and enqueuing priority overridden based on the parameters included in the **action** parameters. When the forwarding class is not specified in the **action** command syntax, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueuing priority is not specified in the action, a matching packet preserves (or inherits) the existing enqueuing priority derived from earlier matches in the classification hierarchy.

When a policer is specified in the action, a matching packet is directed to the configured policer instead of the policer/queue assigned to the forwarding class of the packet.

The **action** command must be executed for the match criteria to be added to the active list of entries. If the entry is designed to prevent more explicit (higher entry ID) entries from matching certain packets, the **fc** *fc-name* and **match** *protocol* fields should not be defined when executing action. This allows packets matching the entry to preserve the forwarding class and enqueuing priority derived from previous classification rules.

Each time action is executed on a specific entry ID, the previously entered values for **fc** *fc-name* and **priority** are overridden with the newly defined parameters or inherit previous matches when a parameter is omitted.

The **no** form of this command removes the entry from the active entry list. Removing an entry on a policy immediately removes the entry from all SAPs using the policy. All previous parameters for the action is lost.

If no action is specified, the action specified by the **default-fc** command will be used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **fc** *fc-name* — The value given for **fc** *fc-name* must be one of the predefined forwarding classes in the system. Specifying the **fc** *fc-name* is required. When a packet matches the rule, the forwarding class is only overridden when the **fc** *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

The *subclass-name* parameter is optional and used with the *fc-name* parameter to define a pre-existing subclass. The *fc-name* and *subclass-name* parameters must be separated by a period (.). If *subclass-name* does not exist in the context of *fc-name*, an error will occur. If *subclass-name* is removed using the **no fc** *fc-name.subclass-name* **force** command, the **default-fc** command will automatically drop the *subclass-name* and only use *fc-name* (the parent forwarding class for the subclass) as the forwarding class.

Values

fc: *class*[.*subclass*]

class: be, l2, af, l1, h2, ef, h1, nc

subclass: 29 characters max

Default Inherit (When **fc** *fc-name* is not defined, the rule preserves the previous forwarding class of the packet.)

priority — The **priority** parameter overrides the default enqueuing priority for all packets received on a SAP using this policy that match this rule. Specifying the priority (**high** or **low**) is optional. When a packet matches the rule, the enqueuing priority is only overridden when the priority parameter is defined on the rule. If the packet matches and priority is not explicitly defined in the rule, the enqueuing priority is inherited based on previous rule matches.

Default Inherit (When the **priority** (**high** or **low**) is not defined, the rule preserves the previous enqueuing priority of the packet)

high — The **high** parameter is used in conjunction with the **priority** parameter. Setting the **priority** enqueuing parameter to **high** for a packet increases the likelihood to enqueue the packet when the queue is congested. The enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the queue, the significance of the enqueuing priority is lost.

low — The **low** parameter is used in conjunction with the **priority** parameter. Setting the **priority** enqueuing parameter to **low** for a packet decreases the likelihood to enqueue the packet when the queue is congested. The enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Default Inherit

policer-id — A valid policer-id must be specified. The parameter policer-id references a policer-id that has already been created within the sap-ingress QoS policy.

Values 1 to 63

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

action

Syntax **action** [**fc** *fc-name*] [**profile** {**in** | **out** | **exceed** | **inplus**}] [**policer** *policer-id*] [**port-redirect-group-queue**] [**queue** *queue-id*] [**use-fc-mapped-queue**]
no action

Context **[Tree]** (config>qos>sap-egress>ip-criteria>entry action)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry action)

Full Context configure qos sap-egress ip-criteria entry action
configure qos sap-egress ipv6-criteria entry action

Description This command defines the reclassification actions that should be performed on any packet matching the defined IP flow criteria within the entries match node. When defined under the **ip-criteria** context, the reclassification only applies to IPv4 packets. When defined under the **ipv6-criteria** context, the reclassification only applies to IPv6 packets.

If an egress packet on the SAP matches the specified IP flow entry, the forwarding class, or profile or egress queue accounting behavior may be overridden. By default, the forwarding class and profile of the packet is derived from ingress classification and profiling functions. Matching an IP flow reclassification entry will override all IP precedence- or DSCP-based reclassification rule actions when an explicit reclassification action is defined for the entry.

It is also possible to redirect the egress packet to a configured policer. The forwarding class or profile can also be optionally specified.

When an IP flow entry is first created, the entry will have no explicit behavior defined as the reclassification actions to be performed. In **show** and **info** commands, the entry will display no action as the specified reclassification action for the entry. When the entry is defined with no action, the entry will not be populated in the IP flow reclassification list used to evaluate packets egressing a SAP with the SAP egress policy defined. An IP flow reclassification entry is only added to the evaluation list when the action command for the entry is executed either with explicit reclassification entries or without any actions defined. Specifying action without any trailing reclassification actions allows packets matching the entry to exit the evaluation list without matching entries lower in the list. Executing no action on an entry removes the entry from the evaluation list and also removes any explicitly defined reclassification actions associated with the entry.

The **fc** keyword is optional. When specified, the egress classification rule will overwrite the forwarding class derived from ingress. The new forwarding class is used for egress remarking and queue mapping decisions.

The **profile** keyword is optional. When specified, the egress classification rule will overwrite the profile of the packet derived from ingress. The new profile value is used for egress remarking and queue congestion behavior.

The **policer** keyword is optional. When specified, the egress packet will be redirected to the configured policer. Optional parameters allow the user to control how the forwarded policed traffic exits the egress port. By default, the policed forwarded traffic will use a queue in the egress port’s policer-output-queue queue group; alternatively, a queue in an instance of a user-configured queue group can be used or a local SAP egress queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes all reclassification actions from the IP flow reclassification entry and also removes the entry from the evaluation list. An entry removed from the evaluation list will not be matched to any packets egress a SAP associated with the SAP egress QoS policy.

Parameters **fc** *fc-name* — The fc reclassification action is optional. When specified, packets matching the IP flow reclassification entry will be explicitly reclassified to the forwarding class specified as fc-name regardless of the ingress classification decision. The fc-name defined must be one of the eight forwarding classes supported by the system. To remove the forwarding class reclassification action for the IP flow entry, the action command must be re-executed without the fc reclassification action defined.

Values

fc	class	
	class	be, l2, af, l1, h2, ef, h1, nc

profile {in | out | exceed | inplus} — The profile reclassification action is optional. When specified, packets matching the IP flow reclassification entry will be explicitly reclassified to the configured profile regardless of the ingress profiling decision. To remove the profile reclassification action for the IP flow reclassification entry, the action command must be re-executed without the profile reclassification action defined.

in — The **in** parameter is mutually exclusive to the **exceed**, **inplus**, and **out** parameters following the profile reclassification action keyword. **In, exceed**, **inplus**, or **out** must be specified when the profile keyword is present. When **in** is specified, any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out — The **out** parameter is mutually exclusive to the **exceed**, **inplus**, and **in** parameters following the profile reclassification action keyword. **In, exceed**, **inplus**, or **out** must be specified when the profile keyword is present. When **out** is specified, any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

exceed — The **exceed** parameter is mutually exclusive to the **out**, **inplus**, and **in** parameters following the profile reclassification action keyword. **In, exceed**, **inplus**, or **out** must be specified when the profile keyword is present. When **exceed** is specified, any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

inplus — The **inplus** parameter is mutually exclusive to the **out**, **exceed**, and **in** parameters following the profile reclassification action keyword. **In, exceed**, **inplus**, or **out** must be specified when the profile keyword is present. When **inplus** is specified, any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer *policer-id* — When the action policer command is executed, a valid policer ID must be specified. The parameter policer ID references a policer ID that has already been created within the SAP egress QoS policy.

Values 1 to 63

port-redirect-group-queue queue *queue-id* — Used to override the forwarding class default egress queue destination to an egress port queue group. The specific egress queue group instance to use is specified at the time the QoS policy is applied to the SAP. Therefore, this parameter is only valid if SAP-based redirection is required. The queue parameter overrides the policer's default egress queue destination to a specified queue-id in the egress port queue group instance.

Values 1 to 8

queue *queue-id* — This parameter overrides the policer's default egress queue destination to a specified local SAP queue of that queue-id. A queue of ID queue-id must exist within the egress QoS policy.

Values 1 to 8

use-fc-mapped-queue — This parameter overrides the policer's default egress queue destination to the queue mapped by the traffic's forwarding class.

Platforms All

action

Syntax **action** [**fc** *fc-name* **profile** {**in** | **out** | **exceed** | **inplus**}] [**port-redirect-group** {**queue** *queue-id* | **policer** *policer-id* [**queue** *queue-id*]}]

Context **[Tree]** (config>qos>network>egress>ip-criteria>entry action)
[Tree] (config>qos>network>egress>ipv6-criteria>entry action)

Full Context configure qos network egress ip-criteria entry action
configure qos network egress ipv6-criteria entry action

Description This command defines the reclassification actions that are performed on any packet matching the defined IP flow criteria within the entry's matched node. When defined under the **ip-criteria** context, the reclassification only applies to IPv4 packets. When defined under the **ipv6-criteria** context, the reclassification only applies to IPv6 packets.

If an egress packet matches the specified IP flow entry, the forwarding class and profile may be overridden. By default, the forwarding class and profile of the packet are derived from ingress classification and profiling functions. Matching an IP flow reclassification entry will override all IP precedence-based or DSCP-based reclassification rule actions when an explicit reclassification action is defined for the entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an IP flow entry is first created, the entry will have no explicit behavior defined as the reclassification actions to be performed. When the entry is defined with no action, the entry will not be populated in the IP flow reclassification list used to evaluate egress packets. An IP flow reclassification entry is only added to the evaluation list when the action command for the entry is executed.

The **fc** and **profile** keywords are optional. When specified, the egress classification rule will overwrite the forwarding class and profile derived from ingress. The new forwarding class and profile are used for egress remarking, queue mapping decisions, and queue congestion behavior.

The **port-redirect-group** keyword is optional. When specified, the egress packet will be redirected to the configured queue or policer in the specified egress network queue group. By default, the policed forwarded traffic will use the regular network queue to which the packet's forwarding class is mapped. Alternatively, a queue in the network egress queue group instance can be used for post-policed traffic by specifying a queue after the **policer** parameter. The **port-redirect-group** keyword requires that the network egress queue group instance is specified when this network QoS policy is applied to a network interface. The **port-redirect-group** is not supported on a 7750 SR-a4/a8.

The **no** form of this command removes all reclassification actions from the IP flow reclassification entry and also removes the entry from the evaluation list. An entry removed from the evaluation list will not be matched to any egress packets.

Default no action

Parameters **fc** *fc-name* — The fc reclassification action is optional. When specified, packets matching the IP flow reclassification entry will be explicitly reclassified to the forwarding class specified as *fc-name* regardless of the ingress classification decision. The *fc-name* defined must be one of the eight forwarding classes supported by the system. The profile reclassification action is mandatory when an **fc** is specified. To remove the forwarding class reclassification action for the IP flow entry, the action command must be re-executed without the fc reclassification action defined.

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out | exceed | inplus} — The profile reclassification action is mandatory when an fc is specified, otherwise it is optional. When specified, packets matching the IP flow reclassification entry will be explicitly reclassified to the configured profile regardless of the ingress profiling decision. **In**, **exceed**, **inplus**, or **out** must be specified when the profile keyword is present. To remove the profile reclassification action for the IP flow reclassification entry, the action command must be re-executed without the profile reclassification action defined.

in — When specified, any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out — When specified, any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

exceed — When specified, any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

inplus — When specified, any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

queue *queue-id* — Used to override the forwarding class default egress queue destination to the specified network egress queue group instance queue. The specific egress queue group instance to use is specified at the time the QoS policy is applied to the network interface.

Values 1 to 8

policer *policer-id* — Specifies a valid policer ID that has already been created within the network egress queue group instance.

Values 1 to 16

queue *queue-id* — The queue following the configured policer overrides the default policed traffic egress queue destination to a specified queue in the network egress queue group instance.

Values 1 to 8

Platforms All

action

Syntax **action fc** *fc-name* **profile** {**in** | **out**}
no action

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry action)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry action)

Full Context configure qos network ingress ip-criteria entry action
configure qos network ingress ipv6-criteria entry action

Description This command defines the reclassification actions that are performed on any packet matching the defined IP flow criteria within the entry's matched node. When defined under the **ip-criteria** context, the reclassification only applies to IPv4 packets. When defined under the **ipv6-criteria** context, the reclassification only applies to IPv6 packets.

If an ingress packet matches the specified IP flow entry, the forwarding class and profile may be overridden. By default, the forwarding class and profile of the packet are derived from ingress classification and profiling functions. Matching an IP flow reclassification entry will override all non-criteria reclassification rule actions when an explicit reclassification action is defined for the entry.

When an IP flow entry is first created, the entry will have no explicit behavior defined as the reclassification actions to be performed. When the entry is defined with no action, the entry will not be populated in the IP flow reclassification list used to evaluate ingress packets. An IP flow reclassification entry is only added to the evaluation list when the action command for the entry is executed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes all reclassification actions from the IP flow reclassification entry and also removes the entry from the evaluation list. An entry removed from the evaluation list will not be matched to any ingress packets.

Default no action

Parameters **fc** *fc-name* — The fc reclassification action is optional. When specified, packets matching the IP flow reclassification entry will be explicitly reclassified to the forwarding class specified as *fc-name* regardless of the ingress classification decision. The *fc-name* defined must be one of the eight forwarding classes supported by the system. The profile reclassification action is mandatory when an **fc** is specified. To remove the forwarding class reclassification action for the IP flow entry, the action command must be re-executed without the fc reclassification action defined.

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out} — The profile reclassification action is mandatory. Packets matching the IP flow reclassification entry will be explicitly reclassified to the configured profile regardless of other ingress profiling decisions. **In** or **out** must be specified when the profile keyword is present. To remove the profile reclassification action for the IP flow reclassification entry, the action command must be re-executed without the profile reclassification action defined.

in — When specified, any packets matching the reclassification rule will be treated as in-profile by the ingress forwarding plane.

out — When specified, any packets matching the reclassification rule will be treated as out-of-profile by the ingress forwarding plane.

Platforms All

action

Syntax **action** {**replace** | **drop** | **keep**}
no action

Context **[Tree]** (config>router>if>dhcp>option action)

Full Context configure router interface dhcp option action

Description This command configures the processing required when the SR-Series router receives a DHCP request that already has a Relay Agent Information Option (Option 82) field in the packet.

The **no** form of this command returns the system to the default value.

Default Per RFC 3046, *DHCP Relay Agent Information Option*, section 2.1.1, *Reforwarded DHCP requests*, the default is to keep the existing information intact. The exception to this is if the GI address of the received packet is the same as the ingress address on the router. In that case the packet is dropped and an error is logged.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **replace** — In the upstream direction (from the user), the existing Option 82 field is replaced with the Option 82 field from the router. In the downstream direction (toward the user) the Option 82 field is stripped (in accordance with RFC 3046).

drop — The packet is dropped, and an error is logged.

keep — The existing information is kept in the packet and the router does not add any additional information. In the downstream direction the Option 82 field is not stripped and is sent on toward the client.

The behavior is slightly different in case of Vendor Specific Options (VSOs). When the keep parameter is specified, the router will insert his own VSO into the Option 82 field. This will only be done when the incoming message has already an Option 82 field.

If no Option 82 field is present, the router will not create the Option 82 field. In this in that case, no VSO will be added to the message.

Platforms All

action

Syntax **action** {*action*}
no action

Context **[Tree]** (config>serv>mrp>mrp-policy>entry action)

Full Context configure service mrp mrp-policy entry action

Description This command specifies the action to be applied to the MMRP attributes (Group B-MACs) whose ISIDs match the specified ISID criteria in the related entry.

The *action* keyword must be entered for the entry to be active. Any filter entry without the action keyword will be considered incomplete and will be inactive. If neither keyword is specified (no action is used), this is considered a No-Op policy entry used to explicitly set an entry inactive without modifying match criteria or removing the entry itself. Multiple action statements entered will overwrite previous actions parameters when defined. To remove a parameter, use the **no** form of the action command with the specified parameter.

The **no** form of the command removes the specified action statement. The entry is considered incomplete and hence rendered inactive without the action keyword.

Default no action

Parameters *action* — Specifies the action for the MRP policy entry.

block — Specifies that the matching MMRP attributes will not be declared or registered on this SAP or SDP.

allow — Specifies that the matching MMRP attributes will be declared and registered on this SAP or SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

end-station — Specifies that an end-station emulation is present on this SAP or SDP for the MMRP attributes related with matching ISIDs. Equivalent action with the block keyword on that SAP or SDP. The attributes associated with the matching ISIDs are not declared or registered on the SAP or SDP. The matching attributes on the other hand are mapped as static MMRP entries on the SAP or SDP which implicitly instantiates in the data plane as a MFIB entry associated with that SAP or SDP for the related Group B-MAC. For the other SAPs/SDPs in the BVPLS with MRP enabled (no shutdown). This means that the permanent declaration of the matching attributes, as in the case when the IVPLS instances associated with these ISIDs were locally configured.

If an MRP policy has end-station action in one entry, the only default action allowed in the policy is block. Also no other actions are allowed to be configured in other entry configured under the policy.

This policy will apply even if the MRP is shutdown on the local SAP or SDP or for the whole BVPLS to allow for manual creation of MMRP entries in the data plane. Specifically the following rules apply:

- If **service vpls mrp shutdown** is executed, and the MMRP on all SAP or SDPs is shutdown, then MRP PDUs pass-through transparently.
- If **service vpls mrp no shutdown**, and the **endstation** statement (even with no ISID values in the related match statement) is used in an MRP policy applied to SAP or SDP, then no declaration is sent on SAP or SDP. The provisioned ISIDs in the match statement are registered on that SAP or SDP and are propagated on all the other MRP enabled endpoints.

Platforms All

action

Syntax **action** {**drop** | **forward**}
no action

Context **[Tree]** (config>log>filter>filter-id>entry action)

Full Context configure log filter filter-id entry action

Description This command specifies a drop or forward action associated with the filter entry. If neither **drop** nor **forward** is specified, the **default-action** will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.

Multiple action statements entered will overwrite previous actions.

The **no** form of this command removes the specified **action** statement.

Default no action

Parameters **drop** — Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

action

Syntax **action** {**permit** | **deny** | **deny-host-unreachable**}
no action

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry action)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry action)
[Tree] (config>system>security>mgmt-access-filter>mac-filter>entry action)

Full Context configure system security management-access-filter ip-filter entry action
configure system security management-access-filter ipv6-filter entry action
configure system security management-access-filter mac-filter entry action

Description This command creates the action associated with the management access filter match criteria entry.

The **action** keyword is required. If no **action** is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.

If the packet does not meet any of the match criteria the configured **default action** is applied.

Parameters **permit** — Specifies that packets matching the configured criteria will be permitted.

deny — Specifies that packets matching the configured selection criteria will be denied and that a ICMP host unreachable message will not be issued.

deny-host-unreachable — Specifies that packets matching the configured selection criteria will be denied and that a host unreachable message will not be issued.

The **deny-host-unreachable** parameter only applies to ip-filter and ipv6-filter.

Platforms All

action

Syntax **action** [**accept** | **drop** | **queue** *queue-id*]
no action

Context **[Tree]** (config>sys>security>cpm-filter>ip-filter>entry action)
[Tree] (config>sys>security>cpm-filter>ipv6-filter>entry action)
[Tree] (config>sys>security>cpm-filter>mac-filter>entry action)

Full Context configure system security cpm-filter ip-filter entry action
configure system security cpm-filter ipv6-filter entry action
configure system security cpm-filter mac-filter entry action

Description This command specifies the action to take for packets that match this filter entry.

Default action drop

Parameters **accept** — Specifies packets matching the entry criteria will be forwarded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

drop — Specifies packets matching the entry criteria will be dropped.

queue *queue-id* — Specifies packets matching the entry criteria will be forward to the specified CPM hardware queue.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

action

Syntax **action** {**deny** | **permit** | **read-only**}

Context **[Tree]** (config>system>security>profile>entry action)

Full Context configure system security profile entry action

Description This command configures the action associated with the profile entry.

Parameters **deny** — Specifies that commands matching the entry command match criteria are to be denied.

permit — Specifies that commands matching the entry command match criteria is permitted.

read-only — Specifies the commands matching the entry command match criteria is available with read-only access.

Platforms All

5.70 action-list

action-list

Syntax **action-list**

Context **[Tree]** (config>log>event-handling>handler action-list)

Full Context configure log event-handling handler action-list

Description Commands in this context configure the EHS handler action list.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.71 action-on-fail

action-on-fail

Syntax **action-on-fail** {**drop** | **passthrough**}
no action-on-fail

Context **[Tree]** (config>python>py-script action-on-fail)

Full Context configure python python-script action-on-fail

Description This command specifies the action taken when Python fails to modify the given message.

The **no** form of this command reverts to the default.

Default action-on-fail drop

Parameters **drop** — Specifies that the packet will be dropped.

passthrough — Specifies that the packet that is sent out without any modifications.

Platforms All

action-on-fail

Syntax **action-on-fail** {**drop** | **passthrough**}
no action-on-fail

Context **[Tree]** (config>aaa>radius-scr-plcy action-on-fail)

Full Context configure aaa radius-script-policy action-on-fail

Description specifies the action taken when Python fails to modify the RADIUS message.

The **no** form of this command reverts to the default.

Default action-on-fail drop

Parameters **drop** — Specifies that the packet will be dropped.

passthrough — Specifies that the packet will be sent out without any modifications.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.72 activate

activate

Syntax **activate** [*file-url*] [**now**]

Context **[Tree]** (admin>system>license activate)

Full Context admin system license activate

Description This command performs an activation on the license file pointed to by the command line argument. The file is first validated as described in the **admin>system>license>validate** command and upon success, replaces the existing license attributes in the system with the information in the new license file.

The license attributes that are active on a system can be viewed with the **show>licensing>entitlements** command.

Note: If the CLM tool is being used for license management, it shall perform the validation and activation and there is no need to enter these commands manually.

Parameters *file-url* — Specifies the file URL location to read the license file.

Values local-url, remote-url

Note: IPv6 addresses apply only to 7750 SR and 7950 XRS.

now — If the **now** keyword is not present, the operator is prompted to confirm the activation. With the **now** keyword the license file is activated without the additional prompt.

Platforms All

5.73 activate-entry-tag

activate-entry-tag

Syntax **activate-entry-tag** *activate-entry-tag*
no activate-entry-tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>apipe>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>apipe>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>cpipe>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>cpipe>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>epipe>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>epipe>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>fpipe>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>fpipe>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>ies>if>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>ies>if>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>ipipe>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>ipipe>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>vpls>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>vpls>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)
[Tree] (config>service>vprn>if>sap>ingress>criteria-overrides>ip-criteria activate-entry-tag)
[Tree] (config>service>vprn>if>sap>ingress>criteria-overrides>ipv6-criteria activate-entry-tag)

Full Context configure service apipe sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service apipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service cpipe sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service cpipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service epipe sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service epipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service fpipe sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service fpipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service ies interface sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service ies interface sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service ipipe sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service ipipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service vpls sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service vpls sap ingress criteria-overrides ipv6-criteria activate-entry-tag
configure service vprn interface sap ingress criteria-overrides ip-criteria activate-entry-tag
configure service vprn interface sap ingress criteria-overrides ipv6-criteria activate-entry-tag

Description This command activates the entry tag.

The **no** form of this command removes any existing entry tags from the SAP.

Parameters *activate-entry-tag* — Specifies the tag identifier value for activation.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress criteria-overrides ip-criteria activate-entry-tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service epipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service vpls sap ingress criteria-overrides ip-criteria activate-entry-tag
- configure service cpipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service fpipe sap ingress criteria-overrides ip-criteria activate-entry-tag
- configure service vpls sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service ies interface sap ingress criteria-overrides ip-criteria activate-entry-tag
- configure service ies interface sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service vprn interface sap ingress criteria-overrides ip-criteria activate-entry-tag
- configure service vprn interface sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service epipe sap ingress criteria-overrides ip-criteria activate-entry-tag
- configure service ipipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag
- configure service ipipe sap ingress criteria-overrides ip-criteria activate-entry-tag

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress criteria-overrides ip-criteria activate-entry-tag
- configure service apipe sap ingress criteria-overrides ipv6-criteria activate-entry-tag

5.74 active-cpm-protocols

active-cpm-protocols

Syntax [**no**] **active-cpm-protocols**

Context **[Tree]** (config>service>vprn>if active-cpm-protocols)

Full Context configure service vprn interface active-cpm-protocols

Description This command enables CPM protocols on this interface.

5.75 active-flow-timeout

active-flow-timeout

Syntax **active-flow-timeout** *seconds*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no active-flow-timeout

Context [Tree] (config>cflowd active-flow-timeout)

Full Context configure cflowd active-flow-timeout

Description This command configures the maximum amount of time before an active flow is aged out of the active cache. If an individual flow is active for the specified amount of time, the flow is aged out and a new flow is created on the next packet sampled for that flow.

Existing flows do not inherit the new **active-flow-timeout** value if this parameter is changed while **cflowd** is active. The **active-flow-timeout** value for a flow is set when the flow is first created in the active cache table and does not change dynamically.

The **no** form of this command resets the timeout back to the default value.

Default active-flow-timeout 1800

Parameters *seconds* — Specifies the value, in seconds, before an active flow is exported.

Values 30 to 36000

Platforms All

5.76 active-hold-delay

active-hold-delay

Syntax **active-hold-delay** *active-hold-delay*
no active-hold-delay

Context [Tree] (config>service>apipe>endpoint active-hold-delay)
[Tree] (config>service>cpipe>endpoint active-hold-delay)
[Tree] (config>service>epipe>endpoint active-hold-delay)
[Tree] (config>service>fpipe>endpoint active-hold-delay)
[Tree] (config>service>ipipe>endpoint active-hold-delay)

Full Context configure service apipe endpoint active-hold-delay
configure service cpipe endpoint active-hold-delay
configure service epipe endpoint active-hold-delay
configure service fpipe endpoint active-hold-delay
configure service ipipe endpoint active-hold-delay

Description This command specifies that the node will delay sending the change in the T-LDP status bits for the VLL endpoint when the MC-LAG transitions the LAG subgroup which hosts the SAP for this VLL endpoint from **active** to **standby** or when any object in the endpoint. For example, SAP, ICB, or regular spoke SDP, transitions from up to down operational state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, when the MC-LAG transitioned the LAG subgroup which hosts the SAP for this VLL endpoint from **active** to **standby**, the node sends immediately new T-LDP status bits indicating the new value of “standby” over the spoke SDPs which are on the mate-endpoint of the VLL. The same applies when any object in the endpoint changes an operational state from up to down.

There is no delay applied to the VLL endpoint status bit advertisement when the MC-LAG transitions the LAG subgroup which hosts the SAP from **standby** to **active** or when any object in the endpoint transitions to an operationally up state.

Default active-hold-delay 0

Parameters *active-hold-delay* — Specifies the active hold delay in 100s of milliseconds.

A value of zero means that when the MC-LAG transitioned the LAG subgroup which hosts the SAP for this VLL endpoint from **active** to **standby,** the node sends immediately new T-LDP status bits indicating the new value of **standby** over the spoke SDPs which are on the mate-endpoint of the VLL. The same applies when any object in the endpoint changes an operational state from up to down.

Values 0 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe endpoint active-hold-delay
- configure service cpipe endpoint active-hold-delay

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe endpoint active-hold-delay

All

- configure service ipipe endpoint active-hold-delay
- configure service epipe endpoint active-hold-delay

5.77 active-instance

active-instance

Syntax **active-instance** *instance-id*
no active-instance

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy>p2mp-candidate-path active-instance)

Full Context configure router p2mp-sr-tree p2mp-policy p2mp-candidate-path active-instance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the active instance of a P2MP candidate path for the P2MP SR tree as a primary or a secondary instance. Before configuring the active instance ID, the candidate path instance must be configured using the **instance** command.

The **no** form of this command removes the active instance.

Parameters *instance-id* — Specifies the active instance as primary (1) or secondary (2).

Values 1, 2

Platforms All

5.78 active-iom-limit

active-iom-limit

Syntax **active-iom-limit** *number*
no active-iom-limit

Context **[Tree]** (config>isa>wlan-gw-group active-iom-limit)

Full Context configure isa wlan-gw-group active-iom-limit

Description This command specifies the number of WLAN-GW IOMs used as active IOMs from the total number of configured WLAN-GW IOMs. If there are more configured IOM than active-iom-limit, then the remaining number of IOMs is designated as backup(s).

The **no** form of this command removes the number from the configuration.

Parameters *number* — Specifies the number of IOMs in this WLAN Gateway ISA group that are intended for active use.

Values 1 to 3

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.79 active-lease-time

active-lease-time

Syntax **active-lease-time** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no active-lease-time

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>dhcp active-lease-time)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>dhcp active-lease-time)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp active-lease-time)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp active-lease-time)

Full Context configure service ies subscriber-interface group-interface wlan-gw dhcp active-lease-time
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp active-lease-time
configure service vprn subscriber-interface group-interface wlan-gw dhcp active-lease-time
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp active-lease-time

Description This command configures the lease time for an authenticated user.

Default active-lease-time min 10

Parameters *hours* — Specifies the number of active lease time hours.

Values 1 to 1

minutes — Specifies the number of active lease time minutes.

Values 5 to 59

seconds — Specifies the number of active lease time seconds.

Values 1 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.80 active-mda-limit

active-mda-limit

Syntax **active-mda-limit** *number*
no active-mda-limit

Context [Tree] (config>isa>wlan-gw-group active-mda-limit)

Full Context configure isa wlan-gw-group active-mda-limit

Description This command specifies how many ISAs may be in active use by the WLAN-GW group at the same time. If the maximum number of active ISAs is reached and more ISAs are added to the group, the new ISAs are considered to be in standby mode.

The **no** form of this command removes the limit on the maximum number of active ISAs.

Parameters *number* — Specifies the number of WLAN-GW ISAs intended for active use.

Values 1 to 14

Platforms 7750 SR, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

active-mda-limit

Syntax **active-mda-limit** *number*
no active-mda-limit

Context **[Tree]** (config>isa>nat-group active-mda-limit)

Full Context configure isa nat-group active-mda-limit

Description This command configures the number of active ISAs in active-standby ISA redundancy model for NAT. The active ISAs are automatically selected by the system and any the remaining ISA beyond the number of active limit will automatically assume the standby role. An ISA in the standby mode is idle until the failure of an active ISA occurs. Standby ISA can accept traffic from exactly one failed active ISA. Multiple standby ISAs can be configured in the system to protect against multiple simultaneous failures.

Once the active ISA fails, the standby ISA will start forwarding traffic. NAT translations from the failed ISA will have to be re-initiated by the clients and consequently setup on the newly active ISA.

In order for this command to take effect, the intra-chassis redundancy mode must be set to active-standby (**config>isa>nat-group>redundancy active-standby**).

Default no active-mda-limit

Parameters *number* — Specifies the active MDA limit.

Values 1 to 14

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.81 active-mda-number

active-mda-number

Syntax **active-mda-number** *number*
no active-mda-number

Context **[Tree]** (config>isa>tunnel-grp active-mda-number)

Full Context configure isa tunnel-group active-mda-number

Description This command specifies the number of active MS-ISA within all configured MS-ISA in the tunnel-group with multi-active enabled. IPsec traffic will be load balanced across all active MS-ISAs. If the number of configured MS-ISA is greater than the active-mda-number then the delta number of MS-ISA will be backup.

Default active-mda-number 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the number of active MDAs.

Values 1 to 16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.82 active-outbound-sa

active-outbound-sa

Syntax **active-outbound-sa** *spi*
no active-outbound-sa

Context **[Tree]** (config>grp-encryp>encryp-keygrp active-outbound-sa)

Full Context configure group-encryption encryption-keygroup active-outbound-sa

Description This command specifies the Security Association, referenced by the Security Parameter Index (SPI), to use when performing encryption and authentication on NGE packets egressing the node for all services configured using this key group.

The **no** form of the command returns the parameter to its default value and is the same as removing this key group from all outbound direction key groups in all services configured with this key group (that is, all packets of services using this key group will egress the node in without being encrypted).

Parameters *spi* — Specifies the SPI to use for packets of services using this key group when egressing the node.

Values 1 to 127

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.83 active-preferred-lifetime

active-preferred-lifetime

Syntax **active-preferred-lifetime** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no active-preferred-lifetime

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 active-preferred-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 active-preferred-lifetime)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>slaac active-preferred-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>slaac active-preferred-lifetime)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 active-preferred-lifetime
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac active-preferred-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 active-preferred-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac active-preferred-lifetime

Description This command specifies the signaled preferred lifetime in DHCPv6 or SLAAC after full authentication. This is only applicable to DSM.

The **no** form of this command reverts to the default.

Default active-preferred-lifetime min 10

Parameters *hours* — Specifies the number of active preferred lifetime hours.

Values 1 to 1

minutes — Specifies the number of active preferred lifetime minutes.

Values 5 to 59

seconds — Specifies the number of active preferred lifetime seconds.

Values 1 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.84 active-psk

active-psk

Syntax **active-psk** *active-pre-shared-key*
no active-psk

Context [Tree] (config>macsec>conn-assoc>static-cak active-psk)

Full Context configure macsec connectivity-association static-cak active-psk

Description This command specifies the active transmitting pre-shared-key. If two pre-shared-keys are configured, the arriving MACsec MKA can be decrypted via CAKs of both pre-shared keys; however, only the active-psk will be used for TX encryption of MKA PDUs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default active-psk 1

Parameters *active-pre-shared-key* — Specifies the value of the pre-shared-key.

Values 1 or 2

Platforms All

5.85 active-source-limit

active-source-limit

Syntax **active-source-limit** *number*
no active-source-limit

Context **[Tree]** (config>service>vprn>msdp active-source-limit)
[Tree] (config>service>vprn>msdp>group active-source-limit)
[Tree] (config>service>vprn>msdp>group>peer active-source-limit)
[Tree] (config>service>vprn>msdp>peer active-source-limit)
[Tree] (config>service>vprn>msdp>source active-source-limit)

Full Context configure service vprn msdp active-source-limit
configure service vprn msdp group active-source-limit
configure service vprn msdp group peer active-source-limit
configure service vprn msdp peer active-source-limit
configure service vprn msdp source active-source-limit

Description This option controls the maximum number of active source messages that will be accepted by Multicast Source Discovery Protocol (MSDP), effectively controlling the number of active sources that can be stored on the system.

The **no** form of this command reverts the number of source message limit to default operation.

Default no active-source-limit

Parameters *number* — Defines how many active sources can be maintained by MSDP.

Values 0 to 1000000

Platforms All

active-source-limit

Syntax **active-source-limit** *number*
no active-source-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>msdp active-source-limit)
[Tree] (config>router>msdp>group active-source-limit)
[Tree] (config>router>msdp>group>peer active-source-limit)
[Tree] (config>router>msdp>peer active-source-limit)
[Tree] (config>router>msdp>source active-source-limit)

Full Context configure router msdp active-source-limit
configure router msdp group active-source-limit
configure router msdp group peer active-source-limit
configure router msdp peer active-source-limit
configure router msdp source active-source-limit

Description This option controls the maximum number of active source messages that will be accepted by Multicast Source Discovery Protocol (MSDP), effectively controlling the number of active sources that can be stored on the system.

The **no** form of this command sets no limit on the number of source active records.

Default no active-source-limit

Parameters *number* — Specifies the number of active sources that can be maintained by MSDP.

Values 0 to 1000000

Platforms All

5.86 active-valid-lifetime

active-valid-lifetime

Syntax **active-valid-lifetime** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no active-valid-lifetime

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 active-valid-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 active-valid-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>slaac active-valid-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>slaac active-valid-lifetime)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 active-valid-lifetime
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac active-valid-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 active-valid-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac active-valid-lifetime

Description This command specifies the signaled valid lifetime in DHCPv6 or SLAAC after full authentication. This is only applicable to DSM.

The **no** form of this command reverts to the default.

Default active-valid-lifetime min 10

Parameters *hours* — Specifies the number of active-valid-lifetime hours.

Values 1 to 1

minutes — Specifies the number of active-valid-lifetime minutes.

Values 5 to 59

seconds — Specifies the number of active-valid-lifetime seconds.

Values 1 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.87 activity-threshold

activity-threshold

Syntax **activity-threshold** *kilobits-per-second*
no activity-threshold

Context **[Tree]** (config>subscr-mgmt>cat-map activity-threshold)

Full Context configure subscriber-mgmt category-map activity-threshold

Description This command configures the threshold that is applied to determine whether or not there is activity. This is only valid for credit-type = time (not volume).

The **no** form of this command reverts to the default.

Parameters *kilobits-per-second* — Specifies the activity threshold value, in kilobits per second.

Values 1 to 100000000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.88 ad-insert

ad-insert

Syntax [**no**] **ad-insert**

Context **[Tree]** (config>isa>video-group ad-insert)

Full Context configure isa video-group ad-insert

Description This command enables the ad insert server for the group. Ad insertion cannot be enabled if an FCC server or local RT server is enabled.

The **no** form of the command disables the server.

Default no ad-insert

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

5.89 ad-per-es-route-target

ad-per-es-route-target

Syntax **ad-per-es-route-target evi-rt**
ad-per-es-route-target evi-rt-set route-distinguisher *ip-address* [**extended-evi-range**]

Context **[Tree]** (config>service>system>bgp-evpn ad-per-es-route-target)

Full Context configure service system bgp-evpn ad-per-es-route-target

Description This command controls how Ethernet AD per-ES routes are generated.

The system can either send a separate Ethernet AD per-ES route per service, or an Ethernet AD per-ES route aggregating the route-targets for multiple services. While both alternatives can interoperate, RFC 7432 states that the EVPN Auto-Discovery per-ES route must be sent with a set of route-targets corresponding to all the EVIs defined on the Ethernet Segment. This command supports both options.

The default **ad-per-es-route-target evi-rt** option configures the system to send a separate AD per-ES route per service.

When enabled, the **evi-rt-set** option allows the aggregation of routes: a single AD per-ES route with the associated RD (ip-address:1) and a set of EVI route-targets are advertised (to a maximum of 128). When a significant number of EVIs are defined in the Ethernet Segment (hence the number of route-targets), the system sends more than one route. For example:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- AD per-ES route for evi-rt-set 1 will be sent with RD ip-address:1
- AD per-ES route for evi-rt-set 2 will be sent with RD ip-address:2

Default ad-per-es-route-target evi-rt

Parameters **evi-rt** — Specifies the option to advertise a separate AD per-ES route per service.

evi-rt-set — Specifies the option to advertise a set of AD per-ES routes aggregating the route-targets for all the services in the Ethernet Segment.

ip-address — Specifies the ip-address part of the route-distinguisher being used in the evi-rt-set option.

extended-evi-range — Specifies that the system reserves the RD *comm-val* 1 to 65535 out of the type 1 RD that is used for AD per-ES routes.

Platforms All

5.90 ad-server

ad-server

Syntax [**no**] **ad-server** *ip-address*

Context **[Tree]** (config>service>ies>video-interface>adi>scte30 ad-server)
[Tree] (config>service>vprn>video-interface>adi>scte30 ad-server)

Full Context configure service ies video-interface adi scte30 ad-server
configure service vprn video-interface adi scte30 ad-server

Description This command configures the ad server address. A TCP session will be accepted for SCTE 30 messaging only for IP addresses that appear in this configuration.

The **no** form of the command removes the address from the ad server configuration.

Parameters *ip-address* — Specifies the IP address of the ad server.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

5.91 ad-validation

ad-validation

Syntax **ad-validation** {**fall-through** | **drop**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ad-validation

Context [Tree] (config>system>dns>dnssec ad-validation)

Full Context configure system dns dnssec ad-validation

Description This command enables validation of the presence of the AD-bit in responses from the DNS servers, and reports a warning to the SECURITY log if DNSSEC validation was not possible.

This command requires either the fall-through or drop parameters be configured. When the fall-through parameter is supplied, the system will allow DNS responses that do not pass DNSSEC validation to be accepted and logged. When the drop parameter is specified, the system will reject and log DNS responses that do not pass DNSSEC validation and the resolution will appear to fail.

Default no ad-validation

Parameters **fall-through** — Specifies that the DNSSEC validator should allow non-DNSSEC responses to fall-through to permit resolution in case of validation failure.

drop — Specifies that the DNSSEC validator should drop non-DNSSEC responses in case of validation failure.

Platforms All

5.92 adapt-qos

adapt-qos

Syntax **adapt-qos** {**link** | **port-fair** | **distribute** [**include-egr-hash-cfg**]}

Context [Tree] (config>lag>access adapt-qos)

Full Context configure lag access adapt-qos

Description This command specifies how the LAG SAP queue and virtual scheduler buffering and rate parameters are adapted over multiple active XMAs/MDAs. This command applies only to access LAGs.

Default adapt-qos distribute

Parameters **link** — Specifies that the LAG will create the SAP queues and virtual schedulers with the actual parameters on each LAG member port.

port-fair — Places the LAG instance into a mode that enforces QoS bandwidth constraints in the following manner:

- all egress QoS objects associated with the LAG instance are created on a per port basis

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- bandwidth is distributed over these per port objects based on the proportion of the port's bandwidth relative to the total of all active ports bandwidth within the LAG
- the **include-egr-hash-cfg** behavior is automatically enabled allowing the system to detect objects that hash to a single egress link in the lag and enabling full bandwidth for that object on the appropriate port

distribute — Creates an additional internal virtual scheduler per IOM/XCM as parent of the configured SAP queues and virtual schedulers per LAG member port on that IOM/XCM. This internal virtual scheduler limits the total amount of egress bandwidth for all member ports on the IOM/XCM to the bandwidth specified in the egress qos policy.

include-egr-hash-cfg — Specifies whether explicitly configured hashing should factor into the egress buffering and rate distribution.

When this parameter is configured, all SAPs on this LAG which have explicit hashing configured, the egress HQoS and HPol (including queues, policers, schedulers and arbiters) will receive 100% of the configured bandwidth (essentially operating in adapt-qos link mode). For any Multi-Service-Sites assigned to such a LAG, bandwidth will continue to be divided according to adapt-qos distribute mode.

A LAG instance that is currently in adapt-qos link mode may be placed at any time in port-fair mode. Similarly, a LAG instance that is currently in adapt-qos port-fair mode may be placed at any time in link mode. However, a LAG instance in adapt-qos distribute mode may not be placed into port-fair (or link) mode while QoS objects are associated with the LAG instance. To move from distribute to port-fair mode it is necessary to remove all QoS objects from the LAG instance.

Platforms All

adapt-qos

Syntax **adapt-qos** {**distribute** | **link** | **port-fair**}
no adapt-qos

Context **[Tree]** (config>eth-tunnel>lag-emulation>access adapt-qos)

Full Context configure eth-tunnel lag-emulation access adapt-qos

Description This command specifies how the emulated LAG queue and virtual scheduler buffering and rate parameters are adapted over multiple active MDAs.

The **no** form of the command reverts to the default.

Parameters **distribute** — Creates an additional internal virtual scheduler per line card as parent of the configured SAP queues and virtual schedulers per member path on that line card. This internal virtual scheduler limits the total amount of egress bandwidth for all member paths on the line card to that line card's share of the bandwidth specified in the egress qos policy. This mode is not supported together with an egress port scheduler or the use of egress queue groups.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

link — Specifies that the emulated LAG will create the SAP queues and virtual schedulers with the bandwidth specified in the egress QoS policy on each member path.

port-fair — Specifies that the emulated LAG will create the SAP queues and virtual schedulers on each member path based on the bandwidth specified in the egress QoS policy divided by the number of active paths.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.93 adaptation-rule

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>qos>sap-egress>queue adaptation-rule)

Full Context configure qos sap-egress queue adaptation-rule

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When a specific **adaptation-rule** is removed, the default constraints for **pir** and **cir** apply.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy.

Default adaptation-rule pir closest cir closest

Parameters **pir** — Defines the constraints enforced when adapting the queue's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **pir** parameter is not specified, the default constraint applies.

Values **max** — Specifies that the operational PIR for the queue will be equal to or less than the requested rate.

min — Specifies that the operational PIR for the queue will be equal to or greater than the requested rate.

closest — Specifies that the operational PIR for the queue will be the rate closest to the requested rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir — Defines the constraints enforced when adapting the queue's CIR defined. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

Values **max** — Specifies that the operational rate for the queue will be equal to or less than the requested rate.

min — Specifies that the operational rate for the queue will be equal to or greater than the requested rate.

closest — Specifies that the operational rate for the queue will be the rate closest to the requested rate.

Platforms All

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>qos>sap-egress>queue adaptation-rule)

Full Context configure qos sap-egress queue adaptation-rule

Description This command defines the method used by the system to derive the operational FIR, CIR, and PIR settings when the queue is provisioned in hardware. For the FIR, CIR, and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When a specific **adaptation-rule** is removed, the default constraints for **pir**, **cir,** and **fir** apply.

The **no** form of this command removes any explicitly defined constraints used to derive the operational FIR, CIR, and PIR created by the application of the policy.

Default adaptation-rule pir closest cir closest fir closest

Parameters **pir** *adaptation-rule* — Defines the constraints enforced when adapting the queue's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **pir** parameter is not specified, the default applies.

Values **max -** The **max** option is mutually exclusive to the **min** and **closest** options. When **max** is specified, the operational rate for the queue will be equal to or less than the requested rate.

min - The **min** option is mutually exclusive to the **max** and **closest** options. When **min** is specified, the operational PIR for the queue will be equal to or greater than the requested rate.

closest - The **closest** parameter is mutually exclusive to the **min** and **max** parameter. When **closest** is specified, the operational PIR for the queue will be the rate closest to the requested rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir *adaptation-rule* — Defines the constraints enforced when adapting the queue's CIR. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

max — Specifies that the operational rate for the queue will be equal to or less than the requested rate.

min — Specifies that the operational PIR for the queue will be equal to or greater than the requested rate.

closest — Specifies that the operational PIR for the queue will be the rate closest to the requested rate.

Platforms All

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue adaptation-rule)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>vpls>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue adaptation-rule)

Full Context configure service ies interface sap egress queue-override queue adaptation-rule
configure service ies interface sap ingress queue-override queue adaptation-rule
configure service ies subscriber-interface group-interface sap egress queue-override queue adaptation-rule
configure service vpls sap egress queue-override queue adaptation-rule
configure service vpls sap ingress queue-override queue adaptation-rule

Description This command overrides specific attributes of the specified queue's adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the adaptation rule is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default no adaptation-rule

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **pir** — Specifies the constraints enforced when adapting the PIR rate defined within the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

cir — Specifies the constraints enforced when adapting the CIR rate defined within the **queue** *queue-id* **rate** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the CIR and PIR adaptation rules.

Values max — The **max** (maximum) option is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the queue is equal to or less than the administrative rate specified using the **rate** command.

min — The **min** (minimum) option is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue is equal to or greater than the administrative rate specified using the **rate** command.

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the queue is the rate closest to the rate specified using the **rate** command.

Platforms All

adaptation-rule

Syntax **adaptation-rule pir** *adaptation-rule* [**cir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>subscr-mgmt>isa-policer adaptation-rule)

Full Context configure subscriber-mgmt isa-policer adaptation-rule

Description For operational efficiency, the operational rate of a policer cannot take on every value in the configurable range. This configuration defines a rule that must be followed when mapping a configured rate to an operational rate.

The cir **adaptation-rule** can only be set on dual-bucket-bandwidth policers.

The **no** form of this command reverts to its default.

Default adaptation-rule pir closest cir closest

Parameters **pir** *adaptation-rule* — Configures the rules to compute the PIR operational rates.

Values **min** — Specifies that the operational rate must minimally be the configured rate. The first operational value bigger or equal to the configured rate is chosen.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max — Specifies that the operational rate may maximally be the configured rate. The first operational value smaller or equal to the configured rate is chosen.

closest — Chooses the operational value closest to the configured value, lower or higher.

cir *adaptation-rule* — Configures the rules to compute the CIR operational rates.

Values adaptation-rule

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** {**max** | **min** | **closest**}]
no adaptation-rule

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover>q adaptation-rule)
[Tree] (config>port>ethernet>access>ing>qgrp>qover>q adaptation-rule)
[Tree] (config>port>ethernet>network>egr>qover>q adaptation-rule)

Full Context configure port ethernet access egress queue-group queue-overrides queue adaptation-rule
configure port ethernet access ingress queue-group queue-overrides queue adaptation-rule
configure port ethernet network egress queue-overrides queue adaptation-rule

Description This command specifies the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case the configuration of the adaptation rule is performed under the **hs-wrr-group** within the egress queue group template.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default adaptation-rule pir closest cir closest

Parameters **pir** — Defines the constraints enforced when adapting the PIR rate defined within the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

cir — Defines the constraints enforced when adapting the CIR rate defined within the **queue** *queue-id* **rate** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

adaptation-rule — Specifies the adaptation rule to be used while computing the operational CIR or PIR value.

Values **max** — The **max** (maximum) option is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The **min** (minimum) option is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the queue will be the rate closest to the rate specified using the **rate** command.

Platforms All

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaption-rule

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue adaptation-rule)
[Tree] (config>service>epipe>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue adaptation-rule)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue adaptation-rule)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue adaptation-rule)

Full Context configure service apipe sap egress queue-override queue adaptation-rule
configure service apipe sap ingress queue-override queue adaptation-rule
configure service epipe sap egress queue-override queue adaptation-rule
configure service epipe sap ingress queue-override queue adaptation-rule
configure service fpipe sap egress queue-override queue adaptation-rule
configure service fpipe sap ingress queue-override queue adaptation-rule
configure service ipipe sap egress queue-override queue adaptation-rule
configure service ipipe sap ingress queue-override queue adaptation-rule

Description This command can be used to override specific attributes of the specified queue's adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case the configuration of the adaptation rule is performed under the hs-wrr-group within the SAP egress QoS policy.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default no adaptation-rule

Parameters **pir** — The **pir** parameter defines the constraints enforced when adapting the PIR rate defined within the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

cir — The **cir** parameter defines the constraints enforced when adapting the CIR rate defined within the **queue** *queue-id* **rate** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

Values **max** — The **max** (maximum) keyword is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The **min** (minimum) keyword is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the queue will be the rate closest to the rate specified using the **rate** command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress queue-override queue adaptation-rule
- configure service fpipe sap ingress queue-override queue adaptation-rule

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress queue-override queue adaptation-rule
- configure service apipe sap egress queue-override queue adaptation-rule

All

- configure service ipipe sap egress queue-override queue adaptation-rule
- configure service epipe sap ingress queue-override queue adaptation-rule
- configure service ipipe sap ingress queue-override queue adaptation-rule

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap egress queue-override queue adaptation-rule

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue adaptation-rule)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue adaptation-rule)

Full Context configure service vprn interface sap egress queue-override queue adaptation-rule
configure service vprn interface sap ingress queue-override queue adaptation-rule

Description This command can be used to override specific attributes of the specified queue's adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the adaptation rule is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default no adaptation-rule

Parameters *pir* — The **pir** parameter defines the constraints enforced when adapting the PIR rate defined within the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

cir — The **cir** parameter defines the constraints enforced when adapting the CIR rate defined within the **queue** *queue-id* **rate** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

Values **max** — The **max** (maximum) keyword is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The **min** (minimum) keyword is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the queue will be the rate closest to the rate specified using the **rate** command.

Platforms All

adaptation-rule

Syntax **adaptation-rule pir** *adaptation-rule* [**cir** {*adaptation-rule*}]
no adaptation-rule

Context **[Tree]** (config>app-assure>group>policer adaptation-rule)

Full Context configure application-assurance group policer adaptation-rule

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined option. To change the CIR adaptation rule only, the current PIR rule must be part of the command executed.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default adaptation-rule pir closest cir closest

Parameters **max** — The operational PIR or CIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

min — The operational PIR or CIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — The operational PIR or CIR for the queue will be the rate closest to the rate specified using the **rate** command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>qos>sap-ingress>policer adaptation-rule)
[Tree] (config>qos>sap-egress>policer adaptation-rule)

Full Context configure qos sap-egress policer adaptation-rule
configure qos sap-ingress policer adaptation-rule

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to define how the policer's configuration parameters are translated into the underlying hardware capabilities used to implement each policer instance. For instance, the configured rates for the policer need to be mapped to the timers and decrement granularity used by the hardware's leaky bucket functions that actually perform the traffic metering. If a rate is defined that cannot be exactly matched by the hardware, the adaptation-rule setting provides guidance for which hardware rate should be used.

The hardware also needs to adapt the given mbs and cbs values into the PIR bucket violate threshold (discard) and the CIR bucket exceed threshold (out-of-profile). The hardware may not have an exact threshold match that it can use. The system treats the mbs and cbs values as minimum threshold values.

The **no** form of this command is used to return the policer's metering and profiling hardware adaptation rules to closest.

Parameters **pir** *adaptation-rule* — When the optional **pir** parameter is specified, the **max**, **min,** or **closest** keyword qualifier must follow.

Values max — Specifies that the metering rate defined for the policer is the maximum allowed rate. The system will choose a hardware supported rate that is closest but not exceeding the specified rate.

min — Specifies that the metering rate defined for the policer is the minimum allowed rate. The system will choose a hardware supported rate that is closest but not lower than the specified rate.

closest — Specifies that the metering rate defined for the policer is the target rate. The system will choose a hardware supported rate that is closest to the specified rate.

Default closest

cir *adaptation-rule* — When the optional **cir** parameter is specified, the **max**, **min**, or **closest** keyword qualifier must follow.

Values max — Specifies that the profiling rate defined for the policer is the maximum allowed rate. The system will choose a hardware supported rate that is closest but not exceeding the specified rate.

min — Specifies that the profiling rate defined for the policer is the minimum allowed rate. The system will choose a hardware supported rate that is closest but not lower than the specified rate.

closest — Specifies that the profiling rate defined for the policer is the target rate. The system will choose a hardware supported rate that is closest to the specified rate.

Default closest

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*] [**fir** {**max** | **min** | **closest**}]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no adaptation-rule

Context [Tree] (config>qos>sap-ingress>queue adaptation-rule)

Full Context configure qos sap-ingress queue adaptation-rule

Description This command defines the method used by the system to derive the operational FIR, CIR and PIR settings when the queue is provisioned in hardware. For the FIR, CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When a specific **adaptation-rule** is removed, the default constraints for **pir**, **cir** and **fir** apply.

The **no** form of this command removes any explicitly defined constraints used to derive the operational FIR, CIR and PIR created by the application of the policy.

Default adaptation-rule pir closest cir closest fir closest

Parameters **pir** *adaptation-rule* — Defines the constraints enforced when adapting the queue's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **pir** parameter is not specified, the default applies.

cir *adaptation-rule* — Defines the constraints enforced when adapting the queue's CIR. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

fir — Defines the constraints enforced when adapting the queue's FIR. The **fir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **fir** parameter is not specified, the default constraint applies. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

max — Specifies that the operational rate for the queue will be equal to or less than the requested rate.

min — Specifies that the operational rate for the queue will be equal to or greater than the requested rate.

closest — Specifies that the operational rate for the queue will be the rate closest to the requested rate.

Platforms All

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*]
no adaptation-rule

Context [Tree] (config>qos>network-queue>hs-wrr-group adaptation-rule)

Full Context configure qos network-queue hs-wrr-group adaptation-rule

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies how the system should resolve differences between the specified scheduling limit derived from the WRR group's rate command and the actual operational rate obtainable in hardware. The **min**, **max**, and **closest** mutually exclusive keywords specify whether the next highest rate, next lowest rate, or closest rate should be selected by the system.

The **no** form of the command reverts to the default value.

Default adaptation-rule pir closest

Parameters *adaptation-rule* — Specifies the adaptation rule (**min**, **max**, or **closest**) to be used while computing the operational PIR value. The adaptation rule specifies the rules to compute the operational values while maintaining minimum offset. The **min**, **max**, and **closest** keywords are mutually exclusive.

Values min — When **min** is specified, the queue's rate parameter is treated as the minimum rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queues shaping rate is the closest possible value without going under the specified rate.

max — When **max** is specified, the queue's rate parameter is treated as the maximum rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queue's shaping rate is the closest possible value without going over the specified rate.

closest — When **closest** is specified, the queue's rate parameter is treated as the target rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queues shaping rate is the closest possible value and can be higher or lower than the specified rate.

Platforms 7750 SR-7/12/12e

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>qos>sap-egress>hs-wrr-group adaptation-rule)

Full Context configure qos sap-egress hs-wrr-group adaptation-rule

Description This command specifies how the system resolves differences between the specified scheduling limit derived from the WRR group's **rate** command and the actual operational rate obtainable in hardware. The mutually exclusive **min**, **max**, and **closest** keywords specify whether the next highest rate, next lowest, or closest rate should be selected by the system.

The **no** form of the command reverts to the default value.

Default adaptation-rule pir closest

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **pir** — Defines the constraints enforced when adapting the PIR rate defined within the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

adaptation-rule — Specifies the adaptation rule (**min**, **max**, or **closest**) to be used while computing the operational PIR value. The adaptation rule specifies the rules to compute the operational values while maintaining minimum offset. The **min**, **max**, and **closest** keywords are mutually exclusive.

Values **min** — When **min** is specified, the queue's rate parameter is treated as the minimum rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queues shaping rate is the closest possible value without going under the specified rate.

max — When **max** is specified, the queue's rate parameter is treated as the maximum rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queue's shaping rate is the closest possible value without going over the specified rate.

closest — When **closest** is specified, the queue's rate parameter is treated as the target rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queues shaping rate is the closest possible value and can be higher or lower than the specified rate.

Platforms 7750 SR-7/12/12e

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*]
no adaptation-rule

Context **[Tree]** (config>qos>qgrps>egr>qgrp>hs-wrr-group adaptation-rule)

Full Context configure qos queue-group-templates egress queue-group hs-wrr-group adaptation-rule

Description This command specifies how the system should resolve differences between the specified scheduling limit derived from the WRR group's rate command and the actual operational rate obtainable in hardware. The mutually exclusive **min**, **max**, and **closest** keywords specify whether the next highest rate, next lowest rate, or closest rate should be selected by the system.

The **no** form of the command reverts to the default value.

Default adaptation-rule pir closest

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *adaptation-rule* — Specifies the adaptation rule (**min**, **max**, or **closest**) to be used while computing the operational PIR value. The adaptation rule specifies the rules to compute the operational values while maintaining minimum offset. The **min**, **max**, and **closest** keywords are mutually exclusive.

Values min — When **min** is specified, the queue's rate parameter is treated as the minimum rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queues shaping rate is the closest possible value without going under the specified rate.

max — When **max** is specified, the queue's rate parameter is treated as the maximum rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queue's shaping rate is the closest possible value without going over the specified rate.

closest — When **closest** is specified, the queue's rate parameter is treated as the target rate to shape the queue. The hardware chooses the appropriate timers and PIR leaky bucket behavior to ensure that the queues shaping rate is the closest possible value and can be higher or lower than the specified rate.

Platforms 7750 SR-7/12/12e

adaptation-rule

Syntax **adaptation-rule** [**pir** {**max** | **min** | **closest**}] [**cir** {**max** | **min** | **closest**}]
no adaptation-rule

Context **[Tree]** (config>qos>queue-group-templates>egress>queue-group>policer adaptation-rule)

Full Context configure qos queue-group-templates egress queue-group policer adaptation-rule

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the policer is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When configured on an egress HSQ queue group queue, the **cir** keywords are ignored. This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the adaptation rule is performed under the **hs-wrr-group** within the egress queue group template.

When a specific **adaptation-rule** is removed, the default constraints for **pir** and **cir** apply.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default adaptation-rule pir closest cir closest

Parameters **pir** — Defines the constraints enforced when adapting the policer's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the policer. When the **pir** parameter is not specified, the default constraint applies.

cir — Defines the constraints enforced when adapting the policer's CIR. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the policer. When the **cir** parameter is not specified, the default constraint applies.

max — Specifies that the operational rate for the policer will be equal to or less than the requested rate.

min — Specifies that the operational rate for the policer will be equal to or greater than the requested rate.

closest — Specifies that the operational rate for the policer will be the rate closest to the requested rate.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

adaptation-rule

Syntax **adaptation-rule** [**pir** {**max** | **min** | **closest**}] [**cir** {**max** | **min** | **closest**}] [**fir** {**max** | **min** | **closest**}]
no adaptation-rule

Context **[Tree]** (config>qos>queue-group-templates>ingress>queue-group>queue adaptation-rule)

Full Context configure qos queue-group-templates ingress queue-group queue adaptation-rule

Description This command defines the method used by the system to derive the operational FIR, CIR and PIR settings when the queue is provisioned in hardware. For the FIR, CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When a specific **adaptation-rule** is removed, the default constraints for **pir**, **cir** and **fir** apply.

The **no** form of this command removes any explicitly defined constraints used to derive the operational FIR, CIR and PIR created by the application of the policy.

Default adaptation-rule pir closest cir closest fir closest

Parameters **pir** — Defines the constraints enforced when adapting the queue's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **pir** parameter is not specified, the default constraint applies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir — Defines the constraints enforced when adapting the queue's CIR. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

fir — Defines the constraints enforced when adapting the queue's FIR. The **fir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **fir** parameter is not specified, the default constraint applies. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

max — Specifies that the operational rate for the queue will be equal to or less than the requested rate.

min — Specifies that the operational rate for the queue will be equal to or greater than the requested rate.

closest — Specifies that the operational rate for the queue will be the rate closest to the requested rate.

Platforms All

adaptation-rule

Syntax **adaptation-rule** [**pir** {**max** | **min** | **closest**}] [**cir** {**max** | **min** | **closest**}]
no adaptation-rule

Context **[Tree]** (config>qos>queue-group-templates>egress>queue-group>queue adaptation-rule)

Full Context configure qos queue-group-templates egress queue-group queue adaptation-rule

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When configured on an egress HSQ queue group queue, the **cir** keywords are ignored. This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the adaptation rule is performed under the **hs-wrr-group** within the egress queue group template.

When a specific **adaptation-rule** is removed, the default constraints for **pir** and **cir** apply.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy.

Default adaptation-rule pir closest cir closest

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **pir** — Defines the constraints enforced when adapting the queue's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **pir** parameter is not specified, the default applies.

cir — Defines the constraints enforced when adapting the queue's CIR defined. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

max — Specifies that the operational rate for the queue will be equal to or less than the requested rate.

min — Specifies that the operational rate for the queue will be equal to or greater than the requested rate.

closest — Specifies that the operational rate for the queue will be the rate closest to the requested rate.

Platforms All

adaptation-rule

Syntax **adaptation-rule** [**pir** {**max** | **min** | **closest**}] [**cir** {**max** | **min** | **closest**}] [**fir** {**max** | **min** | **closest**}]
no adaptation-rule

Context **[Tree]** (config>qos>network-queue>queue adaptation-rule)

Full Context configure qos network-queue queue adaptation-rule

Description This command defines the method used by the system to derive the operational FIR, CIR, and PIR settings when the queue is provisioned in hardware. For the FIR, CIR, and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

When configured on an egress HSQ queue group queue, the **cir** keyword is ignored. This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **adaptation-rule** is performed under the **hs-wrr-group** within the network queue policy.

The **no** form of this command removes any explicitly defined constraints used to derive the operational FIR, CIR, and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **fir**, **cir**, and **pir** apply.

Default adaptation-rule pir closest cir closest fir closest

Parameters **pir** — Defines the constraints enforced when adapting the queue's PIR. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **pir** parameter is not specified, the default applies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir — Defines the constraints enforced when adapting the queue's CIR. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

fir — Defines the constraints enforced when adapting the queue's FIR. The **fir** parameter requires a qualifier that defines the constraint used when deriving the operational FIR for the queue. When the **fir** parameter is not specified, the default constraint applies. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

max — Specifies that the operational rate for the queue will be equal to or less than the requested rate.

min — Specifies that the operational rate for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

closest — Specifies that the operational rate for the queue will be the rate closest to the requested rate.

Platforms All

5.94 adaptive

adaptive

Syntax [**no**] **adaptive**

Context **[Tree]** (config>router>mpls>lsp adaptive)
[Tree] (config>router>mpls>lsp>primary adaptive)
[Tree] (config>router>mpls>lsp>primary-p2mp-instance adaptive)
[Tree] (config>router>mpls>lsp>secondary adaptive)
[Tree] (config>router>mpls>lsp-template adaptive)

Full Context configure router mpls lsp adaptive
configure router mpls lsp primary adaptive
configure router mpls lsp primary-p2mp-instance adaptive
configure router mpls lsp secondary adaptive
configure router mpls lsp-template adaptive

Description This command enables the make-before-break functionality for an LSP or LSP path. When enabled for the LSP, make-before-break will be performed for primary path and all the secondary paths of the LSP.

The **config**>**router**>**mpls**>**lsp**>**primary-p2mp-instance**>**adaptive** command is not supported on the 7450 ESS.

Default adaptive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

5.95 adaptive-load-balancing

adaptive-load-balancing

Syntax **adaptive-load-balancing** [**tolerance** *tolerance-value*] [**interval** *interval*]
no adaptive-load-balancing

Context **[Tree]** (config>lag adaptive-load-balancing)

Full Context configure lag adaptive-load-balancing

Description This command enables adaptive load balancing between LAG links. The tolerance value defines the percentage threshold between the most and the least used link in the LAG. If the tolerance value is exceeded, adaptive load balancing optimizes traffic distribution between LAG links.

The **no** form of this command disables adaptive load balancing.

Default no adaptive-load-balancing

Parameters *tolerance-value* — Specifies the allowed tolerance value expressed as a percentage.

Values 1 to 100

Default 20

interval — Specifies the statistics pooling interval value, in seconds, for the LAG ports.

Values 15, 30, 60, 120

Default 30

Platforms All

5.96 add

add

Syntax **add percent** *percentage* [**min-only**] [**active-min-only**]
add rate *rate* [**min-only**] [**active-min-only**]
no add

Context **[Tree]** (config>qos>adv-config-policy>child-control>offered-measurement add)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos adv-config-policy child-control offered-measurement add

Description This command is used to increase the measured rate of the policer or queue associated with the policy. The offered rate (capped by the administrative PIR configured on the queue or policer) is usually used unaltered by the parent virtual scheduler. The add command allows this measured rate to be increased by the specified amount or by a percentage of the administrative PIR. The resulting rate will not exceed the administrative PIR.

The parent scheduler uses the modified measured rate as the available work load for the queue or policer in determining how much bandwidth the child should receive from the bandwidth distribution algorithm.

One example of when an increase in the measured offered rate may be desired is when a queue or policer is handling VoIP traffic. A characteristic of VoIP is the step nature in how traffic is used. Each call typically adds a certain maximum amount to the overall load. By using the add command, the bandwidth required for the next added call may be included in the current measured rate. This allows the virtual scheduler to allocate sufficient bandwidth to the queue or policer so that when the call is made the scheduling algorithm does not need to run to increase the bandwidth.

A side effect of increasing the measured offered rate is that if the extra bandwidth is allocated by the virtual scheduler, the available bandwidth to lower priority queues or policers is diminished even though the extra allocated bandwidth may not be in use. If this is the case, the effect will be seen as an underrun in the aggregate output of the virtual scheduler.

If the add command is used with a percent-based value, the increase is a function of the configured PIR value on the policer or queue. In this case, care should be taken that the child is either configured with an explicit PIR rate (other than max) or the child's administrative PIR is defined using the percent-rate command with the local parameter enabled if an explicit value is not desired. When a maximum PIR is in use on the child, the system attempts to interpret the maximum child forwarding rate. This rate could be very large if the child is associated with multiple ingress or egress ports.

Except for the overall cap on the offered input into the virtual scheduler, the child's administrative PIR has no effect on the calculated increase if an explicit rate is specified.

If the child's administrative PIR is modified while a percent based add is in effect, the system automatically uses the new relative increase value the next time the child's offered rate is determined.

When the add command is not specified or removed, the child's offered rate used by the child's virtual scheduler is not increased.

The **no** form of this command is used to remove an offered rate increase from all child policers and queues associated with the policy.

Parameters *percent-of-admin-pir* — When the percent qualifier is used, this parameter specifies the percentage of the child's administrative PIR that should be added to the child's offered rate. The new offered rate result is capped by the child's PIR. If a value of 0 or 0.00 is used, the system interprets this equivalent to no add.

Values 1.00 to 100.00

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate-in-kilobits-per-second — When the rate qualifier is used, this parameter specifies an explicit rate, in kb/s, that should be added to the child's offered rate. The new offered rate result is capped by the child's PIR. If a rate increase of 0 is specified, the system interprets this equivalent to no add.

Values 0 to 100,000,000

min-only — This optional parameter is used to reinterpret the increase as a minimum offered rate. When this option is enabled, the system uses the specified increase as a minimum offered rate even for inactive queues or policers associated with the policy.

active-min-only — When this optional parameter is specified, the respective rate or percentage is treated as the minimum offered rate for a queue only when the queue has an actual non-zero offered rate. This is intended to limit the artificial increase in offered rate to queues that are currently active. When a queue's measured offered rate drops to zero, the system stops enforcing the minimum value.

Platforms All

5.97 add-paths

add-paths

Syntax [**no**] **add-paths**

Context **[Tree]** (config>router>bgp add-paths)
[Tree] (config>router>bgp>group add-paths)
[Tree] (config>router>bgp>group>neighbor add-paths)

Full Context configure router bgp add-paths
configure router bgp group add-paths
configure router bgp group neighbor add-paths

Description This command allows the add-paths node to be the configured for one or more families of the BGP instance, a group or a neighbor. The BGP add-paths capability allows the router to send and/or receive multiple paths per prefix to/from a peer. The add-paths command without additional parameters is equivalent to removing Add-Paths support for all address families, which causes sessions that previously negotiated the add-paths capability for one or more address families to go down and come back up without the add-paths capability.

The no form of this command (no add-paths) removes add-paths from the configuration of BGP, the group or the neighbor, causing sessions established using add-paths to go down and come back up without the add-paths capability.

Default no add-paths

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.98 add-paths-send-limit

add-paths-send-limit

Syntax **add-paths-send-limit** *send-limit*
no add-paths-send-limit

Context **[Tree]** (config>router>policy-options>policy-statement>entry add-paths-send-limit)
[Tree] (config>router>policy-options>policy-statement>default-action add-paths-send-limit)

Full Context configure router policy-options policy-statement default-action add-paths-send-limit
configure router policy-options policy-statement entry add-paths-send-limit

Description This command sets the *send-limit* to a specific value for all routes matched by the policy entry or default action. Add-paths allows a BGP router to send multiple paths for the same NLRI/prefix to a peer advertising the add-paths receive capability. The *send-limit* dictates the maximum number of paths that can be advertised.

The default *send-limit* is controlled by the instance, group or neighbor level configuration and applies to all prefixes in a particular address family. Using route policies allows the default send-limit to be overridden to use a larger or smaller maximum value on a per-prefix basis. For example, if, for most prefixes advertised to a peer, at most 1 path should be advertised but for a few exceptional prefixes up to 4 paths should be advertised, then the neighbor-level *send-limit* can be set to a value of 1 and the **add-paths-send-limit** in the policy entry that matches the exceptional routes can be set to a value of 4.

Default no add-paths-send-limit

Parameters *send-limit* — Specifies the maximum number of paths to advertise for matched routes to an Add-Paths peer. If the value is **multipaths**, then BGP advertises all of the used BGP multipaths for each matched route that is the best path for its prefix (NLRI). Add paths can be advertised only if the peer has signaled support for receiving multiple add paths.

Values 1 to 16, none, multipaths

Platforms All

5.99 add-srv6-tlvs

add-srv6-tlvs

Syntax **add-srv6-tlvs locator** *locator-name*
no add-srv6-tlvs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp>srv6>family add-srv6-tlvs)

Full Context configure router bgp segment-routing-v6 family add-srv6-tlvs

Description This command adds a prefix SID attribute containing an SRv6 TLV to routes belonging to the family that are redistributed from another protocol into BGP. This command also adds a prefix SID attribute with SRv6 TLV to BGP routes received from other peers without the SRv6 TLV and that are propagated to other peers with **next-hop-self** applied.

The **no** form of this command reverts to the default value which does not append the SRv6 TLV.

Default no add-srv6-tlvs

Parameters *locator-name* — Specifies an existing locator name, up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

5.100 add-to-received-ebgp

add-to-received-ebgp

Syntax **add-to-received-ebgp** *family* [*family*]
no add-to-received-ebgp

Context [Tree] (config>service>vprn>bgp>group>link-bandwidth add-to-received-ebgp)
[Tree] (config>service>vprn>bgp>group>neighbor>link-bandwidth add-to-received-ebgp)

Full Context configure service vprn bgp group link-bandwidth add-to-received-ebgp
configure service vprn bgp group neighbor link-bandwidth add-to-received-ebgp

Description This command configures BGP to automatically add a link-bandwidth extended community to every route received from a directly connected (single-hop) EBGP peer within the scope of the command, as long as that route belongs to one of the listed address families.

The link-bandwidth extended community added by this command encodes the local-AS number of receiving BGP instance and the bandwidth of the interface to the directly connected EBGP peer.

Up to three families may be configured.

The **no** form of this command removes the link-bandwidth extended community added to received BGP routes.

Default no add-to-received-ebgp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

Platforms All

add-to-received-ebgp

Syntax **add-to-received-ebgp** *family* [*family*]
no add-to-received-ebgp

Context **[Tree]** (config>router>bgp>group>link-bandwidth add-to-received-ebgp)
[Tree] (config>router>bgp>group>neighbor>link-bandwidth add-to-received-ebgp)

Full Context configure router bgp group link-bandwidth add-to-received-ebgp
configure router bgp group neighbor link-bandwidth add-to-received-ebgp

Description This command configures BGP to automatically add a link-bandwidth extended community to every route received from a directly connected (single-hop) EBGP peer within the scope of the command, as long as that route belongs to one of the listed address families.

The link-bandwidth extended community added by this command encodes the local-AS number of receiving BGP instance and the bandwidth of the interface to the directly connected EBGP peer.

Up to six families may be configured.

The **no** form of this command removes the link-bandwidth extended community added to received BGP routes.

Default no add-to-received-ebgp

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

vpn-ipv4 — Adds a link-bandwidth extended community to IPv4 VPN (SAFI 128) routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

label-ipv6 — Adds a link-bandwidth extended community to labeled-unicast IPv6 routes.

vpn-ipv6 — Adds a link-bandwidth extended community to IPv6 VPN (SAFI 128) routes.

Platforms All

5.101 add-tunnel

add-tunnel

Syntax **add-tunnel never**
add-tunnel on *reason* [*reason*]
no add-tunnel

Context **[Tree]** (config>router>l2tp>tunnel-selection-blacklist add-tunnel)
[Tree] (config>service>vprn>l2tp>tunnel-selection-blacklist add-tunnel)

Full Context configure router l2tp tunnel-selection-blacklist add-tunnel
configure service vprn l2tp tunnel-selection-blacklist add-tunnel

Description This command will force the tunnel to the denylist and render it unavailable for new sessions for the duration of preconfigured time. Peers are always forced to the denylist in case they time out (failure to receive response to control packets). In addition to time outs, certain events can be used to trigger placement of the tunnel on the denylist.

Default add-tunnel never

Parameters **never** — When specified, no tunnels will be placed on the denylist under any circumstance. This parameter will available to preserve backward compatibility.

reason — Specifies the return codes or events that determine which tunnels are added to the denylist. A maximum of eight reasons can be specified in a single statement.

Table 24 **Return codes**

Return code	Tunnels added to denylist
cdn-err-code	A tunnel is forced to the denylist if that CDN message with the Result Code 2 (Call disconnected for the reasons indicated in error code) is received.
cdn-inv-dest	A tunnel is forced to the denylist if that CDN message with the Result Codes 6 (Invalid destination) is received.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 24 **Return codes**

Return code	Tunnels added to denylist
cdn-tmp-no-facilities	A tunnel is forced to the denylist if that CDN message with the Result Code 4 is received (Call failed due to lack of appropriate facilities being available - temporary condition) is received.
cdn-perm-no-facilities	A tunnel is forced to the denylist if that CDN message with the Result Codes 5 (Call failed due to lack of appropriate facilities being available - permanent condition) is received.
tx-cdn-not-established-in-time	A tunnel is forced to the denylist if that CDN message with the Result Code 10 (Call was not established within time allotted by LAC) is sent from the LAC to the LNS.
stop-ccn-err-code	A tunnel is forced to the denylist if that StopCCN message with the Result Code 2 (General error – Error Code indicates the problem) is sent or received.
stop-ccn-other	A tunnel is forced to the denylist if that StopCCN message with the following Result Codes is received: (1) General request to clear control connection (4) Requester is not authorized to establish a control channel (5) Protocol version not supported (6) Requester is being shutdown Or in the case that the StopCCN with the following result codes is transmitted: (4) Requester is not authorized to establish a control channel. (5) Protocol version not supported The receipt of the following Result Codes will never denylist a tunnel: (0) Reserved (3) Control channel already exist (7) Finite state machine error (8) Undefined Transmission of the following Result Codes will never denylist a tunnel: (1) General request to clear control connection (3) Control channel already exist (6) Requester is being shutdown (7) Finite state machine error

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 24 **Return codes**

Return code	Tunnels added to denylist
addr-change-timeout	A timed-out tunnel for which the peer IP address has changed mid-session (from the one that is provided initially during configuration) is forced to the denylist. In absence of this configuration option, only the configured peer for the tunnel is, but not the tunnel itself which now has a different peer address than the one initially configured.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.102 address

address

Syntax **address gi-address** [**scope** *scope*]
address *ip-address*[*/prefix-length*]
address pool *pool-name* [**secondary-pool** *sec-pool-name*] [**delimiter** *delimiter*]
address use-pool-from-client [**delimiter** *delimiter*]
no address

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host address)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host address)

Full Context configure subscriber-mgmt local-user-db ipoe host address
configure subscriber-mgmt local-user-db ppp host address

Description This command configures how the IP address is defined for this host.

When the user database is used from a local DHCP server, then this command defines how to define the IP address the server offers to the DHCP-client.

When the user-db is used for PPPoE authentication, the **gi-address** parameter cannot be used. A fixed IP address causes PPPoE to use this IP address. If no IP address is specified, the PPPoE looks for IP address by other means (DHCP). If a pool name is given, this pool is sent in the DHCP request so it can be used in by the DHCP server to determine which address to give to the host.

The **no** form of this command causes no IP address to be assigned to this host. In a user database referred to from a local DHCP server, creating a host without address information causes the matching client never to get an IP address.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **gi-address** — When specified, the gi-address of the DHCP message is taken to look for a subnet in the local DHCP server. The first available free address of the subnet is taken and "offered" to the host. When **local-user-db** is used for PPPoE authentication, this has the same result as **no address**.

ip-address — Specifies the fixed IP address to use for this host.

Values a.b.c.d

pool-name/sec-pool-name — Specifies the primary (and secondary) pool (in the local DHCP server), up to 32 characters, to look for an available address. The first available IP address from any subnet in the pool is used. When the local user database is used for PPPoE authentication, this causes the specified pool name to be sent to the DHCP server in a vendor-specific sub-option under Option 82.

use-pool-from-client — Use the pool-name in the Option 82 vendor-specific sub-option.

delimiter — Specifies a single ASCII character specifies the delimiter of separating primary and secondary pool names in option82 VSO.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** *ipv6-address/prefix-length* [**eui-64**] [**track-srrp** *srrp-instance*] [**modifier** *cga-modifier*] [**dad-disable**] [**primary-preference** *primary-preference*]
no address *ipv6-address/prefix-length*

Context **[Tree]** (config>service>ies>if>ipv6 address)
[Tree] (config>service>vprn>if>ipv6 address)

Full Context configure service ies interface ipv6 address
configure service vprn interface ipv6 address

Description This command assigns an IPv6 address/subnet to the interface.

Up to 16 total primary and secondary IPv4 and IPv6 addresses can be assigned to network interfaces, and up to 256 to access interfaces.

Caution: Configurations must not exceed 16 secondary IP addresses when IPsec, GRE, L2TPv3, or IP in IP protocols are active on an access interface.

The **no** form of this command removes the IPv6 address from the interface.

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address on the interface.

Values

ipv6-address/prefix:	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	x [0 to FFFF]H
	d [0 to 255]D
prefix-length	1 to 128

eui-64 — When the **eui-64** keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM interfaces, the Base MAC address of the chassis is used.

srrp-instance — Specifies the SRRP instance ID that this interface route needs to track.

Values 1 to 4294967295

cga-modifier — Specifies the modifier in 32 hexadecimal nibbles.

Values 0x0–0xFFFFFFFF

dad-disable — Disables Duplicate Address Detection (DAD) and sets the address to preferred, even if there is a duplicated address.

primary-preference — Specifies a *primary-preference* index to an IPv6 address of the interface to enforce the order in which the address is used by control plane protocols and applications which require a fixed address of the interface. These include LDP and Segment Routing.

When originating packets from this interface, the source IPv6 address follows the selection rules in RFC 6724 except for the specific cases where a fixed address is required. In the latter case, the IPv6 address with the lowest primary-preference index is selected. If the selected address is removed, the system selects the IPv6 address with the next lowest *primary-preference* index.

The system assigns the next available index value to any IPv6 address of the interface when configured without the *primary-preference* index value specified. The address index space is unique across all addresses of a given interface.

Values 1 to 4294967295

Platforms All

address

Syntax **address** *ipv6-address/prefix-length* [**pd**] [**wan-host**] [**track-srrp** *srrp-instance*] [**holdup-time** *milli-seconds*]
no address *ipv6-address/prefix-length*

Context **[Tree]** (config>service>ies>sub-if>ipv6 address)
[Tree] (config>service>vprn>sub-if>ipv6 address)

Full Context configure service ies subscriber-interface ipv6 address
configure service vprn subscriber-interface ipv6 address

Description This command assigns an IPv6 address/subnet to the subscriber interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

SRRP and an IPv6 Global Unicast Address on a subscriber interface are mutual exclusive:

- **track-srrp** cannot be enabled on a subscriber interface ipv6 address
- when an ipv6 address is configured on a subscriber interface, SRRP cannot be enabled on its group interfaces

The **no** form of this command removes the IPv6 address from the interface.

Parameters *ipv6-address* — Specifies the 128-bit IPv6 address.

Values 128-bit hexadecimal IPv6 address in compressed form

prefix-length — Specifies the length of any associated aggregate prefix.

Values 32 to 127

pd — Specifies that this aggregate is used by IPv6 ESM hosts for DHCPv6 prefix-delegation.

wan-host — Specifies that this aggregate is used by IPv6 ESM hosts for local addressing or by a routing gateway's WAN interface.

srrp-instance — Specifies the SRRP instance number.

Values 1 to 4294967295

milli-seconds — Specifies the time to wait, in milli-seconds, for the route before it accepts the new state attribute. This timer is used to prevent fluctuations in route advertisement caused by short lived SRRP instabilities, in the case that such condition arises.

Values 100 to 5000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** *ip-prefix*/*ip-prefix-length* [**peer-profile** *profile-name*]
no address *ip-prefix*/*ip-prefix-length*

Context **[Tree]** (config>router>gtp>s11>peer-profile-map address)
[Tree] (config>service>vprn>gtp>s11>peer-profile-map address)
[Tree] (config>router>gtp>uplink>peer-profile-map address)
[Tree] (config>service>vprn>gtp>uplink>peer-profile-map address)

Full Context configure router gtp s11 peer-profile-map address
configure router gtp uplink peer-profile-map address
configure service vprn gtp s11 peer-profile-map address
configure service vprn gtp uplink peer-profile-map address

Description This command configures a mapping of an IP address or subnet to a peer profile. If one peer profile is used for the entire router, it is possible to map the entire IPv4 subnet using 0.0.0.0/0.

If no match is found, the default or default S11 peer profile is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the peer profile mapping, affecting only the setup of new peers.

Parameters *ip-prefix*/*ip-prefix-length* — Specifies the IP prefix and prefix length of the subnet.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	[0 to 32]
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D
ipv6-prefix-le	[0 to 128]

profile-name — Specifies the GTP peer profile associated with the address prefix, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>aaa>diam-peer-plcy>peer address)

Full Context configure aaa diameter-peer-policy peer address

Description This command configures the IPv4 or IPv6 address of the diameter peer.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the diameter peer.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

address

Syntax **address** [*ip-address* | *ipv6-address*]
no address

Context **[Tree]** (config>aaa>diam>node>peer address)

Full Context configure aaa diameter node peer address

Description This command configures IPv4 or IPv6 address for a Diameter peer.

The **no** form of this command removes the IPv4 or IPv6 from the peer configuration.

Parameters *ip-address* — Specifies the IPv4 address in the a.b.c.d form

ipv6-address — Specifies the IPv6 address in the form:

x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
where:
x - [0..FFFF]H
d - [0 to 255] D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*} [**broadcast {all-ones** | **host-ones}**] [**track-srrp** *srrp-instance*]
no address [*ip-address/mask* | *ip-address netmask*]

Context **[Tree]** (config>service>ies>if address)
[Tree] (config>service>vprn>if address)
[Tree] (config>service>vprn>nw-if address)

Full Context configure service ies interface address
configure service vprn interface address
configure service vprn network-interface address

Description This command assigns an IP address, IP subnet, and broadcast address format to an IES IP router interface. Only one IP address can be associated with an IP interface. Use the **secondary** command to assign multiple addresses.

An IP address must be assigned to each IES or VPRN IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

Table 25 **Address Admin and Operational States**

Address	Admin State	Oper State
No address	up	down
No address	down	down
1.1.1.1	up	up
1.1.1.1	down	down

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an administratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface are reinitialized.

The **no** form of this command removes the IP address assignment from the IP interface. When the **no address** command is entered, the interface becomes operationally down.

Parameters *ip-address* — Specifies the IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

/ — The forward slash is a parameter delimiter and separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the "*/*" and the *mask-length* parameter. If a forward slash is not immediately following the *ip-address*, a dotted decimal mask must follow the prefix.

mask-length — Specifies the subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask-length* parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address.

Note: A mask length of 32 is reserved for loopback addresses (includes system addresses).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default 0 to 31

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that is used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.254.

Note: A mask of 255.255.255.255 is reserved for system IP addresses.

broadcast — Overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones** which indicates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) is received by the IP interface.

Default host-ones

all-ones — Specifies the broadcast address used by the IP interface for this IP address is 255.255.255.255, also known as the local broadcast.

host-ones — Specifies that the broadcast address used by the IP interface for this IP address is the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask-length* or *mask* with all the host bits set to binary one. This is the default broadcast address used by an IP interface.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

srrp-instance — Tracks the specified SRRP instance state on the IPv6 address.

Platforms All

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*} [**remote-ip** *ip-address*]
no address

Context **[Tree]** (config>service>vprn>red-if address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn redundant-interface address

Description This command assigns an IP address mask or netmask and a remote IP address to the interface.

The **no** form of this command removes the values from the configuration.

Parameters *ip-address/mask* — Assigns an IP address/IP subnet format to the interface.

ip-address netmask — Assigns an IP address netmask to the interface. Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

remote-ip *ip-address* — Assigns a remote IP to the interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** *ip-address/mask* [*netmask*] [**gw-ip-address** *gw-ip-address*] [**populate-host-routes**] [**track-srrp** *srrp-instance*] [**holdup-time** *milli-seconds*]
no address *ip-address/mask* [*netmask*]

Context **[Tree]** (config>service>vprn>sub-if address)
[Tree] (config>service>ies>sub-if address)

Full Context configure service ies subscriber-interface address
configure service vprn subscriber-interface address

Description This command configures the subscriber interface address along with additional parameters related to multi-chassis redundancy.

The **no** form of this command reverts to the default.

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

/ — The forward slash is a parameter delimiter and separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the "*/*" and the *mask-length* parameter. If a forward slash is not immediately following the *ip-address*, a dotted decimal mask must follow the prefix.

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that is used in a logical AND function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.254.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: A mask of 255.255.255.255 is reserved for system IP addresses.

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

gw-ip-address — Specifies a separate IP address within the subnet for SRRP routing purposes. This parameter must be followed by a valid IP interface that exists within the subscriber subnet created by the address command. The defined gateway IP address cannot currently exist as a subscriber host (static or dynamic). If the defined ip-address already exists as a subscriber host address, the address command will fail. The specified ip-address must be unique within the system.

The *gw-ip-address* parameter may be specified at any time. If the subscriber subnet was created previously, executing the **address** command with a *gw-ip-address* parameter will simply add the SRRP gateway IP address to the existing subnet.

If the **address** command is executed without the *gw-ip-address* parameter when the subscriber subnet is associated with an active SRRP instance, the address will fail. If the SRRP instance is inactive or removed, executing the **address** command without the *gw-ip-address* parameter removes the SRRP gateway IP address from the specified subscriber subnet.

If the **address** command is executed with a new GW address, all SRRP instances associated with the specified subscriber subnet is updated with the new SRRP gateway IP address.

populate-host-routes — Specifies to populate subscriber-host routes in local FDB. Storing them in FDB benefits topologies only where the external router advertises more specific routes than the one corresponding to locally configured subscriber-interface subnets.

milli-seconds — Specifies the time to wait, in milli-seconds, for the route before it accepts the new state attribute. This timer is used to prevent fluctuations in route advertisement caused by short lived SRRP instabilities, in the case that such condition arises.

Values 100 to 5000

srrp-inst — Enables the subscriber interface route to track the SRRP state of the specified SRRP instance. The route updates its state attribute to reflect the *state* of SRRP instance:

- Master = srrp-master
- Any other = srrp-non-master

Routing policy can be applied towards the state attribute in order to customize the advertisement of the route. Only one SRRP instance can be tracked per subscriber interface route. Tracked SRRP instance can be part of the Fate Sharing Group. This command can be enabled at any time.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax [**no**] **address** [*ip-address* | *ipv6-address*]

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw address)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw address)

Full Context configure service ies subscriber-interface group-interface wlan-gw address
configure service vprn subscriber-interface group-interface wlan-gw address

Description This command configures an IPv4 or IPv6 address of a WLAN Gateway.

The **no** form of this command removes the IPv4 or IPv6 address from the configuration.

Parameters *ip-address* — Specifies up to four IPv4 addresses.

Values a.b.c.d

ipv6-address — Specifies up to six gateway IPv6 endpoint addresses.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

ipv6-address — Specifies up to six IPv6 addresses.

address

Syntax **address** *ip-address* [/*mask*] [*netmask*]
no address

Context **[Tree]** (config>service>vpls>interface address)

Full Context configure service vpls interface address

Description This command assigns an IP address, IP subnet, and broadcast address format to an IES IP router interface. Only one IP address can be associated with an IP interface.

An IP address must be assigned to each IES IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

Use the **no** form of this command to remove the IP address assignment from the IP interface. When the **no address** command is entered, the interface becomes operationally down.

Address	Admin State	Oper State
No address	up	down
No address	down	down
1.1.1.1	up	up
1.1.1.1	down	down

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an administratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface will be reinitialized.

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP netmask

The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 to 255.255.255.254. A mask of 255.255.255.255 is reserved for system IP addresses.

Platforms All

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*} [**remote-ip** *ip-address*]
no address

Context **[Tree]** (config>service>ies>redundant-interface address)

Full Context configure service ies redundant-interface address

Description This command assigns an IP address mask or netmask and a remote IP address to the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address/mask* — Assigns an IP address/IP subnet format to the interface.

ip-address netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

Assigns an IP address netmask to the interface.

remote-ip *ip-address* — Assigns a remote IP to the interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>service>vprn>log>syslog address)

Full Context configure service vprn log syslog address

Description This command adds the syslog target host IP address to/from a syslog ID.

The *ip-address* parameter is mandatory. If no **address** is configured, syslog data cannot be forwarded to the syslog target host.

Only one address can be associated with a *syslog-id*. If multiple addresses are entered, the last address entered overwrites the previous address.

The same syslog target host can be used by multiple log IDs.

The **no** form of this command removes the syslog target host IP address.

Default no address

Parameters *ip-address* — Specifies the IP address of the syslog target host in dotted decimal notation.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
	interface: 32 characters maximum, mandatory for link local addresses

The ipv6-address applies to the 7750 SR.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

address

Syntax [**no**] **address** *ipv6-address*

Context **[Tree]** (config>service>vprn>nat>inside>dslite address)

Full Context configure service vprn nat inside dual-stack-lite address

Description This command configures a DS-Lite IPv6 address

The **no** form of this command removes the value from the configuration.

Parameters *ipv6-address* — Specifies the IPv6 address on the interface.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax [**no**] **address** *ip-address*

Context **[Tree]** (config>service>vprn>radius-proxy>server>wlan-gw address)
[Tree] (config>router>radius-proxy>server>wlan-gw address)

Full Context configure router radius-proxy server wlan-gw address
configure service vprn radius-proxy server wlan-gw address

Description This command configures the IPv4 address of the distributed RADIUS proxy server for use by the access points.

The **no** form of this command removes the address from the configuration.

Parameters *ip-address* — Specifies the destination IPv4 address of the RADIUS proxy server.

Values ipv4-address a.b.c.d

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax [**no**] **address** *ip-address/mask*

Context **[Tree]** (config>service>vprn>nat>inside>l2-aware address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn nat inside l2-aware address

Description This command configures a Layer 2-aware NAT address. This address will act as a local address of the system. Hosts connected to the inside service will be able to ARP for this address. To verify connectivity, a host can also ping the address. This address is typically used as next hop of the default route of a Layer 2-aware host. The given mask defines a Layer 2-aware subnet. The (inside) IP address used by a Layer 2-aware host must match one of the subnets defined here or it will be rejected.

Parameters *ip-address* — Specifies the IP address in a.b.c.d format.

mask — Specifies the mask.

Values 16 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax [**no**] **address** *ip-address*

Context **[Tree]** (config>service>vprn>pim>rp>bsr-candidate address)
[Tree] (config>service>vprn>pim>rp>rp-candidate address)

Full Context configure service vprn pim rp bsr-candidate address
configure service vprn pim rp rp-candidate address

Description This command configures a static bootstrap or rendezvous point (RP) as long as the source is not directly attached to this router.

Use the **no** form of this command to remove the static RP from the configuration.

Default No IP address is specified.

Parameters *ip-address* — The static IP address of the RP. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 to 223.255.255.255

Platforms All

address

Syntax [**no**] **address** *ipv6-address*

Context **[Tree]** (config>service>vprn>pim>rp>ipv6>bsr-candidate address)
[Tree] (config>service>vprn>pim>rp>ipv6>rp-candidate address)

Full Context configure service vprn pim rp ipv6 bsr-candidate address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn pim rp ipv6 rp-candidate address

Description This command configures a static bootstrap or rendezvous point (RP) as long as the source is not directly attached to this router.

Use the **no** form of this command to remove the static RP from the configuration.

Default No IP address is specified.

Parameters *ipv6-address* — The static IP address of the RP. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values

ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D

Platforms All

address

Syntax [**no**] **address** *ip-address*

Context **[Tree]** (config>service>vprn>pim>rp>static address)

Full Context configure service vprn pim rp static address

Description This command configures the static rendezvous point (RP) address.

The **no** form of this command removes the static RP entry from the configuration.

Platforms All

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*} [**remote-ip** *ip-address*]
no address

Context **[Tree]** (config>service>vprn>redundant-interface address)

Full Context configure service vprn redundant-interface address

Description This command assigns an IP address mask or netmask and a remote IP address to the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address/mask* — Assigns an IP address/IP subnet format to the interface.

ip-address netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

Assigns an IP address netmask to the interface.

remote-ip *ip-address* — Assigns a remote IP to the interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>app-assure>group>evt-log>syslog address)

Full Context configure application-assurance group event-log syslog address

Description This command configures the target syslog host IP address.

Default no address

Parameters *ip-address* — Specifies the IP address of the target syslog host, either IPv4 or IPv6.

Values ipv4-address a.b.c.d
ipv6-address x:x:x:x:x:x:x:x
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address** {*ip-addressImask* | *ip-address netmask*}
no address [*ip-address/mask* | *ip-address netmask*]

Context **[Tree]** (config>service>ies>aa-interface address)
[Tree] (config>service>vprn>aa-interface address)

Full Context configure service ies aa-interface address
configure service vprn aa-interface address

Description This command assigns an IP address to the interface.

Default no address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address/mask* — Specifies an IP address/IP subnet format to the interface.

ip-address netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

create — Keyword that specifies to create the interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax **address prefix** *ip-prefix/ip-prefix-len*
address from *begin-ip-address* **to** *end-ip-address*
no address

Context **[Tree]** (config>ipsec>ts-list>local>entry address)
[Tree] (config>ipsec>ts-list>remote>entry address)

Full Context configure ipsec ts-list local entry address
configure ipsec ts-list remote entry address

Description This command specifies the address range in the IKEv2 traffic selector.

Default no address

Parameters *ip-prefix/ip-prefix-len* — Specifies the IP prefix and subnet mask.

begin-ip-address — Specifies the beginning address of the range for this entry.

end-ip-address — Specifies the ending address of the range for this entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax [**no**] **address** *ipv6-address*

Context **[Tree]** (config>router>nat>inside>dual-stack-lite address)

Full Context configure router nat inside dual-stack-lite address

Description This command configures a DS-Lite IPv6 address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address

Syntax [**no**] **address** *ip-address/mask*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>nat>inside address)

Full Context configure router nat inside address

Description This command configures the IP address and mask of the subnet.

The **no** form of the command removes the IP address and prefix length from the configuration.

Parameters *ip-address/mask* — Specifies the IP address and mask of the subnet.

Values

ip-address:	a.b.c.d
mask:	16 to 32

address

Syntax [**no**] **address** *ip-address/mask*

Context [Tree] (config>service>ies>video-interface address)
[Tree] (config>service>vpls>video-interface address)
[Tree] (config>service>vprn>video-interface address)

Full Context configure service ies video-interface address
configure service vpls video-interface address
configure service vprn video-interface address

Description This command assigns an IP address to the video interface within the service. Video interface IP addresses are used by video service clients to direct requests for video server services. Up to 16 IP address/subnets can be defined. The addresses defined must all be distinct and cannot be contained within a previously defined address. In the VPLS context, only one IP address can be defined for a video interface.

The **no** form of the command deletes the IP address/subnet from the video interface.

Parameters *ip-address* — Specifies the IP address/subnet of the video interface in dotted decimal notation.

mask — Specifies the subnet mask length for the IP address expressed as an integer.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

address

Syntax **address** *ip-address*
no address

Context [Tree] (config>router>pim>rp>bsr-candidate address)

Full Context configure router pim rp bsr-candidate address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the candidate BSR IP address. This address is for Bootstrap router election.

The **no** form of this command removes the IP address from the BSR candidate configuration.

Default no address

Parameters *ip-address* — Specifies the IP host address used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 – 223.255.255.255

Platforms All

address

Syntax **address** *ipv6-address*
no address

Context **[Tree]** (config>router>pim>rp>ipv6>bsr-candidate address)

Full Context configure router pim rp ipv6 bsr-candidate address

Description This command configures the candidate BSR IPv6 address. This address is for Bootstrap router election.

The **no** form of this command removes the IPv6 address from the BSR candidate configuration.

Default no address

Parameters *ipv6-address* — Specifies the IPv6 host address used by the interface within the subnet.

Values
x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

address

Syntax **address** *ipv6-address*
no address

Context **[Tree]** (config>router>pim>rp>ipv6>rp-candidate address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router pim rp ipv6 rp-candidate address

Description This command configures the local IPv6 RP address. This address is sent in the RP candidate advertisements to the bootstrap router.

The **no** form of this command removes the IPv6 address from the RP candidate configuration.

Default no address

Parameters *ipv6-address* — Specifies the IPv6 RP address.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

prefix-length: 16 to 128

Platforms All

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>router>pim>rp>rp-candidate address)

Full Context configure router pim rp rp-candidate address

Description This command configures the local RP address. This address is sent in the RP candidate advertisements to the bootstrap router.

The **no** form of this command removes the IP address from the RP candidate configuration.

Default no address

Parameters *ip-address* — Specifies the *ip-address.*

Values 1.0.0.0 – 223.255.255.255

Platforms All

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>router>pim>rp>static address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>pim>rp>ipv6>static address)

Full Context configure router pim rp ipv6 static address
configure router pim rp static address

Description This command configures the Rendezvous Point (RP) address that should be used by the router for the range of multicast groups configured by the range command.

The **no** form of this command removes the IP address from the static configuration.

Parameters *ip-address* — Specifies the static IP address of the RP. The *ip-address* portion of the **address** command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 – 223.255.255.255

Platforms All

address

Syntax **address** *ipv4-address*
no address

Context [Tree] (config>li>x-interfaces>lics>lic address)

Full Context configure li x-interfaces lics lic address

Description This command configures the IP address of this LIC.

The **no** form of this command reverts to the default.

Parameters *ipv4-address* — Specifies the IPv4 address of the LIC.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

address

Syntax **address** *ipv4-address*
no address

Context [Tree] (config>li>x-interfaces>x1 address)

Full Context configure li x-interfaces x1 address

Description This command configures the X1 interface IP address that must match an IP address configured on the router.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv4-address* — Specifies the IPv4 address of the LIC.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

address

Syntax **address** *ipv4-address*
no address

Context **[Tree]** (config>li>x-interfaces>x2 address)

Full Context configure li x-interfaces x2 address

Description This command configures the X2 interface IP address that must match an IP address configured on the router.

The **no** form of this command reverts to the default.

Parameters *ipv4-address* — Specifies the IPv4 address of the LIC.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

address

Syntax **address** {*ip-address*/*mask* | *ip-address netmask*} [**broadcast** {**all-ones** | **host-ones**}] [**track-srrp** *srrp-instance*] [**gre-termination**]
no address

Context **[Tree]** (config>router>if address)

Full Context configure router interface address

Description This command assigns an IP address, IP subnet, and broadcast address format to an IP interface. Only one IP address can be associated with an IP interface. Use the **secondary** command to assign additional addresses.

An IP address must be assigned to each IP interface. An IP address and a mask combine to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

From Release 19.10, The overlap restriction is not applicable for host-addresses configured on loopback interfaces. For example, a loopback interface addresses configured with mask of 32 or netmask of 255.255.255.255 can overlap with other prefixes on other IP interfaces in the same routing context within the router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. **Show** commands display CIDR notation and are stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

The **no** form of this command removes the IP address assignment from the IP interface. Interface specific configurations for MPLS are also removed. This will operationally stop any MPLS LSPs that explicitly reference that IP address. When a new IP address is configured, interface specific configurations for MPLS need to be added. IEEE 1588 port based timestamping configured with **ptp-hw-assist** is also disabled.

Default no address

Parameters *ip-address* — Specifies the IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 to 223.255.255.255

/ — The forward slash is a parameter delimiter that separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the "*/*" and the *mask* parameter. If a forward slash does not immediately follow the *ip-address*, a dotted decimal mask must follow the prefix.

mask — Specifies the subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask* parameter. The *mask* parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Allowed values are integers in the range 1— 32. A mask length of 32 is reserved for system IP addresses.

Values 1 to 32

netmask — Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

broadcast — The optional **broadcast** parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones,** which indicates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) will be received by the IP interface.

Default host-ones

Values all-ones, host-ones

all-ones — The **all-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

host-ones — Specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *netmask* with all the host bits set to binary 1. This is the default broadcast address used by an IP interface.

srrp-instance — Specifies the SRRP instance ID that this interface route needs to track.

Values 1 to 4294967295

gre-termination — The optional **gre-termination** keyword allows GRE SDP tunnel packets to terminate on the router interface using the /31 value of the configured IP address. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Services Overview Guide* for information about using **gre-termination**.

Platforms All

address

Syntax **address** *ipv6-address/prefix-length* [**eui-64**] [**track-srrp** *srrp-instance*] [**modifier** *cga-modifier*] [**dad-disable**] [**primary-preference** *primary-preference*]
no address *ipv6-address/prefix-length*

Context **[Tree]** (config>router>if>ipv6 address)

Full Context configure router interface ipv6 address

Description This command assigns an IPv6 address to the interface. Up to 16 total primary and secondary IPv4 and IPv6 addresses can be assigned to network interfaces, and up to 256 to access interfaces.

Caution: Configurations must not exceed 16 IPv6 addresses when IPsec, GRE, L2TPv3, or IP in IP protocols are active on an access interface.

A global IPv6 address together with the *prefix-length* create a locally configured interface IPv6 prefix and subnet. The defined global IP prefix must be unique within the context of a routing instance. It cannot overlap with any other existing global IP prefix defined on another IP interface within the same routing context in the router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This overlap restriction is not applicable for IPv6 host addresses configured on loopback interfaces. For example, an IPv6 loopback host address configured upon a loopback interface may overlap with another prefix subnet configured on another IP interface within the same routing context.

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address on the interface.

Values

ipv6-address/prefix-length:	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x [0 to FFFF]H
		d [0 to 255]D
	prefix-length	1 to 128

eui-64 — When the **eui-64** keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example POS interfaces, the Base MAC address of the chassis should be used.

srrp-instance — Indicates the unique identifier of the tracked SRRP instance.

Values 1 to 4294967295

cga-modifier — Sets the modifier for cryptographically-assigned addresses.

Values 0x0..0xFFFFFFFF...(32 hex nibbles)

dad-disable — Disables Duplicate Address Detection (DAD) and sets the address to preferred, even if there is a duplicated address.

primary-preference — Specifies a *primary-preference* index to an IPv6 address of the interface to enforce the order in which the address is used by control plane protocols and applications which require a fixed address of the interface. These include LDP and Segment Routing.

When originating packets from this interface, the source IPv6 address follows the selection rules in RFC 6724 except for the specific cases where a fixed address is required. In the latter case, the IPv6 address with the lowest primary-preference index is selected. If the selected address is removed, the system selects the IPv6 address with the next lowest *primary-preference* index.

The system assigns the next available index value to any IPv6 address of the interface when configured without the *primary-preference* index value specified. The address index space is unique across all addresses of a given interface.

Values 1 to 4294967295

srrp — Tracks the specified SRRP instance state on the IPv6 address.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

address

Syntax [**no**] **address** *ip-prefix/ip-prefix-length* [**active** | **standby** | **standby/A** | **standby/B** | **standby/C** | **standby/D**]

Context **[Tree]** (bof address)

Full Context bof address

Description This command assigns an IP address to the management Ethernet port on a CPM. This applies during the boot loader and the running image.

On all systems except the 7950 XRS-40, an address must be assigned with the **active** keyword and for systems with a redundant CPM an additional address may be assigned with the **standby** keyword. The active address is used by the active CPM whether its CPM A or CPM B and the standby address, if specified, is used by the standby CPM whether its CPM B or CPM A.

For the 7950 XRS-40, if the extension chassis shall boot from local compact flash then an active and standby address should be defined for use by the master chassis as defined above.

For the 7950 XRS-40, if the extension chassis shall boot from remote URL, then it is required to assign addresses to the management Ethernet ports for CPM C and CPM D. In this case, the BOF should be updated to have addresses defined using the **standby/A**, **standby/B**, **standby/C**, and **standby/D** keywords in addition to an address using the **active** keyword. With these keywords, CPM A shall always use the address defined using the **standby/A** address when CPM A is running as the standby CPM. Similarly, CPM B shall always use the address defined using the **standby/B** address when CPM B is running as the standby CPM. The active CPM of CPM A and CPM B shall use the address defined using the **active** keyword.

Deleting a BOF address entry is not allowed from a remote session.

Note that changing the active and standby addresses without reboot standby CPM may cause a boot-env sync to fail.

The **no** form of this command deletes the IP address from the CPM Ethernet port.

Parameters *ip-prefix/ip-prefix-length* — Specifies the destination address of the aggregate route in dotted decimal notation.

Values

ipv4-prefix	*a.b.c.d* (host bits must be 0)	
ipv4-prefix-length	0 to 32	
ipv6-prefix	*x:x:x:x:x:x:x:x* (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-prefix-length 0 to128

active | **standby** | **standby/A** | **standby/B** | **standby/C** | **standby/D** — specifies which CPM Ethernet address is being configured

Default active

Platforms All

address

Syntax **address** {**01:1b:19:00:00:00**| **01:80:c2:00:00:0e**}

Context **[Tree]** (config>system>ptp>port address)

Full Context configure system ptp port address

Description This command allows for the specification of the mac-address to be used for the destination MAC address of the transmitted ptp messages.

IEEE Std 1588-2008 Annex F defines two reserved addresses for 1588 messages. These are:

- **01-1B-19-00-00-00** — all except the peer delay mechanism messages
- **01-80-C2-00-00-0E** — peer delay mechanism messages

Both addresses are supported for reception independent of the address configured by this command.

The **no** form of this command sets the address to the default address.

Default address 01-1B-19-00-00-00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>log>syslog address)

Full Context configure log syslog address

Description This command adds the syslog target host IP address to/from a syslog ID.

This parameter is mandatory. If no **address** is configured, syslog data cannot be forwarded to the syslog target host.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Only one address can be associated with a *syslog-id*. If multiple addresses are entered, the last address entered overwrites the previous address.

The same syslog target host can be used by multiple log IDs.

The **no** form of this command removes the syslog target host IP address.

Default no address

Parameters *ip-address* — Specifies the IP address of the syslog target host in dotted decimal notation. An IPv6-address applies only to the 7750 SR.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 characters maximum, mandatory for link local
	addressesipv6-address x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 characters maximum, mandatory for link local addresses

Platforms All

address

Syntax **address** *ip-address* [**port** *port*]
no address

Context **[Tree]** (config>system>security>ldap>server address)

Full Context configure system security ldap server address

Description This command configures the IPv4 or IPv6 address for the LDAP server.

The **no** version of this command removes the server address.

Parameters *ip-address* — The IP address of the LDAP server.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0..FFFF]H
d: [0..255]D

port — Specifies the port ID. The port is the LDAP server listening port; by default it is 389 but if the listening port on LDAP server is changed, this command needs to be configured accordingly.

Values 1 to 65535

Default 389

Platforms All

address

Syntax **address** *ip-address*
no address

Context **[Tree]** (config>router>static-route-entry>next-hop>backup-next-hop address)
[Tree] (config>service>vprn>static-route-entry>next-hop>backup-next-hop address)

Full Context configure router static-route-entry next-hop backup-next-hop address
configure service vprn static-route-entry next-hop backup-next-hop address

Description This command specifies the backup IP forwarding address that is used for static route Fast ReRoute (FRR). The configured address, if reachable, acts as pre-installed backup forwarding information that can be used when the primary IP next-hop suddenly fails.

The configured backup next-hop IP address can be directly or indirectly connected (using an IGP or tunnel) to the node. The backup next-hop forwarding information or the Next-hop Label Forwarding Entry (NHLFE) tunnel forwarding information from the IP Routing Table Manager (RTM) is used to preconfigure an IP fast-reroute backup path.

One backup next-hop address can protect a single primary static route entry next-hop address without ECMP and it is only activated when the primary next-hop has no active ECMP.

The configured IP address can be either on the network or the access side.

By default, there is no backup next-hop address configured.

The **no** form of this command deletes the backup next-hop address entry.

Parameters *ip-address* — Specifies the backup IP forwarding address.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0..FFFF]H
d: [0..255]D

Platforms All

address

Syntax [**no**] **address** *ip-address* [*:port*]

Context **[Tree]** (config>app-assure>group>cflowd>direct-export>collector address)

Full Context configure application-assurance group cflowd direct-export collector address

Description This command configures the Cflowd direct export collector remote address. Two addresses can be configured for each collector for redundancy. AA sends the same records to both at the same time.

The **no** form of this command removes the address from the configuration

Parameters *ip-address* — Specifies the IP address of the Cflowd direct export collector, in the a.b.c.d format.

port — Specifies the port of the Cflowd direct export collector.

Values 1 to 65535

Default 4739

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.103 address-avp

address-avp

Syntax [**no**] **address-avp**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp address-avp)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp address-avp

Description This command includes the following subscriber host/session address/prefix AVPs in all Diameter DCCA CCR messages:

- [8] Framed-IP-Address
- [97] Framed-IPv6-Prefix
- [123] Delegated-IPv6-Prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- [6527-99] Alc-IPv6-Address

Note: Only the address/prefix of the subscriber host that triggered the creation of the Diameter Gy session is included.

The **no** form of this command removes the address AVPs from the Diameter DCCA CCR messages.

Default address-avp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.104 address-pref

address-pref

Syntax **address-pref** {**ipv4-only** | **ipv6-first**}
no address-pref

Context **[Tree]** (config>system>dns address-pref)

Full Context configure system dns address-pref

Description This command configures the DNS address resolving order preference. By default, DNS names are queried for A-records only (address-preference is IPv4-only).

If the address-preference is set to IPv6-first, the DNS server will be queried for AAAA-records (IPv6) first and if a successful replied is not received, then the DNS server is queried for A-records. IPv6 applies only to the 7750 SR and 7950 XRS.

Default address-pref ipv4-only

Platforms All

5.105 address-range

address-range

Syntax **no address-range** *start-ip-address end-ip-address* [**failover** {**local** | **remote** | **access-driven**}]
no address-range *start-ip-address end-ip-address*

Context **[Tree]** (config>router>dhcp>server>pool>subnet address-range)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>dhcp>server>pool address-range)

Full Context configure router dhcp local-dhcp-server pool subnet address-range
configure service vprn dhcp server pool address-range

Description This command configures a range of IP addresses to be served from the pool. All IP addresses between the start and end IP addresses are included (other than specific excluded addresses).

The **no** form of this command removes the address-range parameters from the configuration.

Parameters *start-ip-address* — Specifies the start address of this range to include. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

end-ip-address — Specifies the end address of this range to include. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

local — Specifies that the local DHCP server has the ownership of this dress range in a redundant setup under normal operation.

remote — Specifies that the remote DHCP server has the ownership of this address range in a redundant setup under normal operation.

access-driven — Specifies that the DHCP server failover system is in control by the access protection mechanisms (SRRP or MC-LAG).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

address-range

Syntax **address-range** *start-ip-address end-ip-address* [**create**]
no address-range *start-ip-address end-ip-address*

Context [Tree] (config>service>vprn>nat>outside>pool address-range)
[Tree] (config>router>nat>outside>pool address-range)

Full Context configure router nat outside pool address-range
configure service vprn nat outside pool address-range

Description This command configures a NAT address range.

Parameters *start-ip-address* — Specifies the beginning IP address in a.b.c.d form.

end-ip-address — Specifies the ending IP address in a.b.c.d. form.

create — This parameter must be specified to create the address range instance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address-range

Syntax **address-range start** *ipv4-address* **end** *ipv4-address*
no address-range

Context **[Tree]** (config>li>x-interfaces>x3 address-range)

Full Context configure li x-interfaces x3 address-range

Description This command configures the range of IP addresses to use for the X3 interface. The number of addresses should correspond to the number of ISAs used for the x-interface application.

The **no** form of this command reverts to the default.

Parameters *ipv4-address* — Specifies an IPv4 address.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.106 address-source

address-source

Syntax **address-source router** *router-instance* **dhcp-server** *local-dhcp4-svr-name* **pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]
address-source service-name *service-name* **dhcp-server** *local-dhcp4-svr-name* **pool** *dhcp4-server-pool* [**secondary-pool** *secondary-pool-name*]
address-source router *router-instance* **dhcp-server** *local-dhcp6-svr-name* **pool** *dhcp6-server-pool*
address-source service-name *service-name* **dhcp-server** *local-dhcp6-svr-name* **pool** *dhcp6-server-pool*
no address-source

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>lcl-addr-assign>ipv4 address-source)
[Tree] (config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign>ipv4 address-source)
[Tree] (config>service>ies>if>sap>ipsec-gw>lcl-addr-assign>ipv6 address-source)
[Tree] (config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign>ipv6 address-source)

Full Context configure service ies interface sap ipsec-gw local-address-assignment ipv4 address-source
configure service ies interface sap ipsec-gw local-address-assignment ipv6 address-source
configure service vprn interface sap ipsec-gw local-address-assignment ipv4 address-source
configure service vprn interface sap ipsec-gw local-address-assignment ipv6 address-source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the IPv4 or IPv6 source of the local address assignment for the IPsec gateway, which is a pool of a local DHCPv4 or DHCPv6 server. The system will assign an internal address to an IKEv2 remote-access client from the specified pool.

Beside the IP address, netmask and DNS server can also be returned. For IPv4, the netmask and DNS server address can be returned from the specified pool, as well as the IP address. The netmask returned to the IPsec client is derived from the subnet length from the **subnet** *x.x.x.x/m* **create** configuration, not the **subnet-mask** configuration in the subnet context. For IPv6, the DNS server address can be returned from the specified pool, as well as the IP address.

For IPv4, a secondary pool can be optionally specified. The secondary pool is used if the system is unable to assign addresses from the primary pool.

Default no address-source

Parameters *router-instance* — Specifies the router instance ID where the local DHCPv4 or DHCPv6 server is defined, up to 32 characters.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **address-source service-name** *service-name* variant can be used in all configuration modes.

service-name — Specifies the name of the service where the local DHCPv4 or DHCPv6 server is defined, up to 64 characters.

local-dhcp4-svr-name — Specifies the name of the local DHCPv4 server, up to 32 characters.

local-dhcp6-svr-name — Specifies the name of the local DHCv6 server, up to 32 characters.

dhcp4-server-pool — The name of the pool defined in the specified DHCPv4 server, up to 32 characters.

dhcp6-server-pool — The name of the pool defined in the specified DHCPv6 server, up to 32 characters.

secondary-pool-name — The name of the secondary pool defined in the specified server, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.107 address-state

address-state

Syntax [**no**] **address-state**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>aaa>isa-radius-plcy>acct-update-triggers address-state)

Full Context configure aaa isa-radius-policy acct-update-triggers address-state

Description If enabled, an interim-update will be sent for a DSM UE whenever a DHCP, SLAAC or DHCPv6 address gets allocated or freed.

Default no address-state

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.108 address-type

address-type

Syntax **address-type** {**ipv4** | **ipv6** | **not-specified**}
no address-type

Context [Tree] (config>subscr-mgmt>wlan-gw>tunnel-query address-type)

Full Context configure subscriber-mgmt wlan-gw tunnel-query address-type

Description This command specifies the address type to match on tunnels.

The **no** form of this command reverts to the default.

Default address-type not-specified

Parameters **ipv4** — Specifies the IPv4 address to match on tunnels.

ipv6 — Specifies the IPv6 address to match on tunnels.

not-specified — Specifies that no address type matches on tunnels.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

address-type

Syntax **address-type** {**ipv4** | **ipv6** | **ipv4-only** | **ipv6-only** | **ipv4v6** | **not-specified**}
no address-type

Context [Tree] (config>subscr-mgmt>wlan-gw>ue-query address-type)

Full Context configure subscriber-mgmt wlan-gw ue-query address-type

Description This command enables matching on UEs that have an address of the specified type.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default address-type not-specified

Parameters **ipv4** — Specifies matching on UEs that have an IPv4 stack active.

ipv6 — Specifies matching on UEs that have an IPv6 stack active.

ipv4-only — Specifies matching on UEs that have only an IPv4 and no IPv6 stack active.

ipv6-only — Specifies matching on UEs that have only an IPv6 and no IPv4 stack active.

ipv4v6 — Specifies matching on UEs that have both an IPv4 and IPv6 stack active.

not-specified — Specifies that no address type matches on UEs.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.109 adi

adi

Syntax **adi**

Context **[Tree]** (config>service>ies>video-interface adi)
[Tree] (config>service>vprn>video-interface adi)

Full Context configure service ies video-interface adi
configure service vprn video-interface adi

Description Commands in this context configure ad insertion (ADI) for the video interface.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

adi

Syntax **adi** [*zone-channel-name*]
no adi

Context **[Tree]** (debug>service>id>video-interface adi)

Full Context debug service id video-interface adi

Description This command enables debugging for the ad insert server.

Parameters *zone-channel-name* — Specifies the channel name up to 32 characters.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.110 adi-packet

adi-packet

Syntax **adi-packet** [*zone-channel-name*] [**type** {*type-name* [*type-name*] | **all**}]
no adi-packet

Context **[Tree]** (debug>service>id>video-interface adi-packet)

Full Context debug service id video-interface adi-packet

Description This command enables debugging for ADI packets exchanged between the splicer and the ad-server over scte30 sessions.

Parameters *zone-channel-name* — Specifies the channel name up to 32 characters.

type *type-name* — Specifies the ADI packet type.

Values alive, abort, init, splice, cue, all

Output The following is an example output for this command.

Sample Output

```
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-1 type ini
t
A:IPTV-SR7# show debug
debug
    service id 100
        video-interface video-100
            adi-packet 240-1 type init
        exit
    exit
exit
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-1 type ali
ve
A:IPTV-SR7# show debug
debug
    service id 100
        video-interface video-100
            adi-packet 240-1 type alive
        exit
    exit
exit
```

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.111 adj-set

adj-set

Syntax [**no**] **adj-set**

Context **[Tree]** (config>router>isis>segm-rtng>egress-statistics adj-set)
[Tree] (config>router>ospf>segm-rtng>egress-statistics adj-set)
[Tree] (config>router>isis>segm-rtng>ingress-statistics adj-set)
[Tree] (config>router>ospf>segm-rtng>ingress-statistics adj-set)

Full Context configure router isis segment-routing egress-statistics adj-set
configure router isis segment-routing ingress-statistics adj-set
configure router ospf segment-routing egress-statistics adj-set
configure router ospf segment-routing ingress-statistics adj-set

Description This command enables the allocation of statistic indices to each adjacency set. All adjacencies of a set share the same statistics index. If a statistics index is not available at allocation time, the allocation fails, then the system re-tries the allocation. The system generates a log on the first fail and a log on the final successful allocation.

The **no** form of this command disables the allocation of statistic indices to each adjacency set, releases the statistic indices, and clears the associated counters.

Default no adj-set

Platforms All

5.112 adj-sid

adj-sid

Syntax [**no**] **adj-sid**

Context **[Tree]** (config>router>isis>segm-rtng>egress-statistics adj-sid)
[Tree] (config>router>ospf>segm-rtng>egress-statistics adj-sid)
[Tree] (config>router>ospf3>segm-rtng>egress-statistics adj-sid)
[Tree] (config>router>isis>segm-rtng>ingress-statistics adj-sid)
[Tree] (config>router>ospf>segm-rtng>ingress-statistics adj-sid)
[Tree] (config>router>ospf3>segm-rtng>ingress-statistics adj-sid)

Full Context configure router isis segment-routing egress-statistics adj-sid
configure router isis segment-routing ingress-statistics adj-sid
configure router ospf segment-routing egress-statistics adj-sid
configure router ospf segment-routing ingress-statistics adj-sid

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf3 segment-routing egress-statistics adj-sid
configure router ospf3 segment-routing ingress-statistics adj-sid

Description This command enables the allocation of statistic indices to each programmed NHLFE corresponding to Adjacency SIDs (local and received by means of IGP advertisement). All NHLFEs associated to a given SID share the same index. If a statistics index is not available at allocation time, the allocation fails, then the system re-tries the allocation. The system generates a log on the first fail and a log on the final successful allocation.

The **no** form of this command disables the allocation of statistic indices to each adjacency SID, releases the statistic indices, and clears the associated counters.

Default no adj-sid

Platforms All

5.113 adj-sid-hold

adj-sid-hold

Syntax **adj-sid-hold** *seconds*
no adj-sid-hold

Context **[Tree]** (config>router>isis>segment-routing adj-sid-hold)

Full Context configure router isis segment-routing adj-sid-hold

Description This command configures a timer to hold the ILM or LTM of an adjacency SID following a failure of the adjacency.

When an adjacency to a neighbor fails, IGP will withdraw the advertisement of the link TLV information as well as its adjacency SID sub-TLV. However, the LTN or ILM record of the adjacency SID must be kept in data path to maintain forwarding using the LFA or remote LFA backup for a period of time sufficient to allow the ingress LER and other routers which use this adjacency SID to activate a new path after IGP converges.

If the adjacency is restored before the timer expires, the timer is aborted as soon as the new ILM or LTN records are updated with the new primary and backup NHLFE information.

The **no** form of this command removes adjacency SID hold time.

Default adj-sid-hold 15

Parameters *seconds* — Specifies the adjacency SID hold time, in seconds.

Values 1 to 300

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

adj-sid-hold

Syntax **adj-sid-hold** *seconds*
no adj-sid-hold

Context **[Tree]** (config>router>isis>srv6 adj-sid-hold)

Full Context configure router isis segment-routing-v6 adj-sid-hold

Description This command specifies the length of time the system holds the SRv6 adjacency LFA, Remote LFA, or TI-LFA backup path while the adjacency is down. The recommendation is to set the timer to the time it takes for the network IGP processes to converge, which allows the PCE to compute a new path for SR-TE LSPs and SR policies impacted by the adjacency failure.

Note: Each IS-IS instance runs a single timer per adjacency that IPv4 SR-MPLS, IPv6 SR-MPLS, and SRv6 adjacency SIDs share. When you enable both SR-MPLS (**config**>**router**>**isis**>**segment-routing**) and SRv6 (**config**>**router**>**isis**>**segment-routing-v6**) in the IS-IS instance, the system programs the higher of the two timer values for all SIDs on the adjacency

The **no** form of this command reverts to the default value.

Default adj-sid-hold 15

Parameters *seconds* — Specifies the adjacency SID hold time, in seconds.

Values 1 to 300

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

adj-sid-hold

Syntax **adj-sid-hold** *seconds*
no adj-sid-hold

Context **[Tree]** (config>router>ospf>segm-rtng adj-sid-hold)
[Tree] (config>router>ospf3>segm-rtng adj-sid-hold)

Full Context configure router ospf segment-routing adj-sid-hold
configure router ospf3 segment-routing adj-sid-hold

Description This command configures a timer to hold the ILM or LTM of an adjacency SID following a failure of the adjacency.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an adjacency to a neighbor fails, the IGP will withdraw the advertisement of the link TLV information as well as its adjacency SID sub-TLV. However, the LTN or ILM record of the adjacency SID must be kept in the data path to maintain forwarding using the LFA or remote LFA backup for sufficient length of time to allow the ingress LER and other routers that use this adjacency SID to activate a new path after the IGP converges.

If the adjacency is restored before the timer expires, the timer is aborted as soon as the new ILM or LTN records are updated with the new primary and backup NHLFE information.

The **no** form of this command removes the adjacency SID hold time.

Default adj-sid-hold 15

Parameters *seconds* — Specifies the adjacency SID hold time, in seconds.

Values 1 to 300

Platforms All

5.114 adjacency

adjacency

Syntax [**no**] **adjacency**

Context **[Tree]** (debug>service>id>pim-snooping adjacency)

Full Context debug service id pim-snooping adjacency

Description This command enables or disables debugging for PIM adjacencies.

Platforms All

adjacency

Syntax [**no**] **adjacency**

Context **[Tree]** (debug>router>pim adjacency)

Full Context debug router pim adjacency

Description This command enables debugging for PIM adjacencies.

The **no** form of this command disables debugging for PIM adjacencies.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

adjacency

Syntax [**no**] **adjacency** [*ip-int-name* | *ip-address* | *nbr-system-id*]

Context **[Tree]** (debug>router>isis adjacency)

Full Context debug router isis adjacency

Description This command enables debugging for IS-IS adjacency.

The **no** form of the command disables debugging.

Parameters *ip-address* — When specified, only adjacencies with the specified interface address are debugged.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

ip-int-name — When specified, only adjacencies with the specified interface name are debugged.

nbr-system-id — When specified, only the adjacency with the specified ID is debugged.

Platforms All

5.115 adjacency-set

adjacency-set

Syntax [**no**] **adjacency-set** *id*

Context **[Tree]** (config>router>ospf>segm-rtng adjacency-set)
[Tree] (config>router>isis>segm-rtng adjacency-set)

Full Context configure router isis segment-routing adjacency-set
configure router ospf segment-routing adjacency-set

Description This command creates an adjacency set. An adjacency set consists of one or more adjacency SIDs originating on this node. The constituent adjacencies may terminate on different nodes.

The **no** form of this command removes the specified adjacency set.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *id* — Specifies an unsigned integer representing the identifier of the adjacency set.

Values 1 to 4294967295

Platforms All

adjacency-set

Syntax [**no**] **adjacency-set** *id*

Context **[Tree]** (config>router>ospf>area>interface adjacency-set)
[Tree] (config>router>isis>interface adjacency-set)

Full Context configure router isis interface adjacency-set
configure router ospf area interface adjacency-set

Description This command associates an interface with an adjacency set. The adjacency set must have been defined under the IS-IS or OSPF segment-routing context.

The **no** form of this command removes the association.

Parameters *id* — Specifies an unsigned integer representing the identifier of the adjacency set.

Values 1 to 4294967295

Platforms All

5.116 adjacency-sid

adjacency-sid

Syntax **adjacency-sid label** *value*
no adjacency-sid

Context **[Tree]** (config>router>ospf>area>interface adjacency-sid)

Full Context configure router ospf area interface adjacency-sid

Description This command allows a static value to be assigned to an adjacency SID in OSPF segment routing.

The **label** option specifies that the value is assigned to an MPLS label.

The **no** form of this command removes the adjacency SID.

Parameters **label** *value* — Specifies the value of adjacency SID label.

Values 18432 to 52428 | 1048575 (FP4 only)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

5.117 adjust-down

adjust-down

Syntax **adjust-down** *percent* [**bw** *bandwidth-in-mbps*]
no adjust-down

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth adjust-down)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth adjust-down)

Full Context configure router mpls lsp auto-bandwidth adjust-down
configure router mpls lsp-template auto-bandwidth adjust-down

Description This command configures the minimum threshold for decreasing the bandwidth of an LSP based on active measurement of LSP bandwidth.

The **no** form of this command is equivalent to **adjust-down** 5.

Default adjust-down 5 bw 0

Parameters *percent* — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as a percentage of the current bandwidth, for decreasing the bandwidth of the LSP.

Values 1 to 100

bandwidth-in-mbps — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as an absolute bandwidth (Mb/s), for decreasing the bandwidth of the LSP.

Values 0 to 6400000

Platforms All

5.118 adjust-up

adjust-up

Syntax **adjust-up** *percent* [**bw** *bandwidth-in-mbps*]
no adjust-up

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth adjust-up)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>mpls>lsp-template>auto-bandwidth adjust-up)

Full Context configure router mpls lsp auto-bandwidth adjust-up
configure router mpls lsp-template auto-bandwidth adjust-up

Description This command configures the minimum threshold for increasing the bandwidth of an LSP based on active measurement of LSP bandwidth.

The **no** form of this command is equivalent to **adjust-up** 5.

Default adjust-up 5 bw 0

Parameters *percent* — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as a percentage of the current bandwidth, for increasing the bandwidth of the LSP.

Values 1 to 100

bandwidth-in-mbps — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as an absolute bandwidth (Mb/s), for increasing the bandwidth of the LSP

Values 0 to 6400000

Platforms All

5.119 admin

admin

Syntax **admin**

Context **[Tree]** (admin)

Full Context admin

Description Commands in this context configure administrative system parameters. Only authorized users can execute the commands in the **admin** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.120 admin-bw

admin-bw

Syntax **admin-bw** *kbps*
no admin-bw

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle admin-bw)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel admin-bw)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>src-override admin-bw)

Full Context configure mcast-management multicast-info-policy bundle admin-bw
configure mcast-management multicast-info-policy bundle channel admin-bw
configure mcast-management multicast-info-policy bundle channel source-override admin-bw

Description This command specifies an administrative bandwidth for multicast channels. The specified bandwidth rate can be used by the multicast ingress path manger, multicast CAC manager or multicast ECMP manager.

The *kbps* value is closely tied to the **bw-activity** command. When the bw-activity command is set to use-admin-bw, the multicast ingress path manager uses the configured administrative bandwidth value as the managed ingress bandwidth. The **admin-bw** value must be defined for the **bw-activity use-admin-bw** command to succeed. Once the bw-activity command is set to use the admin-bw value, the value cannot be set to 0 and the no admin-bw command fails. Setting the bw-activity command to dynamic (the default setting), breaks the association between the commands.

The **no** form of this command restores the default value for admin-bw. If the command is executed in the **channel** context, the channels administrative bandwidth value is set to null. If the command is executed in the **source-override** context, the source override administrative bandwidth value is set to null.

Parameters *kbps* — Specifies the administrative bandwidth for multicast channels.

Values 1 to 40000000 kb/s

Bundle default:	0
Channel default:	Null (undefined)
Source-override default:	Null (undefined)

Override sequence — The channel setting overrides the bundle setting. The source-override setting overrides the channel and bundle settings.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.121 admin-bw-threshold

admin-bw-threshold

Syntax **admin-bw-threshold** *kilo-bits-per-second*
no admin-bw-threshold

Context **[Tree]** (config>mcast-mgmt>bw-plcy admin-bw-threshold)

Full Context configure mcast-management bandwidth-policy admin-bw-threshold

Description This command defines at which bandwidth rate a multicast channel configured to use an administrative rate starts and stop using that rate as the in-use ingress bandwidth when managing ingress multicast paths. This parameter only applies to channels that are configured to use the admin-bw rate with the **bw-activity use-admin-bw** command (both are configured in the multicast-info-policy associated with the channel context).

To be effective, the **admin-bw-threshold** value must be less than the channels configured admin-bw. If the administrative bandwidth configured on the channel is less than the administrative bandwidth threshold defined in the bandwidth policy, the admin-bw value is ignored for ingress multicast path management and the system continually uses the dynamic ingress bandwidth associated with the channel. Since the value is defined in the bandwidth-policy and the channel admin-bw value is defined in the **multicast-info-policy**, it is not possible to pre-determine that a given administrative bandwidth value is less than an administrative bandwidth threshold. Since a typical administrative bandwidth threshold is set significantly lower than any administrative bandwidth values, this corner case is not expected to be prevalent. However, if the case does arise in a production environment, no ill behavior is expected as the threshold is simply a tuning parameter used to detect when the bandwidth associated with a channel has risen above any OAM or background type traffic.

While a channel that is configured to the **use-admin-bw** parameter (in the **bw-activity** command) current bandwidth is less than the admin-bw-threshold, the system treats the channel as a dynamic type channel. Once the threshold is crossed, the system immediately allocates the full admin-bw value to the channel and manages the ingress multicast path accordingly. If the bandwidth monitored on the channel rises above the admin-bw value, the system reverts to dynamic bandwidth management operation. If the bandwidth drops below the admin-bw value, but is above the **admin-bw-threshold**, the system uses the admin-bw value. If the bandwidth drops below the admin-bw-threshold, the system goes back to dynamic bandwidth management operation.

This command has no effect on multicast ECMP or egress CAC management operations.

The **no** form of this command reverts to the default, which is 10 kb/s.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *kilobits-per-second* — Specifies the defines the rate at which channels configured to use administrative bandwidths change from dynamic bandwidth management to using the channels configured administrative bandwidth. The parameter is expressed as an integer value and represents multiples of 1,000 bits per second. A value of 3000 indicates 3,000,000 bits per second.

Values 1 to 40,000,000

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

5.122 admin-group

admin-group

Syntax [**no**] **admin-group** *group-name* [*group-name*]
no admin-group

Context **[Tree]** (config>router>if>if-attribute admin-group)
[Tree] (config>service>ies>if>if-attribute admin-group)
[Tree] (config>service>vprn>if>if-attribute admin-group)
[Tree] (config>router>mpls>interface admin-group)

Full Context configure router interface if-attribute admin-group
configure router mpls interface admin-group
configure service ies interface if-attribute admin-group
configure service vprn interface if-attribute admin-group

Description This command configures the admin group membership of an interface. The user can apply admin groups to an IES, VPRN, network IP, or MPLS interface.

Each single operation of the **admin-group** command allows a maximum of five (5) groups to be specified at a time. However, a maximum of 32 groups can be added to a given interface through multiple operations. Once an admin group is bound to one or more interface, its value cannot be changed until all bindings are removed.

The configured **admin-group** membership will be applied in all levels or areas the interface is participating in. The same interface cannot have different memberships in different levels or areas.

Only the admin groups bound to an MPLS interface are advertised in TE link TLVs and sub-TLVs when the **traffic-engineering** option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

The **no** form of this command deletes one or more of the admin-group memberships of an interface. The user can also delete all memberships of an interface by not specifying a group name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no admin-group

Parameters *group-name* — Specifies up to five groups, each up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain. Each single operation of the **admin-group** command allows a maximum of 5 groups to be specified. However, a maximum of 32 groups can be added to a given interface through multiple operations.

Platforms All

admin-group

Syntax **admin-group** *group-name* **value** *group-value*
no admin-group *group-name*

Context **[Tree]** (config>router>if-attribute admin-group)

Full Context configure router if-attribute admin-group

Description This command defines an administrative group (admin-group) that can be associated with an IP or MPLS interface.

Admin groups, also known as affinity, are used to tag IP and MPLS interfaces that share a specific characteristic with the same identifier. For example, an admin group identifier can represent all links that connect to core routers, or all links that have a bandwidth higher than 10G, or all links that are dedicated to a specific service.

The user first configures locally on each router the name and identifier of each admin group. A maximum of 32 admin groups can be configured per system.

The user then configures the admin group membership of an interface. The user can apply admin groups to a IES, VPRN, network IP, or MPLS interface.

When applied to MPLS interfaces, the interfaces can be included or excluded in the LSP path definition by inferring the admin-group name. CSPF will compute a path that satisfies the admin-group include and exclude constraints.

When applied to IES, VPRN, or network IP interfaces, the interfaces can be included or excluded in the route next-hop selection by inferring the admin-group name in a route next-hop policy template applied to an interface or a set of prefixes.

The following provisioning rules are applied to admin group configuration. The system will reject the creation of an admin-group if it re-uses the same name but with a different group value than an existing group. The system will also reject the creation of an admin-group if it re-uses the same group value but with a different name than an existing group.

Only the admin groups bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the **traffic-engineering** option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-name* — Specifies the name of the group with up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain

group-value — Specifies the integer value associated with the group. The association of group name and value should be unique within an IP/MPLS domain.

Values 0 to 31

Platforms All

admin-group

Syntax **admin-group** *admin-group*
no admin-group *admin-group*

Context **[Tree]** (config>router>fad>flex-algo>exclude admin-group)

Full Context configure router flexible-algorithm-definitions flex-algo exclude admin-group

Description This command configures an administrative group link that will be excluded from the topology graph of the flexible algorithm. If multiple administrative groups are configured, they are all excluded from the topology graph.

Administrative groups are attributes associated with a link. Frequently these administrative groups are described as link colors.

The **no** form of this command removes the admin-group from being excluded from the topology graph.

Default no admin-group

Parameters *admin-group* — Configures an administrative group link to exclude from the topology graph of the configured FAD.

Platforms All

admin-group

Syntax **admin-group** *admin-group*
no admin-group *admin-group*

Context **[Tree]** (config>router>fad>flex-algo>include-all admin-group)

Full Context configure router flexible-algorithm-definitions flex-algo include-all admin-group

Description This command configures an administrative group link that will be included in the topology graph of the defined FAD. If multiple administrative groups are configured, groups must be present in a link before the link is included in the flexible algorithm topology graph.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the specified *admin-group* from being included in the topology graph.

Default no admin-group

Parameters *admin-group* — Configures an administrative group to include in topology graph of the configured FAD.

Platforms All

admin-group

Syntax **admin-group** *admin-group*
no admin-group *admin-group*

Context **[Tree]** (config>router>fad>flex-algo>include-any admin-group)

Full Context configure router flexible-algorithm-definitions flex-algo include-any admin-group

Description This command configures an administrative group link that will be included in the topology graph of the configured FAD. If multiple administrative groups are configured, at least one of the administrative groups must be present in a link before the link is included into the flexible algorithm topology graph.

The **no** form of this command removes the *admin-group* from being included in the topology graph.

Default no admin-group

Parameters *admin-group* — Configures an administrative group to include in the topology graph of the configured FAD.

Platforms All

5.123 admin-group-frr

admin-group-frr

Syntax [**no**] **admin-group-frr**

Context **[Tree]** (config>router>mpls admin-group-frr)

Full Context configure router mpls admin-group-frr

Description This command enables the use of the admin-group constraints in the association of a manual or dynamic bypass LSP with the primary LSP path at a Point-of-Local Repair (PLR) node.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this command is enabled, each PLR node reads the admin-group constraints in the FAST_REROUTE object in the Path message of the LSP primary path. If the FAST_REROUTE object is not included in the Path message, then the PLR will read the admin-group constraints from the Session Attribute object in the Path message.

If the PLR is also the ingress LER for the LSP primary path, then it just uses the admin-group constraint from the LSP and/or path level configurations.

The PLR node then uses the admin-group constraints along with other constraints, such as hop-limit and SRLG, to select a manual or dynamic bypass among those that are already in use.

If none of the manual or dynamic bypass LSP satisfies the admin-group constraints, and/or the other constraints, the PLR node will request CSPF for a path that merges the closest to the protected link or node and that includes or excludes the specified admin-group IDs.

If the user changes the configuration of the above command, it will not have any effect on existing bypass associations. The change will only apply to new attempts to find a valid bypass.

The **no** form of this command disables the use of administrative group constraints on a FRR backup LSP at a PLR node.

Default no frr-admin-group

Platforms All

5.124 admin-password

admin-password

Syntax **admin-password** *password* [**hash** | **hash2**]
no admin-password

Context **[Tree]** (config>system>security>password admin-password)

Full Context configure system security password admin-password

Description This command allows a user (with admin permissions) to configure a password that enables a user to become an administrator.

This password is valid only for one session. When enabled, no authorization to TACACS+ or RADIUS is performed and the user is locally regarded as an admin user.

This functionality can be enabled in two contexts:

config>system>security>password>admin-password

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

<global> enable-admin

If the admin-password is configured in the **config>system>security>password** context, then any user can enter the special mode by entering the **enable-admin** command.

enable-admin is in the default profile. By default, all users are given access to this command.

After the **enable-admin** command is entered, the user is prompted for a password. If the password matches, user is given unrestricted access to all the commands.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password are determined by the **complexity** command.

Note: The *password* argument of this command is not sent to the servers. This is consistent with other commands that configure secrets.

The usernames and passwords in the FTP and TFTP URLs will not be sent to the authorization or accounting servers when the **file>copy** *source-url dest-url* command is executed.

For example:

file copy ftp://test:secret@10.20.31.79/test/srcfile cf1:\destfile

In this example, the username 'test' and password 'secret' will not be sent to the AAA servers (or to any logs). They will be replaced with '"*****"'.

The **no** form of this command removes the admin password from the configuration.

Note: This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

Default no admin-password

Parameters *password* — Configures the password that enables a user to become a system administrator. The maximum length can be up to 56 characters if unhashed, 60 characters if hashed with bcrypt, from 87 to 92 characters if hashed with sha2-pbkdf2, 32 characters if the hash keyword is specified, or 54 characters if the hash2 keyword is specified. The unhashed clear text password form should meet all the requirements that are defined by the **complexity** command.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form or hashed with bcrypt or PBKDF2. For security, all keys are stored in the configuration file in hashed form (using bcrypt or PBKDF2, depending on the hashing configuration parameter) or, for backward compatibility, can be stored in encrypted form with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form or hashed with bcrypt or PBKDF2. For security, all keys are stored in the configuration file in hashed form (using bcrypt or PBKDF2, depending on the hashing configuration parameter) or, for backward compatibility, can be stored in encrypted form with the **hash** or **hash2** parameter specified.

Platforms All

5.125 admin-state

admin-state

Syntax **admin-state** {**up** | **down**}
no admin-state

Context **[Tree]** (config>router>l2tp>group>tunnel>mlppp admin-state)
[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp admin-state)

Full Context configure router l2tp group tunnel mlppp admin-state
configure service vprn l2tp group tunnel mlppp admin-state

Description This command enables MLPPP for this tunnel group and is applicable only to LNS.

The tunnel can be explicitly activated (if the parent group is in a **no shutdown** state) or deactivated by the **up** and **down** keywords.

If there the admin state is not configured, the tunnel inherits its administrative state from its parent (group).

The **no** form of this command causes the tunnel administrative state to be inherited from the group.

Parameters **up** — Specifies that the tunnel is to be administratively up.

down — Specifies that the tunnel is to be administratively down.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.126 admin-status

admin-status

Syntax **admin-status** {**rx** | **tx** | **tx-rx** | **disabled**}

Context **[Tree]** (config>port>ethernet>lldp>dstmac admin-status)

Full Context configure port ethernet lldp dest-mac admin-status

Description This command configures LLDP transmission/reception frame handling.

Default admin-status disabled

Parameters **rx** — Specifies the LLDP agent will receive, but will not transmit LLDP frames on this port.

tx — Specifies that the LLDP agent will transmit LLDP frames on this port and will not store any information about the remote systems connected.

tx-rx — Specifies that the LLDP agent transmits and receives LLDP frames on this port.

disabled — Specifies that the LLDP agent does not transmit or receive LLDP frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port's admin status becomes disabled, then the information will naturally age out.

Platforms All

5.127 admin-tag

admin-tag

Syntax [**no**] **admin-tag** *tag-value*

Context **[Tree]** (config>router>mpls>lsp admin-tag)
[Tree] (config>router>mpls>lsp-template admin-tag)

Full Context configure router mpls lsp admin-tag
configure router mpls lsp-template admin-tag

Description This assigns an administrative tag to an LSP. The administrative tag can be used to enable routes with certain administrative tags to resolve using LSPs of matching administrative tags.

Up to four tags can be assigned to an LSP.

The administrative tag must exist under **config>router>admin-tags**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the administrative tag.

Parameters *tag-value* — The value of the admin-tag, up to 32 characters.

Platforms All

admin-tag

Syntax [**no**] **admin-tag** *tag*

Context **[Tree]** (config>router>admin-tags admin-tag)

Full Context configure router admin-tags admin-tag

Description This command configures an admin tag value in the nodal LSP administrative tag database.

Up to 256 admin tags can be configured.

The **no** form of this command removes the admin tag.

Parameters *tag* — The value of the administrative tag, up to 32 characters.

Platforms All

5.128 admin-tag-policy

admin-tag-policy

Syntax **admin-tag-policy** *policy-name*
no admin-tag-policy

Context **[Tree]** (config>router>policy-options>policy-statement>default-action admin-tag-policy)
[Tree] (config>router>policy-options>policy-statement>entry>action admin-tag-policy)

Full Context configure router policy-options policy-statement default-action admin-tag-policy
configure router policy-options policy-statement entry action admin-tag-policy

Description This command assigns a route admin tag policy as an action in a route policy.

The admin tag policy must exist under **config>router>admin-tags**.

The **no** form of this command removes the admin tag policy.

Parameters *policy-name* — Specifies the name of the admin tag policy, up to 64 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.129 admin-tags

admin-tags

Syntax **admin-tags**

Context **[Tree]** (config>router admin-tags)

Full Context configure router admin-tags

Description Commands in this context configure admin tags and router admin tag policy templates used for route resolution to LSPs.

Platforms All

5.130 adspec

adspec

Syntax [**no**] **adspec**

Context **[Tree]** (config>router>mpls>lsp adspec)
[Tree] (config>router>mpls>lsp-template adspec)

Full Context configure router mpls lsp adspec
configure router mpls lsp-template adspec

Description When enabled, the ADSPEC object will be included in RSVP messages for this LSP. The ADSPEC object is used by the ingress LER to discover the minimum value of the MTU for links in the path of the LSP. By default, the ingress LER derives the LSP MTU from that of the outgoing interface of the LSP path.

A bypass LSP always signals the ADSPEC object since it protects both primary paths which signal the ADSPEC object and primary paths which do not. This means that MTU of LSP at ingress LER may change to a different value from that derived from the outgoing interface even if the primary path has ADSPEC disabled.

Default no adspec — No ADSPEC objects are included in RSVP messages.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.131 adv-adj-addr-only

adv-adj-addr-only

Syntax [**no**] **adv-adj-addr-only**

Context **[Tree]** (config>router>ldp>session-params>peer adv-adj-addr-only)

Full Context configure router ldp session-parameters peer adv-adj-addr-only

Description This command provides a means for an LDP router to advertise only the local IPv4 or IPv6 interfaces it uses to establish hello adjacencies with an LDP peer. By default, when a router establishes an LDP session with a peer, it advertises in an LDP Address message the addresses of all local interfaces to allow the peer to resolve LDP FECs distributed by this router. Similarly, a router sends a Withdraw Address message to of all its peers to withdraw a local address if the corresponding interface went down or was deleted.

This new option reduces CPU processing when a large number of LDP neighbors come up or go down. The new CLI option is strongly recommended in mobile backhaul networks where the number of LDP peers can be very large.

The **no** form of this command reverts LDP to the default behavior of advertising all local interfaces.

Platforms All

5.132 adv-config-policy

adv-config-policy

Syntax **adv-config-policy** *policy-name* [**create**]
no adv-config-policy *policy-name*

Context **[Tree]** (config>qos adv-config-policy)

Full Context configure qos adv-config-policy

Description Commands in this context configure an advanced QoS policy. This command contains only queue and policer child control parameters within a child-control node.

The parameters within the **child-control** node are intended to allow more precise control of the method that hierarchical virtual scheduling employs to emulate the effect of a scheduling context upon a member child queue or policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a policy is created, it may be applied to a queue or policer defined within a **sap-egress** or **sap-ingress** QoS policy. It may also be applied to a queue or policer defined within an ingress or **egress queue-group** template. When a policy is currently associated with a QoS policy or template, the policy may be modified but not deleted (even in the event that the QoS policy or template is not in use).

While the system maintains default values for the advanced configuration parameters, no default **adv-config-policy** exists.

The **no** form of this command removes the specified advanced policy.

Parameters *policy-name* — The name of the advanced QoS policy. A policy-name must be specified and conform to the policy naming guidelines. If the specified name does not exist, the optional **create** keyword requirements are met and the total number of policies per system will not be exceeded, an **adv-config-policy** of that name will be created. If the specified name does exist, the system will switch context to that **adv-config-policy** for the purpose of modification of the policy's contents.

Values Valid names consist of any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Platforms All

adv-config-policy

Syntax **adv-config-policy** *policy-name*
no adv-config-policy

Context **[Tree]** (config>qos>sap-ingress>policer adv-config-policy)
[Tree] (config>qos>sap-egress>policer adv-config-policy)
[Tree] (config>qos>sap-ingress>queue adv-config-policy)
[Tree] (config>qos>sap-egress>queue adv-config-policy)

Full Context configure qos sap-egress policer adv-config-policy
configure qos sap-egress queue adv-config-policy
configure qos sap-ingress policer adv-config-policy
configure qos sap-ingress queue adv-config-policy

Description This command specifies the advanced QoS policy. The advanced QoS policy contains only queue and policer child control parameters within a child-control node.

When a policy is created, it may be applied to a queue or policer defined within a **sap-egress** or **sap-ingress** QoS policy. It may also be applied to a queue or policer defined within an **ingress** or **egress queue-group** template. When a policy is currently associated with a QoS policy or template, the policy may be modified but not deleted (even in the event that the QoS policy or template is not in use).

The **no** form of this command removes the specified advanced policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no adv-config-policy

Parameters *policy-name* — The name of the advanced QoS policy.

Values Valid names consist of any string up to 63 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-ingress policer adv-config-policy
- configure qos sap-egress policer adv-config-policy

All

- configure qos sap-egress queue adv-config-policy
- configure qos sap-ingress queue adv-config-policy

adv-config-policy

Syntax **adv-config-policy** *adv-config-policy-name*
no adv-config-policy

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer adv-config-policy)
[Tree] (config>qos>qgrps>egr>qgrp>queue adv-config-policy)
[Tree] (config>qos>qgrps>ing>qgrp>policer adv-config-policy)
[Tree] (config>qos>qgrps>ing>qgrp>queue adv-config-policy)

Full Context configure qos queue-group-templates egress queue-group policer adv-config-policy
configure qos queue-group-templates egress queue-group queue adv-config-policy
configure qos queue-group-templates ingress queue-group policer adv-config-policy
configure qos queue-group-templates ingress queue-group queue adv-config-policy

Description This command specifies the name of the advanced configuration policy to be applied with this policer.

Parameters *adv-config-policy-name* — Specifies an existing advanced configuration policy up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos queue-group-templates ingress queue-group policer adv-config-policy
- configure qos queue-group-templates egress queue-group policer adv-config-policy

All

- configure qos queue-group-templates egress queue-group queue adv-config-policy
- configure qos queue-group-templates ingress queue-group queue adv-config-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

adv-config-policy

Syntax **adv-config-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy adv-config-policy)

Full Context configure qos copy adv-config-policy

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters **adv-config-policy** — Indicates that the source policy ID and the destination policy ID are advanced policy IDs. Specify the source advanced policy ID that the copy command will attempt to copy from and specify the destination advanced policy ID to which the command will copy a duplicate of the policy.

overwrite — Specifies that this policy is to replace the existing destination advanced policy. Everything in the existing destination policy will be overwritten with the contents of the source advanced policy. If **overwrite** is not specified, an error will occur if the destination policy ID exists, as shown here:

```
ALA-7>config>qos# copy adv-config-policy default sp1
MINOR: CLI Destination "sp1" exists - use {overwrite}
ALA-7>config>qos#overwrite
```

Platforms All

5.133 adv-local-lsr-id

adv-local-lsr-id

Syntax [**no**] **adv-local-lsr-id**

Context **[Tree]** (config>router>ldp>session-params>peer adv-local-lsr-id)
[Tree] (config>router>ldp>targeted-session>peer-template adv-local-lsr-id)

Full Context configure router ldp session-parameters peer adv-local-lsr-id
configure router ldp targeted-session peer-template adv-local-lsr-id

Description This command advertises a local LSR ID over a specified LDP session.

Advertisement of a local LSR ID over a given LDP session is configured using the **adv-local-lsr-id** command in the peer session-parameters. If a user disables the **adv-local-lsr-id** command, then the system will withdraw the FEC for the local LSR ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SR OS router uses the following rules when advertising a local LSR ID:

- If the session parameters have the default configuration and the targeted peer template has the default configuration, the local LSR ID is not advertised.
- If the session parameters have the default configuration but the targeted peer template has an explicit configuration for advertisement of the local LSR ID, the targeted peer template configuration is used.
- If the session parameters have an explicit configuration for advertisement of the local LSR ID but the targeted peer template has the default configuration, the session parameter configuration is used.
- If both the session parameters and the targeted peer template have an explicit configuration for advertisement of the local LSR ID, then the session parameter configuration is used.

The **no** form of this command withdraws the FEC for the local LSR ID.

Default no adv-local-lsr-id

Platforms All

5.134 adv-mtu-override

adv-mtu-override

Syntax [**no**] **adv-mtu-override**

Context **[Tree]** (config>service>sdp adv-mtu-override)

Full Context configure service sdp adv-mtu-override

Description This command overrides the advertised VC-type MTU of all spoke-sdps of L2 services using this SDP-ID. When enabled, the router signals a VC MTU equal to the service MTU, which includes the Layer 2 header. It also allows this router to accept an MTU advertised by the far-end PE which value matches either its advertised MTU or its advertised MTU minus the L2 headers.

By default, the router advertises a VC-MTU equal to the L2 service MTU minus the Layer 2 header and always matches its advertised MTU to that signaled by the far-end PE router, otherwise the spoke-sdp goes operationally down.

When this command is enabled on the SDP, it has no effect on a spoke-sdp of an IES/VPRN spoke interface using this SDP-ID. The router continues to signal a VC MTU equal to the net IP interface MTU, which is min{ip-mtu, sdp operational path mtu - L2 headers}. The router also continues to make sure that the advertised MTU values of both PE routers match or the spoke-sdp goes operationally down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command disables the VC-type MTU override and returns to the default behavior.

Default no adv-mtu-override

Platforms All

5.135 adv-noaddrs-global

adv-noaddrs-global

Syntax **adv-noaddrs-global** [**esm-proxy**] [**esm-relay**] [**relay**] [**server**]
no adv-noaddrs-global

Context **[Tree]** (config>system>dhcp6 adv-noaddrs-global)

Full Context configure system dhcp6 adv-noaddrs-global

Description This command configures the different DHCPv6 applications to send the NoAddrsAvail Status-Code in DHCPv6 Advertise messages at the global DHCP message level.

By default, all applications send the NoAddrsAvail Status-Code in DHCPv6 Advertise messages at the IA_NA Option level.

Different applications for which NoAddrsAvail Status-Code in DHCPv6 Advertise messages can be configured at the global DHCP message level.

The only valid combination in current SR OS is **adv-noaddrs-global esm-relay server**.

The **no** form of this command reverts to the default.

Default no adv-noaddrs-global. All applications send the NoAddrsAvail Status-Code in DHCPv6 Advertise messages at the IA_NA Option level.

Parameters **esm-proxy** — Specifies the DHCPv6 proxy server on subscriber group-interfaces. Not supported in current SR OS.

esm-relay — Specifies the DHCPv6 relay on subscriber group-interfaces. Must be enabled together with the DHCPv6 server (server) application.

relay — Specifies the DHCPv6 relay on regular IES or VPRN interfaces. Not supported in current SR OS.

server — Specifies the DHCPv6 server. Must be enabled together with the DHCPv6 relay on subscriber interfaces (esm-relay) application.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.136 adv-service-mtu

adv-service-mtu

Syntax **adv-service-mtu** *octets*
no adv-service-mtu

Context **[Tree]** (config>service>epipe>spoke-sdp adv-service-mtu)

Full Context configure service epipe spoke-sdp adv-service-mtu

Description This command configures the MTU value signaled in targeted LDP for the spoke-SDP and the value used to validate the value signaled by the far-end PE. If configured, this value is used instead of the service MTU. However, the configuration does not affect the locally enforced value, which is still based on the service MTU. This command for the MTU cannot be configured on a spoke-SDP that is bound to an SDP with the **adv-mtu-override** command.

When unconfigured, an adjusted service MTU is used. See the **service-mtu** command for more information.

The **no** form of this command removes the configuration.

Default no adv-service-mtu

Parameters *octets* — The size of the MTU in octets, expressed as a decimal integer.

Values 0 to 9782

Platforms All

adv-service-mtu

Syntax **adv-service-mtu** *number*
no adv-service-mtu

Context **[Tree]** (config>service>epipe>bgp adv-service-mtu)
[Tree] (config>service>vpls>bgp adv-service-mtu)

Full Context configure service epipe bgp adv-service-mtu
configure service vpls bgp adv-service-mtu

Description This command configures the Layer 2 MTU value that is advertised for BGP signaling for the service and for validation with the value signaled by the far-end PE. However, the configuration does not effect the locally enforced value, which is still based on the service MTU.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default Layer 2 MTU value for BGP signaling for the service, which uses an adjusted **service-mtu** value. See the **service-mtu** command for more information.

Default no adv-service-mtu

Parameters *number* — Specifies the size, in octets, of the Layer 2 MTU value to advertise for BGP signaling for the service.

Values 0 to 9782

Platforms All

5.137 advertise

advertise

Syntax **advertise** {**static** | **dynamic**} [**route-tag** [*1..255*]]
no advertise {**static** | **dynamic**}

Context **[Tree]** (config>service>ies>if>vpls>evpn>arp advertise)
[Tree] (config>service>ies>if>vpls>evpn>nd advertise)
[Tree] (config>service>vprn>if>vpls>evpn>arp advertise)
[Tree] (config>service>vprn>if>vpls>evpn>nd advertise)

Full Context configure service ies interface vpls evpn arp advertise
configure service ies interface vpls evpn nd advertise
configure service vprn interface vpls evpn arp advertise
configure service vprn interface vpls evpn nd advertise

Description This command enables the advertisement of static and dynamic ARP and ND entries that are installed in the ARP and ND cache into EVPN MAC/IP routes. This command must be used along with **no learn-dynamic**.

Default no advertise

Parameters **static** — Enables ARP/ND host routes to be created in the route table from EVPN ARP/ND entries

dynamic — Enables ARP/ND host routes to be created in the route table out of dynamic ARP/ND entries (learned from ARP/ND messages received from the hosts).

route-tag — Specifies the route tag that is added in the route table for ARP/ND host routes of type **dynamic**, or **static**. This tag can be matched on BGP VRF export and BGP peer export policies.

Values 1 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

advertise

Syntax **advertise** *fad-name*
no advertise

Context **[Tree]** (config>router>isis>flex-algos>flex-algo advertise)
[Tree] (config>router>ospf>flex-algos>flex-algo advertise)

Full Context configure router isis flexible-algorithms flex-algo advertise
configure router ospf flexible-algorithms flex-algo advertise

Description This command enables the advertisement of a locally configured Flexible Algorithm Definition (FAD).

A locally defined FAD is only advertised if it is administratively enabled. A router can advertise only a single locally defined FAD by using the *fad-name* as reference anchor.

The winning FAD used by a router must be consistent with the winning FAD on all other routers. This avoids routing loops and traffic blackholing. The winning FAD is selected using a tie-breaker algorithm that first selects the highest advertised FAD priority and next the highest system Id.

The **no** form of this command removes the advertisement of a flexible algorithm definition.

Default no advertise

Parameters *fad-name* — Configures the FAD name, up to 32 characters. By default, no locally configured FAD is advertised.

Platforms All

advertise

Syntax **advertise** {**mvpn-pim** | **mvpn-only**| **pim-only**}

Context **[Tree]** (config>service>vpls>bind>evpn-mcast-gateway advertise)

Full Context configure service vpls allow-ip-int-bind evpn-mcast-gateway advertise

Description This command signals the OISM gateway function type in the Inclusive Multicast Ethernet Tag routes.

Default advertise mvpn-pim

Parameters **mvpn-pim** — Specifies that the router signals the MVPN-to-OISM (MEG) and PIM-to-OISM (PEG) gateway capabilities.

mvpn-only — Specifies that the router signals the MVPN-to-OISM (MEG) gateway capabilities.

pim-only — Specifies that the router signals the PIM-to-OISM (PEG) gateway capabilities.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

5.138 advertise-bgp

advertise-bgp

Syntax **advertise-bgp route-distinguisher** *rd* [**community** *community*]
no advertise-bgp route-distinguisher *rd*

Context **[Tree]** (config>service>pw-routing>local-prefix advertise-bgp)

Full Context configure service pw-routing local-prefix advertise-bgp

Description This command enables a given prefix to be advertised in MP-BGP for dynamic MS-PW routing.

The **no** form of this command will explicitly withdraw a route if it has been previously advertised.

Default no advertise-bgp

Parameters *rd* — Specifies an 8-octet route distinguisher associated with the prefix. Up to 4 unique route distinguishers can be configured and advertised for a given prefix though multiple instances of the advertise-bgp command. This parameter is mandatory.

Values (6 bytes, other 2 Bytes of type will be automatically generated) asn:number1 (RD Type 0): 2bytes ASN and 4 bytes locally administered number ip-address:number2 (RD Type 1): 4bytes IPv4 and 2 bytes locally administered number;

community — An optional BGP communities attribute associated with the advertisement. To delete a previously advertised community, advertise-bgp route-distinguisher must be run again with the same value for the RD but excluding the community attribute.

Values

community	{2-byte-as-number:comm-va1}
2-byte-asnumber	0 to 65535
comm.-val	0 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.139 advertise-capabilities

advertise-capabilities

Syntax **advertise-capabilities**

Context **[Tree]** (config>port>ethernet>efm-oam>discovery advertise-capabilities)

Full Context configure port ethernet efm-oam discovery advertise-capabilities

Description This is the top level of the hierarchy which allows for the overriding of default advertising of capabilities to a remote peer.

Platforms All

5.140 advertise-external

advertise-external

Syntax [**no**] **advertise-external** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**]

Context **[Tree]** (config>router>bgp advertise-external)

Full Context configure router bgp advertise-external

Description This command allows BGP to advertise its best external route to a destination even when its best overall route is an internal route. Entering the command (or its **no** form) with no address family parameters is equivalent to specifying all supported address families.

The **no** form of this command disables Advertise Best External for the BGP family.

Default no advertise-external

Parameters **ipv4** — Enables the best-external advertisement for unlabeled unicast IPv4 routes.

ipv6 — Enables the best-external advertisement for unlabeled unicast IPv6 routes.

label-ipv4 — Enables the best-external advertisement for labeled-unicast IPv4 routes.

label-ipv6 — Enables the best-external advertisement for labeled-unicast IPv6 routes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.141 advertise-inactive

advertise-inactive

Syntax [**no**] **advertise-inactive**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy advertise-inactive)

Full Context configure subscriber-mgmt bgp-peering-policy advertise-inactive

Description This command enables the advertising of inactive BGP routers to other BGP peers.

By default, BGP only advertises BGP routes to other BGP peers if a given BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the most preferred route within the system for a given destination.

The **no** form of this command disables the advertising.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

advertise-inactive

Syntax [**no**] **advertise-inactive**

Context **[Tree]** (config>service>vprn>bgp advertise-inactive)
[Tree] (config>service>vprn>bgp>group advertise-inactive)
[Tree] (config>service>vprn>bgp>group>neighbor advertise-inactive)

Full Context configure service vprn bgp advertise-inactive
configure service vprn bgp group advertise-inactive
configure service vprn bgp group neighbor advertise-inactive

Description This command enables or disables the advertising of inactive BGP routers to other BGP peers.

By default, BGP only advertises BGP routes to other BGP peers if a given BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the most preferred route within the system for a given destination.

When the BGP **advertise-inactive** command is configured so that it applies to a BGP session it has the following effect on the IPv4, IPv6, mcast-ipv4, mcast-ipv6, label-IPv4 and label-IPv6 routes advertised to that peer:

- If the active route for the IP prefix is a BGP route then that route is advertised.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If the active route for the IP prefix is a non-BGP route and there is at least one valid but inactive BGP route for the same destination then the best of the inactive and valid BGP routes is advertised unless the non-BGP active route is matched and accepted by an export policy applied to the session.
- If the active route for the IP prefix is a non-BGP route and there are no (valid) BGP routes for the same destination then no route is advertised for the prefix unless the non-BGP active route is matched and accepted by an export policy applied to the session.

Default no advertise-inactive

Platforms All

advertise-inactive

Syntax [**no**] **advertise-inactive**

Context **[Tree]** (config>router>bgp advertise-inactive)
[Tree] (config>router>bgp>group advertise-inactive)
[Tree] (config>router>bgp>group>neighbor advertise-inactive)

Full Context configure router bgp advertise-inactive
configure router bgp group advertise-inactive
configure router bgp group neighbor advertise-inactive

Description This command enables the advertising of inactive BGP routes to other BGP peers. By default, BGP only advertises BGP routes to other BGP peers if a given BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the used route within the system for a given destination.

The **no** form of this command disables the advertising of inactive BGP routers to other BGP peers.

Default no advertise-inactive

Platforms All

5.142 advertise-interval

advertise-interval

Syntax **advertise-interval** *advertise-interval*
no advertise-interval

Context **[Tree]** (config>port>aps advertise-interval)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port aps advertise-interval

Description This command specifies the time interval, in 100s of milliseconds, between 'I am operational' messages sent by both protect and working circuits to their neighbor for multi-chassis APS.

The **advertise-interval** value is valid only for a multi-chassis APS as indicated by the value of the **neighbor** command value if it is not set to 0.0.0.0.

Default 10

Parameters *advertise-interval* — Specifies the time interval, in 100s of milliseconds, between 'I am operational' messages sent by both protect and working circuits to their neighbor for multi-chassis APS.

Values 10 to 650

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

5.143 advertise-ipv6-next-hops

advertise-ipv6-next-hops

Syntax **advertise-ipv6-next-hops** [**ipv4**]
no advertise-ipv6-next-hops

Context **[Tree]** (config>service>vprn>bgp advertise-ipv6-next-hops)
[Tree] (config>service>vprn>bgp>group advertise-ipv6-next-hops)
[Tree] (config>service>vprn>bgp>group>neighbor advertise-ipv6-next-hops)

Full Context configure service vprn bgp advertise-ipv6-next-hops
configure service vprn bgp group advertise-ipv6-next-hops
configure service vprn bgp group neighbor advertise-ipv6-next-hops

Description When this command is configured, with the IPv4 option, so that it applies to a BGP session established on top of IPv6 transport, IPv4 BGP routes can be advertised with a true IPv6 address when originated or when **next-hop-self** (configured or automatic) is applied.

If an IPv4 route must originate or be advertised with a **next-hop-self** and the corresponding **advertise-ipv6-next-hops** command option does not apply to the session or if an appropriate **extended-nh-encoding** capability was not received from the remote peer, then the route is advertised with the IPv4 system address as the BGP next-hop.

If an IPv4 route is matched by a BGP export policy entry that tries to change the next hop to an IPv6 address and the corresponding **advertise-ipv6-next-hops** command option does not apply to the session or if an appropriate **extended-nh-encoding** capability was not received from the remote peer, then the route is handled as though it was rejected by the policy entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command has no effect on sessions established over IPv4 transport.

The **no** form of this command reverts to the default.

Default no advertise-ipv6-next-hops

Parameters **ipv4** — Allows IPv4 unicast routes to be advertised to IPv6-transport peers with an IPv6 address as the BGP next-hop in cases of route origination or **next-hop-self** (configured or automatic). It also allows export policies to change the BGP next-hop of an IPv4 route to an IPv6 address. All of these cases require the remote peer to advertise the necessary extended NH encoding capability. It may be necessary to configure the **forward-ipv4-packets** command under the appropriate **interface>ipv6** contexts in order to enable datapath support for these control plane exchanges.

Platforms All

advertise-ipv6-next-hops

Syntax **advertise-ipv6-next-hops** [**vpn-ipv6**] [**label-ipv6**] [**evpn**] [**vpn-ipv4**] [**label-ipv4**] [**ipv4**]
no advertise-ipv6-next-hops

Context **[Tree]** (config>router>bgp advertise-ipv6-next-hops)
[Tree] (config>router>bgp>group advertise-ipv6-next-hops)
[Tree] (config>router>bgp>group>neighbor advertise-ipv6-next-hops)

Full Context configure router bgp advertise-ipv6-next-hops
configure router bgp group advertise-ipv6-next-hops
configure router bgp group neighbor advertise-ipv6-next-hops

Description This command applies to a BGP session established on top of IPv6 transport; BGP routes belonging to the specified families can be advertised with a true IPv6 address when originated or when **next-hop-self** (configured or automatic) is applied.

This command has no effect on routes advertised to IPv4 peers.

When this command is not enabled, the following considerations apply:

- If a VPN IPv6 or label IPv6 route needs to be originated or advertised with **next-hop-self** to an IPv6 transport peer the route is advertised with the IPv4 system address as BGP next-hop (encoded as an IPv4-mapped IPv6 address).
- If a VPN-IPv4 or label IPv4 route needs to be originated or advertised with **next-hop-self** or if an appropriate **extended-nh-encoding** capability was not received from the remote peer, the route is advertised with the IPv4 system address as the BGP next-hop.
- If a VPN IPv4 or label IPv4 route is matched by a BGP export policy entry that tries to change the next-hop to an IPv6 address and an appropriate **extended-nh-encoding** capability was not received from the remote peer, the route is handled as though it was rejected by the policy entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the setting of next hops to a global IPv6 address for the family.

Default no advertise-ipv6-next-hops

Parameters **vpn-ipv6** — Allows VPN IPv6 routes to be advertised to IPv6 transport peers with an IPv6 address as the BGP next-hop in cases of route origination or **next-hop-self** (configured or automatic).

label-ipv6 — Allows label IPv6 routes to be advertised to IPv6 transport peers with an IPv6 address as the BGP next-hop in cases of route origination or **next-hop-self** (configured or automatic).

vpn-ipv4 — Allows VPN IPv4 routes to be advertised to IPv6 transport peers with an IPv6 address as the BGP next-hop in cases of route origination or **next-hop-self** (configured or automatic). It also allows export policies to change the BGP next-hop of a VPN IPv4 route to an IPv6 address. All of these cases require the remote peer to advertise the necessary extended NH encoding capability.

label-ipv4 — Allows label IPv4 routes to be advertised to IPv6 transport peers with an IPv6 address as the BGP next-hop in cases of route origination or **next-hop-self** (configured or automatic). It also allows export policies to change the BGP next-hop of a label IPv4 route to an IPv6 address. All of these cases require the remote peer to advertise the necessary extended NH encoding capability.

ipv4 — Instructs BGP to advertise an extended NH encoding capability for NLRI AFI=1, NLRI SAFI=1 and next-hop AFI=2.

evpn — Allows EVPN routes to be advertised to IPv6 transport peers.

Platforms All

5.144 advertise-label

advertise-label

Syntax **advertise-label** {**per-prefix** | **pop** | **pop-and-forward**}
no advertise-label

Context **[Tree]** (config>router>policy-options>policy-statement>default-action advertise-label)
[Tree] (config>router>policy-options>policy-statement>entry>action advertise-label)

Full Context configure router policy-options policy-statement default-action advertise-label
configure router policy-options policy-statement entry action advertise-label

Description This command configures the label allocation method for advertised routes. The effect of the **advertise-label** command depends on the context where the associated policy is applied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Use the **per-prefix** option and configure the command in the default action or entry-specific action of a VRF export policy to advertise every qualifying matched route with a per-prefix label in the resulting VPN-IP routes. In this situation, non-qualifying routes include local interface routes and BGP-VPN routes. The command overrides, for specific routes, the configured label-mode of the exporting VPRN service.

Use the per-prefix option and configure the command in the default action or entry-specific action of a BGP import policy to assign a per-prefix label to qualifying label-IPv4 and label-IPv6 routes when:

- these routes are the best path for their prefix in the respective RIB
- there is a BGP next-hop change

A label-IPv4 or label-IPv6 route advertised with a pre-prefix label supports ECMP forwarding across multiple BGP next-hops.

The **pop** option is applicable in route-table-import policies. The advertised BGP label is programmed for a pop operation when:

- a /32 IPv4 static, OSPF, or IS-IS route is matched and accepted by a label-IPv4 or label-IPv6 RIB route-table-import policy entry or default-action with this command
- the route is a candidate to be advertised as a label-IPv4 or label-IPv6 route (due to a BGP export policy)

When the label-IPv4 RIB imports a /32 static, OSPF, or IS-IS route and then exports the route as a BGP route, the default behavior is to program a swap operation in the datapath, which swaps the BGP label with the tunnel label that takes traffic to the destination of the /32 route.

The **pop-and-forward** option is applicable in route-table-import policies, when these policies match an unlabeled BGP route and apply this policy action.

Use the **pop-and-forward** option to program the label that is advertised in the BGP-LU route to forward the packet according to the resolution of the unlabeled route that triggered the origination of the BGP-LU route. The forwarding is done without an IP FIB lookup, which can be useful in situations where the IP FIB at the exit of the MPLS tunnel is not synchronized with the FIB at the head-end of the MPLS tunnel. The advertisement of a pop-and-forward label overrides the configuration to advertise label-ipv6 routes with an explicit null label and the configuration to advertise BGP-LU with a prefix SID attribute. Those features are not available when using the pop-and-forward label.

Default no advertise-label

Parameters **per-prefix** — Sets the per-prefix label allocation for matched routes. This takes effect only in VRF export policies and BGP import policies, and only for certain types of routes.

pop — Sets the pop label allocation for matched routes. This takes effect only in label-IPv4 route-table-import policies and only applies to /32 IPv4 routes that were learned through static configuration, OSPF, or IS-IS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pop-and-forward — Sets the pop-and-forward label allocation for matched routes. This takes effect only when an unlabeled BGP IPv4 or IPv6 route is matched by a label-IPv4 or label-IPv6 route-table-import policy.

Platforms All

5.145 advertise-ldp-prefix

advertise-ldp-prefix

Syntax [**no**] **advertise-ldp-prefix**

Context **[Tree]** (config>router>bgp>group>neighbor advertise-ldp-prefix)

Full Context configure router bgp group neighbor advertise-ldp-prefix

Description This command, when configured for a session that supports the IPv4 labeled-unicast address family, allows (subject to BGP export policies) active /32 LDP FEC prefixes to be advertised to the BGP peer with an RFC 3107 label, even though there may be BGP paths for the same prefix.

Default no advertise-ldp-prefix

Platforms All

5.146 advertise-local

advertise-local

Syntax [**no**] **advertise-local**

Context **[Tree]** (config>service>vpls>isid-policy>entry advertise-local)

Full Context configure service vpls isid-policy entry advertise-local

Description The **no advertise-local** option prevents the advertisement of any locally defined I-VPLS ISIDs or static-isids in the range in a B-VPLS. For I-VPLS services or static-isids that are primarily unicast traffic, the use-def-mcast and no advertise-local options allows the forwarding of ISID based multicast frames locally using the default multicast. The **no advertise-local** option also suppresses this range of ISIDs from being advertised in ISIS. When using the **use-def-mcast** and **no advertise-local** policies, the ISIDs configured under this **static-isid** declarations SPBM treats the ISIDs as belonging to the default tree.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default advertise-local

Platforms All

5.147 advertise-ne-profile

advertise-ne-profile

Syntax **advertise-ne-profile** *name*
no advertise-ne-profile

Context **[Tree]** (config>service>vprn>ospf>area advertise-ne-profile)

Full Context configure service vprn ospf area advertise-ne-profile

Description This command enables advertising of a specific NE profile using OSPFv2 LSA type 10 opaque.

The **no** version of this command disables advertising of NE profiles.

Default no advertise-ne-profile

Parameters *name* — Specifies the name of the NE profile to be advertised, up to 32 characters.

Platforms All

5.148 advertise-passive-only

advertise-passive-only

Syntax [**no**] **advertise-passive-only**

Context **[Tree]** (config>service>vprn>isis advertise-passive-only)

Full Context configure service vprn isis advertise-passive-only

Description This command enables IS-IS for the VPRN instance to advertise only prefixes that belong to passive interfaces.

The **no** form of this command disables IS-IS for the VPRN instance from advertising only prefixes that belong to passive interfaces.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

advertise-passive-only

Syntax [**no**] **advertise-passive-only**

Context **[Tree]** (config>router>isis advertise-passive-only)

Full Context configure router isis advertise-passive-only

Description This command enables and disables IS-IS to advertise only prefixes that belong to passive interfaces.

Default no advertise-passive-only

Platforms All

5.149 advertise-router-capability

advertise-router-capability

Syntax **advertise-router-capability** {**area** | **as**}
no advertise-router-capability

Context **[Tree]** (config>service>vprn>isis advertise-router-capability)
[Tree] (config>service>vprn>isis>level advertise-router-capability)

Full Context configure service vprn isis advertise-router-capability
configure service vprn isis level advertise-router-capability

Description This command enables advertisement of a router's capabilities to its neighbors for informational and troubleshooting purposes. A new TLV as defined in RFC 4971 advertises the TE Node Capability Descriptor capability.

The parameters (area & as) control the scope of the capabilities advertisements.

The **no** form of this command disables this capability.

Default no advertise-router-capability

Parameters **area** — Capabilities are only advertised within the area of origin.

as — Capabilities are only advertised throughout the entire autonomous system.

Platforms All

advertise-router-capability

Syntax **advertise-router-capability**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

advertise-router-capability {**link** | **area** | **as**}
no advertise-router-capability

Context [Tree] (config>service>vprn>ospf advertise-router-capability)
[Tree] (config>service>vprn>ospf3 advertise-router-capability)
[Tree] (config>service>vprn>ospf>area advertise-router-capability)
[Tree] (config>service>vprn>ospf>area>if advertise-router-capability)
[Tree] (config>service>vprn>ospf3>area>if advertise-router-capability)

Full Context configure service vprn ospf advertise-router-capability
configure service vprn ospf area advertise-router-capability
configure service vprn ospf area interface advertise-router-capability
configure service vprn ospf3 advertise-router-capability
configure service vprn ospf3 area interface advertise-router-capability

Description This command enables advertisement of a router's capabilities to its neighbors for informational and troubleshooting purposes. A Router Information (RI) LSA as defined in RFC 4970 advertises the following capabilities:

- OSPF graceful restart capable: no
- OSPF graceful restart helper: yes, when enabled
- OSPF Stub Router support: yes
- OSPF Traffic Engineering support: yes, when enabled
- OSPF point-to-point over LAN: yes
- OSPF Experimental TE: no

The parameters (**link**, **area** and **as**) control the advertisement scope of the router capabilities.

The **no** form of this command disables this capability.

Default no advertise-router-capability

Parameters **link** — Capabilities are only advertised over local link and not flooded beyond.

area — Capabilities are only advertised within the area of origin.

as — Capabilities are only advertised throughout the entire autonomous system.

Platforms All

advertise-router-capability

Syntax **advertise-router-capability** {**area** | **as**}
no advertise-router-capability

Context [Tree] (config>router>isis advertise-router-capability)

Full Context configure router isis advertise-router-capability

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables advertisement of a router's capabilities to its neighbors for informational and troubleshooting purposes. A TLV as defined in RFC 4971 advertises the TE Node Capability Descriptor capability.

The parameters (area and as) control the scope of the capability advertisements.

The **no** form of this command disables this capability.

Parameters **area** — Specifies to only advertise within the area of origin.

as — Specifies to advertise throughout the entire autonomous system.

Platforms All

advertise-router-capability

Syntax [**no**] **advertise-router-capability**

Context **[Tree]** (config>router>isis>level advertise-router-capability)

Full Context configure router isis level advertise-router-capability

Description This command enables router advertisement capabilities.

The **no** form of this command disables router advertisement capabilities.

Default advertise-router-capability

Platforms All

advertise-router-capability

Syntax **advertise-router-capability** {**link** | **area** | **as**}
no advertise-router-capability

Context **[Tree]** (config>router>ospf advertise-router-capability)
[Tree] (config>router>ospf3 advertise-router-capability)

Full Context configure router ospf advertise-router-capability
configure router ospf3 advertise-router-capability

Description This command enables advertisement of a router's capabilities to its neighbors for informational and troubleshooting purposes. A Router Information (RI) LSA as defined in RFC 4970 advertises the following capabilities:

- OSPF graceful restart capable: no
- OSPF graceful restart helper: yes, when enabled
- OSPF stub router support: yes
- OSPF traffic engineering support: yes, when enabled

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- OSPF point-to-point over LAN: yes
- OSPF experimental TE: no

The parameters (**link**, **area** and **as**) control the scope of the capability advertisements.

The **no** form of this command disables this capability.

Default no advertise-router-capability

Parameters **link** — capabilities are only advertised over local links and not flooded beyond.

area — capabilities are only advertised within the area of origin.

as — capabilities are advertised throughout the entire autonomous system.

Platforms All

advertise-router-capability

Syntax [**no**] **advertise-router-capability**

Context **[Tree]** (config>router>ospf>area advertise-router-capability)
[Tree] (config>router>ospf>area>interface advertise-router-capability)
[Tree] (config>router>ospf3>area advertise-router-capability)
[Tree] (config>router>ospf3>area>interface advertise-router-capability)

Full Context configure router ospf area advertise-router-capability
configure router ospf area interface advertise-router-capability
configure router ospf3 area advertise-router-capability
configure router ospf3 area interface advertise-router-capability

Description This command enables advertisement of a router's capabilities to its neighbors for informational and troubleshooting purposes. A Router Information (RI) LSA as defined in RFC 4970 advertises the following capabilities:

- OSPF graceful restart capable: no
- OSPF graceful restart helper: yes, when enabled
- OSPF stub router support: yes
- OSPF traffic engineering support: yes, when enabled
- OSPF point-to-point over LAN: yes
- OSPF experimental TE: no

The **no** form of this command disables this capability.

Default advertise-router-capability

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.150 advertise-selection

advertise-selection

Syntax **advertise-selection**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay advertise-selection)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay advertise-selection)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay advertise-selection)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection

Description Commands in this context configure a solicit delay or a DHCPv6 preference option value to influence the advertise selection of DHCPv6 clients.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.151 advertise-stale-to-all-neighbors

advertise-stale-to-all-neighbors

Syntax **advertise-stale-to-all-neighbors** [**without-no-export**]
no advertise-stale-to-all-neighbors

Context **[Tree]** (config>service>vprn>bgp>graceful-restart>long-lived advertise-stale-to-all-neighbors)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived advertise-stale-to-all-neighbors)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived advertise-stale-to-all-neighbors)

Full Context configure service vprn bgp graceful-restart long-lived advertise-stale-to-all-neighbors
configure service vprn bgp group graceful-restart long-lived advertise-stale-to-all-neighbors
configure service vprn bgp group neighbor graceful-restart long-lived advertise-stale-to-all-neighbors

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows BGP routes marked as LLGR stale to be advertised to BGP peers that did not advertise the LLGR capability when the session was opened. The **no** version of this command causes advertisement behavior to follow the rule that stale routes cannot be advertised to a peer that does not understand or implement the LLGR capability. Stale routes are withdrawn towards such peers.

When this command is configured with the **without-no-export** option, LLGR stales routes can be advertised to any peer (EBGP or IBGP) that did not signal the LLGR capability. Towards IBGP and confederation-EBGP peers that did not advertise the LLGR capability, the LOCAL_PREFERENCE attribute in the advertised stale routes is automatically set to zero.

When this command is configured without the **without-no-export** option, LLGR stale routes are not advertised to any EBGP peer that did not signal the LLGR capability. Towards IBGP and confederation-EBGP peers that did not advertise the LLGR capability the LOCAL_PREFERENCE attribute in the advertised stale routes is automatically set to zero and a NO_EXPORT standard community is automatically added to the routes.

Default no advertise-stale-to-all-neighbors

Parameters **without-no-export** — Allows LLGR stale routes to be advertised to all peers, such that they can exit the local AS.

Platforms All

advertise-stale-to-all-neighbors

Syntax **advertise-stale-to-all-neighbors** [**without-no-export** | **no without-no-export**]
no advertise-stale-to-all-neighbors

Context **[Tree]** (config>router>bgp>graceful-restart>long-lived advertise-stale-to-all-neighbors)
[Tree] (config>router>bgp>group>graceful-restart>long-lived advertise-stale-to-all-neighbors)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived advertise-stale-to-all-neighbors)

Full Context configure router bgp graceful-restart long-lived advertise-stale-to-all-neighbors
configure router bgp group graceful-restart long-lived advertise-stale-to-all-neighbors
configure router bgp group neighbor graceful-restart long-lived advertise-stale-to-all-neighbors

Description This command allows BGP routes marked as LLGR stale to be advertised to BGP peers that did not advertise the LLGR capability when the session was opened.

When this command is configured with the **without-no-export** option, LLGR stale routes can be advertised to any peer (EBGP or IBGP) that did not signal the LLGR capability. Towards IBGP and confederation-EBGP peers that did not advertise the LLGR capability, the LOCAL_PREFERENCE attribute in the advertised stale routes is automatically set to zero.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this command is configured without the **without-no-export** option, LLGR stale routes are not advertised to any EBGP peer that did not signal the LLGR capability. Towards IBGP and confederation-EBGP peers that did not advertise the LLGR capability the LOCAL_PREFERENCE attribute in the advertised stale routes is automatically set to zero and a NO_EXPORT standard community is automatically added to the routes.

The **no** version of this command causes advertisement behavior to follow the rule that stale routes cannot be advertised to a peer that does not understand or implement the LLGR capability. Stale routes are withdrawn towards such peers.

Default no advertise-stale-to-all-neighbors

Parameters **without-no-export** — Allows LLGR stale routes to be advertised to all peers, such that they can exit the local AS.

Platforms All

5.152 advertise-subnet

advertise-subnet

Syntax [**no**] **advertise-subnet**

Context **[Tree]** (config>service>vprn>ospf>area>if advertise-subnet)

Full Context configure service vprn ospf area interface advertise-subnet

Description This command enables advertising point-to-point interfaces as subnet routes (network number and mask). When disabled, point-to-point interfaces are advertised as host routes.

This command is not supported in the OSPF3 context.

The **no** form of this command disables advertising point-to-point interfaces as subnet routes meaning they are advertised as host routes.

Default advertise-subnet — Advertises point-to-point interfaces as subnet routes.

Platforms All

advertise-subnet

Syntax [**no**] **advertise-subnet**

Context **[Tree]** (config>router>ospf>area>interface advertise-subnet)

Full Context configure router ospf area interface advertise-subnet

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables advertising point-to-point interfaces as subnet routes (network number and mask). When disabled, point-to-point interfaces are advertised as host routes.

The **no** form of this command disables advertising point-to-point interfaces as subnet routes meaning they are advertised as host routes.

Default advertise-subnet

Platforms All

5.153 advertise-tunnel-link

advertise-tunnel-link

Syntax [**no**] **advertise-tunnel-link**

Context **[Tree]** (config>router>isis advertise-tunnel-link)
[Tree] (config>router>ospf advertise-tunnel-link)

Full Context configure router isis advertise-tunnel-link
configure router ospf advertise-tunnel-link

Description This command enables the forwarding adjacency feature. With this feature, IS-IS or OSPF advertises an RSVP LSP as a link so that other routers in the network can include it in their SPF computations. The RSVP LSP is advertised as an unnumbered point-to-point link and the link LSP or LSA has no Traffic Engineering opaque sub-TLVs, as per RFC 3906. An SR-TE LSP is not supported with forwarding adjacency.

The forwarding adjacency feature can be enabled independently from the IGP shortcut feature in CLI. If both **igp-shortcut** and **advertise-tunnel-link** options are enabled for a given IGP instance, then the **advertise-tunnel-link** takes precedence.

When the forwarding adjacency feature is enabled, each node advertises a p2p unnumbered link for each best metric tunnel to the router ID of any endpoint node. The node does not include the tunnels as IGP shortcuts in SPF computation directly. Instead, when the LSA or LSP that advertises the corresponding P2P unnumbered link is installed in the local routing database, the node performs an SPF using it like any other link LSA or LSP. The bidirectional check of the link requires that a link, regular or tunnel, exists in the reverse direction for the tunnel to be used in SPF.

The **igp-shortcut** option under the LSP name governs the use of the LSP with both the **igp-shortcut** and the **advertise-tunnel-link** options in IGP. In other words, the user can exclude a specific RSVP LSP from being used as a forwarding adjacency by entering the command **config>router>mpls>lsp>no igp-shortcut**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Support is provided for resolving and forwarding IPv4 and IPv6 prefixes over IPv4 forwarding adjacency RSVP-TE LSP. Specifically, the forwarding adjacency feature supports family IPv4 in OSPFv2, family IPv6 in OSPFv3, families IPv4 and IPv6 in ISIS MT=0, and family IPv6 in ISIS MT=2.

In addition, both IPv4 and IPv6 SR-ISIS tunnels can be resolved and further tunneled over one or more RSVP-TE LSPs used as forwarding adjacencies. This is enabled by configuring both segment routing and forwarding adjacency features within an IS-IS instance in a multi-topology MT=0.

IS-IS forwarding adjacency using the **advertise-tunnel-link** command is not supported in combination with the IS-IS link bundling and the IS-IS metric link quality adjustment features.

The **no** form of this command disables forwarding adjacency and disables the advertisement of RSVP LSP into IGP.

Default no advertise-tunnel-link

Platforms All

5.154 advertised-stale-time

advertised-stale-time

Syntax **advertised-stale-time** *seconds*
no advertised-stale-time

Context **[Tree]** (config>service>vprn>bgp>graceful-restart>long-lived advertised-stale-time)
[Tree] (config>service>vprn>bgp>graceful-restart>long-lived>family advertised-stale-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived advertised-stale-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived>family advertised-stale-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived advertised-stale-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived>family advertised-stale-time)

Full Context configure service vprn bgp graceful-restart long-lived advertised-stale-time
configure service vprn bgp graceful-restart long-lived family advertised-stale-time
configure service vprn bgp group graceful-restart long-lived advertised-stale-time
configure service vprn bgp group graceful-restart long-lived family advertised-stale-time
configure service vprn bgp group neighbor graceful-restart long-lived advertised-stale-time
configure service vprn bgp group neighbor graceful-restart long-lived family advertised-stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the value of the long-lived stale time that is advertised by the router in its LLGR capability. When configured in the long-lived configuration context, **advertised-stale-time** applies to all AFI/SAFI in the advertised LLGR capability except for any AFI/SAFI with a family-specific override. A family-specific override is configured with the **advertised-stale-time** command in a family context.

The **no** version of this command sets the **advertised-stale-time** value to 24 hours (86400 seconds).

Default no advertised-stale-time

Parameters *seconds* — Specifies the advertised long-lived stale time in seconds.

Values 0 to 16777215

Platforms All

advertised-stale-time

Syntax **advertised-stale-time** *seconds*
no advertised-stale-time

Context **[Tree]** (config>router>bgp>graceful-restart>long-lived advertised-stale-time)
[Tree] (config>router>bgp>graceful-restart>long-lived>family advertised-stale-time)
[Tree] (config>router>bgp>group>graceful-restart>long-lived advertised-stale-time)
[Tree] (config>router>bgp>group>graceful-restart>long-lived>family advertised-stale-time)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived advertised-stale-time)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived>family advertised-stale-time)

Full Context configure router bgp graceful-restart long-lived advertised-stale-time
configure router bgp graceful-restart long-lived family advertised-stale-time
configure router bgp group graceful-restart long-lived advertised-stale-time
configure router bgp group graceful-restart long-lived family advertised-stale-time
configure router bgp group neighbor graceful-restart long-lived advertised-stale-time
configure router bgp group neighbor graceful-restart long-lived family advertised-stale-time

Description This command sets the value of the long-lived stale time that is advertised by the router in its LLGR capability. When configured in the long-lived configuration context, **advertised-stale-time** applies to all AFI/SAFI in the advertised LLGR capability except for any AFI/SAFI with a family-specific override. A family-specific override is configured with the **advertised-stale-time** command in a **family** context.

The **no** version of this command sets the **advertised-stale-time** value to 24 hours (86400 seconds).

Default no advertised-stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the advertised long-lived stale time in seconds.

Values 0 to 16777215

Platforms All

5.155 advertising-timeout

advertising-timeout

Syntax **advertising-timeout** *seconds*
no advertising-timeout

Context **[Tree]** (config>system>bluetooth advertising-timeout)

Full Context configure system bluetooth advertising-timeout

Description When the power is enabled, this timer controls the amount of time the Bluetooth device will advertise that is ready to pair. If an external device does not complete the pairing within this time, then the pairing must be re-initiated.

The **no** form of this command disables the timeout.

Default advertising-timeout 30

Parameters *seconds* — Specifies the paring timeout interval.

Values 30 to 3600

Platforms 7750 SR-1, 7750 SR-s

5.156 age-time

age-time

Syntax **age-time** *seconds*
no age-time

Context **[Tree]** (config>service>vpls>proxy-arp age-time)
[Tree] (config>service>vpls>proxy-nd age-time)

Full Context configure service vpls proxy-arp age-time
configure service vpls proxy-nd age-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the aging timer per proxy-ARP/proxy-ND entry for dynamic entries. When the aging expires, the entry is flushed. The age is reset when a new ARP/GARP/NA for the same MAC-IP is received. If the corresponding FDB MAC entry is flushed, the proxy-ARP/proxy-ND entry goes inactive and subsequent ARP/NS lookups are treated as "missed". EVPN will withdraw the IP→MAC if the entry goes inactive. The **age-time** should be set at *send-refresh * 3* to ensure that no active entries are unnecessarily removed.

Default no age-time

Parameters *seconds* — Specifies the age-time in seconds.

Values 60 to 86400

Platforms All

5.157 agg-rate

agg-rate

Syntax **agg-rate** *rate*
no agg-rate

Context **[Tree]** (config>port>sonet-sdh>path>access>egress>vport agg-rate)

Full Context configure port sonet-sdh path access egress vport agg-rate

Description This command configures an aggregate rate for the Vport. The **agg-rate** *rate*, **port-scheduler-policy** and **scheduler-policy** commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an agg-rate/port-scheduler-policy involves removing the existing command and applying the new command. Applying a **scheduler-policy** to a Vport is only applicable to Ethernet interfaces.

The **no** form of this command reverts to the default.

Parameters *rate* — Specifies the rate limit for the Vport.

Values 1 to 800000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

agg-rate

Syntax [**no**] **agg-rate**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress agg-rate)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress agg-rate)
[Tree] (config>service>ies>if>sap>egress agg-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface sap egress agg-rate
configure service ies subscriber-interface group-interface sap egress agg-rate
configure service vprn subscriber-interface group-interface sap egress agg-rate

Description Commands in this context configure aggregation rate parameters. This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, **and queue-frame-based-accounting**.

When specified under a Vport, the **agg-rate**, **port-scheduler-policy** and **scheduler-policy** commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an **agg-rate** or **port-scheduler-policy** involves removing the existing command and applying the new command.

The **no** form of this command disables the aggregation rate.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap egress agg-rate
- configure service ies subscriber-interface group-interface sap egress agg-rate

All

- configure service ies interface sap egress agg-rate

agg-rate

Syntax [**no**] **agg-rate**

Context **[Tree]** (config>port>ethernet>access>egr>qgrp agg-rate)
[Tree] (config>port>ethernet>access>egr>vport agg-rate)
[Tree] (config>port>ethernet>network>egr>qgrp agg-rate)

Full Context configure port ethernet access egress queue-group agg-rate
configure port ethernet access egress vport agg-rate
configure port ethernet network egress queue-group agg-rate

Description This command controls an H-QoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, **and queue-frame-based-accounting**.

When specified under a Vport, the agg-rate rate, port-scheduler-policy and scheduler-policy commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an agg-rate/port-scheduler-policy involves removing the existing command and applying the new command.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

agg-rate

Syntax [**no**] **agg-rate**

Context **[Tree]** (config>service>apipe>sap>egress agg-rate)
[Tree] (config>service>cpipe>sap>egress agg-rate)
[Tree] (config>service>epipe>sap>egress agg-rate)
[Tree] (config>service>fpipe>sap>egress agg-rate)
[Tree] (config>service>ipipe>sap>egress agg-rate)

Full Context configure service apipe sap egress agg-rate
configure service cpipe sap egress agg-rate
configure service epipe sap egress agg-rate
configure service fpipe sap egress agg-rate
configure service ipipe sap egress agg-rate

Description This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, and **queue-frame-based-accounting**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress agg-rate
- configure service fpipe sap egress agg-rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress agg-rate

All

- configure service epipe sap egress agg-rate
- configure service ipipe sap egress agg-rate

agg-rate

Syntax [**no**] **agg-rate**

Context **[Tree]** (config>service>vpls>sap>egress agg-rate)
[Tree] (config>service>template>vpls-sap-template>egress agg-rate)
[Tree] (config>service>vpls>sap>egress>encap-defined-qos>encap-group agg-rate)

Full Context configure service template vpls-sap-template egress agg-rate
configure service vpls sap egress agg-rate
configure service vpls sap egress encap-defined-qos encap-group agg-rate

Description This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, **and queue-frame-based-accounting**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

agg-rate

Syntax [**no**] **agg-rate**

Context **[Tree]** (config>service>vprn>if>sap>egress agg-rate)

Full Context configure service vprn interface sap egress agg-rate

Description This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, **and queue-frame-based-accounting**.

Platforms All

agg-rate

Syntax [**no**] **agg-rate**

Context **[Tree]** (config>service>cust>multi-service-site>egress agg-rate)

Full Context configure service customer multi-service-site egress agg-rate

Description Commands in this context control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, **and queue-frame-based-accounting**.

The **no** form of the command disables the aggregate rate limit parameters.

Platforms All

5.158 agg-rate-limit

agg-rate-limit

Syntax **agg-rate-limit** *agg-rate* [**min-resv-bw** *min-rate*] [**queue-frame-based-accounting**]
no agg-rate-limit

Context **[Tree]** (config>subscr-mgmt>sub-prof>egress agg-rate-limit)

Full Context configure subscriber-mgmt sub-profile egress agg-rate-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines a subscriber aggregate limit when the subscriber profile is directly associated with an egress port based scheduler instead of a scheduler policy. The optional queue-frame-based-accounting keyword allows the subscriber queues to operate in the frame based accounting mode.

Once egress frame based accounting is enabled on the subscriber profile, all queues associated with the subscriber (created through the sla-profile associated with each subscriber host) will have their rate and CIR values interpreted as frame based values. When shaping, the queues will include the 12-byte Inter-Frame Gap (IFG) and 8-byte preamble for each packet scheduled out the queue. The profiling CIR threshold will also include the 20-byte frame encapsulation overhead. Statistics associated with the queue do not include the frame encapsulation overhead. Packet byte offset settings are not included in the applied rate when queue frame based accounting is configured, however the offsets are applied to the statistics.

The **queue-frame-based-accounting** keyword does not change the behavior of the egress-agg-rate-limit rate value. Since the egress-agg-rate-limit is always associated with egress port based scheduling and egress port based scheduling is dependent on frame based operation, the egress-agg-rate-limit rate is always interpreted as a frame based value.

Enabling queue-frame-based-accounting will not cause statistics for queues associated with the subscriber to be cleared.

The **no** form of this command removes both an egress aggregate rate limit and egress frame based accounting for all subscribers associated with the sub-profile. If a subscriber's accounting mode is changed, the subscriber's queue statistics are cleared.

Parameters *agg-rate* — Specifies the egress aggregate rate.

Values 1 to 800000000, **max**

min-rate — Specifies the minimum rate of the minimum reserved bandwidth for unicast data traffic. Since minimum rate can oversubscribe subscriber bandwidth to guarantee a minimum bandwidth for unicast traffic, care must be taken in QoS provisioning to prioritize packets accordingly (downstream network elements such as the access node or aggregation nodes) when congestion occurs.

Values 0 to 800000000

queue-frame-based-accounting — Specifies whether to use frame-based accounting when evaluating the aggregation rate limit for the egress queues for this SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

agg-rate-limit

Syntax **agg-rate-limit** *agg-rate*
no agg-rate-limit

Context **[Tree]** (config>port>ethernet>access>egress>vport agg-rate-limit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet access egress vport agg-rate-limit

Description This command configures an aggregate rate for the Vport. This command is mutually exclusive with the **port-scheduler-policy** command.

The **no** form of this command reverts to the default.

Parameters *agg-rate* — Specifies the rate limit for the Vport.

Values max, 1 to 10000000

agg-rate-limit

Syntax **agg-rate-limit** *kilobits-per-second*
no agg-rate-limit

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>egress agg-rate-limit)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>egress agg-rate-limit)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress agg-rate-limit
configure service vprn subscriber-interface group-interface wlan-gw egress agg-rate-limit

Description This command configures an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, **and queue-frame-based-accounting**.

The **no** form of this command removes the rate from the configuration.

Parameters *kilobits-per-second* — Specifies the aggregate rate limit.

Values 1 to 100000000, **max**

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

agg-rate-limit

Syntax **agg-rate-limit** *agg-rate* **[min-resv-bw** *min-rate***] [queue-frame-based-accounting] [adaptation-rule** *adaptation-rule***] [burst-limit** *size***] [bytes| kilobytes]**
no agg-rate-limit

Context **[Tree]** (config>subscr-mgmt>sub-prof>egr agg-rate-limit)

Full Context configure subscriber-mgmt sub-profile egress agg-rate-limit

Description This command configures a hardware-assisted HQoS aggregate rate limit.

The **no** form of this command removes the rate from the configuration.

Parameters *agg-rate* — Specifies the aggregate rate limit in kb/s.

Values 1 to 800000000, **max**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

min-rate — Specifies the minimum reserved bandwidth rate.

Values 0 to 800000000, **max**

queue-frame-based-accounting — Enables frame-based accounting at the queue level.

adaptation-rule — Specifies the adaptation rule for the PIR value of the subscriber aggregate rate. This rule determines which configured value is adapted to **oper-agg-rate** based on hardware capabilities.

Values **max, min, closest**

Default closest

size — Specifies the burst limit size.

Values 1 to 14000000, default

bytes | kilobytes — Specifies whether the value is in bytes or kilobytes.

Default bytes

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.159 agg-shaper-weight

agg-shaper-weight

Syntax **agg-shaper-weight** *weight*
no agg-shaper-weight

Context **[Tree]** (config>qos>sap-egress>queue agg-shaper-weight)

Full Context configure qos sap-egress queue agg-shaper-weight

Description This command specifies the aggregate shaper weight of the sap-egress queue.

The **no** form of this command returns the aggregate shaper weight to the default value.

Default agg-shaper-weight 1

Parameters *weight* — Specifies the aggregate shaper weight.

Values 1 to 100

Platforms 7750 SR-1, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.160 aggregate

aggregate

Syntax [**no] aggregate**

Context **[Tree]** (config>port>ethernet>egress>hs-sec-shaper aggregate)

Full Context configure port ethernet egress hs-secondary-shaper aggregate

Description Commands in this context configure aggregate parameters.

The **no** form of this command removes all of the aggregate parameter values from the configuration of this HS secondary shaper.

Platforms 7750 SR-7/12/12e

aggregate

Syntax **aggregate** *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number:ip-address*] [**discard-component-communities**] [**black-hole** [**generate-icmp**]] [**community** *comm-id* [*comm-id*] [**local-preference** *local-pref*]] [**description** *description*] [**tunnel-group** *tunnel-group-id*]

aggregate *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number:ip-address*] [**discard-component-communities**] [**community** *comm-id* [*comm-id*]] [**indirect** *ip-address*] [**local-preference** *local-pref*]] [**description** *description*] [**tunnel-group** *tunnel-group-id*]

no aggregate *ip-prefix/ip-prefix-length*

Context **[Tree]** (config>service>vprn aggregate)

Full Context configure service vprn aggregate

Description This command creates an aggregate route. Use this command to automatically install an aggregate route in the routing table when there are one or more component routes. A component route is any route used for forwarding that is a more specific match of the aggregate.

The use of aggregate routes can reduce the number of routes that need to be advertised to neighbor routers, leading to smaller routing table sizes.

Overlapping aggregate routes may be configured; in this case a route becomes a component of only the one aggregate route with the longest prefix match. For example if one aggregate is configured as 10.0.0.0/16 and another as 10.0.0.0/24, then route 10.0.128/17 would be aggregated into 10.0.0.0/16, and route 10.0.0.128/25 would be aggregated into 10.0.0.0/24. If multiple entries are made with the same prefix and the same mask the previous entry is overwritten.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A list of up to 12 BGP communities (any mix of standard, extended, and large communities) may be associated with an aggregate route. These communities can be matched in route policies and are automatically added to BGP routes that are created from the aggregate route.

By default, aggregate routes are not installed in the forwarding table, however there are configuration options that allow an aggregate route to be installed with a black-hole next hop or with an indirect IP address as next hop.

Aggregate routes can be advertised via MP-BGP to other PEs within the network. Aggregate routes advertised using MP-BGP do not include aggregated BGP path attributes from the component routes which were used to activate the aggregate route. The aggregate route will be advertised with the minimal set of path attributes as if the aggregate was originated by the advertising routes. Export route policies should be used to control and modify the advertisement and path attributes of the aggregate routes.

The **no** form of this command removes the aggregate.

Default no aggregate

Parameters *ip-prefix* — The destination address of the aggregate route in dotted decimal notation.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-length	0 to 128

the ipv6-prefix and ipv6-prefix-length apply only to the 7750 SR and 7950 XRS

the mask associated with the network address expressed as a mask length

Values: 0 to 32

summary-only — This optional parameter suppresses advertisement of more specific component routes for the aggregate.

To remove the **summary-only** option, enter the same aggregate command without the **summary-only** parameter.

as-set — This optional parameter is only applicable to BGP and creates an aggregate where the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Use this feature carefully as it can increase the amount of route churn due to best path changes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

aggregator *as-number*:*ip-address* — This optional parameter specifies the BGP aggregator path attribute to the aggregate route. When configuring the aggregator, a two-octet AS number used to form the aggregate route must be entered, followed by the IP address of the BGP system that created the aggregate route.

discard-component-communities — This optional keyword causes the aggregate to be advertised with only the configured BGP community set, none of the communities from the component routes activating the aggregate are included. (Component attributes are never included in aggregate routes advertised to other PE routers via MP-BGP).

black-hole — This optional parameter installs the aggregate route, when activated, in the FIB with a black-hole next-hop, where packets matching this route are discarded.

generate-icmp — This optional parameter keyword generates an ICMP.

community — This configuration option associates a BGP community with the aggregate route. The community can be matched in route policies and is automatically added to BGP routes exported from the aggregate route.

comm-id — Specifies a BGP community value, up to 72 characters.

Values [*as-num:comm-val* | *well-known-comm* | *ext-comm* | *large-comm*]

where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **null** | **no-export** | **no-export-subconfed** | **no-advertise** | **llgr-stale** | **no-llgr** | **blackhole**
- *ext-comm* — the extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - color:co-bits:*color-value*

  where:
  - *target* — route target
  - *origin* — route origin
  - *ip-address* — a.b.c.d
  - *ext-comm-val* — 0 to 4294967295
  - *ext-asnum* — 0 to 4294967295
  - *val-in-mbps* — 0 to 16777215
  - *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
  - *value1* — 0000 to FFFF

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *value2* — 0 to FFFFFFFFFFFF
- *co-bits* — 00, 01, 10 or 11
- *color-value* — 0 to 4294967295

• *large-comm — asn-or-ex:val-or-ex:val-or-ex*

description — Specifies a text description stored in the configuration file for a configuration context.

local-preference — Specifies a BGP local-preference value with the aggregate route. The local-preference overrides the default local preference value of a BGP route originated by exporting the aggregate route.

Values 0 to 4294967295

indirect *ip-address* — This configuration option specifies that the aggregate route should be installed in the FIB with a next-hop taken from the route used to forward packets to ip-address.

Values

ipv4-prefix	a.b.c.d
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

The ipv6-prefix applies only to the 7750 SR and 7950 XRS.

tunnel-group-id — Specifies that the MC-IPsec state of the specific tunnel-group is added to the aggregate route.

Values 1 to 16

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

aggregate

Syntax **aggregate** *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number:ip-address*] [**discard-component-communities**] [**black-hole** [**generate-icmp**]] [**community** *comm-id* [*comm-id*]] [**description** *description*] [**local-preference** *local-pref*erence] [**policy** *policy-name*]

aggregate *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number:ip-address*] [**discard-component-communities**] [**community** *comm-id* [*comm-id*]] [**indirect** *ip-address*] [**description** *description*] [**local-preference** *local-preference*] [**policy** *policy-name*]

no aggregate *ip-prefix/ip-prefix-length*

Context **[Tree]** (config>router aggregate)

Full Context configure router aggregate

Description This command creates an aggregate route.

Use this command to automatically install an aggregate route in the routing table when there are one or more component routes. A component route is any route used for forwarding that is a more-specific match of the aggregate.

The use of aggregate routes can reduce the number of routes that need to be advertised to neighbor routers, leading to smaller routing table sizes.

Overlapping aggregate routes may be configured; in this case a route becomes a component of only the one aggregate route with the longest prefix match. For example if one aggregate is configured as 10.0.0.0/16 and another as 10.0.0.0/24, then route 10.0.128/17 would be aggregated into 10.0.0.0/16, and route 10.0.0.128/25 would be aggregated into 10.0.0.0/24. If multiple entries are made with the same prefix and the same mask the previous entry is overwritten.

A standard 4-byte BGP community may be associated with an aggregate route in order to facilitate route policy matching.

By default aggregate routes are not installed in the forwarding table, however there are configuration options that allow an aggregate route to be installed with a black-hole next hop or with an indirect IP address as next hop.

The **no** form of this command removes the aggregate.

Default no aggregate

Parameters *ip-prefix* — Specifies the destination address of the aggregate route in dotted decimal notation.

Values The following values apply to the 7750 SR and 7950 XRS:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-prefix	a.b.c.d (host bits must be 0)	
ipv4-prefix-length	0 to 32	
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D
ipv6-prefix-length	0 to 128	

Values The following values apply to the 7450 ESS:

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32

ip-prefix-length — Specifies the mask associated with the network address expressed as a mask length.

Values 0 to 32

summary-only — Suppresses advertisement of more specific component routes for the aggregate.

To remove the **summary-only** option, enter the same aggregate command without the **summary-only** parameter.

as-set — This optional parameter is only applicable to BGP and creates an aggregate where the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Use this feature carefully as it can increase the amount of route churn due to best path changes.

as-number:ip-address — Specifies the BGP aggregator path attribute to the aggregate route. When configuring the aggregator, a two-octet AS number used to form the aggregate route must be entered, followed by the IP address of the BGP system that created the aggregate route.

discard-component-communities — Causes the aggregate to be advertised with only the configured BGP community set, none of the communities from the component routes activating the aggregate are included.

black-hole — Installs the aggregate route, when activated, in the FIB with a black-hole next-hop, where packets matching this route are discarded.

generate-icmp — Mandatory keyword to generate an ICMP.

community — Associates a BGP community with the aggregate route. The community can be matched in route policies and is automatically added to BGP routes exported from the aggregate route.

comm-id — Specifies a BGP community value, up to 72 characters. A maximum of twelve community IDs can be specified in a single statement.

Values [*as-num:comm-val* | *well-known-comm* | *ext-comm* | *large-comm*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **null** | **no-export** | **no-export-subconfed** | **no-advertise** | **llgr-stale** | **no-llgr** | **blackhole**
- *ext-comm* — the extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - color:co-bits:*color-value*

  where:
  - *target* — route target
  - *origin* — route origin
  - *ip-address* — a.b.c.d
  - *ext-comm-val* — 0 to 4294967295
  - *ext-asnum* — 0 to 4294967295
  - *val-in-mbps* — 0 to 16777215
  - *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
  - *value1* — 0000 to FFFF
  - *value2* — 0 to FFFFFFFFFFFF
  - *co-bits* — 00, 01, 10 or 11
  - *color-value* — 0 to 4294967295
- *large-comm* — *asn-or-ex:val-or-ex:val-or-ex*

indirect *ip-address* — Specifies that the aggregate route should be installed in the FIB with a next-hop taken from the route used to forward packets to ip-address.

Values The following values apply to the 7750 SR and 7950 XRS:

ipv4-prefix	a.b.c.d
ipv6-prefix	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Values The following values apply to the 7450 ESS:

ipv4-prefix: a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

description — Specifies a text description stored in the configuration file for a configuration context, up to 80 characters.

local-preference — Specifies a BGP local-preference value with the aggregate route. The local-preference overrides the default local preference value of a BGP route originated by exporting the aggregate route.

Values 0 to 4294967295

policy-name — Specifies the route policy, up to 64 characters.

Platforms All

5.161 aggregate-contributor

aggregate-contributor

Syntax [**no**] **aggregate-contributor**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from>aggregate-contributor aggregate-contributor)

Full Context configure router policy-options policy-statement entry from aggregate-contributor aggregate-contributor

Description This command matches all routes (BGP and non-BGP) that contributed to an active aggregate route. If the prefix tree above a particular route includes no active aggregate routes, or the most specific active aggregate route in the prefix tree above this route has a policy that rejects the route, then it is not considered as an aggregate-contributor.

This match condition is only supported when used in a BGP export policy. If it is used in an entry of a BGP import policy, VRF export policy or VRF import policy, no routes are matched by that entry.

The **no** form of this command disables matching of routes (BGP and non-BGP) that contributed to an active aggregate route.

5.162 aggregate-prefix-match

aggregate-prefix-match

Syntax [**no**] **aggregate-prefix-match**

Context **[Tree]** (config>router>ldp aggregate-prefix-match)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ldp aggregate-prefix-match

Description The command enables the use by LDP of the aggregate prefix match procedures.

When this option is enabled, LDP performs the following procedures for all prefixes. When an LSR receives a FEC-label binding from an LDP neighbor for a given specific FEC1 element, it will install the binding in the LDP FIB if:

- It is able to perform a successful longest IP match of the FEC prefix with an entry in the routing table, and
- The advertising LDP neighbor is the next-hop to reach the FEC prefix.

When such a FEC-label binding has been installed in the LDP FIB, then LDP programs an NHLFE entry in the egress data path to forward packets to FEC1. It also advertises a new FEC-label binding for FEC1 to all its LDP neighbors.

When a new prefix appears in the routing table, LDP inspects the LDP FIB to determine if this prefix is a better match (a more specific match) for any of the installed FEC elements. For any FEC for which this is true, LDP may have to update the NHLFE entry for this FEC.

When a prefix is removed from the routing table, LDP inspects the LDP FIB for all FEC elements which matched this prefix to determine if another match exists in the routing table. If so, it updates the NHLFE entry accordingly. If not, it sends a label withdraw message to its LDP neighbors to remove the binding.

When the next hop for a routing prefix changes, LDP updates the LDP FIB entry for the FEC elements which matched this prefix. It also updates the NHLFE entry for these FEC elements accordingly.

The **no** form of this command disables the use by LDP of the aggregate prefix procedures and deletes the configuration. LDP resumes performing exact prefix match for FEC elements.

Default no aggregate-prefix-match

Platforms All

5.163 aggregate-sample-window

aggregate-sample-window

Syntax **aggregate-sample-window**

Context **[Tree]** (config>test-oam>link-meas>template aggregate-sample-window)

Full Context configure test-oam link-measurement measurement-template aggregate-sample-window

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the aggregate sample window parameters to be used when the measurement template is assigned to an IP interface. The aggregate sample window is the collection of sample windows.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.164 aggregate-shapers

aggregate-shapers

Syntax **aggregate-shapers**

Context **[Tree]** (config>qos>fp-resource-policy aggregate-shapers)

Full Context configure qos fp-resource-policy aggregate-shapers

Description This command enters the aggregate-shapers context.

Platforms 7750 SR-1, 7750 SR-s

5.165 aggregate-stats

aggregate-stats

Syntax **aggregate-stats export-using** *export-method* [*export-method*...(up to 2 max)]
aggregate-stats no-export

Context **[Tree]** (config>app-assure>group>statistics>aa-sub aggregate-stats)

Full Context configure application-assurance group statistics aa-sub aggregate-stats

Description This command configures aa-sub accounting statistics for export of aggregate statistics of a given subscriber.

Default aggregate-stats no-export

Parameters *export-method* — Specifies the method of statistics export to be used.

Values accounting-policy (this is the only option for sub-aggregate statistics, and it is only supported in residential and VPN sub-scale modes).

no-export — Disables the export.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.166 aggregate-used-paths

aggregate-used-paths

Syntax **aggregate-used-paths** *family* [*family*]
no aggregate-used-paths

Context **[Tree]** (config>service>vprn>bgp>group>link-bandwidth aggregate-used-paths)
[Tree] (config>service>vprn>bgp>group>neighbor>link-bandwidth aggregate-used-paths)

Full Context configure service vprn bgp group link-bandwidth aggregate-used-paths
configure service vprn bgp group neighbor link-bandwidth aggregate-used-paths

Description This command configures BGP to aggregate the bandwidth values from the link-bandwidth extended communities of the used multipaths towards an IP prefix when it is re-advertising a route with next-hop-self towards peers within the scope of the command, as long as the route belongs to one of the listed address families.

Aggregation is not supported unless all of the used multipaths (up to the configured ECMP limit) correspond to received BGP routes with a link-bandwidth extended community. If add-path is also enabled toward the peer, then all of the add-paths advertised to the peer encode the aggregated bandwidth in a link-bandwidth extended community.

Up to three families may be configured.

The **no** form of this command disables aggregation in a next-hop-self scenario and the link-bandwidth extended community in the advertised route is a copy of the link-bandwidth extended community in the received route (which may have been added by import policy or by the effect of the **add-to-received-ebgp** command).

Default no aggregate-used-paths

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

Platforms All

aggregate-used-paths

Syntax **aggregate-used-paths** *family* [*family*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no aggregate-used-paths

Context [Tree] (config>router>bgp>group>link-bandwidth aggregate-used-paths)
[Tree] (config>router>bgp>group>neighbor>link-bandwidth aggregate-used-paths)

Full Context configure router bgp group link-bandwidth aggregate-used-paths
configure router bgp group neighbor link-bandwidth aggregate-used-paths

Description This command configures BGP to aggregate the bandwidth values from the link-bandwidth extended communities of the used multipaths towards an IP prefix when it is re-advertising a route with next-hop-self towards peers within the scope of the command, as long as the route belongs to one of the listed address families.

Aggregation is not supported unless all of the used multipaths (up to the configured ECMP limit) correspond to received BGP routes with a link-bandwidth extended community. If add-path is also enabled toward the peer, then all of the add-paths advertised to the peer encode the aggregated bandwidth in a link-bandwidth extended community.

Up to six families may be configured.

The **no** form of this command disables aggregation in a next-hop-self scenario and the link-bandwidth extended community in the advertised route is a copy of the link-bandwidth extended community in the received route (which may have been added by import policy or by the effect of the **add-to-received-ebgp** command).

Default no aggregate-used-paths

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

vpn-ipv4 — Adds a link-bandwidth extended community to IPv4 VPN (SAFI 128) routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

label-ipv6 — Adds a link-bandwidth extended community to labeled-unicast IPv6 routes.

vpn-ipv6 — Adds a link-bandwidth extended community to IPv6 VPN (SAFI 128) routes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.167 aggregation

aggregation

Syntax [**no**] **aggregation**

Context **[Tree]** (config>cflowd>collector aggregation)

Full Context configure cflowd collector aggregation

Description This command configures the type of aggregation scheme to be exported.

Specifies the type of data to be aggregated and to the collector.

To configure aggregation, you must decide which type of aggregation scheme to configure: autonomous system, destination prefix, protocol port, raw, source destination, or source prefix.

This can only be configured if the collector version is configured as V8.

The **no** form of this command removes all aggregation types from the collector configuration.

Default no aggregation

Platforms All

5.168 aggregator-id-zero

aggregator-id-zero

Syntax [**no**] **aggregator-id-zero**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy aggregator-id-zero)

Full Context configure subscriber-mgmt bgp-peering-policy aggregator-id-zero

Description This command is used to set the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes that contain different AS paths.

When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the AS number and router ID to the aggregator path attribute.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this command is enabled, BGP adds the router ID to the aggregator path attribute. The **no** form of this command used at the global level reverts to default where BGP adds the AS number and router ID to the aggregator path attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

aggregator-id-zero

Syntax [**no**] **aggregator-id-zero**

Context **[Tree]** (config>service>vprn>bgp aggregator-id-zero)
[Tree] (config>service>vprn>bgp>group aggregator-id-zero)
[Tree] (config>service>vprn>bgp>group>neighbor aggregator-id-zero)

Full Context configure service vprn bgp aggregator-id-zero
configure service vprn bgp group aggregator-id-zero
configure service vprn bgp group neighbor aggregator-id-zero

Description This command is used to set the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes that contain different AS paths.

When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the AS number and router ID to the aggregator path attribute.

When this command is enabled, BGP adds the router ID to the aggregator path attribute. This command is used at the group level to revert to the value defined under the global level, while this command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of this command used at the global level reverts to default where BGP adds the AS number and router ID to the aggregator path attribute.

The **no** form of this command used at the group level reverts to the value defined at the group level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no aggregator-id-zero — BGP adds the AS number and router ID to the aggregator path attribute.

Platforms All

aggregator-id-zero

Syntax [**no**] **aggregator-id-zero**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp aggregator-id-zero)
[Tree] (config>router>bgp>group aggregator-id-zero)
[Tree] (config>router>bgp>group>neighbor aggregator-id-zero)

Full Context configure router bgp aggregator-id-zero
configure router bgp group aggregator-id-zero
configure router bgp group neighbor aggregator-id-zero

Description This command sets the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes for the same prefix with different path attributes.

When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the AS number and router ID to the aggregator path attribute.

When this command is enabled, BGP adds the router ID to the aggregator path attribute. This command is used at the group level to revert to the value defined under the global level, while this command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of this command used at the global level reverts to default where BGP adds the AS number and router ID to the aggregator path attribute.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no aggregator-id-zero

Platforms All

5.169 agi

agi

Syntax **agi** *agi*
no agi

Context [Tree] (config>service>apipe>spoke-sdp>pw-path-id agi)
[Tree] (config>service>cpipe>spoke-sdp>pw-path-id agi)
[Tree] (config>service>epipe>spoke-sdp>pw-path-id agi)
[Tree] (config>service>vpls>spoke-sdp>pw-path-id agi)

Full Context configure service apipe spoke-sdp pw-path-id agi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service cpipe spoke-sdp pw-path-id agi
configure service epipe spoke-sdp pw-path-id agi
configure service vpls spoke-sdp pw-path-id agi

Description This command configures the attachment group identifier for an MPLS-TP PW.

Parameters *agi* — Specifies the attachment group identifier.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service epipe spoke-sdp pw-path-id agi
- configure service cpipe spoke-sdp pw-path-id agi
- configure service vpls spoke-sdp pw-path-id agi

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp pw-path-id agi

agi

Syntax **agi** *agi*
no agi

Context **[Tree]** (config>service>ies>if>spoke-sdp>pw-path-id agi)
[Tree] (config>service>ies>red-if>spoke-sdp>pw-path-id agi)

Full Context configure service ies interface spoke-sdp pw-path-id agi
configure service ies redundant-interface spoke-sdp pw-path-id agi

Description This command configures the attachment group identifier for an MPLS-TP PW.

Parameters *agi* — Specifies the attachment group identifier.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies redundant-interface spoke-sdp pw-path-id agi

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp pw-path-id agi

agi

Syntax **agi** *attachment-group-identifier*
no agi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>if>spoke-sdp>pw-path-id agi)
[Tree] (config>service>vprn>red-if>spoke-sdp>pw-path-id agi)

Full Context configure service vprn interface spoke-sdp pw-path-id agi
configure service vprn redundant-interface spoke-sdp pw-path-id agi

Description This command configures the attachment group identifier for an MPLS-TP PW.

Parameters *attachment-group-identifier* — Specifies the attachment group identifier.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn redundant-interface spoke-sdp pw-path-id agi

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp pw-path-id agi

agi

Syntax **agi** *route-identifier*
no agi

Context [Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp>pw-path-id agi)
[Tree] (config>mirror>mirror-dest>spoke-sdp>pw-path-id agi)

Full Context configure mirror mirror-dest remote-source spoke-sdp pw-path-id agi
configure mirror mirror-dest spoke-sdp pw-path-id agi

Description This command configures the attachment group identifier for an MPLS-TP PW.

Parameters *route-identifier* — Specifies the attachment group identifier.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.170 aging

aging

Syntax **aging** *days*
no aging

Context [Tree] (config>system>security>password aging)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security password aging

Description This command configures the number of days a user password is valid before the user must change their password. This parameter can be used to force the user to change the password at the configured interval. Note the aging starts after the last password configuration or update. This timer is persistence (per user) over a node reboot or activity switch between CPMs. When the user changes the password, the timer is reset to the maximum age. When the password for a user ages out, the user is prompted at login to change the password. Console/SSH/Telnet supports password change prompt.

The **no** form of this command reverts to the default value.

Parameters *days* — Specifies the maximum number of days the password is valid.

Values 1 to 500

Note: This command applies to local users.

Platforms All

5.171 ah-ext-hdr

ah-ext-hdr

Syntax **ah-ext-hdr** {**true** | **false**}
no ah-ext-hdr

Context **[Tree]** (config>filter>ipv6-filter>entry>match ah-ext-hdr)

Full Context configure filter ipv6-filter entry match ah-ext-hdr

Description This command enables match on existence of AH Extension Header in the IPv6 filter policy.

The **no** form of this command ignores AH Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default no ah-ext-hdr

Parameters **true** — Matches a packet with an AH Extension Header.

false — Matches a packet without an AH Extension Header.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.172 aigp

aigp

Syntax [**no**] **aigp**

Context **[Tree]** (config>router>bgp>group aigp)
[Tree] (config>router>bgp>group>neighbor aigp)

Full Context configure router bgp group aigp
configure router bgp group neighbor aigp

Description This command enables or disables Accumulated IGP (AIGP) path attribute support with one or more BGP peers. BGP path selection among routes with an associated AIGP metric is based on the end-to-end IGP metrics of the different BGP paths, even when these BGP paths span more than one AS and IGP instance.

The effect of disabling AIGP (using the **no** form of this command or implicit) is to remove the AIGP attribute from advertised routes, if present, and to ignore the AIGP attribute in received routes.

Default no aigp

Platforms All

5.173 aigp-metric

aigp-metric

Syntax **aigp-metric** *metric*
aigp-metric add
aigp-metric igp
no aigp-metric

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action aigp-metric)
[Tree] (config>router>policy-options>policy-statement>default-action aigp-metric)

Full Context configure router policy-options policy-statement default-action aigp-metric
configure router policy-options policy-statement entry action aigp-metric

Description This command assigns a BGP AIGP metric to routes matching the entry. The effect of this command on a route matched and accepted by a route policy entry depends on how the policy is applied (BGP import policy vs. BGP export policy), the type of route and the specific form of this command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In a BGP import policy this command is used to:

- Associate an AIGP metric with an IBGP route received with an empty AS path and no AIGP attribute.
- Associate an AIGP metric with an EBGP route received without an AIGP attribute that has an AS path containing only AS numbers belonging to the local AIGP administrative domain.
- Modify the received AIGP metric value prior to BGP path selection.

In a BGP export policy this command is used to:

- Add the AIGP attribute and set the AIGP metric value in a BGP route originated by exporting a direct, static or IGP route from the routing table.
- Remove the AIGP attribute from a route advertisement to a particular peer.
- Modify the AIGP metric value in a route advertisement to a particular peer.

Default no aigp-metric

Parameters *metric* — Administratively defined metric.

Values 0 to 4294967295

Default name — The AIGP metric parameter variable name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

add — Adds the AIGP attribute.

igp — Sets the AIGP metric to the IGP metric.

Platforms All

5.174 ais-enable

ais-enable

Syntax [**no**] **ais-enable**

Context **[Tree]** (config>port>ethernet>eth-cfm>mep ais-enable)
[Tree] (config>lag>eth-cfm>mep ais-enable)

Full Context configure lag eth-cfm mep ais-enable
configure port ethernet eth-cfm mep ais-enable

Description This command enables the reception of AIS messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default values.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ais-enable

Syntax [**no**] **ais-enable**

Context **[Tree]** (config>service>epipe>sap>eth-cfm ais-enable)
[Tree] (config>service>epipe>sap>eth-cfm>mep ais-enable)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep ais-enable)

Full Context configure service epipe sap eth-cfm ais-enable
configure service epipe sap eth-cfm mep ais-enable
configure service epipe spoke-sdp eth-cfm mep ais-enable

Description This command enables the generation and the reception of AIS messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ais-enable

Syntax [**no**] **ais-enable**

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>mep ais-enable)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep ais-enable)
[Tree] (config>service>vpls>sap>eth-cfm>mep ais-enable)

Full Context configure service vpls mesh-sdp eth-cfm mep ais-enable
configure service vpls sap eth-cfm mep ais-enable
configure service vpls spoke-sdp eth-cfm mep ais-enable

Description This command enables the generation and the reception of AIS messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ais-enable

Syntax [**no**] **ais-enable**

Context **[Tree]** (config>service>ies>if>spoke-sdp>eth-cfm ais-enable)

Full Context configure service ies interface spoke-sdp eth-cfm ais-enable

Description This command configures the reception of Alarm Indication Signal (AIS) message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ais-enable

Syntax [**no**] **ais-enable**

Context **[Tree]** (config>service>vprn>sap>eth-cfm>mep ais-enable)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm ais-enable)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm ais-enable)

Full Context configure service vprn interface spoke-sdp eth-cfm ais-enable
configure service vprn sap eth-cfm mep ais-enable
configure service vprn subscriber-interface group-interface sap eth-cfm ais-enable

Description This command configures the reception of Alarm Indication Signal (AIS) message.

ais-enable

Syntax [**no**] **ais-enable**

Context **[Tree]** (config>router>mpls>if>mpls-tp-mep ais-enable)

Full Context configure router mpls interface mpls-tp-mep ais-enable

Description This command enables MPLS-TP AIS insertion for the forward and reverse directions of all MPLS-TP transit paths using the MPLS interface. This causes the generation of AIS packets in the forward or reverse directions of a path if a fault is detected on the applicable underlying interface for the ingress of the path direction.

The **no** form of this command disables AIS insertion.

Default no ais-enable

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.175 alarm

alarm

Syntax **alarm** *rmon-alarm-id* **variable-oid** *oid-string* **interval** *seconds* [*sample-type*] [**startup-alarm** *alarm-type*] [**rising-event** *rmon-event-id* **rising-threshold** *threshold*] [**falling-event** *rmon-event-id* **falling-threshold** *threshold*] [**owner** *owner-string*]
no alarm *rmon-alarm-id*

Context **[Tree]** (config>system>thresholds>rmon alarm)

Full Context configure system thresholds rmon alarm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The alarm command configures an entry in the RMON-MIB alarmTable. The alarm command controls the monitoring and triggering of threshold crossing events. In order for notification or logging of a threshold crossing event to occur there must be at least one associated rmon>event configured.

The agent periodically takes statistical sample values from the MIB variable specified for monitoring and compares them to thresholds that have been configured with the alarm command. The alarm command configures the MIB variable to be monitored, the polling period (interval), sampling type (absolute or delta value), and rising and falling threshold parameters. If a sample has crossed a threshold value, the associated event is generated.

Use the **no** form of this command to remove an rmon-alarm-id from the configuration.

Parameters *rmon-alarm-id* — Specifies a numerical identifier for the alarm being configured. The number of alarms that can be created is limited to 1200. Alarm ID values above 65400 are used for dynamic system threshold commands and should be avoided.

Values 1 to 65535

oid-string — Specifies the SNMP object identifier of the particular variable to be sampled. Only SNMP variables that resolve to an ASN.1 primitive type of integer (integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. The oid-string, up to 255 characters, may be expressed using either the dotted string notation or as object name plus dotted instance identifier. For example, "1.3.6.1.2.1.2.2.1.10.184582144" or "ifInOctets.184582144".

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds. When setting this interval value, care should be taken in the case of ’delta’ type sampling - the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2147483647 - 1 during a single sampling interval. Care should also be taken not to set the interval value too low to avoid creating unnecessary processing overhead.

Values 1 to 2147483647

sample-type — Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds.

Values absolute — Specifies that the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval.

delta — Specifies that the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

Default absolute

alarm-type — Specifies the alarm that may be sent when this alarm is first created.

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, then a single rising threshold crossing event is generated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

rising-event *rmon-event-id* — Specifies the identifier of the **rmon>event** that specifies the action to be taken when a rising threshold crossing event occurs.

If there is no corresponding event configured for the specified rmon-event-id, then no association exists and no action is taken.

If the **rising-event** *rmon-event-id* has a value of zero (0), no associated event exists.

If a **rising-event** *rmon-event-id* is configured, the CLI requires a **rising-threshold** to also be configured.

Values 0 to 65535

Default 0

rising-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the **falling-threshold** value.

Values -2147483648 to 2147483647

Default 0

falling-event *rmon-event-id* — Specifies the identifier of the **rmon>event** that specifies the action to be taken when a falling threshold crossing event occurs. If there is no corresponding event configured for the specified rmon-event-id, then no association exists and no action is taken. If the **falling-event** has a value of zero (0), no associated event exists.

If a **falling-event** is configured, the CLI requires a **falling-threshold** to also be configured.

Values 0 to 65535

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Values -2147483648 to 2147483647

Default 0

owner-string — Specifies the owner string; the owner identifies the creator of this alarm. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarmTable by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner will not normally be configured by CLI users and can be a maximum of 80 characters long.

Default TiMOS CLI

Configuration example

```
alarm 3 variable-oid ifInOctets.184582144 interval 20 sample-type delta
start-alarm either rising-event 5 rising-threshold 10000 falling-event 5
falling-threshold 9000 owner "TiMOS CLI"
```

Platforms All

alarm

Syntax [**no**] **alarm**

Context **[Tree]** (config>sys>security>cpu-protection>policy alarm)

Full Context configure system security cpu-protection policy alarm

Description This command enables the generation of an event when a rate is exceed. The event includes information about the offending source. Only one event is generated per monitor period.

The **no** form of this command disables the notifications.

Default no alarm

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

5.176 alarm-cells

alarm-cells

Syntax [**no**] **alarm-cells**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap>atm alarm-cells)
[Tree] (config>service>vprn>if>sap>atm>oam alarm-cells)

Full Context configure service vpls sap atm alarm-cells
configure service vprn interface sap atm oam alarm-cells

Description This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC termination to monitor and report the status of their connection by propagating fault information through the network and by driving PVCCs operational status.

When alarm-cells functionality is enabled, PVCCs operational status is affected when a PVCC goes into AIS or RDI state because of an AIS/RDI processing (that is assuming nothing else affects PVCCs operational status, PVCC goes DOWN, when it enters a fault state and comes back UP, when it exits that fault state) and RDI cell are generated when PVCC is operationally DOWN. No OAM-specific SNMP trap is raised whenever an endpoint enters/exits an AIS or RDI states, however, if as result of an OAM state change, the PVCC changes operational status, then a trap is expected from an entity the PVCC is associated with (for example a SAP).

The **no** form of this command disables alarm-cells functionality for a PVCC. When alarm-cells functionality is disabled, PVCCs operational status is no longer affected by PVCCs OAM state changes due to AIS/RDI processing (when alarm-cells is disabled, a PVCC changes operational status to UP, if it was DOWN because of the alarm-cell processing) and RDI cells are not generated as result of PVCC going into AIS or RDI state, however, PVCCs OAM status records OAM faults as described above.

Default Enabled for PVCCs delimiting IES SAPs

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

alarm-cells

Syntax [**no**] **alarm-cells**

Context [Tree] (config>service>apipe>sap>atm>oam alarm-cells)
[Tree] (config>service>epipe>sap>atm>oam alarm-cells)
[Tree] (config>service>ipipe>sap>atm>oam alarm-cells)

Full Context configure service apipe sap atm oam alarm-cells
configure service epipe sap atm oam alarm-cells
configure service ipipe sap atm oam alarm-cells

Description This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC terminations to monitor and report the status of their connection by propagating fault information through the network and by driving PVCC’s operational status.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When alarm-cells functionality is enabled, a PVCC's operational status is affected when a PVCC goes into an AIS or RDI state because of an AIS/RDI processing (assuming nothing else affects PVCC's operational status, for example, if the PVCC goes operationally down, or enters a fault state and becomes operationally up, or exits that fault state). RDI cells are generated when PVCC is operationally down. No OAM-specific SNMP trap is raised whenever an endpoint enters/exits an AIS or RDI state, however, if as result of an OAM state change, the PVCC changes operational status, then a trap is expected from an entity the PVCC is associated with (for example a SAP).

The **no** command disables alarm-cells functionality for a PVCC. When alarm-cells functionality is disabled, a PVCC's operational status is no longer affected by a PVCC's OAM state changes due to AIS/RDI processing (when **alarm-cells** is disabled, a PVCC will change operational status to operationally up due to alarm-cell processing) and RDI cells are not generated as result of the PVCC going into AIS or RDI state. The PVCC's OAM status, however, will record OAM faults as previously described.

Default Enabled for PVCCs delimiting IES SAPs

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

alarm-cells

Syntax [**no**] **alarm-cells**

Context **[Tree]** (config>service>ies>if>sap>atm>oam alarm-cells)

Full Context configure service ies interface sap atm oam alarm-cells

Description This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC termination to monitor and report the status of their connection by propagating fault information through the network and by driving PVCC's operational status.

When alarm-cells functionality is enabled, a PVCC's operational status is affected when a PVCC goes into an AIS or RDI state because of an AIS/RDI processing (assuming nothing else affects PVCC's operational status, for example, if the PVCC goes DOWN, or enters a fault state and comes back UP, or exits that fault state). RDI cells are generated when PVCC is operationally DOWN. No OAM-specific log event is raised whenever an endpoint enters/exits an AIS or RDI state, however, if as result of an OAM state change, the PVCC changes operational status, then a trap is expected from an entity the PVCC is associated with (for example a SAP).

The **no** command disables alarm-cells functionality for a PVCC. When alarm-cells functionality is disabled, a PVCC's operational status is no longer affected by a PVCC's OAM state changes due to AIS/RDI processing (when alarm-cells is disabled, a PVCC will change operational status to UP due to alarm-cell processing) and RDI cells are not generated as result of the PVCC going into AIS or RDI state. The PVCC's OAM status, however, will record OAM faults as described above.

Default Enabled for PVCCs delimiting IES SAPs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

5.177 alarm-contact-in-power

alarm-contact-in-power

Syntax **alarm-contact-in-power** {**on** | **off**}

Context **[Tree]** (config>system alarm-contact-in-power)

Full Context configure system alarm-contact-in-power

Description This command allows the user to enable a supply of +24V output power on the +24VDC pin of the Alarm Interface Port of the CPM. When enabled, the power supplied through the +24VDC output pin can be used as a source voltage for the alarm contact input pins. The +24VDC output can be used to supply power for monitoring external sensor devices such as cabinet door sensors instead of using an external power source. If users want to use a separate external power source, they should disable the supply of power to the +24VDC output pin by using this CLI command.

Default alarm-contact-in-power off

Parameters **on** — Specifies to turn on power to the +24VDC output pin of the Alarm Interface Port of the CPM.

off — Specifies to turn off power to the +24VDC output pin of the Alarm Interface Port of the CPM.

Platforms 7750 SR-a

5.178 alarm-contact-input

alarm-contact-input

Syntax **alarm-contact-input** *input-pin-number*

Context **[Tree]** (config>system alarm-contact-input)

Full Context configure system alarm-contact-input

Description Commands in this context configure the alarm contact input pin parameters for the specified input pin.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *input-pin-number* — Specifies the alarm contact input pin.

Values 1 to 4

Platforms 7750 SR-a

5.179 alarm-notification

alarm-notification

Syntax **alarm-notification**

Context [Tree] (config>eth-tunnel>path>eth-cfm>mep alarm-notification)
[Tree] (config>lag>eth-cfm>mep alarm-notification)

Full Context configure eth-tunnel path eth-cfm mep alarm-notification
configure lag eth-cfm mep alarm-notification

Description This command configures the MEP alarm notification parameter.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

alarm-notification

Syntax **alarm-notification**

Context [Tree] (config>service>vpls>eth-cfm>mep alarm-notification)
[Tree] (config>service>epipe>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>vpls>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>vpls>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>ies>if>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>vprn>if>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep alarm-notification)
[Tree] (config>service>vprn>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep alarm-notification)
[Tree] (config>service>ipipe>sap>eth-cfm>mep alarm-notification)
[Tree] (config>port>ethernet>eth-cfm>mep alarm-notification)
[Tree] (config>lag>eth-cfm>eth-cfm>mep alarm-notification)
[Tree] (config>router>if>eth-cfm>mep alarm-notification)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context

configure lag eth-cfm eth-cfm mep alarm-notification
configure port ethernet eth-cfm mep alarm-notification
configure router interface eth-cfm mep alarm-notification
configure service epipe sap eth-cfm mep alarm-notification
configure service epipe spoke-sdp eth-cfm mep alarm-notification
configure service ies interface sap eth-cfm mep alarm-notification
configure service ies interface spoke-sdp eth-cfm mep alarm-notification
configure service ies subscriber-interface group-interface sap eth-cfm mep alarm-notification
configure service ipipe sap eth-cfm mep alarm-notification
configure service vpls eth-cfm mep alarm-notification
configure service vpls mesh-sdp eth-cfm mep alarm-notification
configure service vpls sap eth-cfm mep alarm-notification
configure service vpls spoke-sdp eth-cfm mep alarm-notification
configure service vprn interface sap eth-cfm mep alarm-notification
configure service vprn interface spoke-sdp eth-cfm mep alarm-notification
configure service vprn sap eth-cfm mep alarm-notification
configure service vprn subscriber-interface group-interface sap eth-cfm mep alarm-notification

Description

Commands in this context configure the Fault Notification Generation time values for raising the alarm and resetting the CCM defect alarm. These timers are used for network management processes and are not tied into delaying the notification to the fault management system on the network element. These timers do not affect fault propagation mechanisms.

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep alarm-notification
- configure service ies subscriber-interface group-interface sap eth-cfm mep alarm-notification

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep alarm-notification
- configure service vprn interface spoke-sdp eth-cfm mep alarm-notification
- configure service vpls spoke-sdp eth-cfm mep alarm-notification
- configure port ethernet eth-cfm mep alarm-notification
- configure service ies interface spoke-sdp eth-cfm mep alarm-notification
- configure service vpls sap eth-cfm mep alarm-notification
- configure router interface eth-cfm mep alarm-notification
- configure service vpls mesh-sdp eth-cfm mep alarm-notification
- configure service vprn interface sap eth-cfm mep alarm-notification
- configure service vpls eth-cfm mep alarm-notification
- configure service epipe sap eth-cfm mep alarm-notification
- configure service epipe spoke-sdp eth-cfm mep alarm-notification
- configure service ipipe sap eth-cfm mep alarm-notification

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

alarm-notification

Syntax **alarm-notification**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep alarm-notification)

Full Context configure eth-ring path eth-cfm mep alarm-notification

Description Commands in this context configure the MEP alarm notification parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.180 alarms

alarms

Syntax **alarms**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer alarms)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer alarms)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer alarms)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms
configure mcast-management multicast-info-policy bundle channel video analyzer alarms
configure mcast-management multicast-info-policy bundle video analyzer alarms

Description Commands in this context configure alarms for the analyzer (VQM).

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

alarms

Syntax **alarms**

Context **[Tree]** (config>li>x-interfaces>x3 alarms)

Full Context configure li x-interfaces x3 alarms

Description This command enables the configuration of X3 alarms.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

alarms

Syntax **alarms**

Context **[Tree]** (config>system alarms)

Full Context configure system alarms

Description Commands in this context configure facility alarm parameters. Alarm support is intended to cover a focused subset of router states that are likely to indicate service impacts (or imminent service impacts) related to the overall state of hardware assemblies (cards, fans, links, and so on).

Platforms All

5.181 alc-acct-triggered-reason

alc-acct-triggered-reason

Syntax [**no**] **alc-acct-triggered-reason**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute alc-acct-triggered-reason)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute alc-acct-triggered-reason

Description This command includes the **alc-acct-triggered-reason** attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.182 alc-error-code

alc-error-code

Syntax [**no**] **alc-error-code**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute alc-error-code)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute alc-error-code

Description This command enables RADIUS accounting messages to include an error number and error code when the subscriber host session terminates. To obtain a complete list of error numbers and their corresponding codes, use the **tools>dump>aaa>radius-acct-terminate-cause** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.183 alg

alg

Syntax **alg**

Context **[Tree]** (config>service>nat>nat-policy alg)
[Tree] (config>service>nat>firewall-policy alg)
[Tree] (config>service>nat>up-nat-policy alg)

Full Context configure service nat firewall-policy alg
configure service nat nat-policy alg
configure service nat up-nat-policy alg

Description Commands in this context configure application layer gateway (ALG) parameters of this policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy alg
- configure service nat up-nat-policy alg

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy alg

5.184 algorithm

algorithm

Syntax **algorithm** *flex-algo-id*
no algorithm

Context **[Tree]** (config>router>segment-routing>srv6>locator algorithm)

Full Context configure router segment-routing segment-routing-v6 locator algorithm

Description This command creates an IGP flexible algorithm identifier for an SRv6 locator.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A locator can only be part of a single algorithm but can be used in multiple IGP instances.

The **no** form of this command returns the locator to the base IGP algorithm 0.

Default no algorithm

Parameters *flex-algo-id* — Specifies the flexible algorithm ID.

Values 128 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

5.185 alias

alias

Syntax **alias** *alias-name alias-command-name*
no alias *alias-name*

Context **[Tree]** (environment alias)

Full Context environment alias

Description This command enables the substitution of a command line (or part of a command line) by an alias. Use the **alias** command to create alternative or easier to remember/understand names for an entity or command string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The special characters “/” and “\” cannot be used as the first character inside an alias string. An alias can contain a double quote character by preceding the quote with a “\” character (for example, **alias my-alias "\| match \"***string***\""**). Only a single command can be present in the command string (the command can be long with many parameters but there is no support for aliases that include multiple CLI commands/lines). The **alias** command can be entered in any context but must be created in the **root>environment** context.

For example, to create an alias named **soi** to display OSPF interfaces, enter:

alias soi “show router ospf interface”

Complex aliases can be created to have shortcuts for customized show routine output:

environment alias my-summary "\| match expression \"----\|Description\|Interface\|Admin State\|Oper State\|Transceiver Type\|Optical Compliance\|Link Length\" \| match invert-match expression \"Ethernet Interface\|OTU Interface\" \| match invert-match expression \"----\" post-lines 1"

and then used like this:

show port detail my-summary

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *alias-name* — Specifies the alias name, up to 80 characters. Do not use a valid command string for the name of the alias. If the alias specified is an actual command, this causes the command to be replaced by the alias.

alias-command-name — Specifies the command name to be associated, up to 320 characters.

Platforms All

alias

Syntax **alias**

Context **[Tree]** (global alias)

Full Context global alias

Description This command displays a list of existing aliases.

Output The following output is an example of alias information, and Table 26 describes the output fields.

Sample Output

```
A:ALA-103>config>system# show alias
===============================================================================
Alias-Name                    Alias-command-name
===============================================================================
sri                           show router interface
sse                           show service service-using epipe
ssvpls                        show service service-using vpls
ssvprn                        show service service-using vprn
ssi                           show service service-using ies
-------------------------------------------------------------------------------
Number of aliases : 5
===============================================================================
A:ALA-103>config>system#
```

Table 26 **Show Alias Output Fields**

Label	Description
Alias-Name	Displays the name of the alias.
Alias-command-name	The command and parameter syntax that define the alias.
Number of aliases	The total number of aliases configured on the router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.186 align

align

Syntax [**no**] **align**

Context **[Tree]** (config>log>acct-policy align)

Full Context configure log accounting-policy align

Description This command enables alignment of statistics collection to the nearest interval within an hour. Enabling the alignment allows statistics collection into an accounting file that is being synchronized across multiple network nodes in the network.

The **no** form of this command disables alignment of statistics collection.

Default no align

Platforms All

5.187 all

all

Syntax **all** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no all

Context **[Tree]** (debug>service>id>pim-snooping all)

Full Context debug service id pim-snooping all

Description This command enables or disables debugging for all the PIM modules.

Parameters *grp-ip-address* — Debugs information associated with all PIM modules

Values multicast group address (IPv4 or IPv6)

ip-address — Debugs information associated with all PIM modules

Values IPv4 or IPv6 address

detail — Debugs detailed information on all PIM modules

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

all

Syntax [**no**] **all**

Context **[Tree]** (debug>router>gmpls>event all)

Full Context debug router gmpls event all

Description This command enables and disables debugging for GMPLS All events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

all

Syntax **all** [**detail**]
no all

Context **[Tree]** (debug>router>gmpls>packet all)

Full Context debug router gmpls packet all

Description This command enables debugging for GMPLS All packets.

The **no** form of the command disables debugging for GMPLS All packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

all

Syntax **all** [**detail**]
no all

Context **[Tree]** (debug>router>mpls>event all)
[Tree] (debug>router>rsvp>event all)

Full Context debug router mpls event all
debug router rsvp event all

Description This command debugs all events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about all events.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

all

Syntax **all** [**detail**]
no all

Context **[Tree]** (debug>router>rsvp>packet all)

Full Context debug router rsvp packet all

Description This command debugs all packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about all RSVP packets.

Platforms All

all

Syntax **all** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no all

Context **[Tree]** (debug>router>pim all)

Full Context debug router pim all

Description This command enables debugging for all the PIM modules.

The **no** form of this command disables debugging PIM modules.

Parameters *grp-ip-address* — Debugs information associated with all PIM modules.

Values IPv4 or IPv6 address

ip-address — Debugs information associated with all PIM modules.

Values IPv4 or IPv6 address

detail — Debugs detailed information on all PIM modules.

Platforms All

all

Syntax [**no**] **all**

Context **[Tree]** (debug>router>rpki-session>packet all)

Full Context debug router rpki-session packet all

Description This command enables debugging for all RPKI packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables debugging for all RPKI packets.

Platforms All

all

Syntax **all**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-cntr all)
[Tree] (config>log>acct-policy>cr>aa>aa-from-sub-cntr all)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr all)
[Tree] (config>log>acct-policy>cr>aa>aa-sub-attr all)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters all
configure log accounting-policy custom-record aa-specific aa-sub-attributes all
configure log accounting-policy custom-record aa-specific aa-sub-counters all
configure log accounting-policy custom-record aa-specific to-aa-sub-counters all

Description This command includes all counters and only applies to the 7750 SR.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.188 all-authorized-session-addresses

all-authorized-session-addresses

Syntax [**no**] **all-authorized-session-addresses**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute all-authorized-session-addresses)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute all-authorized-session-addresses

Description This command specifies to include all included and authorized address/prefix attributes in session accounting and is applicable only for session-accounting mode.

With this flag enabled, all IP address attributes explicitly enabled to be included are the following:

- delegated-ipv6-prefix
- framed-ip-address
- framed-ip-netmask
- framed-ipv6-prefix
- ipv6-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

These are included if the corresponding addresses or prefixes are authorized (via access-accept or ludb) and independent if they are used or not.

The **no** form of this command reverts to the default.

Default no all-authorized-session-addresses

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.189 all-events

all-events

Syntax **all-events**

Context **[Tree]** (debug>service>id>mrp all-events)

Full Context debug service id mrp all-events

Description This command enables MRP debugging for the applicant, leave all, periodic and registrant state machines and enables debugging of received and transmitted MRP PDUs.

Platforms All

all-events

Syntax **all-events**

Context **[Tree]** (debug>service>id>stp all-events)

Full Context debug service id stp all-events

Description This command enables STP debugging for all events.

The **no** form of the command disables debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.190 all-l1isis

all-l1isis

Syntax **all-l1isis** *ieee-address*
no all-l1isis

Context **[Tree]** (config>service>vprn>isis all-l1isis)

Full Context configure service vprn isis all-l1isis

Description This command specifies the MAC address to use for the VPRN instance of the Layer 1 IS-IS routers. The MAC address should be a multicast address.

The **no** form of this command reverts to the default value.

Default all-l1isis 01:80:c2:00:00:14

Parameters *ieee-address* — Specifies the destination MAC address for all Layer 1 I-IS neighbors on the link for this ISIS instance.

Platforms All

all-l1isis

Syntax **all-l1isis** *ieee-address*
no all-l1isis

Context **[Tree]** (config>router>isis all-l1isis)

Full Context configure router isis all-l1isis

Description This command enables you to specify the MAC address to use for all Layer 1 IS-IS routers. The MAC address should be a multicast address.

The **no** form of this command reverts to the default value.

Default 01:80:c2:00:00:14

Parameters *ieee-address* — Specifies the destination MAC address for all Layer 1 I-IS neighbors on the link for this IS-IS instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.191 all-l2isis

all-l2isis

Syntax **all-l2isis** *ieee-address*
no all-l2isis

Context **[Tree]** (config>service>vprn>isis all-l2isis)

Full Context configure service vprn isis all-l2isis

Description This command specifies the MAC address to use for Layer 2 IS-IS routers for the VPRN instance. The MAC address should be a multicast address.

The **no** form of this command reverts to the default value.

Default all-l2isis 01:80:c2:00:00:15

Parameters *ieee-address* — Specifies the destination MAC address for all Layer 2 ISIS neighbors on the link for this ISIS instance.

Platforms All

all-l2isis

Syntax **all-l2isis** *ieee-address*
no all-l2isis

Context **[Tree]** (config>router>isis all-l2isis)

Full Context configure router isis all-l2isis

Description This command enables you to specify the MAC address to use for all Layer 2 IS-IS routers. The MAC address should be a multicast address.

The **no** form of this command reverts to the default value.

Default 01:80:c2:00:00:15

Parameters *ieee-address* — Specifies the destination MAC address for all Layer 2 IS-IS neighbors on the link for this IS-IS instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.192 all-octets-offered-count

all-octets-offered-count

Syntax [**no**] **all-octets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters all-octets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters all-octets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters all-octets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters all-octets-offered-count

Description This command includes all octets offered in the count.

The **no** form of this command excludes the octets offered in the count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

all-octets-offered-count

Syntax [**no**] **all-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters all-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters all-octets-offered-count)

Full Context configure log accounting-policy custom-record queue i-counters all-octets-offered-count
configure log accounting-policy custom-record ref-queue i-counters all-octets-offered-count

Description This command includes all octets offered in the count.

The **no** form of this command excludes the octets offered in the count.

Default no all-octets-offered-count

Platforms All

5.193 all-packets-offered-count

all-packets-offered-count

Syntax [**no**] **all-packets-offered-count**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>acct-plcy>cr>queue>i-counters all-packets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters all-packets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters all-packets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters all-packets-offered-count

Description This command includes all packets offered in the count.

The **no** form of this command excludes the packets offered in the count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

all-packets-offered-count

Syntax [**no**] **all-packets-offered-count**

Context [Tree] (config>log>acct-policy>cr>queue>i-counters all-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters all-packets-offered-count)

Full Context configure log accounting-policy custom-record queue i-counters all-packets-offered-count
configure log accounting-policy custom-record ref-queue i-counters all-packets-offered-count

Description This command includes all packets offered in the count.

The **no** form of this command excludes the packets offered in the count.

Default no all-packets-offered-count

Platforms All

5.194 allocation

allocation

Syntax **allocation explicit-percent** *percent-of-parent-pool*
allocation port-bw-weight *pool-weight*
no allocation

Context [Tree] (config>qos>hs-port-pool-policy>alt-port-class-pools>class-pool allocation)
[Tree] (config>qos>hs-port-pool-policy>std-port-class-pools>class-pool allocation)

Full Context configure qos hs-port-pool-policy alt-port-class-pools class-pool allocation
configure qos hs-port-pool-policy std-port-class-pools class-pool allocation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sizes the associated class-pool based on either the specified **explicit-percent** *percent-of-parent-pool* or based on the dynamic port bandwidth portioning mechanism. Setting an explicit percentage prevents the port-class pool from participating in the dynamic port level bandwidth-based distribution of the mid-pool's size as the port bandwidth weight of the port-class pool becomes zero (0). Setting a port bandwidth weight causes the explicit percent value to become zero (0) disabling explicit sizing of the port-class pool.

The **no** form of the command sets the *percent-of-parent-pool* value to zero (0) and the *pool-weight* parameter to 1 for the port-class pool, restoring the default settings.

Default allocation 1

Parameters *percent-of-parent-pool* — Specifies the percentage of parent pool being allocated. This parameter must be configured when specifying the **explicit-percent**. The *percent-of-parent-pool* value is expressed as a percentage with two decimal places (100th of a percent) that indicates that the port-class pool should be sized by applying the value to the parent mid-pool size. Specifying **explicit-percent** forces the **port-bw-weight** to a zero (0) value (disabled).

Values 0.01 to 100.00

pool-weight — Specifies port bandwidth weight being allocated. The **port-bw-weight** and **explicit-percent** commands are mutually exclusive. The *pool-weight* parameter is required when specifying the port bandwidth weight and defines both that the port-class pool should be sized in the port bandwidth distribution of the mid-pool's size and what the distribution weight should be for the port-class pool compared to other port-class pools associated with the same mid-pool when competing for the port's distribution portion.

Values 1 to 100

Platforms 7750 SR-7/12/12e

5.195 allocation-percent

allocation-percent

Syntax **allocation-percent** *percent-of-parent-pool*
no allocation-percent

Context **[Tree]** (config>qos>hs-pool-policy>mid-tier>mid-pool allocation-percent)

Full Context configure qos hs-pool-policy mid-tier mid-pool allocation-percent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sizes the associated mid-pool based on the specified percent of the parent pool. The size is obtained by applying the specified percentage value to the current root-pool size acting as the mid-pool's parent. Whenever the parent root-pool is changed to a new root-pool or the size of the current parent root-pool is modified, the mid-pool's size is updated.

The **no** form of the command reverts to the default.

Default allocation-percent 1.00

Parameters *percent-of-parent-pool* — Specifies the percent of the parent pool. This parameter is required when the **allocation-percent** command is executed. This parameter defines the percentage of the root pool's size to derive the size of the mid-pool. The value is specified as a percentage with two decimal places (100th of a percent).

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

5.196 allocation-weight

allocation-weight

Syntax **allocation-weight** *pool-weight*
no allocation-weight

Context **[Tree]** (config>qos>hs-pool-policy>root-tier>root-pool allocation-weight)

Full Context configure qos hs-pool-policy root-tier root-pool allocation-weight

Description This command specifies the weight that is applied to the root pool and is divided by the sum of all root pool weights to derive the pool's buffer allocation factor. The amount of buffers remaining after the system-reserve percentage is applied is multiplied by the buffer allocation factor to derive the pool size.

Root pools function as an oversubscription control mechanism. A root pool acts as the root of a hierarchy of buffer pools and queues with respect to buffer allocation. Because the sum of the root pool sizes does not exceed the total number of buffers available, the number of buffers indicated by the root pools size is always be available to the queues within the root pools hierarchy, queues from one hierarchy can never steal buffers from another.

A root pool hierarchy is based on the dynamic parenting of one or more mid-tier pools to a root pool. A mid-tier pool represents the buffering allowed for all port-class pools mapped to the mid-tier pool. Each mid-tier pool is sized as a percentage of the root pool to which it is parented. The sum of the mid-tier pools percentages for a root pool may be greater than 100 percent, which allows the root pool to be oversubscribed. This can be beneficial when large fluctuations in mid-tier buffer utilization are expected and a given mid-tier pool should be allowed to exceed its fair share of buffering.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Through the mapping hierarchy presented above, each queue is mapped to a port-class pool, mid-tier pool, and root pool.

A root pool with an **allocation-weight** set to “0” is considered inactive and is not allocated buffers. Mid-tier pools cannot be parented to a root pool with a weight set to “0”. After a mid-tier pool is associated with a root pool, the root pool’s weight cannot be set to “0”.

As port classes are mapped to mid-tier pools in a different policy than mid-tier pools are mapped to root pools, a port-class pool can be mapped to a mid-tier pool that is not parented to a root pool. A queue mapped indirectly to a non-parented mid-tier pool has its operational MBS value set to zero and drops all incoming packets.

When a root pool’s allocation weight is modified, all root pools, mid-tier pools, and port class pool sizes are reevaluated and modified when necessary.

The **no** form of the command restores the default **allocation-weight** value to the associated root pool. Root pool 1 has a different default weight than root pools 2 through 8. The **no allocation-weight** command fails for root pools 2 through 8 if the root pool is currently parented to a class pool.

Default root-pool 1: allocation-weight 100

root-pool 2 to 16: allocation-weight 0

Parameters *pool-weight* — Defines the weight of the associated **root-pool** *root-pool-id* and is used by the system to calculate the size of the root buffer pool. This parameter is required when executing the **allocation-weight** command. Setting the *pool-weight* to 0 disables the pool and prevents the root pool from being a parent to any class pools. Root pool 1 cannot be set with an allocation weight of 0.

Values root-pool 1:1 to 100
root-pool 2 to 16:0 to 100

Platforms 7750 SR-7/12/12e

5.197 allow-boot-license-violations

allow-boot-license-violations

Syntax [**no**] **allow-boot-license-violations**

Context **[Tree]** (config>system allow-boot-license-violations)

Full Context configure system allow-boot-license-violations

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures whether the system should allow successful execution of the bootup configuration file when it contains license violations. When enabled, the system will not error on any configuration that causes a license violation and as a result permits the system to come into service. However, if violations are detected, the system reboots after a period of time if the violations are not fixed. See the *7450 ESS, 7750 SR, 7950 XRS and VSR Pay-as-You-Grow Licensing Reference Guide* for more information.

Platforms All

5.198 allow-directed-broadcasts

allow-directed-broadcasts

Syntax [**no**] **allow-directed-broadcasts**

Context **[Tree]** (config>router>if allow-directed-broadcasts)
[Tree] (config>service>ies>if allow-directed-broadcasts)
[Tree] (config>service>vprn>if allow-directed-broadcasts)
[Tree] (config>service>vprn>nw-if allow-directed-broadcasts)

Full Context configure router interface allow-directed-broadcasts
configure service ies interface allow-directed-broadcasts
configure service vprn interface allow-directed-broadcasts
configure service vprn network-interface allow-directed-broadcasts

Description This command enables the forwarding of directed broadcasts out of the IP interface.

A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. The **allow-directed-broadcasts** command on an IP interface enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface is sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts as it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface are counted in the normal discard counters for the egress SAP.

Note: Allowing directed broadcasts is a well-known mechanism used for denial-of-service attacks.

By default, directed broadcasts are not allowed and are discarded at this egress IP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the forwarding of directed broadcasts out of the IP interface. All broadcasts are dropped.

Default no allow-directed-broadcasts — Directed broadcasts are dropped.

Platforms All

5.199 allow-dot1q-msaps

allow-dot1q-msaps

Syntax [**no**] **allow-dot1q-msaps**

Context **[Tree]** (config>service>vpls>sap allow-dot1q-msaps)

Full Context configure service vpls sap allow-dot1q-msaps

Description This command enables support for single tagged traffic triggering managed SAP creation on a qinq encapsulated capture SAP.

With this command enabled, a single tagged trigger packet received on a qinq encapsulated capture SAP (x/y/z:*.* or x/y/z:tag.*) can trigger the creation of an x/y/z:tag.0 managed SAP (MSAP).

The **config>system>ethernet>new-qinq-untagged-sap** command should be configured:

- as a prerequisite for an x/y/z:tag.* capture-sap
- where x/y/z:tag1.0 and x/y/z:tag1.tag2 MSAPs for an x/y/z:*.* capture-sap should co-exist

Note that enabling new-qinq-untagged-sap affects the behavior of existing <port-id>:tag.0 SAPs.

With the allow-dot1q-msaps command disabled (default), a single tagged trigger packet received on a qinq encapsulated capture SAP (x/y/z:*.* or x/y/z:tag.*) is dropped as “Invalid QTag”.

This command cannot be enabled on:

- a dot1q encapsulated **capture-sap**
- an inverse capture sap (x/y/z:*.tag)

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.200 allow-egress-remark-dscp

allow-egress-remark-dscp

Syntax [**no**] **allow-egress-remark-dscp**

Context **[Tree]** (config>oam-pm>session>ip allow-egress-remark-dscp)

Full Context configure oam-pm session ip allow-egress-remark-dscp

Description This command instructs the egress QoS process to modify the DSCP based on the egress QoS configuration. This command exposes the DSCP to egress DSCP processing rules.

The **no** form of this command instructs the egress QoS process to ignore the DSCP and allow it to bypass egress QoS. If the **config**>**qos**>**network**>**egress**>**remark force** command is configured for the network egress QoS profile, the egress QoS process is applied and the DSCP can be overwritten regardless of the **allow-egress-remark-dscp** configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

allow-egress-remark-dscp

Syntax [**no**] **allow-egress-remark-dscp**

Context **[Tree]** (config>test-oam>link-meas>template>twl allow-egress-remark-dscp)

Full Context configure test-oam link-measurement measurement-template twamp-light allow-egress-remark-dscp

Description This command instructs the egress QoS process to modify the DSCP based on the egress QoS configuration. This command exposes the DSCP to egress DSCP processing rules.

If the **config>qos>network>egress>remark-force** command is configured for the network egress QoS profile, the egress QoS process is applied and the DSCP can be overwritten regardless of the **allow-egress-remark-dscp** configuration.

The **no** form of this command reverts to the default value, bypassing egress QoS processing of the DSCP.

Default no allow-egress-remark-dscp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.201 allow-export-bgp-vpn

allow-export-bgp-vpn

Syntax [**no**] **allow-export-bgp-vpn**

Context **[Tree]** (config>service>vprn allow-export-bgp-vpn)

Full Context configure service vprn allow-export-bgp-vpn

Description This command allows routes leaked from another local VPRN service to be re-exported by this VPRN in the form of new VPN-IP routes. The service label, route targets, and BGP next-hop of the re-advertised routes are based on the configuration and default values of the re-exporting VPRN.

When re-exporting leaked routes, the following restrictions apply.

- The **allow-export-bgp-vpn** command is not configurable in combination with any of the following commands: **carrier-carrier-vpn** (CSC), **label-mode next-hop** (LPN), **type** {**hub** | **spoke** | **subscriber-split-horizon**}, **redundant-interface**, and **export-inactive-bgp**.
- Re-exported routes always have the per-VRF label of the exporting VPRN; label-per-prefix advertisement is not supported.
- The best-external (inactive BGP) routes leaked by another VPRN cannot be re-exported by a VPRN configured with **allow-export-bgp-vpn**.

Caution: When a VPRN configured with **allow-export-bgp-vpn** advertises a leaked route, the **split-horizon** context is lost. A re-exported route can be easily advertised back to the sending peer unless this is blocked by BGP export policies. This can cause route flaps or other similar instability.

If the **no** form of this command is configured, leaked routes cannot be re-advertised as VPN-IP routes; they can only be re-advertised to PE-CE BGP peers of the VPRN.

Default no allow-export-bgp-vpn

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.202 allow-flex-algo-fallback

allow-flex-algo-fallback

Syntax [**no**] **allow-flex-algo-fallback**

Context **[Tree]** (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family allow-flex-algo-fallback)
[Tree] (config>router>bgp>next-hop-resolution>shortcut-tunnel>family allow-flex-algo-fallback)
[Tree] (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel allow-flex-algo-fallback)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel allow-flex-algo-fallback)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel allow-flex-algo-fallback)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel allow-flex-algo-fallback)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family allow-flex-algo-fallback
configure router bgp next-hop-resolution shortcut-tunnel family allow-flex-algo-fallback
configure service epipe bgp-evpn mpls auto-bind-tunnel allow-flex-algo-fallback
configure service vpls bgp-evpn mpls auto-bind-tunnel allow-flex-algo-fallback
configure service vprn bgp-evpn mpls auto-bind-tunnel allow-flex-algo-fallback
configure service vprn bgp-ipvpn mpls auto-bind-tunnel allow-flex-algo-fallback

Description This command configures a router to relax the strictly enforced Flex-Algorithm aware autobind, which is enabled through an import policy configured with the **action flex-algo** command.

If the **allow-flex-algo-fallback** command is enabled, the BGP router can autobind to a fallback algorithm 0 tunnel if no target Flex-Algorithm tunnel is available. If the **allow-flex-algo-fallback** command is disabled, the BGP autobind is strictly enforced to an intended Flex-Algorithm tunnel, which may cause traffic loss if no corresponding Flex-Algorithm tunnel exists.

The **no** form of this command removes the **allow-flex-algo-fallback** command from the configuration.

Default no allow-flex-algo-fallback

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.203 allow-fragmentation

allow-fragmentation

Syntax [**no**] **allow-fragmentation**

Context **[Tree]** (config>service>pw-template allow-fragmentation)
[Tree] (config>service>sdp allow-fragmentation)

Full Context configure service pw-template allow-fragmentation
configure service sdp allow-fragmentation

Description This command disables the setting of the **do-not-fragment** bit in the IP header of GRE encapsulated service traffic. This feature is only applicable to GRE SDPs and will be applied to all service traffic using the associated GRE SDP.

The **no** form of this command removes the command from the active configuration and returns the associated SDP to its default which is to set the **do-not-fragment** bit in all GRE encapsulated service traffic.

Default no allow-fragmentation

Platforms All

5.204 allow-ftp

allow-ftp

Syntax [**no**] **allow-ftp**

Context **[Tree]** (config>service>vprn>management allow-ftp)

Full Context configure service vprn management allow-ftp

Description This commands allows access to the FTP server from VPRN.

The **no** form of this command removes FTP access for this VPRN.

Platforms All

allow-ftp

Syntax [**no**] **allow-ftp**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>system>security>management allow-ftp)

Full Context configure system security management allow-ftp

Description This command allows access to the FTP server from Base and Management routers if it is operationally up.

The **no** form of this command disallows access to the FTP server.

Default allow-ftp

Platforms All

5.205 allow-grpc

allow-grpc

Syntax [**no**] **allow-grpc**

Context **[Tree]** (config>system>security>management allow-grpc)

Full Context configure system security management allow-grpc

Description This command allows access to the gRPC server from Base and Management routers if it is operationally up.

The **no** form of this command disallows access to the gRPC server.

Platforms All

allow-grpc

Syntax [**no**] **allow-grpc**

Context **[Tree]** (config>service>vprn>management allow-grpc)

Full Context configure service vprn management allow-grpc

Description This commands allows access to the GRPC server from VPRN.

The **no** form of this command removes GRPC access for this VPRN.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.206 allow-icmp-redirect

allow-icmp-redirect

Syntax [**no**] **allow-icmp-redirect**

Context **[Tree]** (config>router allow-icmp-redirect)

Full Context configure router allow-icmp-redirect

Description This command allows ICMP redirects received on the management interface.

The **no** form of this command drops the ICMP redirects received on the management interface.

Platforms All

5.207 allow-icmp6-redirect

allow-icmp6-redirect

Syntax [**no**] **allow-icmp-redirect**

Context **[Tree]** (config>router allow-icmp6-redirect)

Full Context configure router allow-icmp6-redirect

Description This command allows IPv6 ICMP redirects received on the management interface.

The **no** form of this command drops the IPv6 ICMP redirects received on the management interface.

Platforms All

5.208 allow-immediate

allow-immediate

Syntax [**no**] **allow-immediate**

Context **[Tree]** (config>system>management-interface>cli>classic-cli allow-immediate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system management-interface cli classic-cli allow-immediate

Description This command enables writable access in the **configure** classic CLI branch.

The **no** form of this command, when configured under the **management-interface**>**cli**>**classic-cli** context, blocks writeable access and configuration changes in the **configure** classic CLI branch. This causes the running configuration datastore from the **configure** classic CLI branch to be read-only.

This command can be used to enforce the use of candidate configuration and the **commit** command, instead of allowing immediate mode line-by-line configuration changes.

Default allow-immediate

Platforms All

5.209 allow-ip-int-bind

allow-ip-int-bind

Syntax [**no**] **allow-ip-int-bind**

Context **[Tree]** (config>service>vpls allow-ip-int-bind)

Full Context configure service vpls allow-ip-int-bind

Description The allow-ip-int-bind command that sets a flag on the VPLS or I-VPLS service that enables the ability to attach an IES or VPRN IP interface to the VPLS service in order to make the VPLS service routable. When the allow-ip-int-bind command is not enabled, the VPLS service cannot be attached to an IP interface.

VPLS Configuration Constraints for Enabling allow-ip-int-bind

When attempting to set the allow-ip-int-bind VPLS flag, the system first checks to see if the correct configuration constraints exist for the VPLS service and the network ports. The following VPLS features must be disabled or not configured for the allow-ip-int-bind flag to set:

- SAP ingress QoS policies applied to the VPLS SAPs cannot have MAC match criteria defined
- The VPLS service type cannot be B-VPLS or M-VPLS
- MVR from Routed VPLS and to another SAP is not supported
- Enhanced and Basic Subscriber Management (ESM and BSM) features
- Network domain on SDP bindings

Once the VPLS allow-ip-int-bind flag is set on a VPLS service, the above features cannot be enabled on the VPLS service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Network Port Hardware Constraints

The system also checks to ensure that all ports configured in network mode are associated with FlexPath2 forwarding planes. If a port is currently in network mode and the port is associated with a FlexPath1 forwarding plane, the allow-ip-int-bind command will fail. Once the allow-ip-int-bind flag is set on any VPLS service, attempting to enable network mode on a port associated with a FlexPath1 forwarding plane will fail.

VPLS SAP Hardware Constraints

Besides VPLS configuration and network port hardware association, the system also checks to that all SAPs within the VPLS are created on Ethernet ports and the ports are associated with FlexPath2 forwarding planes. Certain Ethernet ports and virtual Ethernet ports are not supported which include CCAG virtual ports (VSM based). If a SAP in the VPLS exists on an unsupported port type or is associated with a FlexPath1 forwarding plane, the allow-ip-int-bind command will fail. Once the allow-ip-int-bind flag is set on the VPLS service, attempting to create a VPLS SAP on the wrong port type or associated with a FlexPath1 forwarding plane will fail.

VPLS Service Name Bound to IP Interface without allow-ip-int-bind flag Set

If a service name is applied to a VPLS service and that service name is also bound to an IP interface but the allow-ip-int-bind flag has not been set on the VPLS service context, the system attempt to resolve the service name between the VPLS service and the IP interface will fail. After the allow-ip-int-bind flag is successfully set on the VPLS service, either the service name on the VPLS service must be removed and reapplied or the IP interface must be re-initialized using the **shutdown** / **no shutdown** commands. This will cause the system to reattempt the name resolution process between the IP interface and the VPLS service.

The **no** form of this command resets the allow-ip-int-bind flag on the VPLS service. If the VPLS service currently has an IP interface from an IES or VPRN service attached, the no allow-ip-int-bind command will fail. Once the allow-ip-int-bind flag is reset on the VPLS service, the configuration and hardware restrictions associated with setting the flag are removed. The port network mode hardware restrictions are also removed.

Platforms All

5.210 allow-ipv6-udp-checksum-zero

allow-ipv6-udp-checksum-zero

Syntax [**no**] **allow-ipv6-udp-checksum-zero**

Context **[Tree]** (config>router>twamp-light>reflector allow-ipv6-udp-checksum-zero)
[Tree] (config>service>vprn>twamp-light>reflector allow-ipv6-udp-checksum-zero)
[Tree] (config>test-oam>link-meas>template>twl allow-ipv6-udp-checksum-zero)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router twamp-light reflector allow-ipv6-udp-checksum-zero
configure service vprn twamp-light reflector allow-ipv6-udp-checksum-zero
configure test-oam link-measurement measurement-template twamp-light allow-ipv6-udp-checksum-zero

Description This command configures the acceptance of IPv6 packets with UDP checksums of 0.This optional configuration allows the router to process arriving IPv6 TWAMP Test packets that contain IPv6 UDP checksum of 0x0000. The UDP port specific to this TWAMP Light test bypasses the default discard IPv6 UDP checksum 0x0000. If this optional command is not configured, IPv6 UDP checksum 0x000 arriving packets are discarded.

The **no** form of this command reverts to the default value, discarding packets that arrive with an IPv6 UDP checksum of 0x0000.

Default no allow-ipv6-udp-checksum-zero

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.211 allow-lease-query

allow-lease-query

Syntax [**no**] **allow-lease-query**

Context **[Tree]** (config>router>dhcp6>server allow-lease-query)
[Tree] (config>service>vprn>dhcp6>server allow-lease-query)

Full Context configure router dhcp6 local-dhcp-server allow-lease-query
configure service vprn dhcp6 local-dhcp-server allow-lease-query

Description If enabled, the local DHCPv6 server will handle and reply to lease query messages.

The **no** form of this command disables lease query support.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.212 allow-list

allow-list

Syntax **allow-list** *allow-list-name*
no allow-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>url-filter>local-filtering allow-list)

Full Context configure application-assurance group url-filter local-filtering allow-list

Description This command adds an allow-list URL list to the local filtering URL filter policy.

The **no** form of this command removes the URL list object.

Default no allow-list

Parameters *allow-list-name* — Specifies the URL list name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.213 allow-local-management

allow-local-management

Syntax [**no**] **allow-local-management**

Context [Tree] (config>service>vprn>grt-lookup>enable-grt allow-local-management)

Full Context configure service vprn grt-lookup enable-grt allow-local-management

Description Enables the support of specific management protocols over VPRN interfaces that terminate on Base routing context IPv4 and IPv6 interface addresses, including Base loopback and system addresses. Global Routing Table (GRT) leaking is used to enable visibility/access of the Base interface addresses in the VPRN. The supported protocols are Telnet, FTP, SNMP, TACACS+, RADIUS (IPv4 only, not IPv6), and SSH (including applications that ride over the standard SSH TCP port 22 such as SCP and SFTP). NETCONF is supported when configured to run over the standard SSH TCP port 22, but not when it is configured to run over the NETCONF standard TCP port 830.

Ping and traceroute responses from the Base router interfaces are supported and are not configurable.

The **allow-local-management** command does not control the support for management protocols terminating on VPRN interfaces directly. See Node Management Using VPRN for more information. Also, see the **access** command in the **config**>**service**>**vprn**>**snmp** context, and the commands in the **config**>**service**>**vprn**>**management** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.214 allow-multiple-wan-addresses

allow-multiple-wan-addresses

Syntax [**no**] **allow-multiple-wan-addresses**

Context **[Tree]** (config>service>ies>sub-if>ipv6 allow-multiple-wan-addresses)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 allow-multiple-wan-addresses)
[Tree] (config>service>vprn>sub-if>ipv6 allow-multiple-wan-addresses)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 allow-multiple-wan-addresses)

Full Context configure service ies subscriber-interface group-interface ipv6 allow-multiple-wan-addresses
configure service ies subscriber-interface ipv6 allow-multiple-wan-addresses
configure service vprn subscriber-interface group-interface ipv6 allow-multiple-wan-addresses
configure service vprn subscriber-interface ipv6 allow-multiple-wan-addresses

Description This command enables host to have two WAN addresses, one from DHCP IA_NA and one from SLAAC assignment.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.215 allow-netconf

allow-netconf

Syntax [**no**] **allow-netconf**

Context **[Tree]** (config>system>security>management allow-netconf)

Full Context configure system security management allow-netconf

Description This command allows access to the NETCONF server from Base and Management routers if it is operationally up.

The **no** form of this command disallows access to the NETCONF server.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

allow-netconf

Syntax [**no**] **allow-netconf**

Context **[Tree]** (config>service>vprn>management allow-netconf)

Full Context configure service vprn management allow-netconf

Description This commands allows access to the NETCONF server from VPRN.

The **no** form of this command removes NETCONF access for this VPRN.

Platforms All

5.216 allow-qinq-network-interface

allow-qinq-network-interface

Syntax [**no**] **allow-qinq-network-interface**

Context **[Tree]** (config>system>ip allow-qinq-network-interface)

Full Context configure system ip allow-qinq-network-interface

Description This command is a system-wide option that allows the creation of network interfaces on a QinQ encapsulated VLAN.

When enabled, the maximum number of allowed MPLS labels is reduced by 1 to allow for the additional VLAN tag at egress processing.

The **no** form of this command reverts the option to the default value, which is to not allow network interfaces on QinQ encapsulated VLANs.

Default no allow-qinq-network-interface

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.217 allow-reverse-route-override

allow-reverse-route-override

Syntax **allow-reverse-route-override** [*type*]
no allow-reverse-route-override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>ipsec allow-reverse-route-override)

Full Context configure service vprn ipsec allow-reverse-route-override

Description This command allows a new dynamic LAN-to-LAN tunnel that terminates in the private VPRN service to be created with an overlapping reverse route.

The **no** form of this command reverts to the default value.

Default no allow-reverse-route-override

Parameters *type* — Specifies the action to take when the system accepts a new reverse route.

Values same-idi — Specifies that the system accepts a new reverse route and removes the existing route only if the IDi of the new tunnel is the same as existing route.

any-idi — Specifies that the system accepts a new reverse route and removes the existing route regardless of the IDi.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.218 allow-ssh

allow-ssh

Syntax [**no**] **allow-ssh**

Context [Tree] (config>service>vprn>management allow-ssh)

Full Context configure service vprn management allow-ssh

Description This command allows configuration of the SSH parameters.

The **no** form of this command disallows configuration of the SSH parameters.

Platforms All

allow-ssh

Syntax [**no**] **allow-ssh**

Context [Tree] (config>system>security>management allow-ssh)

Full Context configure system security management allow-ssh

Description This command allows the SSH parameters to be configured from Base and Management routers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disallows SSH parameters from being configured.

Default allow-ssh

Platforms All

5.219 allow-static

allow-static

Syntax **allow-static**
no allow-static

Context **[Tree]** (config>router>bgp>next-hop-res>labeled-routes allow-static)

Full Context configure router bgp next-hop-resolution labeled-routes allow-static

Description This command allows the BGP next-hop of label-IPv4, label-IPv6, VPN-IPv4, and VPN-IPv6 routes received from any EBGP or IBGP peer to be resolved using static routes, except for static default routes (0/0 and ::/0).

A static route is less preferred than a local or interface route for resolving the BGP next-hop of labeled route, but more preferred than other IGP routes or tunnels.

Note: A label-IPv4 or label-IPv6 route can be resolved by a static blackhole route, even when the **allow-static** command is not configured, but only if the static blackhole route is the longest prefix match (LPM) static route for the BGP next-hop address.

Default no allow-static

Platforms All

5.220 allow-telnet

allow-telnet

Syntax [**no**] **allow-telnet**

Context **[Tree]** (config>service>vprn>management allow-telnet)

Full Context configure service vprn management allow-telnet

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows access to the Telnet server from a VPRN.

The **no** form of this command removes the Telnet access.

Platforms All

allow-telnet

Syntax [**no**] **allow-telnet**

Context **[Tree]** (config>system>security>management allow-telnet)

Full Context configure system security management allow-telnet

Description This command allows access to the Telnet server from Base and Management routers if it is operationally up.

The **no** form of this command disallows access to the Telnet server.

Default allow-telnet

Platforms All

5.221 allow-telnet6

allow-telnet6

Syntax [**no**] **allow-telnet6**

Context **[Tree]** (config>service>vprn>management allow-telnet6)

Full Context configure service vprn management allow-telnet6

Description This command allows access to the Telnet IPv6 server from a VPRN.

The **no** form of this command removes the Telnet IPv6 access.

Platforms All

allow-telnet6

Syntax [**no**] **allow-telnet6**

Context **[Tree]** (config>system>security>management allow-telnet6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security management allow-telnet6

Description This command allows access to the Telnet IPv6 server from Base and Management routers if it is operationally up.

The **no** form of this command disallows access to the Telnet IPv6 server.

Default allow-telnet6

Platforms All

5.222 allow-unmatching-prefixes

allow-unmatching-prefixes

Syntax [**no**] **allow-unmatching-prefixes**

Context **[Tree]** (config>service>ies>sub-if>ipv6 allow-unmatching-prefixes)
[Tree] (config>service>vprn>sub-if>ipv6 allow-unmatching-prefixes)

Full Context configure service ies subscriber-interface ipv6 allow-unmatching-prefixes
configure service vprn subscriber-interface ipv6 allow-unmatching-prefixes

Description This command allows address assignment for IPoEv6 and PPPoEv6 hosts in cases where the subscriber host assigned IPv6 address or prefix falls outside of the subscriber-prefix range explicitly configured for the subscriber-interface (**configure>service>vprn/ies>sub-if>ipv6**) or the subscriber-prefix is not configured at all.

SLAAC hosts is installed in the FDB as /64 entries, the length of the installed DHCP-PD prefix is dictated by the prefix-length and the DHCP-NA host is installed as /128 entries.

IPv4 subscriber hosts are unaffected by this command.

The **no** form of this command reverts to the default.

Default no allow-unmatching-prefixes

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.223 allow-unmatching-subnets

allow-unmatching-subnets

Syntax [**no**] **allow-unmatching-subnets**

Context **[Tree]** (config>service>vprn>subscriber-interface allow-unmatching-subnets)

Full Context configure service vprn subscriber-interface allow-unmatching-subnets

Description This command specifies whether subscriber hosts with a subnet that does not match any of the subnets configured on this interface, are allowed.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

allow-unmatching-subnets

Syntax [**no**] **allow-unmatching-subnets**

Context **[Tree]** (config>service>ies>sub-if>ipv6 allow-unmatching-subnets)
[Tree] (config>service>vprn>sub-if>ipv6 allow-unmatching-subnets)

Full Context configure service ies subscriber-interface ipv6 allow-unmatching-subnets
configure service vprn subscriber-interface ipv6 allow-unmatching-subnets

Description This command allows address assignment for IPoEv6 and PPPoEv6 hosts in cases where the subscriber host assigned IPv6 address or prefix falls outside of the subscriber-prefix range explicitly configured for the subscriber-interface (**configure>service>vprn/ies>sub-if>ipv6**) or the subscriber-prefix is not configured at all.

SLAAC hosts are installed in the FDB as /64 entries, the length of the installed DHCP-PD prefix is dictated by the prefix-length and the DHCP-NA host is installed as /128 entries.

IPv4 subscriber hosts are unaffected by this command.

The **no** form of this command reverts to the default.

allow-unmatching-subnets

Syntax [**no**] **allow-unmatching-subnets**

Context **[Tree]** (config>service>ies>subscriber-interface allow-unmatching-subnets)

Full Context configure service ies subscriber-interface allow-unmatching-subnets

Description This command specifies whether subscriber hosts with a subnet that does not match any of the subnets configured on this interface, are allowed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.224 allow-unresolved-leaking

allow-unresolved-leaking

Syntax [**no**] **allow-unresolved-leaking**

Context **[Tree]** (config>router>bgp>next-hop-res allow-unresolved-leaking)

Full Context configure router bgp next-hop-resolution allow-unresolved-leaking

Description This command instructs BGP, in the base router instance, to allow its routes to be leaked to other (VPRN) BGP instances, even if the routes to be leaked do not have a BGP next hop that can be resolved by the base instance.

By default, BGP routes cannot be leaked to another BGP instance unless they are resolvable by the instance that receives them.

The **no** form of this command provides the default behavior.

Default no allow-unresolved-leaking

Platforms All

5.225 allow-unsecure-connection

allow-unsecure-connection

Syntax [**no**] **allow-unsecure-connection**

Context **[Tree]** (config>system>grpc allow-unsecure-connection)

Full Context configure system grpc allow-unsecure-connection

Description This command enables unsecure operation of gRPC connections. This means that TCP connections are not encrypted, including username and password information.

This command can be enabled only if there is no TLS profile assigned to the gRPC server.

The **no** form of this command enables TLS encryption on gRPC connections.

Default no allow-unsecure-connection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

allow-unsecure-connection

Syntax [**no**] **allow-unsecure-connection**

Context **[Tree]** (config>system>management-interface>remote-management allow-unsecure-connection)

Full Context configure system management-interface remote-management allow-unsecure-connection

Description This command enables unsecure operation of all remote manager connections. In an unsecured operation, connections are not encrypted, including the username and password information.

This command and **client-tls-profile** are mutually exclusive. This means it can be used only if there are no TLS profiles assigned to the server.

If this command is also configured in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command disables unsecured connections.

Default no allow-unsecure-connection

Platforms All

allow-unsecure-connection

Syntax [**no**] **allow-unsecure-connection**

Context **[Tree]** (config>system>management-interface>remote-management>manager allow-unsecure-connection)

Full Context configure system management-interface remote-management manager allow-unsecure-connection

Description This command enables an unsecure connection for a specific remote manager.

This command and **client-tls-profile** are mutually exclusive.

This command takes precedence over the same command configured in the **config**>**system**>**management-interface**>**remote-management** context, if applicable.

The **no** form of this command disables unsecured connections for the specified manager.

Default no allow-unsecure-connection

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

allow-unsecure-connection

Syntax [**no**] **allow-unsecure-connection**

Context **[Tree]** (config>system>telemetry>destination-group allow-unsecure-connection)

Full Context configure system telemetry destination-group allow-unsecure-connection

Description This command enables an unsecured connection for a specified destination group.

This command is mutually exclusive with the **tls-client-profile** command.

The **no** form of this command disables unsecured connections for the specified destination group.

Default no allow-unsecure-connection

Platforms All

allow-unsecure-connection

Syntax [**no**] **allow-unsecure-connection**

Context **[Tree]** (config>system>grpc-tunnel>destination-group allow-unsecure-connection)

Full Context configure system grpc-tunnel destination-group allow-unsecure-connection

Description This command enables an unsecured connection for a specified destination group, which allows a gRPC tunnel to run without a secured transport protocol. Data is transferred in unencrypted form.

This command is mutually exclusive with the **tls-client-profile** command.

The **no** form of this command disables unsecured connections for the specified destination group.

Default no allow-unsecure-connection

Platforms All

5.226 allow-unsecured-msgs

allow-unsecured-msgs

Syntax [**no**] **allow-unsecured-msgs**

Context **[Tree]** (config>service>ies>if>ipv6>secure-nd allow-unsecured-msgs)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface ipv6 secure-nd allow-unsecured-msgs

Description This command specifies whether unsecured messages are accepted. When Secure Neighbor Discovery (SeND) is enabled, only secure messages are accepted by default.

The **no** form of this command disables accepting unsecured messages.

Platforms All

allow-unsecured-msgs

Syntax [**no**] **allow-unsecured-msgs**

Context **[Tree]** (config>service>vprn>if>secure-nd allow-unsecured-msgs)

Full Context configure service vprn interface secure-nd allow-unsecured-msgs

Description This command specifies whether unsecured messages are accepted. When Secure Neighbor Discovery (SeND) is enabled, only secure messages are accepted by default.

The **no** form of this command disables accepting unsecured messages.

allow-unsecured-msgs

Syntax [**no**] **allow-unsecured-msgs**

Context **[Tree]** (config>router>if>ipv6>secure-nd allow-unsecured-msgs)

Full Context configure router interface ipv6 secure-nd allow-unsecured-msgs

Description This command specifies whether unsecured messages are accepted. When Secure Neighbor Discovery (SeND) is enabled, only secure messages are accepted by default.

The **no** form of this command disables accepting unsecured messages.

Platforms All

5.227 allow-user-name

allow-user-name

Syntax [**no**] **allow-user-name**

Context **[Tree]** (config>system>security>password>complexity-rules allow-user-name)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security password complexity-rules allow-user-name

Description The user name is allowed to be used as part of the password.

The **no** form of this command does not allow user name to be used as password.

Default no allow-user-name

Platforms All

5.228 allowed-peer-as

allowed-peer-as

Syntax [**no**] **allowed-peer-as** *min-as-number* [**max** *max-as-number*]

Context **[Tree]** (config>service>vprn>bgp>group>dynamic-neighbor>match>prefix allowed-peer-as)

Full Context configure service vprn bgp group dynamic-neighbor match prefix allowed-peer-as

Description This command configures a single peer AS value or a contiguous range of peer AS values to associate with a prefix from which dynamic BGP sessions can be accepted.

If an incoming dynamic BGP session is associated with the prefix then the peer's AS, as reported in the OPEN message, is checked against the list of allowed-peer-as values. If the peer AS is not contained in one of the **allowed-peer-as** commands, then the connection is rejected with a Bad_Peer_AS error. If there is no **allowed-peer-as** configuration in the matched prefix, then the ASN in the peer's OPEN message, is checked against the group level peer-as.

The **no** form of this command removes an allowed-peer-as entry.

Default no allowed-peer-as

Parameters *min-as-number* — Specifies an allowed peer AS value as well as the start of an allowed range if the *max-as-number* value is also configured.

Values 1 to 4294967295

max-as-number — Specifies the end of an allowed range.

Values 1 to 4294967295

Platforms All

allowed-peer-as

Syntax [**no**] **allowed-peer-as** *min-as-number* [**max** *max-as-number*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp>group>dynamic-neighbor>match>prefix allowed-peer-as)

Full Context configure router bgp group dynamic-neighbor match prefix allowed-peer-as

Description This command configures a single peer AS value or a contiguous range of peer AS values to associate with a prefix from which dynamic BGP sessions can be accepted.

If an incoming dynamic BGP session is associated with the prefix, then the peer's AS, as reported in the OPEN message, is checked against the list of allowed-peer-as values. If the peer AS is not contained in one of the **allowed-peer-as** commands, then the connection is rejected with a Bad_Peer_AS error. If there is no **allowed-peer-as** configuration in the matched prefix, then the ASN in the peer's OPEN message, is checked against the group level peer-as.

The **no** form of this command removes an allowed-peer-as entry.

Default no allowed-peer-as

Parameters *min-as-number* — Specifies an allowed peer AS value as well as the start of an allowed range if the *max-as-number* value is also configured.

Values 1 to 4294967295

max-as-number — Specifies the end of an allowed range.

Values 1 to 4294967295

Platforms All

5.229 allowed-source-macs

allowed-source-macs

Syntax **allowed-source-macs**

Context [Tree] (config>port>ethernet>dot1x>per-host-authentication allowed-source-macs)

Full Context configure port ethernet dot1x per-host-authentication allowed-source-macs

Description Commands in this context add the source MAC addresses of the hosts to the allowed MAC list.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.230 already-signed-in

already-signed-in

Syntax [**no**] **already-signed-in**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state already-signed-in)

Full Context configure subscriber-mgmt wlan-gw ue-query state already-signed-in

Description This command enables matching on UEs that are already signed in.

The **no** form of this command disables matching on UEs that are already signed in, unless all state matching is disabled.

Default no already-signed-in

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.231 alt-port-class-pools

alt-port-class-pools

Syntax **alt-port-class-pools**

Context **[Tree]** (config>qos>hs-port-pool-policy alt-port-class-pools)

Full Context configure qos hs-port-pool-policy alt-port-class-pools

Description Commands in this context configure alternate port class pools parameters. Within this context, the corresponding port-class pools can be associated with a mid-pool, explicitly sized as a percentage of the mid-pool size, dynamically sized based on relative port bandwidth, or have a slope policy applied.

Platforms 7750 SR-7/12/12e

5.232 always-compare-med

always-compare-med

Syntax **always-compare-med** {**zero** | **infinity**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no always-compare-med strict-as {**zero** | **infinity**}
no always-compare-med

Context [Tree] (config>router>bgp>best-path-selection always-compare-med)
[Tree] (config>service>vprn>bgp>path-selection always-compare-med)

Full Context configure router bgp best-path-selection always-compare-med
configure service vprn bgp best-path-selection always-compare-med

Description This command configures the comparison of BGP routes based on the MED attribute. The default behavior of SR OS (equivalent to the **no** form of this command) is to only compare two routes on the basis of MED if they have the same neighbor AS (the first non-confed AS in the received AS_PATH attribute). Also by default, a route without a MED attribute is handled the same as though it had a MED attribute with the value 0. The **always-compare-med** command without the **strict-as** keyword allows MED to be compared even if the paths have a different neighbor AS; in this case, if neither **zero** nor **infinity** is specified, the **zero** option is inferred, meaning a route without a MED is handled the same as though it had a MED attribute with the value 0. When the **strict-as** keyword is present, MED is only compared between paths from the same neighbor AS, and in this case, **zero** or **infinity** is mandatory and tells BGP how to interpret paths without a MED attribute.

Default no always-compare-med

Parameters **zero** — Specifies that for routes learned without a MED attribute that a zero (0) value is used in the MED comparison. The routes with the lowest metric are the most preferred.

infinity — Specifies for routes learned without a MED attribute that a value of infinity (2^32-1) is used in the MED comparison. This in effect makes these routes the least desirable.

strict-as — Specifies that the BGP MED values are only compared if the route comes from the same neighbor AS.

Platforms All

5.233 always-set-sender-for-ir

always-set-sender-for-ir

Syntax [**no**] **always-set-sender-for-ir**

Context [Tree] (config>system>security>pki>ca-profile>cmpv2 always-set-sender-for-ir)

Full Context configure system security pki ca-profile cmpv2 always-set-sender-for-ir

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies to always set the sender field in CMPv2 header of all Initial Registration (IR) messages with the subject name. By default, the sender field is only set if an optional certificate is specified in the CMPv2 request.

Default no always-set-sender-for-ir

Platforms All

5.234 amber-alarm-threshold

amber-alarm-threshold

Syntax **amber-alarm-threshold** *percentage*
no amber-alarm-threshold

Context **[Tree]** (config>port>access>egress>pool amber-alarm-threshold)
[Tree] (config>port>access>ingress>pool amber-alarm-threshold)
[Tree] (config>port>network>egress>pool amber-alarm-threshold)

Full Context configure port access egress pool amber-alarm-threshold
configure port access ingress pool amber-alarm-threshold
configure port network egress pool amber-alarm-threshold

Description This command configures the threshold for the amber alarm on the over-subscription allowed.

Users can selectively enable amber or red alarm thresholds. But if both are enabled (non-zero), the amber alarm threshold cannot be more than the red alarm threshold.

The **no** form of this command reverts to the default value.

Default no amber-alarm-threshold

Parameters *percentage* — Specifies the amber alarm threshold.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

amber-alarm-threshold

Syntax **amber-alarm-threshold** *percentage*
no amber-alarm-threshold

Context **[Tree]** (config>card>fp>ingress>network>pool amber-alarm-threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure card fp ingress network pool amber-alarm-threshold

Description This command configures the threshold for the amber alarm on the over-subscription allowed.

Users can selectively enable amber or red alarm thresholds. But if both are enabled (non-zero) then the red alarm threshold must be greater than the amber alarm threshold.

The **no** form of this command reverts to the default value.

Default no amber-alarm-threshold

Parameters *percentage* — Specifies the amber alarm threshold.

Values 1 to 1000

Platforms All

5.235 ambr

ambr

Syntax **ambr down-link** *down-link-kbps* **up-link** *up-link-kbps*
no ambr

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile>ggsn>qos ambr)
[Tree] (config>subscr-mgmt>gtp>peer-profile>pgw>qos ambr)
[Tree] (config>subscr-mgmt>gtp>peer-profile>mme>qos ambr)

Full Context configure subscriber-mgmt gtp peer-profile ggsn qos ambr
configure subscriber-mgmt gtp peer-profile mme qos ambr
configure subscriber-mgmt gtp peer-profile pgw qos ambr

Description This command configures the Aggregated Maximum Bit Rate (AMBR) to be sent in the APN AMBR IE. The contents of this IE can be overridden by RADIUS or report-rate mechanisms. If those mechanisms specify a partial value, such as only specifying the **down-link** parameter, the other value is picked up from the **ambr** configuration.

For GTPv1, the **no** form of this command implies that the IE will not be sent. If a partial value is received from another source, the missing value will use the following defaults:

- 10000 kb/s up-link
- 20000 kb/s down-link

For GTPv2, the **no** form of this command reverts to the default of 10000 kb/s up-link and 20000 kb/s down-link.

Default no ambr - for ggsn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ambr down-link 20000 up-link 10000 - for mme and pgw

Parameters *down-link-kbps* — Specifies the downlink AMBR.

Values 0 to 10000000

up-link-kbps — Specifies the uplink AMBR.

Values 0 to 10000000

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.236 ambr-qos-mapping

ambr-qos-mapping

Syntax **ambr-qos-mapping**

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn ambr-qos-mapping)

Full Context configure subscriber-mgmt gtp apn-policy apn ambr-qos-mapping

Description Mapping of an incoming APN-AMBR to SR OS QoS overrides.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.237 an-gw-address

an-gw-address

Syntax [**no**] **an-gw-address**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp an-gw-address)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp an-gw-address

Description This command configures the IPv4 address of the node.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.238 analyze-gre-payload

analyze-gre-payload

Syntax [**no**] **analyze-gre-payload**

Context **[Tree]** (config>cflowd analyze-gre-payload)

Full Context configure cflowd analyze-gre-payload

Description This command enables cflowd analysis of the inner IP packet in a sampled GRE packet that is transiting the local router.

If the GRE packet terminates on the local node, the inner IP payload is analyzed and reported using existing IPv4 or IPv6 flow templates. This behavior is not affected by this command.

If this parameter is enabled and a GRE packet is transiting the local node, the inner payload is reported using the GRE Flow Template. (Template ID 308 or 309)

This behavior is only supported with V10 (IPFIX) collectors.

The **no** form of this command disables cflowd analysis of the inner IP packet in a sampled GRE packet.

Platforms All

5.239 analyze-l2tp-traffic

analyze-l2tp-traffic

Syntax [**no**] **analyze-l2tp-traffic**

Context **[Tree]** (config>cflowd analyze-l2tp-traffic)

Full Context configure cflowd analyze-l2tp-traffic

Description This command causes cflowd to look for and analyze the inner IP header of an L2TPv2 frame.

L2TPv2 traffic is identified by either the source or destination UDP port numbering that is set to 1701.

The **no** form of this command disables this function.

Default no analyze-l2tp-traffic

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.240 analyze-v4overv6-traffic

analyze-v4overv6-traffic

Syntax [**no**] **analyze-v4overv6-traffic**

Context **[Tree]** (config>cflowd analyze-v4overv6-traffic)

Full Context configure cflowd analyze-v4overv6-traffic

Description This command causes cflowd to look for and analyze the inner IPv4 header of IPv4overIPv6 frames that include MAP-E as well as DS-Lite and SAM traffic.

The **no** form of this command disables this function.

Default no analyze-v4overv6-traffic

Platforms All

5.241 analyzer

analyzer

Syntax [**no**] **analyzer**

Context **[Tree]** (config>isa>video-group analyzer)

Full Context configure isa video-group analyzer

Description This command specifies whether or not the video analyzer is enabled for all streams on this video group.

The **no** form of the command disables the analyzer for the group.

Default no analyzer

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

analyzer

Syntax [**no**] **analyzer**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video analyzer)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video analyzer)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video analyzer)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer
configure mcast-management multicast-info-policy bundle channel video analyzer
configure mcast-management multicast-info-policy bundle video analyzer

Description This command enables or disables the analyzer for the group.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

5.242 ancp

ancp

Syntax **ancp**

Context [Tree] (config>subscr-mgmt ancp)
[Tree] (config>subscr-mgmt>sub-prof ancp)

Full Context configure subscriber-mgmt ancp
configure subscriber-mgmt sub-profile ancp

Description Commands in this context configure Access Node Control Protocol (ANCP) parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ancp

Syntax **ancp**

Context [Tree] (config>service>vpls>gsmp>group ancp)
[Tree] (config>service>vprn>gsmp>group ancp)

Full Context configure service vpls gsmp group ancp
configure service vprn gsmp group ancp

Description Commands in this context configure Access Node Control Protocol (ANCP) parameters for this GSMP group.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ancp

Syntax [**no**] **ancp**

Context **[Tree]** (config>service>vprn>gsmp>group ancp)

Full Context configure service vprn gsmp group ancp

Description Commands in this context configure ANCP parameters for this GSMP group.

The **no** form of this command disables the ANCP parameters configured in this context.

Platforms All

ancp

Syntax **ancp ancp-string** *ancp-string* **loopback** [**count** *send-count*] [**timeout** *timeout*] [**alarm**]
ancp subscriber *sub-ident-string* **loopback** [**count** *send-count*] [**timeout** *timeout*] [**alarm**]

Context **[Tree]** (oam ancp)

Full Context oam ancp

Description This command sends an OAM request to the access node. ANCP can be used to send OAM messages to the access node. The access node must be able to accept these messages and signals such support by the capability negotiations. If the operator attempts to send an OAM command to an access node that does not support, the operation results in an error.

Parameters *ancp-string* — Specifies an existing ANCP string, up to 63 characters.

loopback — Sends an OAM loopback test request to the access node.

send-count — Specifies the number of messages the access node uses to test the circuit. If omitted, the number is determined by the access node via local policy.

Values 1 to 32

timeout — Specifies the length of time, in seconds, that the controlling node waits for a result.

Values 1 to 255

alarm — Specifies that the CLI the result is returned to the CLI and a trap is issued to indicate the test has finished. If the flag is used through SNMP the results are available in the results MIB and after the node sends the trap to indicate the results are ready.

sub-ident-string — Specifies an existing subscriber-id, up to 32 characters. The node uses the *ancp-string* value associated with the provided subscriber-id to identify the circuit.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ancp

Syntax **ancp**

Context **[Tree]** (config>system>persistence ancp)

Full Context configure system persistence ancp

Description This command configures ANCP persistence parameters.

Platforms All

5.243 ancp-policy

ancp-policy

Syntax **ancp-policy** *policy-name* [**create**]
no ancp-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt>ancp ancp-policy)

Full Context configure subscriber-mgmt ancp ancp-policy

Description This command creates an Access Node Control Protocol (ANCP) policy. The policy is associated with either the ANCP string (static case) or subscriber-profile (dynamic case) and defines the behavior of the hosts belonging to these profiles.

ANCP policies control rates and subscribers based on port-up/port-down messages from the access node. When configured, the 7450 ESS or 7750 SR should stop SHCV to a host that is part of a port defined to be down (by port-down message). When the node receives a port-up message for a port that was in port-down state, the node will initiate the SHCV process immediately to verify connectivity.

When ANCP is used with Enhanced Subscriber Management, the ANCP string last associated with the subscriber is used. All hosts of a subscriber is updated with the new ANCP string.

The **no** form of this command removes the policy name from the ANCP configuration.

Parameters *policy-name* — Configures the ANCP policy name, up to 32 characters.

create — Keyword used to create the ANCP policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ancp-policy

Syntax **ancp-policy** *name*

Context **[Tree]** (config>subscr-mgmt>sub-prof>ancp ancp-policy)

Full Context configure subscriber-mgmt sub-profile ancp ancp-policy

Description This command specifies an existing Access Node Control Protocol (ANCP) policy to associate with the subscriber profile. The policy is associated with either the ANCP string (static case) or subscriber-profile (dynamic case) and defines the behavior of the hosts belonging to these profiles.

The **no** form of this command removes the policy name from the ANCP configuration.

Parameters *name* — Specifies an existing ANCP policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.244 ancp-static-map

ancp-static-map

Syntax **ancp-static-map**

Context **[Tree]** (config>subscr-mgmt>ancp ancp-static-map)

Full Context configure subscriber-mgmt ancp ancp-static-map

Description Commands in this context configure a static ANCP name map.

Default ancp-static-map

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.245 ancp-string

ancp-string

Syntax **ancp-string** *ancp-string*
no ancp-string

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings ancp-string)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings ancp-string)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings ancp-string
configure subscriber-mgmt local-user-db ppp host identification-strings ancp-string

Description This command specifies the ANCP string which is encoded in the identification strings.

The **no** form of this command returns to the default.

Parameters *ancp-string* — Specifies the ANCP string, up to 63 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ancp-string

Syntax **ancp-string** *ancp-string*
no ancp-string

Context [Tree] (config>service>ies>if>sap>static-host ancp-string)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host ancp-string)
[Tree] (config>service>vpls>sap>static-host ancp-string)
[Tree] (config>service>vprn>if>sap>static-host ancp-string)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host ancp-string)

Full Context configure service ies interface sap static-host ancp-string
configure service ies subscriber-interface group-interface sap static-host ancp-string
configure service vpls sap static-host ancp-string
configure service vprn interface sap static-host ancp-string
configure service vprn subscriber-interface group-interface sap static-host ancp-string

Description This command specifies the ANCP string associated to this SAP host.

The **no** form of this command reverts to the default.

Parameters *ancp-string* — Specifies the ANCP string up to 63 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.246 anno-rx-timeout

anno-rx-timeout

Syntax **anno-rx-timeout** *count*
no anno-rx-timeout

Context [Tree] (config>system>ptp anno-rx-timeout)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system ptp anno-rx-timeout

Description This command configures the announceReceiptTimeout value for all peer associations. This defines the number of Announce message intervals that must expire with no received Announce messages before declaring an ANNOUNCE_RECIPT_TIMEOUT event.

The **announce-rx-timeout** cannot be changed unless PTP is shut down.

Default anno-rx-timeout 3

Parameters *count* — Specifies the announce packet interval, in log form.

Values 2 to 10

Default 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.247 announce

announce

Syntax [**no**] **announce**

Context **[Tree]** (config>service>nat>pcp-server-policy>opcode announce)

Full Context configure service nat pcp-server-policy opcode announce

Description This command enables/disables support for the **announce** opcode.

Default no announce

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.248 anti-spoof

anti-spoof

Syntax **anti-spoof** *type*
no anti-spoof

Context **[Tree]** (config>service>ies>sap anti-spoof)
[Tree] (config>service>vpls>sap anti-spoof)
[Tree] (config>service>ies>sub-if>grp-if>pppoe anti-spoof)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>sap anti-spoof)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters anti-spoof)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe anti-spoof)
[Tree] (config>service>vprn>sub-if>grp-if>sap anti-spoof)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters anti-spoof)
[Tree] (config>subscr-mgmt>msap-policy>ies-vprn-only-sap-parameters anti-spoof)

Full Context

configure service ies sap anti-spoof
configure service ies subscriber-interface group-interface pppoe anti-spoof
configure service ies subscriber-interface group-interface sap anti-spoof
configure service ies subscriber-interface group-interface sap-parameters anti-spoof
configure service vpls sap anti-spoof
configure service vprn subscriber-interface group-interface pppoe anti-spoof
configure service vprn subscriber-interface group-interface sap anti-spoof
configure service vprn subscriber-interface group-interface sap-parameters anti-spoof
configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters anti-spoof

Description

This command enables anti-spoof filtering and optionally changes the anti-spoof matching type for the SAP.

The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to lookup an entry in the anti-spoof filter table. The type parameter (**ip**, **mac**, **ip-mac**) defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

Enabling anti-spoof filtering on a subscriber-facing SAP causes the anti-spoof table to be populated with all static and dynamic host information available on the SAP. Enabling anti-spoof filtering on the SAP will fail if any static hosts are defined without the proper addresses specified for the selected anti-spoof filter type.

When enabled, forwarding IP packets that ingress the SAP is dependent on a successful anti-spoof table match with an entry in the table. DHCP and non-IP packets (including ARP) are not subject to anti-spoof filtering. If an entry does not match the ingress packet, the packet is silently discarded while incrementing the SAP discard counter.

Anti-spoof filtering is only allowed on VPLS SAPs, IES SAP-based IP interfaces, and VPRN SAP-based IP interfaces. Anti-spoof filtering is not available on IES or VPRN SDP bound IP interfaces. Anti-spoof filtering is not supported on Epipe and other VLL type services. Support for anti-spoofing is dependent on SAP based service interfaces. Note VPRN and VLL are supported on the 7750 SR only.

Note: Anti-spoofing filters, with type **ip-mac**, must be enabled to perform Enhanced Subscriber Management (as described in the Triple Play Enhanced Subscriber Management section).

The **no** form of this command disables anti-spoof filtering on the SAP.

Default

no anti-spoof

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *type* — Specifies the anti-spoof filtering type for this SAP.

Values ip — Specifies to use only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the **anti-spoof ip** command fails.

ip-mac — Specifies to use both the source IP address and the source MAC address in its lookup.

mac — Specifies to use only the source MAC address in its lookup. If a static host exists on the SAP without a specified MAC address, the **anti-spoof mac** command fails.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap anti-spoof
- configure service ies subscriber-interface group-interface sap anti-spoof
- configure service ies subscriber-interface group-interface pppoe anti-spoof
- configure service vpls sap anti-spoof
- configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters anti-spoof
- configure service vprn subscriber-interface group-interface pppoe anti-spoof

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap-parameters anti-spoof
- configure service ies subscriber-interface group-interface sap-parameters anti-spoof

anti-spoof

Syntax **anti-spoof** *pppoe-anti-spoofing-type*
no anti-spoof

Context **[Tree]** (config>service>ies>sub-if>grp-if>pppoe anti-spoof)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe anti-spoof)

Full Context configure service ies subscriber-interface group-interface pppoe anti-spoof
configure service vprn subscriber-interface group-interface pppoe anti-spoof

Description This command specifies the type of PPPoE anti-spoof filtering to use.

The **no** form of this command reverts to the default.

Default anti-spoof mac-sid

Parameters *pppoe-anti-spoofing-type* — Specifies the PPPoE anti-spoof filtering.

Values mac-sid, mac-sid-ip

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

anti-spoof

Syntax **anti-spoof** {**ip** | **ip-mac** | **nh-mac**}
no anti-spoof

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap anti-spoof)
[Tree] (config>service>vprn>sub-if>grp-if>sap anti-spoof)

Full Context configure service ies subscriber-interface group-interface sap anti-spoof
configure service vprn subscriber-interface group-interface sap anti-spoof

Description This command configures the anti-spoof type of the MSAP.

The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to lookup an entry in the anti-spoof filter table. The type parameter (**ip**, **ip-mac**) defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

The **no** form of this command reverts to the default.

Note: For IES and VPRN subscriber group interfaces, setting no anti-spoof sets the default anti-spoofing type which is **ip-mac**.

Parameters **ip** — Configures SAP anti-spoof filtering to use only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the anti-spoof type **ip** command fails.

Note: This parameter is not applicable in the **config>subscr-mgmt>msap-policy** context.

ip-mac — Configures SAP anti-spoof filtering to use both the source IP address and the source MAC address in its lookup. The anti-spoof type **ip-mac** command fails if the default anti-spoof filter type of the SAP is **ip-mac** and the default is not overridden, or if the SAP does not support Ethernet encapsulation.

nh-mac — Indicates that the ingress anti-spoof is based on the source MAC and egress anti-spoof is based on the nh-ip-address .

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

anti-spoof

Syntax **anti-spoof** *type*
no anti-spoof

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap anti-spoof)
[Tree] (config>service>vpls>sap anti-spoof)
[Tree] (config>service>vprn>if>sap anti-spoof)

Full Context configure service ies interface sap anti-spoof
configure service vpls sap anti-spoof
configure service vprn interface sap anti-spoof

Description This command enables anti-spoof filtering and optionally changes the anti-spoof matching type for the SAP.

The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to lookup an entry in the anti-spoof filter table. The type parameter (**ip**, **mac**, **ip-mac**) defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

The **no** form of the command disables anti-spoof filtering on the SAP.

Default no anti-spoof

Parameters *type* — Specifies the anti-spoof filtering type for this SAP.

Values ip — Configures SAP anti-spoof filtering to use only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the anti-spoof type **ip** command fails.

ip-mac — Configures SAP anti-spoof filtering to use both the source IP address and the source MAC address in its lookup. If a static host exists on the SAP without both the IP address and MAC address specified, the anti-spoof type **ip-mac** command fails. This is also true if the default anti-spoof filter type of the SAP is **ip-mac** and the default is not overridden. The anti-spoof type **ip-mac** command will also fail if the SAP does not support Ethernet encapsulation.

mac — Configures SAP anti-spoof filtering to use only the source MAC address in its lookup. Setting the anti-spoof filter type to **mac** is not allowed on non-Ethernet encapsulated SAPs. If a static host exists on the SAP without a specified MAC address, the anti-spoof type **mac** command fails. The anti-spoof type **mac** command will also fail if the SAP does not support Ethernet encapsulation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

anti-spoof

Syntax **anti-spoof** {**ip** | **mac** | **ip-mac** | **nh-mac**}
no anti-spoof-type

Context [Tree] (config>service>vprn>if>sap anti-spoof)

Full Context configure service vprn interface sap anti-spoof

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables anti-spoof filtering and optionally changes the anti-spoof matching type for the interface.

The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to lookup an entry in the anti-spoof filter table. The type parameter (**ip**, **mac**, **ip-mac, nh-mac**) defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

The **no** form of this command reverts to the default.

Default Filter type default types:

- anti-spoof ip (Non-Ethernet encapsulated SAP)
- anti-spoof ip-mac (Ethernet encapsulated SAP)
- no anti-spoof-type (other SAPs)

Parameters **ip** — Configures SAP anti-spoof filtering to use only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the anti-spoof type **ip** command fails.

mac — Configures SAP anti-spoof filtering to use only the source MAC address in its lookup. Setting the anti-spoof filter type to **mac** is not allowed on non-Ethernet encapsulated SAPs. If a static host exists on the SAP without a specified MAC address, the anti-spoof type **mac** command fails. The anti-spoof type **mac** command will also fail if the SAP does not support Ethernet encapsulation.

ip-mac — Configures SAP anti-spoof filtering to use both the source IP address and the source MAC address in its lookup. If a static host exists on the SAP without both the IP address and MAC address specified, the anti-spoof type **ip-mac** command fails. This is also true if the default anti-spoof filter type of the SAP is **ip-mac** and the default is not overridden. The anti-spoof type **ip-mac** command will also fail if the SAP does not support Ethernet encapsulation.

nh-mac — Indicates that the ingress anti-spoof is based on the source MAC address and the egress anti-spoof is based on the nh-ip-address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

anti-spoof

Syntax [**no**] **anti-spoof**

Context **[Tree]** (config>app-assure>group>http-enrich>field anti-spoof)

Full Context configure application-assurance group http-enrich field anti-spoof

Description This command configures the HTTP header enrichment anti-spoofing functionality.

The **no** form of this command disables anti-spoofing functionality.

Default no anti-spoof

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.249 anycast

anycast

Syntax [**no**] **anycast** *rp-ip-address*

Context **[Tree]** (config>service>vprn>pim>rp anycast)

Full Context configure service vprn pim rp anycast

Description This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of this command removes the anycast instance from the configuration.

Parameters *rp-ip-address* — Configure the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no ip-address is entered then the command is simply used to enter the anycast CLI level.

Values Any valid loopback address configured on the node.

Platforms All

anycast

Syntax **anycast** *ipv6-address*
no anycast *ipv6-address*

Context **[Tree]** (config>service>vprn>pim>rp>ipv6 anycast)

Full Context configure service vprn pim rp ipv6 anycast

Description This command configures an IPv6 PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of this command removes the anycast instance from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-address* — Configures the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no address is entered then the command is simply used to enter the anycast CLI context.

Values

ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D

Platforms All

anycast

Syntax [**no**] **anycast** *rp-ip-address*

Context **[Tree]** (config>router>pim>rp anycast)

Full Context configure router pim rp anycast

Description This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of this command removes the anycast instance from the configuration.

Parameters *rp-ip-address* — Specifies the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no ip-address is entered then the command is simply used to enter the anycast CLI level.

Values Any valid loopback address configured on the node.

Platforms All

anycast

Syntax [**no**] **anycast** *ipv6-address*

Context **[Tree]** (config>router>pim>rp>ipv6 anycast)

Full Context configure router pim rp ipv6 anycast

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of this command removes the anycast instance from the configuration.

Parameters *ipv6-address* — Specifies the loopback IPv6 address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address is replaced with the new address. If no *ipv6-address* is entered then the command is simply used to enter the anycast CLI level.

Values Any valid loopback address configured on the node.

Platforms All

5.250 ap-mac-learn-failed

ap-mac-learn-failed

Syntax **ap-mac-learn-failed** {**true** | **false** | **not-specified**}

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query ap-mac-learn-failed)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ap-mac-learn-failed

Description This command specifies the matching criteria of tunnels based on whether or not learning the associated AP-MAC address last failed.

Default ap-mac-learn-failed not-specified

Parameters **true** — Specifies matching of tunnels status where learning of the AP-MAC address succeeded.

false — Specifies matching of tunnels status where learning of the AP-MAC address failed.

not-specified — Specifies no matching on the AP-MAC address learning status.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.251 apipe

apipe

Syntax **apipe** *service-id* [**customer** *customer-id*] [**vpn** *vpn-id*] [**vc-type** {**atm-vcc** | **atm-sdu** | **atm-vpc** | **atm-cell**}] [**vc-switching**] [**test**] [**create**] [**name** *name*]
no apipe *service-id*

Context **[Tree]** (config>service apipe)

Full Context configure service apipe

Description The Apipe service provides a point-to-point Layer 2 VPN connection to a remote SAP or to another local SAP. An Apipe can connect an ATM or Frame Relay endpoint either locally or over a PSN to a remote endpoint of the same type or of a different type and perform interworking between the two access technologies.

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7450 ESS or 7750 SR on which this service is defined.

Values *service-id*: 1 to 2147483647
svc-name: up to 64 characters

customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

Values 1 to 2147483647

Default null (0)

vc-type — Keyword that specifies a 15 bit value that defines the type of the VC signaled to the peer. Its values are defined in IETF Draft *draft-ietf-pwe3-iana-allocation* and it defines both the signaled VC type as well as the resulting data path encapsulation over the Apipe.

Values atm-vcc, atm-sdu, atm-vpc, atm-cell

Default atm-sdu

vc-switching — Specifies if the pseudowire switching signaling is used for the spoke SDPs configured in this service.

test — Specifies a unique test service type for the service context which will contain only a SAP configuration. The test service can be used to test the throughput and performance of a path for MPLS-TP PWs. This parameter is not supported on the 7950 XRS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name *name* — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Values *name*: up to 64 characters

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

5.252 apn

apn

Syntax **apn** *apn*
no apn

Context **[Tree]** (config>router>gtp>uplink apn)
[Tree] (config>service>vprn>gtp>uplink apn)

Full Context configure router gtp uplink apn
configure service vprn gtp uplink apn

Description This command configures the Network Identifier part of the APN.

The **no** form of this command removes the string from the configuration.

Default no apn

Parameters *apn* — Specifies the APN used for this IMSI to connect to this Mobile Gateway, up to 80 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

apn

Syntax **apn** {*apn-name* | **unknown**} [**create**]
no apn {*apn-name* | **unknown**}

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy apn)

Full Context configure subscriber-mgmt gtp apn-policy apn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the parameters that should be applied to incoming connections with the APN specified. Multiple APN nodes can be defined per APN policy.

For each APN-policy, one **unknown** APN entry can be created. This APN is used by all connections not matching another APN.

The **no** form of this command removes the APN from the policy. Only new sessions are affected by the removal.

Parameters *apn-name* — Specifies the APN name as it appears in GTP messaging, up to 80 characters.

create — Creates an *apn-name* instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

apn

Syntax [**no**] **apn**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute apn)
[Tree] (config>subscr-mgmt>auth-plcy>include-radius-attribute apn)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute apn
configure subscriber-mgmt authentication-policy include-radius-attribute apn

Description This command enables the inclusion of the APN n AAA protocols as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

apn

Syntax **apn** *apn-string*
no apn

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>imsi-apn-fltr>entry apn)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter entry apn

Description This command configures a matching condition for an APN configured as a GTP filter.

Parameters *apn-string* — Specifies the match string, which can include 1 to 32 characters.
If no APN is specified, the entry will not check for the APN IE in GTP-C packets.

Values *string*: The extracted APN must match *string* exactly.
^*string*: The extracted APN must start with *string*.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

*string***$**: The extracted APN must end with *string*.

WILDCARD_APN: Special string that indicates that the extracted APN must be "*" (that is, a length octet with value one, followed by the ASCII code for the asterisk)

EMPTY_APN: Special string that indicates that the extracted APN must be empty (that is, "")

ANY_APN: Special string that indicates that the extracted APN IE must be present and can have any value in order for the filter entry to match

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.253 apn-ambr

apn-ambr

Syntax [**no**] **apn-ambr**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp apn-ambr)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp apn-ambr

Description This command enables the inclusion of the APN-Aggregate-Max-Bitrate-DL and APN-Aggregate-Max-Bitrate-UL AVPs inside the QoS-Information AVP, as signaled in the incoming GTP message.

The **no** form of this command disables the inclusion of the AVPs.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.254 apn-ambr-dl

apn-ambr-dl

Syntax **apn-ambr-dl agg-rate**
apn-ambr-dl arbiter *arbiter-name*
apn-ambr-dl hs-sla-agg-rate
apn-ambr-dl policer *policer-id*
apn-ambr-dl queue *queue-id*
apn-ambr-dl scheduler *scheduler-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no apn-ambr-dl

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx>3gpp-qos-mapping apn-ambr-dl)

Full Context configure subscriber-mgmt diameter-application-policy gx 3gpp-qos-mapping apn-ambr-dl

Description This command configures the APN-Aggregate-Max-Bitrate-DL AVP. When enabled, the AVP is interpreted as a rate override for the specified egress QoS object. For queues and policers, the PIR is overridden.

This override uses the same QoS override mechanism as the native Gx and RADIUS-based QoS overrides. Therefore, a subsequent Gx/RADIUS-based override removes this override and an APN-AMBR based override removes any preceding Gx/RADIUS-based override.

The **no** form of this command disables the override mechanism based on APN-AMBR.

Parameters **agg-rate** — Specifies to map to an aggregate rate.

arbiter-name — Specifies the name of the arbiter to be overridden.

hs-sla-agg-rate — Specifies to map to an HS SLA aggregate rate.

policer-id — Specifies the ID of the policer to be overridden.

queue-id — Specifies the ID of the queue to be overridden.

scheduler-name — Specifies the name of the scheduler to be overridden.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.255 apn-ambr-ul

apn-ambr-ul

Syntax **apn-ambr-ul arbiter** *arbiter-name*
apn-ambr-ul policer *policer-id*
apn-ambr-ul queue *queue-id*
apn-ambr-ul scheduler *scheduler-name*
no apn-ambr-ul

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx>3gpp-qos-mapping apn-ambr-ul)

Full Context configure subscriber-mgmt diameter-application-policy gx 3gpp-qos-mapping apn-ambr-ul

Description This command configures the APN-Aggregate-Max-Bitrate-UL AVP. When enabled, the AVP is interpreted as a rate override for the specified egress QoS object. For queues and policers, the PIR is overridden.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This override uses the same QoS override mechanism as the native Gx and RADIUS-based QoS overrides. Therefore, a subsequent Gx/RADIUS-based override removes this override and an APN-AMBR based override removes any preceding Gx/RADIUS-based override.

The **no** form of this command disables the override mechanism based on APN-AMBR.

Parameters *arbiter-name* — Specifies the name of the arbiter to be overridden.

policer-id — Specifies the ID of the policer to be overridden.

queue-id — Specifies the ID of the queue to be overridden.

scheduler-name — Specifies the name of the scheduler to be overridden.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.256 apn-policy

apn-policy

Syntax **apn-policy** *apn-policy-name*
no apn-policy

Context **[Tree]** (config>router>gtp>s11>interface apn-policy)
[Tree] (config>service>vprn>gtp>s11>interface apn-policy)

Full Context configure router gtp s11 interface apn-policy
configure service vprn gtp s11 interface apn-policy

Description This command configures an Access Point Name (APN) policy for the S11 interface.

The **no** form of this command removes the APN policy.

Parameters *apn-policy-name* — Specifies the name of the policy, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

apn-policy

Syntax **apn-policy** *policy-name* [**create**]
no apn-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt>gtp apn-policy)

Full Context configure subscriber-mgmt gtp apn-policy

Description This command configures an APN policy that defines parameters to be used when setting up a new incoming GTP connection. Each APN can be mapped to its own set of parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the policy from the system. A policy can only be removed if it is not in use.

Parameters *policy-name* — Specifies the name of the policy, up to 32 characters.

create — Creates an entry.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.257 app-filter

app-filter

Syntax **app-filter**

Context **[Tree]** (config>app-assure>group>policy app-filter)

Full Context configure application-assurance group policy app-filter

Description Commands in this context configure an application filter for application assurance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.258 app-group

app-group

Syntax **app-group** *app-group-name* [*rate*]
no app-group *app-group-name*

Context **[Tree]** (config>app-assure>group>cflowd>rtp-perf app-group)
[Tree] (config>app-assure>group>cflowd>tcp-perf app-group)
[Tree] (config>app-assure>group>cflowd>comp app-group)

Full Context configure application-assurance group cflowd comprehensive app-group
configure application-assurance group cflowd rtp-performance app-group
configure application-assurance group cflowd tcp-performance app-group

Description This command configures application groups to export performance records with cflowd.

The **no** form of this command removes the parameters from the configuration.

Parameters *app-group-name* — Specifies the application group name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate — Specifies which sampling flow rate to use; flow-rate or flow-rate2.

Values flow-rate, flow-rate2

Default flow-rate

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

app-group

Syntax **app-group** *application-group-name* [**create**]
no app-group *application-group-name*

Context **[Tree]** (config>app-assure>group>policy app-group)

Full Context configure application-assurance group policy app-group

Description This command creates an application group for an application assurance policy.

The **no** form of this command deletes the application group from the configuration. All associations must be removed in order to delete a group.

Default no app-group

Parameters *application-group-name* — A string of up to 32 characters uniquely identifying this application group in the system.

create — Mandatory keyword used when creating an application group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

app-group

Syntax **app-group** *app-group-name*

Context **[Tree]** (config>app-assure>group>policy>application app-group)

Full Context configure application-assurance group policy application app-group

Description This command associates an application with an application group of an application assurance policy.

Parameters *app-group-name* — A string of up to 32 characters uniquely identifying an existing application in the system.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

app-group

Syntax **app-group** {**eq** | **neq**} *application-group-name*
no app-group

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match app-group)

Full Context configure application-assurance group policy app-qos-policy entry match app-group

Description This command adds app-group to match criteria used by this AQP entry.

The **no** form of this command removes the app-group from match criteria for this AQP entry.

Default no app-group

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

application-group-name — Specifies the name of the existing application group entry. The application-group-name is configured in the **config>app-assure>group>policy>aqp>entry>match** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

app-group

Syntax **app-group** *app-group-name* **export-using** *export-method* [*export-method*...(up to 2 max)]
app-group *app-group-name* **no-export**
no app-group *app-group-name*

Context **[Tree]** (config>app-assure>group>statistics>aa-sub app-group)

Full Context configure application-assurance group statistics aa-sub app-group

Description Commands in this context configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition.

The **no** form of this command removes the application group name.

Parameters *app-group-name* — Specifies an existing application group name, up to 32 characters.

export-method — Specifies the method of statistics export to be used.

Values accounting-policy, radius-accounting-policy

no-export — Allows the operator to enable the referred to application group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the **export-using** parameter is selected for the respective application group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Usage monitoring must be enabled at the group:partition level (**config>app-assure>group>statistics>aa-sub>usage-monitoring**) as well in order to allow any application/application group/charging group usage monitoring.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.259 app-profile

app-profile

Syntax **app-profile** *app-profile-name*
no app-profile

Context **[Tree]** (config>service>ies>if>sap app-profile)
[Tree] (config>service>ies>if>sap>static-host app-profile)
[Tree] (config>service>ies>if>spoke-sdp app-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap app-profile)
[Tree] (config>service>vpls>sap app-profile)
[Tree] (config>service>vpls>sap>static-host app-profile)
[Tree] (config>service>vpls>spoke-sdp app-profile)
[Tree] (config>service>vprn>if>sap app-profile)
[Tree] (config>service>vprn>if>sap>static-host app-profile)
[Tree] (config>service>vprn>if>spoke-sdp app-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap app-profile)

Full Context configure service ies interface sap app-profile
configure service ies interface sap static-host app-profile
configure service ies interface spoke-sdp app-profile
configure service ies subscriber-interface group-interface sap app-profile
configure service vpls sap app-profile
configure service vpls sap static-host app-profile
configure service vpls spoke-sdp app-profile
configure service vprn interface sap app-profile
configure service vprn interface sap static-host app-profile
configure service vprn interface spoke-sdp app-profile
configure service vprn subscriber-interface group-interface sap app-profile

Description This command specifies an application profile name.

The **no** form of this command reverts to the default.

Parameters *app-profile-name* — Specifies the application profile name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

app-profile

Syntax **app-profile** *app-profile-name* [**scope** *scope-type*]
no app-profile

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host app-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host app-profile)

Full Context configure service ies subscriber-interface group-interface sap static-host app-profile
configure service vprn subscriber-interface group-interface sap static-host app-profile

Description This command specifies an application profile name.

Parameters *app-profile-name* — Specifies the application profile name up to 32 characters in length.

scope-type — Specifies the scope to which the application profile is assigned in the context.

Values subscriber - The application profile applies to this context with subscriber scope (all hosts or devices).

mac - The application profile applies to this context with MAC scope (single device).

Default subscriber

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

app-profile

Syntax **app-profile** *app-profile-name*
no app-profile

Context **[Tree]** (config>service>epipe>sap app-profile)
[Tree] (config>service>epipe>spoke-sdp app-profile)
[Tree] (config>service>ipipe>sap app-profile)
[Tree] (config>service>ipipe>spoke-sdp app-profile)

Full Context configure service epipe sap app-profile
configure service epipe spoke-sdp app-profile
configure service ipipe sap app-profile
configure service ipipe spoke-sdp app-profile

Description This command configures the application profile name.

Parameters *app-profile-name* — Specifies an existing application profile name configured in the **config>app-assure>group>policy** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service epipe spoke-sdp app-profile
- configure service epipe sap app-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service ipipe spoke-sdp app-profile
- configure service ipipe sap app-profile

app-profile

Syntax **app-profile** *app-profile-name* [**create**]
no app-profile *app-profile-name*

Context **[Tree]** (config>app-assure>group>policy app-profile)

Full Context configure application-assurance group policy app-profile

Description This command creates an application profile and commands in this context configure the profile parameters.

The **no** form of this command removes the application profile from the configuration.

Parameters *app-profile-name* — Specifies the name of the application profile up to 32 characters.

create — Mandatory keyword used when creating an application profile. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

app-profile

Syntax [**no**] **app-profile**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-attributes app-profile)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-attributes app-profile

Description This command enables the subscriber app-profile attribute information to be exported in the AA subscriber's custom record.

The **no** form of this command excludes the subscriber app-profile attribute from the AA subscriber's custom record.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.260 app-profile-map

app-profile-map

Syntax **app-profile-map**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol app-profile-map)

Full Context configure subscriber-mgmt sub-ident-policy app-profile-map

Description Commands in this context configure an application profile mapping.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.261 app-profile-string

app-profile-string

Syntax **app-profile-string** *app-profile-string*
no app-profile-string

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings app-profile-string)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings app-profile-string)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings app-profile-string
configure subscriber-mgmt local-user-db ppp host identification-strings app-profile-string

Description This command specifies the application profile string which is encoded in the identification strings.

The **no** form of this command returns to the default.

Parameters *app-profile-string* — Specifies the application profile string, up to 16 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.262 app-qos-policy

app-qos-policy

Syntax **app-qos-policy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>policy app-qos-policy)

Full Context configure application-assurance group policy app-qos-policy

Description Commands in this context configure an application QoS policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.263 app-route-notifications

app-route-notifications

Syntax **app-route-notifications**

Context [Tree] (config>log app-route-notifications)

Full Context configure log app-route-notifications

Description Specific system applications in SR OS can take action based on a route to certain IP destinations being available. This CLI branch contains configuration related to these route availability notifications. A delay can be configured between the time that a route is determined as available in the CPM, and the time that the application is notified of the available route. For example, this delay may be used to increase the chances that other system modules (such as IOMs/XCMs/MDAs/XMAs) are fully programmed with the new route before the application takes action. Currently, the only application that acts upon these *route available* or *route changed* notifications with their configurable delays is the SNMP replay feature, which receives notifications of route availability to the SNMP trap receiver destination IP address.

Platforms All

5.264 app-service-options

app-service-options

Syntax **app-service-options**

Context [Tree] (config>app-assure>group>policy app-service-options)

Full Context configure application-assurance group policy app-service-options

Description Commands in this context configure application service option characteristics.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

app-service-options

Syntax [**no**] **app-service-options**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-attributes app-service-options)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-attributes app-service-options

Description This command enables the subscriber application service option attributes to be exported in the AA subscriber's custom record.

The **no** form of this command excludes the subscriber application service option attributes from the AA subscriber's custom record.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.265 applicant-sm

applicant-sm

Syntax [**no**] **applicant-sm**

Context **[Tree]** (debug>service>id>mrp applicant-sm)

Full Context debug service id mrp applicant-sm

Description This command enables debugging of the applicant state machine.

The **no** form of this command disables debugging of the applicant state machine.

Platforms All

5.266 application

application

Syntax **application** {**gx** | **gy** | **nasreq**}
no application

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy application)

Full Context configure subscriber-mgmt diameter-application-policy application

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the Diameter application for which this policy contains the configuration details, such as AVPs to include and their format.

Applications are mutually exclusive.

The **no** form of this command reverts to the default.

Parameters **gx** — Specifies that Gx is the supported application of this DIAMETER policy.

gy — Specifies that Gy is the supported application of this DIAMETER policy.

nasreq — Specifies that NASREQ is the supported application of this DIAMETER policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application**

Context **[Tree]** (debug>diam application)

Full Context debug diameter application

Description This command debugs application processing for the Diameter node. This level is session aware (the session state is maintained at this level). Connection level messages are not reported on this level.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application** *dscp-app-name* **dscp** {*dscp-value* | *dscp-name*}
application *dot1p-app-name* **dot1p** *dot1p-priority*
no application {*dscp-app-name* | *dot1p-app-name*}

Context **[Tree]** (config>router>sgt-qos application)
[Tree] (config>service>vprn>sgt-qos application)

Full Context configure router sgt-qos application
configure service vprn sgt-qos application

Description This command configures DSCP/dot1p remarking for self-generated application traffic. When an application is configured using this command, the specified DSCP name/value is used for all packets generated by this application within the router instance it is configured. The instances can be base router, vprn, or management.

Using the value configured in this command:

- Sets the DSCP bits in the IP packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Maps to the FC. This value will be signaled from the CPM to the egress forwarding complex.
- Based on this signaled FC, the egress forwarding complex QoS policy sets the Ethernet 802.1p and MPLS EXP bits.
- The Ethernet 802.1p and MPLS EXP bits are set by the egress complex for all packets based on the signaled FC. This includes ARP, PPPoE, and IS-IS packets that, due to their nature, do not carry DSCP bits.
- The DSCP value in the egress IP header will be as configured in this command. The egress QoS policy will not overwrite this value.

Only one DSCP name/value can be configured per application, if multiple entries are configured, the subsequent entry overrides the previous configured entry.

The **no** form of this command reverts back to the default value.

Parameters *dscp-app-name* — Specifies the DSCP application name.

Values Some of the following values may only apply to specific products. Refer to the *SR OS 22.x*.R*x* Software Release Notes for details about application support for different SR OS products:

bgp, bmp, call-trace, cflowd, dhcp, diameter, dns, ftp, grpc, gtp, http, icmp, igmp, igmp-reporter, l2tp, ldp, mld, mpls-udp-return, msdp, mtrace2, ndis, ntp, ospf, pcep, pim, ptp, radius, rip, rsvp, sflow, snmp, snmp-notification, srrp, ssh, syslog, tacplus, telnet, tftp, traceroute, vrrp

dscp-value — Specifies a value when this packet egresses; the respective egress policy should provide the mapping for the DSCP value to either LSP-EXP bits or IEEE 802.1p (dot1p) bits as appropriate. Otherwise, the default mapping applies.

Values 0 to 63

dscp-name — Specifies the DSCP name.

Values none, be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dot1p-priority — Specifies the dot1p priority.

Values none, 0 to 7

dot1p-app-name — Specifies the dot1p application name.

Values Some of the following values may only apply to specific products. Refer to the *SR OS 22.x*.R*x* Software Release Notes for details about application support for different SR OS products:

arp, isis, pppoe

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

application

Syntax **application** *app* [*ip-int-name* | *ip-address*]
no application *app*

Context **[Tree]** (config>service>vprn>source-address application)

Full Context configure service vprn source-address application

Description This command specifies the source address and application.

Parameters *app* — Specifies the application name.

Values cflowd, ntp, ping, ptp, ssh, telnet, traceroute, icmp-error

ip-int-name | *ip-address* — Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms All

application

Syntax **application** {**eq** | **neq**} *application-id*
no application

Context **[Tree]** (config>service>vprn>log>filter>entry>match application)

Full Context configure service vprn log filter entry match application

Description This command adds an OS application as an event filter match criterion.

An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES and so on Only one application can be specified. The latest **application** command overwrites the previous command.

The **no** form of this command removes the application as a match criterion.

Default no application — no application match criterion is specified

Parameters **eq | neq** — The operator specifying the type of match.

Values

eq	equal to
neq	not equal to

application-id — The application name string.

Values port, ppp, rip, route, policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

application

Syntax **application** *application-name* [*rate*]
no application *application-name*

Context **[Tree]** (config>app-assure>group>cflowd>rtp-perf application)
[Tree] (config>app-assure>group>cflowd>tcp-perf application)
[Tree] (config>app-assure>group>cflowd>comp application)

Full Context configure application-assurance group cflowd comprehensive application
configure application-assurance group cflowd rtp-performance application
configure application-assurance group cflowd tcp-performance application

Description This command configures applications to export performance records with cflowd.

The **no** form of this command removes the parameters from the configuration.

Parameters *application-name* — Specifies the name defined for the application.

rate — Specifies which sampling flow rate to use; flow-rate or flow-rate2.

Values flow-rate, flow-rate2

Default flow-rate

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application** *application-name* [**create**]
no application *application-name*

Context **[Tree]** (config>app-assure>group>policy application)

Full Context configure application-assurance group policy application

Description This command creates an application of an application assurance policy.

The **no** form of this command deletes the application. To delete an application, all associations to the application must be removed.

Parameters *application-name* — Specifies a string of up to 32 characters uniquely identifying this application in the system.

create — Mandatory keyword used when creating an application. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

application

Syntax **application** *application-name*

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry application)

Full Context configure application-assurance group policy app-filter entry application

Description This command assigns this application filter entry to an existing application. Assigning the entry to **Unknown** application restores the default configuration.

Parameters *application-name* — Specifies an existing application name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application** {**eq** | **neq**} *application-name*
no application

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match application)

Full Context configure application-assurance group policy app-qos-policy entry match application

Description This command adds an application to match criteria used by this AQP entry.

The **no** form of this command removes the application from match criteria for this AQP entry.

Default no application

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

application-name — Specifies the name of name existing application name. The application-group-name is configured in the **config>app-assure>group>policy>aqp>entry>match** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application** *application-name* **export-using** *export-method* [*export-method*...(up to 2 max)]
application *application-name* **no-export**
no application *application-name*

Context **[Tree]** (config>app-assure>group>statistics>aa-sub application)

Full Context configure application-assurance group statistics aa-sub application

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures aa-sub accounting statistics for export of applications of a given AA ISA group/partition.

The no form of this command removes the application name.

Parameters *application-name* — Specifies an existing application name, up to 32 characters.

export-method — Specifies the method of statistics export to be used.

Values accounting-policy, radius-accounting-policy

no-export — Allows the operator to enable the referred application group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the **export-using** parameter is selected for the respective application group.

Usage monitoring must be enabled at the group:partition level (**config>app-assure>group>statistics>aa-sub>usage-monitoring**) as well in order to allow any application/application group/charging group usage monitoring.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application** {**eq** | **neq**} *application-name*
no application

Context **[Tree]** (debug>app-assure>group>traffic-capture>match application)

Full Context debug application-assurance group traffic-capture match application

Description This command configures debugging on an application.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application

Syntax [**no**] **application** *application-name*

Context **[Tree]** (debug>app-assure>group>port-recorder application)

Full Context debug application-assurance group port-recorder application

Description This commands specifies the applications used as input by the port-recorder. Applications responsible for unknown or unidentified traffic are meant to be used by this tool.

Output The following sample configuration records TCP and UDP port numbers for the application “Unidentified TCP”.

Sample Output

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
7750# show debug
debug
    application-assurance
        group 1:1
            port-recorder
                application "Unidentified TCP"
                rate 100
                no shutdown
            exit
        exit
    exit
exit
```

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application

Syntax **application** {**eq** | **neq**} *application-id*
no application

Context **[Tree]** (config>log>filter>entry>match application)

Full Context configure log filter entry match application

Description This command adds an OS application as an event filter match criterion.

An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES and so on. Only one application can be specified. The latest **application** command overwrites the previous command.

The **no** form of this command removes the application as a match criterion.

Parameters **eq** | **neq** — Specifies the operator match type. Valid operators are listed in Table 27.

Table 27 **Valid Operators**

Operator	Notes
eq	equal to
neq	not equal to

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

application-id — The application name string.

Values application_assurance, aps, atm, bgp, cflowd, chassis, debug, dhcp, dhcps, diameter, dynsvc, efm_oam, elmi, ering, eth_cfm, etun, fiter, gsmp, igh, igmp, igmp_snooping, ip, ipsec, isis, l2tp, lag, ldp, li, lldp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, mpls_tp, msdp, nat, ntp, oam, open_flow, ospf, pim, pim_snooping, port, ppp, pppoe, ptp, radius, rip, rip_ng, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, video, vrrp, vrtr, wlan_gw, wpp

Platforms All

application

Syntax **application** *app* [*ip-int-name* | *ip-address*]
no application *app*

Context **[Tree]** (config>system>security>source-address application)

Full Context configure system security source-address application

Description This command configures the source IPv4 address specified by the **source-address** command.

The **no** form of this command removes the interface name or address from the command.

Parameters *app* — Specifies the application name.

Values cflowd, dns, ftp, ntp, ldap, ping, ptp, radius, sflow, snmptrap, sntp, ssh, syslog, tacplus, telnet, traceroute, mcreporter, icmp-error

ip-int-name | *ip-address* — Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

application

Syntax **application** *application* **[keychain** *keychain-name***]**
no application *application*

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync>transport-encryption application)

Full Context configure redundancy multi-chassis peer sync transport-encryption application

Description This command configures transport encryption.

The **no** form of this command removes the specified application.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *application* — Specifies a Multi-Chassis Synchronization (MCS) client application

keychain-name — Specifies a keychain name, up to 32 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.267 application-assurance

application-assurance

Syntax **application-assurance**

Context **[Tree]** (admin application-assurance)

Full Context admin application-assurance

Description Commands in this context perform Application Assurance (AA) configuration operations.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application-assurance

Syntax **application-assurance**

Context **[Tree]** (config application-assurance)

Full Context configure application-assurance

Description Commands in this context perform Application Assurance (AA) configuration operations.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

application-assurance

Syntax **application-assurance**

Context **[Tree]** (config>system>persistence application-assurance)

Full Context configure system persistence application-assurance

Description Commands in this context configure application assurance persistence parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

application-assurance

Syntax **application-assurance** *app-profile-name*

Context **[Tree]** (config>subscr-mgmt>http-rdr-plcy application-assurance)

Full Context configure subscriber-mgmt http-redirect-policy application-assurance

Description This command specifies the AA application profile used for HTTP redirect portal authentication. This forwards all UDP/TCP traffic to AA for packet filtering. Any forwarding entries under the HTTP redirect policy are not taken into account because only UDP/TCP can be configured. Outbound ICMP and ICMPv6 traffic is always dropped.

Parameters *app-profile-name* — Specifies an AA application profile name, up to 32 characters, that is configured in the **config**>**app-assur**>**group**>**policy**>**app-prof** context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.268 application-assurance-group

application-assurance-group

Syntax **application-assurance-group** *application-assurance-group-index* [**create**] [**aa-sub-scale** *sub-scale*]
no application-assurance-group *application-assurance-group-index*

Context **[Tree]** (config>isa application-assurance-group)

Full Context configure isa application-assurance-group

Description Commands in this context create an application assurance group with the specified system-unique index and configure that group's parameters.

The **no** form of this command deletes the specified application assurance group from the system. The group must be shutdown first.

Parameters *application-assurance-group-index* — Specifies an integer to identify the AA group

Values 1 to 255

create — Mandatory keyword used when creating an application assurance group in the ISA context. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-scale — Specifies the set of scaling limits that are supported with regards to the maximum number of AA subscribers per ISA, the max flow scale, and the corresponding policy scale that can be specified.

Values

residential	Scaling limits for ISA2 residential operation (on VSR, it has the same scale as residential-8k)
residential-8k	Scaling limits for VSR or ESA-vm residential 8k sub operation
residential-16k	Scaling limits for VSR or ESA-vm residential 16k sub operation
residential-32k	Scaling limits for VSR or ESA-vm residential 32k sub operation
residential-64k	Scaling limits for VSR or ESA-vm residential 64k sub operation
vpn	Scaling limits for SR AA VPN operation
vpn-1k	Scaling limits for VSR or ESA-vm AA VPN 1k sub operation
vpn-2k	Scaling limits for VSR or ESA-vm AA VPN 2k sub operation
vpn-4k	Scaling limits for VSR or ESA-vm AA VPN 4k sub operation
vpn-8k	Scaling limits for VSR or ESA-vm AA VPN 8k sub operation
lightweight-internet	Scaling limits for ISA2 or VSR operation as a wireless LAN gateway using DSM subscribers
lightweight-internet-512k	Scaling limits for VSR or ESA-vm 512k sub operation as a wireless LAN gateway using DSM subscribers

Default residential

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.269 application-link-attributes

application-link-attributes

Syntax [**no**] **application-link-attributes**

Context **[Tree]** (config>router>isis>traffic-engineering-options application-link-attributes)

Full Context configure router isis traffic-engineering-options application-link-attributes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the advertisement of the TE attributes of each link on a per-application basis. Two applications are supported in SR OS: RSVP-TE and SR-TE.

The legacy mode of advertising TE attributes that is used in RSVP-TE is still supported but it can be disabled by using the **no legacy** command, which also enables per-application TE attribute advertisement for RSVP-TE.

The **no** form of this command deletes the context.

Default no application-link-attributes

Platforms All

5.270 application-policy

application-policy

Syntax [**no**] **application-policy** *name*

Context **[Tree]** (config>app-assure>group>transit-ip>diameter application-policy)

Full Context configure application-assurance group transit-ip-policy diameter application-policy

Description This command specifies the Diameter application to be used by seen IP transit subs. The application policy is defined using the **config**>**subscr-mgmt**>**diameter-application-policy** command.

The **no** form of this command removes the policy.

Default no application-policy

Parameters *name* — Specifies the name of the application policy configured using the **diameter-application-policy** command up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.271 application6

application6

Syntax **application6** *app ipv6-address*
no application6 *app*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>source-address application6)

Full Context configure service vprn source-address application6

Description This command specifies the IPv6 source address and application.

The **no** form of this command removes the application and IPv6 address from the configuration.

Parameters *app* — Specifies the application name.

Values cflowd, ntp, ping, ssh, telnet, traceroute, icmp6-error

ipv6-address — Specifies the IPv6 address.

Platforms All

application6

Syntax **application6** *app ipv6-address*
no application6

Context [Tree] (config>system>security>source-address application6)

Full Context configure system security source-address application6

Description This command configures the application to use the source IPv6 address specified by the **source-address** command.

The **no** form of this command removes the application and IPv6 address from the configuration.

Parameters *app* — Specifies the application name.

Values cflowd, dns, ftp, ldap, ntp, ping, radius, sflow, snmptrap, ssh, syslog, tacplus, telnet, traceroute, icmp6-error

ipv6-address — Specifies the IPv6 address.

Platforms All

5.272 applications

applications

Syntax **applications all**
applications [**connectivity-management**] [**gx**] [**gy**] [**nasreq**] [**radius-auth**] [**radius-acct**] [**python**] [**ludb**] [**msap**] [**ppp-event**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no applications

Context [Tree] (config>call-trace>trace-profile applications)

Full Context configure call-trace trace-profile applications

Description This command enables tracing of messages and events for the specified applications.

Default applications all

Parameters **all** — Enables tracing of all packets and events, with the exception of PPP events.

connectivity-management — Enables tracing for connectivity protocols, such as DHCP, ARP, and DHCPv6, and events related to connectivity management; for example, migrant or data-triggered host creation, idling, or session timeout.

gx — Enables tracing of Diameter Gx messages.

gy — Enables tracing of Diameter Gy messages.

nasreq — Enables tracing of Diameter NASREQ messages.

radius-auth — Enables tracing of messages and events related to RADIUS authentication, including CoA and Disconnect.

radius-acct — Enables tracing of messages and events related to RADIUS-based accounting.

python — Enables tracing of python script execution.

ludb — Enables tracing of local user database lookups.

msap — Enables tracing of MSAP creation events.

ppp-event — Enables tracing of all events related to the PPP state machine. This can result in a large amount of event messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

applications

Syntax **applications** {[**gx**] [**gy**] [**nasreq**]}
no applications

Context [Tree] (config>aaa>diam-peer-plcy applications)

Full Context configure aaa diameter-peer-policy applications

Description This command specifies which applications are advertised in the Capability Exchange Request (CER) messages sent on the peers.

Applications that can be configured on a Diameter peer policy:

- client and proxy role:
  - gx

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- nasreq
- gx nasreq

- client role only:
  - gy

Note: Gx and nasreq applications can be enabled simultaneously on a single diameter peer.

The **no** form of this command reverts to the default.

Parameters **gx** — Specifies that Gx application support is advertised in CER.

gy — Specifies that Gy (DCCA) application support is advertised in CER.

nasreq — Specifies that NASREQ application support is advertised in CER.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.273 apply-bgp-nh-override

apply-bgp-nh-override

Syntax [**no**] **apply-bgp-nh-override**

Context **[Tree]** (config>service>vprn>pim apply-bgp-nh-override)

Full Context configure service vprn pim apply-bgp-nh-override

Description This command forces the RPF check to be performed via IPv4 VPN AF next-hop and not via IPv4 VPN AF VRF import extended community.

Default no apply-bgp-nh-override

Platforms All

5.274 apply-function-specific-behavior

apply-function-specific-behavior

Syntax **[no] apply-function-specific-behavior**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>url-filter apply-function-specific-behavior)

Full Context configure application-assurance group url-filter apply-function-specific-behavior

Description If this command is enabled, the **default-action**, **default-http-redirect**, and **http-redirect** commands at the **url-filter** function level (ICAP, local filtering and web service) will apply.

The **no** form of this command indicates that the configuration at the **url-filter** level will apply to all of the configured **url-filter** functions.

Default no apply-function-specific-behavior

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.275 apply-path

apply-path

Syntax [**no**] **apply-path**

Context [Tree] (config>filter>match-list>ip-prefix-list apply-path)
[Tree] (config>filter>match-list>ipv6-prefix-list apply-path)

Full Context configure filter match-list ip-prefix-list apply-path
configure filter match-list ipv6-prefix-list apply-path

Description Commands in this context configure the auto-generation of address prefixes for IPv4 or IPv6 address prefix match lists. The context in which the command is executed governs whether IPv4 or IPv6 prefixes will be auto-generated.

The **no** form of this command removes all auto-generation configuration under the **apply-path** context.

Default no apply path

Platforms All

5.276 apply-to

apply-to

Syntax **apply-to** {**all** | **none**}

Context [Tree] (config>service>vprn>pim apply-to)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn pim apply-to

Description This command creates a PIM interface with default parameters.

If a manually created interface or modified interface is deleted, the interface will be recreated when the **apply-to** command is executed. If PIM is not required on a specific interface, then execute a **shutdown** command.

The **apply-to** command is saved first in the PIM configuration structure, all subsequent commands either create new structures or modify the defaults as created by the **apply-to** command.

Default apply-to none

Parameters **all** — Specifies that all VPRN and non-VPRN interfaces are automatically applied in PIM.

none — No interfaces are automatically applied in PIM. PIM interfaces must be manually configured.

Platforms All

apply-to

Syntax **apply-to** {**ies** | **non-ies** | **all** | **none**}

Context **[Tree]** (config>router>pim apply-to)

Full Context configure router pim apply-to

Description This command creates a PIM interface with default parameters.

If a manually created or a modified interface is deleted, the interface is recreated when (re)processing the **apply-to** command and if PIM is not required on a specific interface a shutdown should be executed.

The **apply-to** command is first saved in the PIM configuration structure. Then, all subsequent commands either create new structures or modify the defaults as created by the apply-to command.

Default apply-to none

Parameters **ies** — Specifies to apply all IES interfaces in PIM.

non-ies — Specifies to apply non-IES interfaces created in PIM.

all — Specifies to apply all IES and non-IES interfaces created in PIM.

none — Removes all interfaces that are not manually created or modified. It also removes explicit no interface commands if present.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.277 aps

aps

Syntax **aps**

Context **[Tree]** (config>port aps)

Full Context configure port aps

Description This command configures APS (Automatic Protection Switching). APS is used by SONET/SDH add/drop multiplexers (ADMs) or other SONET/SDH-capable equipment to protect against circuit or equipment failure.

An APS group contains a working and a protect circuit and can span a single node (SC-APS) or two nodes (MC-APS).

The working and protection configurations on the 7750 SRs must match the circuit configurations on the peer. This means that the working circuit on the 7750 SR must be connected to the peer's working circuit and the protect circuit must be connected to the peer's protection circuit.

The **aps** command is only available for APS groups and not physical ports.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

5.278 aqp-initial-lookup

aqp-initial-lookup

Syntax **aqp-initial-lookup**
no aqp-initial-lookup

Context **[Tree]** (config>app-assure>group:[partition] aqp-initial-lookup)

Full Context configure application-assurance group:[partition] aqp-initial-lookup

Description This command allows AA to perform AQP lookups on flows prior to complete application identification. As usual, AQP will be looked up again on identification complete. Without this, AA executes AQPs that are part of what so called "sub-default policy". Sub-default policy is formed by regular AQPs that contain ASOs, subID and/or flow direction as matching conditions.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This behavior is required, for example, in order to be able apply GTP and SCTP filtering on the first packet of a new GTP/SCTP flow (AQP matching conditions in this case contains protocol id).

The **no** form of this command forces complete AQP look up on identification finish stage only.

Default no aqp-initial-lookup

5.279 arbiter

arbiter

Syntax **arbiter** *arbiter-name* [**create**]
no arbiter *arbiter-name*

Context **[Tree]** (config>qos>plcr-ctrl-plcy>tier arbiter)

Full Context configure qos policer-control-policy tier arbiter

Description This command is used to create an arbiter within the context of **tier 1** or **tier 2**. An arbiter is a child policer bandwidth control object that manages the throughput of a set of child policers. An arbiter allows child policers or other arbiters to parent to one of eight strict levels. Each arbiter is itself parented to either another tiered arbiter or to the **root** arbiter.

The root arbiter starts with its defined maximum rate and distributes the bandwidth to its directly attached child policers and arbiters beginning with priority 8. As the children at each priority level are distributed bandwidth according to their needs and limits, the root proceeds to the next lower priority until either all children's needs are met or it runs out of bandwidth. The bandwidth given to a tiered arbiter is then divided between that arbiter's children (child policers or a tier 2 arbiter) in the same fashion. A tiered arbiter may also have a rate limit defined that limits the amount of bandwidth it may receive from its parent.

An arbiter that is currently parented by another arbiter cannot be deleted.

Each time the **policer-control-policy** is applied to either a SAP, or a subscriber (through association with a sub-profile that has the policy applied), or a multiservice site, an instance of the parent policer and the arbiters is created.

Any child policer that uses the arbiter's name in its parenting command will be associated with the arbiter instance. The child policer will also become associated with any arbiter to which its parent arbiter is parented (grandparent). Having child policers parented to an arbiter does not prevent that arbiter from being removed from the **policer-control-policy**. When removed, the child policers become orphaned.

You can create up to 31 tiered arbiters within the **policer-control-policy** on either tier 1 or tier 2 (in addition to the arbiter).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command is used to remove an arbiter from tier 1 or tier 2. If the specified arbiter does not exist, the command returns without an error. If the specified arbiter is currently specified as the parent for another arbiter, the command will fail. When an arbiter is removed from a **policer-control-policy**, all instances of the arbiter will also be removed. Any child policers currently parented to the arbiter instance will become orphans and will not be bandwidth managed by the policer control policy instances parent policer.

Parameters *arbiter-name* — Any unique name within the policy. Up to 31 arbiters may be created.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

5.280 area

area

Syntax [**no**] **area** *area-id*

Context **[Tree]** (config>service>vprn>ospf area)
[Tree] (config>service>vprn>ospf3 area)

Full Context configure service vprn ospf area
configure service vprn ospf3 area

Description This command creates the context to configure an OSPF area. An area is a collection of network segments within an AS that have been administratively grouped together. The area ID can be specified in dotted decimal notation or as a 32-bit decimal integer.

The **no** form of this command deletes the specified area from the configuration. Deleting the area also removes the OSPF configuration of all the interfaces, virtual-links, sham-links, address-ranges and so on, that are currently assigned to this area.

Default no area — No OSPF areas are defined.

Parameters *area-id* — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values 0.0.0.0 to 255.255.255.255 (dotted decimal)
0 to 4294967295 (decimal integer)

Platforms All

area

Syntax [**no**] **area** *area-id*

Context **[Tree]** (config>router>ospf area)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ospf3 area)

Full Context configure router ospf area
configure router ospf3 area

Description This command creates the context to configure an OSPF or OSPF3 area. An area is a collection of network segments within an AS that have been administratively grouped together. The area ID can be specified in dotted decimal notation or as a 32-bit decimal integer.

The **no** form of this command deletes the specified area from the configuration. Deleting the area also removes the OSPF configuration of all the interfaces, virtual-links, and address-ranges and so on, that are currently assigned to this area.

Default no area

Parameters *area-id* — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values 0.0.0.0 to 255.255.255.255 (dotted decimal), 0 to 4294967295 (decimal integer)

Platforms All

area

Syntax **area** [*area-id*]
no area

Context **[Tree]** (debug>router>ospf area)
[Tree] (debug>router>ospf3 area)

Full Context debug router ospf area
debug router ospf3 area

Description This command enables debugging for an OSPF area.

Parameters *area-id* — Specifies the OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values ip-address — a.b.c.d
area — 0 to 4294967295

Platforms All

area

Syntax **area** *area-id*
no area

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>policy-options>policy-statement>entry>from area)

Full Context configure router policy-options policy-statement entry from area

Description This command configures an OSPF area as a route policy match criterion.

This match criterion is only used in export policies.

All OSPF routes (internal and external) are matched using this criterion if the best path for the route is by the specified area.

The **no** form of this command removes the OSPF area match criterion.

Default no area

Parameters *area-id* — Specifies the OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values 0.0.0.0 to 255.255.255.255 (dotted decimal), 0 to 4294967295 (decimal)

Platforms All

5.281 area-id

area-id

Syntax [**no**] **area-id** *area-address*

Context [Tree] (config>service>vprn>isis area-id)

Full Context configure service vprn isis area-id

Description This command configures the area ID portion of NSAP addresses for the VPRN instance. This identifies a point of connection to the network, such as a router interface, and is called a Network Service Access Point (NSAP). Addresses in the IS-IS protocol are based on the ISO NSAP addresses and Network Entity Titles (NETs), not IP addresses.

A maximum of 3 **area addresses** can be configured for the VPRN instance.

NSAP addresses are divided into three parts. Only the area ID portion is configurable.

- Area ID — A variable length field between 1 and 13 bytes long. This includes the Authority and Format Identifier (AFI) as the most significant byte and the area ID.
- System ID — A six-byte system identification. This value is not configurable. The system ID is derived from the system or router ID.
- Selector ID — A one-byte selector identification that must contain zeros when configuring a NET. This value is not configurable. The selector ID is always 00.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The NET is constructed like an NSAP but the selector byte contains a 00 value. NET addresses are exchanged in hello and LSP PDUs. All net addresses configured on the node are advertised to its neighbors.

For Level 1 interfaces, neighbors can have different area IDs, but, they must have at least one area ID (AFI + area) in common. Sharing a common area ID, they become neighbors and area merging between the potentially different areas can occur.

For Level 2 (only) interfaces, neighbors can have different area IDs. However, if they have no area IDs in common, they become only Level 2 neighbors and Level 2 LSPs are exchanged.

For Level 1 and Level 2 interfaces, neighbors can have different area IDs. If they have at least one area ID (AFI + area) in common, they become neighbors. In addition to exchanging Level 2 LSPs, area merging between potentially different areas can occur.

If multiple **area-id** commands are entered, the system ID of all subsequent entries must match the first **area** address.

The **no** form of this command removes the area address.

Platforms All

area-id

Syntax [**no**] **area-id** *area-address*

Context **[Tree]** (config>router>isis area-id)

Full Context configure router isis area-id

Description This command was previously named the **net** *network-entity-title* command. The **area-id** command allows you to configure the area ID portion of NSAP addresses which identifies a point of connection to the network, such as a router interface, and is called a Network Service Access Point (NSAP). Addresses in the IS-IS protocol are based on the ISO NSAP addresses and Network Entity Titles (NETs), not IP addresses.

A maximum of three **area addresses** can be configured.

NSAP addresses are divided into three parts. Only the area ID portion is configurable.

- Area ID — A variable length field between 1 and 13 bytes long. This includes the Authority and Format Identifier (AFI) as the most significant byte and the area ID.
- System ID — A six-byte system identification. This value is not configurable. The system ID is derived from the system or router ID.
- Selector ID — A one-byte selector identification that must contain zeros when configuring a NET. This value is not configurable. The selector ID is always 00.

The NET is constructed like an NSAP but the selector byte contains a 00 value. NET addresses are exchanged in hello and LSP PDUs. All net addresses configured on the node are advertised to its neighbors.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For Level 1 interfaces, neighbors can have different area IDs, but, they must have at least one area ID (AFI + area) in common. Sharing a common area ID, they become neighbors and area merging between the potentially different areas can occur.

For Level 2 (only) interfaces, neighbors can have different area IDs. However, if they have no area IDs in common, they become only Level 2 neighbors and Level 2 LSPs are exchanged.

For Level 1 and Level 2 interfaces, neighbors can have different area IDs. If they have at least one area ID (AFI + area) in common, they become neighbors. In addition to exchanging Level 2 LSPs, area merging between potentially different areas can occur.

If multiple **area-id** commands are entered, the system ID of all subsequent entries must match the first **area** address.

The **no** form of this command removes the area address.

Parameters *area-address* — Specifies a 1 — 13-byte address. Of the total 20 bytes comprising the NET, only the first 13 bytes can be manually configured. As few as one byte can be entered or, at most, 13 bytes. If less than 13 bytes are entered, the rest is padded with zeros.

Platforms All

5.282 area-range

area-range

Syntax **area-range** *ip-prefix/prefix-length* [**advertise** | **not-advertise**]
no area-range *ip-prefixImask*
area-range *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**]
no area-range *ipv6-prefix/prefix-length*

Context **[Tree]** (config>service>vprn>ospf>area area-range)
[Tree] (config>service>vprn>ospf3>area area-range)
[Tree] (config>service>vprn>ospf>area>nssa area-range)
[Tree] (config>service>vprn>ospf3>area>nssa area-range)

Full Context configure service vprn ospf area area-range
configure service vprn ospf area nssa area-range
configure service vprn ospf3 area area-range
configure service vprn ospf3 area nssa area-range

Description This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When a range is created, it is configured to be advertised or not advertised into other areas. Multiple range commands are used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The **no** form of this command deletes the range (non) advertisement.

Default no area-range

Special Cases **NSSA Context —** In the NSSA context, the command specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context — If this command is not configured under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.

Parameters *ipv6-prefix/prefix-length* — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-length	0 to 128

mask — The subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values 0 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

advertise | not-advertise — Specifies whether or not to advertise the summarized range of addresses into other areas. The **advertise** keyword indicates the range will be advertised, and the keyword **not-advertise** indicates the range will not be advertised.

The default is **advertise**.

Platforms All

area-range

Syntax **area-range** *ip-prefixlmask* [**advertise** | **not-advertise**]
no area-range *ip-prefixlmask*

Context **[Tree]** (config>router>ospf>area area-range)
[Tree] (config>router>ospf>area>nssa area-range)

Full Context configure router ospf area area-range
configure router ospf area nssa area-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When a range is created, the range is configured to be advertised or not advertised into other areas. Multiple range commands may be used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The **no** form of this command deletes the range (non) advertisement.

Default no area-range

Special Cases **NSSA Context —** In the NSSA context, the option specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context — If this command is not entered under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.

Parameters *ip-prefix* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ip-prefix/mask: ip-prefix a.b.c.d (host bits must be 0)

mask — Specifies the subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values 0 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

advertise | **not-advertise** — Specifies whether to advertise the summarized range of addresses into other areas. The **advertise** keyword indicates the range will be advertised, and the keyword **not-advertise** indicates the range will not be advertised.

Default advertise

Platforms All

area-range

Syntax **area-range** *ipv4-prefix/mask* | *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**]
no area-range *ipv4-prefix/mask* | *ipv6-prefixIprefix-length*

Context **[Tree]** (config>router>ospf3>area area-range)
[Tree] (config>router>ospf3>area>nssa area-range)

Full Context configure router ospf3 area area-range
configure router ospf3 area nssa area-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When a range is created, the range is configured to be advertised or not advertised into other areas. Multiple range commands may be used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The **no** form of this command deletes the range (non) advertisement.

Default no area-range

Special Cases **NSSA Context —** In the NSSA context, the option specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context — If this command is not entered under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.

Parameters *ip-prefix/prefix-length* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ip-prefix/mask:

- ip-prefix a.b.c.d (host bits must be 0)

ipv6-prefix:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

prefix-length: 0 to 128

advertise | **not-advertise** — Specifies whether or not to advertise the summarized range of addresses into other areas. The **advertise** keyword indicates the range will be advertised, and the keyword **not-advertise** indicates the range will not be advertised.

Default advertise

Platforms All

area-range

Syntax **area-range** [*ip-address*]
no area-range

Context **[Tree]** (debug>router>ospf area-range)
[Tree] (debug>router>ospf3 area-range)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router ospf area-range
debug router ospf3 area-range

Description This command enables debugging for an OSPF area range.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address for the range used by the ABR to advertise the area into another area.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

5.283 arp

arp

Syntax **arp** *arp-value*
no arp

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile>ggsn>qos arp)
[Tree] (config>subscr-mgmt>gtp>peer-profile>pgw>qos arp)
[Tree] (config>subscr-mgmt>gtp>peer-profile>mme>qos arp)

Full Context configure subscriber-mgmt gtp peer-profile ggsn qos arp
configure subscriber-mgmt gtp peer-profile mme qos arp
configure subscriber-mgmt gtp peer-profile pgw qos arp

Description The command configures the allocation and retention priority to be used in the GTP messages as QoS IE (for a Gn interface) or Bearer QoS (for GTPv2).

The **no** form of this command reverts to the default.

Default arp 1

Parameters *arp-value* — Specifies the Allocation/Retention Priority (ARP).

Values 1 to 3 (for ggsn context)

Values 1 to 15 (for pgw and mme context)

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

arp

Syntax **arp**

Context **[Tree]** (config>service>ies>if>vpls>evpn arp)
[Tree] (config>service>vprn>if>vpls>evpn arp)

Full Context configure service ies interface vpls evpn arp
configure service vprn interface vpls evpn arp

Description Commands in this context configure ARP host route parameters.

Platforms All

arp

Syntax **arp**

Context **[Tree]** (debug>router>ip arp)

Full Context debug router ip arp

Description This command configures route table debugging.

Platforms All

5.284 arp-host

arp-host

Syntax **arp-host**

Context **[Tree]** (config>service>ies>sub-if>grp-if arp-host)
[Tree] (config>service>vpls>sap arp-host)
[Tree] (config>service>vprn>sub-if>grp-if arp-host)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only arp-host)

Full Context configure service ies subscriber-interface group-interface arp-host
configure service vpls sap arp-host
configure service vprn subscriber-interface group-interface arp-host
configure subscriber-mgmt msap-policy vpls-only-sap-parameters arp-host

Description Commands in this context configure ARP host parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

arp-host

Syntax [**no**] **arp-host**

Context **[Tree]** (debug>service>id arp-host)

Full Context debug service id arp-host

Description This command enables and configures ARP host debugging.

The **no** form of this command disables ARP host debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.285 arp-host-route

arp-host-route

Syntax **arp-host-route**

Context **[Tree]** (config>service>ies>if arp-host-route)
[Tree] (config>service>vprn>if arp-host-route)

Full Context configure service ies interface arp-host-route
configure service vprn interface arp-host-route

Description Commands in this context configure ARP host routes to populate.

Platforms All

5.286 arp-learn-unsolicited

arp-learn-unsolicited

Syntax [**no**] **arp-learn-unsolicited**

Context **[Tree]** (config>router>if arp-learn-unsolicited)
[Tree] (config>service>ies>if arp-learn-unsolicited)
[Tree] (config>service>vprn>if arp-learn-unsolicited)

Full Context configure router interface arp-learn-unsolicited
configure service ies interface arp-learn-unsolicited
configure service vprn interface arp-learn-unsolicited

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the ARP application to learn new entries based on any received ARP message (GARP, ARP-Request, or ARP-Reply, such as any frame with ethertype 0x0806).

The **no** form of this command disables the above behavior and causes ARP entries to only be learned when needed, that is, when the router receives an ARP-reply after an ARP-request triggered by received traffic.

Platforms All

5.287 arp-limit

arp-limit

Syntax **arp-limit** *limit* [**log-only**] [**threshold** *percent*]
no arp-limit

Context **[Tree]** (config>service>ies>interface arp-limit)

Full Context configure service ies interface arp-limit

Description This command configures the maximum amount of dynamic IPv4 ARP entries that can be learned on an IP interface.

When the number of dynamic ARP entries reaches the configured percentage of this limit, a log event is raised. When the limit is exceeded, no new entries are learned until an entry expires and traffic to these destinations will be dropped. Entries that have already been learned will be refreshed.

The **no** form of this command removes the **arp-limit**.

Default no arp-limit

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, entries above the limit will be learned.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

Default 90

limit — The number of entries that can be learned on an IP interface expressed as a decimal integer. If the limit is set to 0, dynamic ARP learning is disabled and no dynamic ARP entries are learned.

Values 0 to 524288

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

arp-limit

Syntax **arp-limit** *limit* [**log-only**] [**threshold** *percent*]
no arp-limit

Context **[Tree]** (config>service>vprn>if arp-limit)

Full Context configure service vprn interface arp-limit

Description This command configures the maximum amount of dynamic IPv4 ARP entries that can be learned on an IP interface.

When the number of dynamic ARP entries reaches the configured percentage of this limit, an SNMP trap is sent. When the limit is exceeded, no new entries are learned until an entry expires and traffic to these destinations will be dropped. Entries that have already been learned will be refreshed.

The **no** form of this command removes the **arp-limit**.

Default 90 percent

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, entries above the limit will be learned.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

limit — The number of entries that can be learned on an IP interface expressed as a decimal integer. If the limit is set to 0, dynamic ARP learning is disabled and no dynamic ARP entries are learned.

Values 0 to 524288

Platforms All

arp-limit

Syntax **arp-limit** *limit* [**log-only**] [**threshold** *percent*]
no arp-limit

Context **[Tree]** (config>router>if arp-limit)

Full Context configure router interface arp-limit

Description This command configures the maximum amount of dynamic IPv4 ARP entries that can be learned on an IP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the number of dynamic ARP entries reaches the configured percentage of this limit, an SNMP trap is sent. When the limit is exceeded, no new entries are learned until an entry expires and traffic to these destinations will be dropped. Entries that have already been learned will be refreshed.

The **no** form of this command removes the **arp-limit.**

Default no arp-limit

Parameters *limit* — The number of entries that can be learned on an IP interface expressed as a decimal integer. If the limit is set to 0, dynamic ARP learning is disabled and no dynamic ARP entries are learned.

Values 0 to 524288

log-only — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, entries above the limit will be learned.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

Platforms All

5.288 arp-populate

arp-populate

Syntax [**no**] **arp-populate**

Context **[Tree]** (config>service>ies>if arp-populate)
[Tree] (config>service>ies>sub-if>grp-if arp-populate)
[Tree] (config>service>vprn>if arp-populate)
[Tree] (config>service>vprn>sub-if>grp-if arp-populate)

Full Context configure service ies interface arp-populate
configure service ies subscriber-interface group-interface arp-populate
configure service vprn interface arp-populate
configure service vprn subscriber-interface group-interface arp-populate

Description This command, when enabled, disables dynamic learning of ARP entries. Instead, the ARP table is populated with static and dynamic entries from the DHCP Lease State Table (enabled with **lease-populate**), and optionally with static entries entered with the **host** command.

The host's IP address and MAC address are placed in the system ARP cache as a managed entry. Static hosts must be defined on the interface using the **host** command. Dynamic hosts are enabled on the system through enabling lease-populate in the IP interface DHCP context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In the event that both a static host and a dynamic host share the same IP and MAC address, the system's ARP cache retains the host information until both the static and dynamic information are removed.

Both static and dynamic hosts override static ARP entries. Static ARP entries are marked as inactive when they conflict with static or dynamic hosts and will be repopulated once all static and dynamic host information for the IP address are removed. Since static ARP entries are not possible when static subscriber hosts are defined or when DHCP lease state table population is enabled, conflict between static ARP entries and the arp-populate function is not an issue.

Enabling the **arp-populate** command removes any dynamic ARP entries learned on this interface from the ARP cache.

The **arp-populate** command fails if an existing static ARP entry exists for this interface.

The **arp-populate** command fails if an existing static subscriber host on the SAP does not have both MAC and IP addresses specified.

Once **arp-populate** is enabled, creating a static subscriber host on the SAP without both an IP address and MAC address fails.

When **arp-populate** is enabled, the system does not send out ARP requests for hosts that are not in the ARP cache. Only statically configured and DHCP learned hosts are reachable through an IP interface with **arp-populate** enabled. The **arp-populate** command can only be enabled on IES and VPRN interfaces supporting Ethernet encapsulation.

The **no** form of this command disables ARP cache population functions for static and dynamic hosts on the interface. All static and dynamic host information for this interface is removed from the system's ARP cache. Any existing static ARP entries previously inactive due to static or dynamic hosts will be populated in the system ARP cache.

Default no arp-populate

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface arp-populate
- configure service ies subscriber-interface group-interface arp-populate

All

- configure service vprn interface arp-populate
- configure service ies interface arp-populate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.289 arp-populate-host-route

arp-populate-host-route

Syntax [**no**] **arp-populate-host-route**

Context **[Tree]** (config>service>ies>if arp-populate-host-route)

Full Context configure service ies interface arp-populate-host-route

Description This command enables the addition or deletion of host routes in the route table derived from ARP entries in the ARP cache. To enable this command, the interface must be shut down. The command triggers the population of host routes in the route table out of their corresponding static, dynamic, or EVPN types in the ARP table. ARP entries installed by subscriber management, local interfaces, and others, do not create host routes.

The **no** form of this command disables the creation of host routes from the ARP cache.

5.290 arp-proactive-refresh

arp-proactive-refresh

Syntax [**no**] **arp-proactive-refresh**

Context **[Tree]** (config>service>ies>if arp-proactive-refresh)

Full Context configure service ies interface arp-proactive-refresh

Description This command enables the router to always send out a single refresh message with no entries 30 seconds prior to the timeout of the entry.

The **no** form of this command sets the default behavior, in which an entry is marked as stale 30 seconds prior to age-out, and the router only sends an ARP request to refresh the entry if the IOM receives traffic that uses it. If so, the IOM asks the ARP application to send a refresh message. With **arp-proactive-refresh** enabled, the ARP module sends a refresh message regardless of whether the IOM receives traffic.

Platforms All

arp-proactive-refresh

Syntax [**no**] **arp-proactive-refresh**

Context **[Tree]** (config>service>vprn>if arp-proactive-refresh)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface arp-proactive-refresh

Description This command enables the router to always send out a refresh message 30 seconds prior to the timeout of the entry (a single refresh message with no retries).

The **no** form of this command sets the default behavior, in which an entry is marked as stale 30 seconds prior to age-out, and the router only sends an ARP request to refresh the entry if the IOM receives traffic that uses it. If so, the IOM asks the ARP application to send a refresh message. With **arp-proactive-refresh** enabled, the ARP module sends a refresh message regardless of the IOM receiving traffic.

Platforms All

arp-proactive-refresh

Syntax [**no**] **arp-proactive-refresh**

Context **[Tree]** (config>router>if arp-proactive-refresh)

Full Context configure router interface arp-proactive-refresh

Description This command enables the router to always send out a refresh message 30 seconds prior to the timeout of the entry (a single refresh message with no retries).

The **no** form of this command sets the default behavior, in which an entry is marked as stale 30 seconds prior to age-out, and the router only sends an ARP request to refresh the entry if the IOM receives traffic that uses it. If so, the IOM asks the ARP application to send a refresh message. With **arp-proactive-refresh** enabled, the ARP module sends a refresh message regardless of the IOM receiving traffic.

Platforms All

5.291 arp-reply-agent

arp-reply-agent

Syntax **arp-reply-agent** [**sub-ident**]
no arp-reply-agent

Context **[Tree]** (config>service>vpls>sap arp-reply-agent)

Full Context configure service vpls sap arp-reply-agent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables a special ARP response mechanism in the system for ARP requests destined to static or dynamic hosts associated with the SAP. The system responds to each ARP request using the host's MAC address as the both the source MAC address in the Ethernet header and the target hardware address in the ARP header.

ARP replies and requests received on a SAP with **arp-reply-agent** enabled is evaluated by the system against the anti-spoof filter entries associated with the ingress SAP (if the SAP has anti-spoof filtering enabled). ARPs from unknown hosts on the SAP is discarded when anti-spoof filtering is enabled.

The ARP reply agent only responds if the ARP request enters an interface (SAP, spoke SDP or mesh SDP) associated with the VPLS instance of the SAP.

A received ARP request that is not in the ARP reply agent table is flooded to all forwarding interfaces of the VPLS capable of broadcast except the ingress interface while honoring split-horizon constraints.

Static hosts can be defined on the SAP using the **host** command. Dynamic hosts are enabled on the system by enabling the **lease-populate** command in the SAP's **dhcp** context. If both a static host and a dynamic host share the same IP and MAC address, the VPLS ARP reply agent will retain the host information until both the static and dynamic information are removed. If both a static and dynamic host share the same IP address, but different MAC addresses, the VPLS ARP reply agent is populated with the static host information.

The **arp-reply-agent** command fails if an existing static host on the SAP does not have both MAC and IP addresses specified. Once the ARP reply agent is enabled, creating a static host on the SAP without both an IP address and MAC address will fail.

The apr-reply-agent can only be enabled on SAPs supporting Ethernet encapsulation.

The **no** form of the command disables arp-reply-agent functions for static and dynamic hosts on the SAP.

Default no arp-reply-agent

Parameters *sub-ident* — Configures the arp-reply-agent to discard ARP requests received on the SAP that are targeted for a known host on the same SAP with the same subscriber identification.

Hosts are identified by their subscriber information. For DHCP subscriber hosts, the subscriber hosts, the subscriber information is configured using the optional subscriber parameter string.

When arp-reply-agent is enabled with **sub-ident**:

- If the subscriber information for the destination host exactly matches the subscriber information for the originating host and the destination host is known on the same SAP as the source, the ARP request is silently discarded.
- If the subscriber information for the destination host or originating host is unknown or undefined, the source and destination hosts are not considered to be the same subscriber. The ARP request is forwarded outside the SAP's Split Horizon Group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- When **sub-ident** is not configured, the arp-reply-agent does not attempt to identify the subscriber information for the destination or originating host and will not discard an ARP request based on subscriber information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

arp-reply-agent

Syntax **arp-reply-agent** [**sub-ident**]
no arp-reply-agent

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only arp-reply-agent)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters arp-reply-agent

Description This command enables a special ARP response mechanism in the system for ARP requests destined to static or dynamic hosts associated with the SAP. The system responds to each ARP request using the hosts MAC address as the both the source MAC address in the Ethernet header and the target hardware address in the ARP header.

ARP replies and requests received on an MSAP with **arp-reply-agent** enabled is evaluated by the system against the anti-spoof filter entries associated with the ingress SAP (if the SAP has anti-spoof filtering enabled). ARPs from unknown hosts on the SAP is discarded when anti-spoof filtering is enabled.

The ARP reply agent only responds if the ARP request enters an interface (SAP, spoke-SDP or mesh-SDP) associated with the VPLS instance of the MSAP.

A received ARP request that is not in the ARP reply agent table is flooded to all forwarding interfaces of the VPLS capable of broadcast except the ingress interface while honoring split-horizon constraints.

Static hosts can be defined using the **host** command. Dynamic hosts are enabled on the system by enabling the **lease-populate** command in the **dhcp** context. In the event that both a static host and a dynamic host share the same IP and MAC address, the VPLS ARP reply agent will retain the host information until both the static and dynamic information are removed. In the event that both a static and dynamic host share the same IP address, but different MAC addresses, the VPLS ARP reply agent is populated with the static host information.

The **arp-reply-agent** command will fail if an existing static host does not have both MAC and IP addresses specified. Once the ARP reply agent is enabled, creating a static host on the MSAP without both an IP address and MAC address will fail.

The ARP-reply-agent may only be enabled on SAPs supporting Ethernet encapsulation.

The **no** form of this command disables ARP-reply-agent functions for static and dynamic hosts on the MSAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **sub-ident** — Configures the arp-reply-agent to discard ARP requests received on the MSAP that are targeted for a known host on the same MSAP with the same subscriber identification.

Hosts are identified by their subscriber information. For DHCP subscriber hosts, the subscriber hosts, the subscriber information is configured using the optional subscriber parameter string.

When arp-reply-agent is enabled with **sub-ident**:

- If the subscriber information for the destination host exactly matches the subscriber information for the originating host and the destination host is known on the same MSAP as the source, the ARP request is silently discarded.
- If the subscriber information for the destination host or originating host is unknown or undefined, the source and destination hosts are not considered to be the same subscriber. The ARP request is forwarded outside the MSAP's Split Horizon Group.
- When **sub-ident** is not configured, the arp-reply-agent does not attempt to identify the subscriber information for the destination or originating host and will not discard an ARP request based on subscriber information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.292 arp-retry-timer

arp-retry-timer

Syntax **arp-retry-timer** *timer-multiple*
no arp-retry-timer

Context **[Tree]** (config>service>ies>if arp-retry-timer)

Full Context configure service ies interface arp-retry-timer

Description This command allows the arp retry timer to be configured to a specific value.

The timer value is entered as a multiple of 100 ms. So a timer value of 1, means the ARP timer will be set to 100 ms.

The **no** form of this command removes the command from the active configuration and returns the ARP retry timer to its default value of 5 seconds.

Default arp-retry-timer 50

Parameters *timer-multiple* — Specifies the multiple of 100 ms that the ARP retry timer will be configured as.

Values 1 to 300 (equally a timer range of 100 ms to 30,000 ms)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

arp-retry-timer

Syntax **arp-retry-timer** *timer-multiple*
no arp-retry-timer

Context **[Tree]** (config>service>vprn>if arp-retry-timer)
[Tree] (config>service>vprn>network-interface arp-retry-timer)

Full Context configure service vprn interface arp-retry-timer
configure service vprn network-interface arp-retry-timer

Description This command allows the arp retry timer to be configured to a specific value.

The timer value is entered as a multiple of 100 ms. So a timer value of 1, means the ARP timer will be set to 100 ms.

The **no** form of this command removes the command from the active configuration and returns the ARP retry timer to its default value of 5 s.

Default arp-retry-timer 50

Parameters *timer-multiple* — Specifies the multiple of 100 ms that the ARP retry timer will be configured as.

Values 1 to 300 (equally a timer range of 100 ms to 30 000 ms)

Platforms All

arp-retry-timer

Syntax **arp-retry-timer** *timer-multiple*
no arp-retry-timer

Context **[Tree]** (config>router>if arp-retry-timer)

Full Context configure router interface arp-retry-timer

Description This command allows the arp retry timer to be configured to a specific value.

The timer value is entered as a multiple of 100 ms. So a timer value of 1, means the ARP timer will be set to 100 ms.

The **no** form of this command removes the command from the active configuration and returns the ARP retry timer to its default value of 5 seconds.

Default arp-retry-timer 50

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *timer-multiple* — Specifies the multiple of 100 ms that the ARP retry timer will be configured as.

Values 1 to 300 (equally a timer range of 100 ms to 30,000 ms)

Platforms All

5.293 arp-route-tag

arp-route-tag

Syntax **arp-route-tag** *tag*
arp-route-tag

Context **[Tree]** (config>service>ies>if arp-route-tag)

Full Context configure service ies interface arp-route-tag

Description This command adds a route tag to the ARP-ND host routes generated from the ARP entries in the interface which can be used to match ARP-ND routes in BGP export policies.

The **no** form of this command removes the route tag for the ARP-ND host routes.

Parameters *tag* — Specifies the route tag value.

Values 1 to 255

5.294 arp-timeout

arp-timeout

Syntax **arp-timeout** *seconds*
no arp-timeout

Context **[Tree]** (config>service>ies>if arp-timeout)
[Tree] (config>service>ies>sub-if>grp-if arp-timeout)
[Tree] (config>service>vprn>if arp-timeout)
[Tree] (config>service>vprn>sub-if>grp-if arp-timeout)

Full Context configure service ies interface arp-timeout
configure service ies subscriber-interface group-interface arp-timeout
configure service vprn interface arp-timeout
configure service vprn subscriber-interface group-interface arp-timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the minimum time in seconds an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise, the ARP entry is aged from the ARP table. If **arp-timeout** is set to a value of zero seconds, ARP aging is disabled.

When the **arp-populate** and **lease-populate** commands are enabled on an IES interface, the ARP table entries will no longer be dynamically learned, but instead by snooping DHCP ACK message from a DHCP server. In this case the configured **arp-timeout** value has no effect.

The default value for **arp-timeout** is 14400 seconds (4 hours).

The **no** form of this command reverts to the default value.

Default arp-timeout 14400

Parameters *seconds* — Specifies the minimum number of seconds a learned ARP entry is stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface arp-timeout
- configure service ies subscriber-interface group-interface arp-timeout

All

- configure service vprn interface arp-timeout
- configure service ies interface arp-timeout

arp-timeout

Syntax **arp-timeout** *seconds*
no arp-timeout

Context **[Tree]** (config>service>vpls>interface arp-timeout)

Full Context configure service vpls interface arp-timeout

Description This command configures the minimum time in seconds an ARP entry learned on the IP interface will be stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise, the ARP entry is aged from the ARP table. If **arp-timeout** is set to a value of zero seconds, ARP aging is disabled.

For the 7450 ESS or 7750 SR, when the **arp-populate** and **lease-populate** commands are enabled on an interface, the ARP table entries will no longer be dynamically learned, but instead by snooping DHCP ACK message from a DHCP server. In this case the configured **arp-timeout** value has no effect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default value for **arp-timeout** is 14400 seconds (4 hours).

The **no** form of this command restores **arp-timeout** to the default value.

Default arp-timeout 14400

Parameters *seconds* — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

Values 0 to 65535

Platforms All

arp-timeout

Syntax **arp-timeout** *seconds*
no arp-timeout

Context **[Tree]** (config>router>if arp-timeout)

Full Context configure router interface arp-timeout

Description This command configures the minimum time, in seconds, an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host. Otherwise, the ARP entry is aged from the ARP table. If the **arp-timeout** value is set to 0 seconds, ARP aging is disabled.

The **no** form of this command reverts to the default value.

Default no arp-timeout

Parameters *seconds* — The minimum number of seconds a learned ARP entry is stored in the ARP table, expressed as a decimal integer. A value of 0 specifies that the timer is inoperative and learned ARP entries will not be aged.

Values 0 to 65535

Platforms All

5.295 as-matrix

as-matrix

Syntax [**no**] **as-matrix**

Context **[Tree]** (config>cflowd>collector>aggregation as-matrix)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure cflowd collector aggregation as-matrix

Description This command specifies that the aggregation data should be based on autonomous system (AS) information. An AS matrix contains packet and byte counters for traffic from either source-destination autonomous systems or last-peer to next-peer autonomous systems.

The **no** form of this command removes this type of aggregation from the collector configuration.

Default no as-matrix

Platforms All

5.296 as-override

as-override

Syntax [**no**] **as-override**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy as-override)

Full Context configure subscriber-mgmt bgp-peering-policy as-override

Description This command replaces all instances of the peer's AS number with the local AS number in a BGP route's AS_PATH.

This command breaks BGP's loop detection mechanism. It should be used carefully.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

as-override

Syntax [**no**] **as-override**

Context **[Tree]** (config>service>vprn>bgp>group as-override)
[Tree] (config>service>vprn>bgp>group>neighbor as-override)

Full Context configure service vprn bgp group as-override
configure service vprn bgp group neighbor as-override

Description This command replaces all instances of the peer's AS number with the local AS number in a BGP route's AS_PATH.

This command breaks BGP's loop detection mechanism. It should be used carefully.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no as-override

Platforms All

as-override

Syntax [**no**] **as-override**

Context **[Tree]** (config>router>bgp>group as-override)
[Tree] (config>router>bgp>group>neighbor as-override)

Full Context configure router bgp group as-override
configure router bgp group neighbor as-override

Description This command enables BGP to monitor the outbound routes toward the peer and whenever there is a route with the peer's autonomous system number (ASN) in the AS_PATH, all occurrences are removed and replaced with the advertising router's local ASN (or its confederation ID if the peer is outside the confederation).

In the group context, the **no** form of this command disables the functionality. In the neighbor context, the **no** form of this command causes the setting to be inherited from the group level.

Default no as-override

Platforms All

5.297 as-path

as-path

Syntax [**no**] **as-path** *name*

Context **[Tree]** (config>router>policy-options as-path)

Full Context configure router policy-options as-path

Description This command creates a route policy AS path to use in route policy entries.

The **no** form of this command deletes the AS path.

Default no as-path

Parameters *name* — The AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

as-path

Syntax **as-path** *name*
no as-path

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from as-path)

Full Context configure router policy-options policy-statement entry from as-path

Description This command configures an AS path regular expression statement as a match criterion for the route policy entry.

If no AS path criterion is specified, any AS path is considered to match.

AS path regular expression statements are configured at the global route policy level (**config>router>policy-options>as-path** *name*).

The **no** form of this command removes the AS path regular expression statement as a match criterion.

Default no as-path

Parameters *name* — Specifies the AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end", "@variable@end", or "start@variable@".

Platforms All

as-path

Syntax **as-path** {**add** | **replace**} *name*
no as-path

Context **[Tree]** (config>router>policy-options>policy-statement>default-action as-path)
[Tree] (config>router>policy-options>policy-statement>entry>action as-path)

Full Context configure router policy-options policy-statement default-action as-path
configure router policy-options policy-statement entry action as-path

Description This command assigns a BGP AS path list to routes matching the route policy statement entry.

If no AS path list is specified, the AS path attribute is not changed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the AS path list editing action from the route policy entry.

Default no as-path

Parameters **add** — Specifies that the AS path list is to be prepended to an existing AS list.

replace — Specifies AS path list replaces any existing as path attribute.

name — Specifies the AS path list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end"," @variable@end", or "start@variable@".

The *name* specified must already be defined.

Platforms All

5.298 as-path-group

as-path-group

Syntax [**no**] **as-path-group** *name*

Context **[Tree]** (config>router>policy-options as-path-group)

Full Context configure router policy-options as-path-group

Description This command creates a route policy AS path regular expression statement to use in route policy entries.

The **no** form of this command deletes the AS path regular expression statement.

Default no as-path-group

Parameters *name* — Specifies the AS path regular expression name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

as-path-group

Syntax **as-path-group** *name*
no as-path-group *name*

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from as-path-group)

Full Context configure router policy-options policy-statement entry from as-path-group

Description This command creates a route policy AS path regular expression statement to use in route policy entries.

The **no** form of this command deletes the AS path regular expression statement.

Default no as-path-group

Parameters *name* — Specifies the AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end", "@variable@end", or "start@variable@".

Platforms All

5.299 as-path-ignore

as-path-ignore

Syntax **as-path-ignore** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**]
no as-path-ignore

Context **[Tree]** (config>service>vprn>bgp>path-selection as-path-ignore)

Full Context configure service vprn bgp best-path-selection as-path-ignore

Description This command configures whether AS path length is considered in the selection of the best BGP route for a prefix.

If an address family is listed in this command, the length of AS paths is not a factor in the route selection process for routes of that address family.

The **no** form of this command removes the parameter from the configuration.

Default no as-path-ignore

Parameters **ipv4** — Specifies that the AS path length is ignored for all unlabeled unicast IPv4 routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6 — Specifies that the AS path length is ignored for all unlabeled unicast IPv6 routes.

label-ipv4 — Specifies that the AS path length is ignored for all labeled unicast IPv4 routes.

label-ipv6 — Specifies that the AS path length is ignored for all labeled unicast IPv6 routes.

Platforms All

as-path-ignore

Syntax **as-path-ignore** [**ipv4**] [**label-ipv4**] [**vpn-ipv4**] [**ipv6**] [**label-ipv6**] [**vpn-ipv6**] [**mcast-ipv4**] [**mcast-ipv6**] [**mvpn-ipv4**] [**mvpn-ipv6**] [**l2-vpn**]
no as-path-ignore

Context **[Tree]** (config>router>bgp>best-path-selection as-path-ignore)

Full Context configure router bgp best-path-selection as-path-ignore

Description This command configures whether AS path length is considered in the selection of the best BGP route for a prefix.

If an address family is listed in this command, then the length of AS paths is not a factor in the route selection process for routes of that address family.

The **no** form of this command removes the parameter from the configuration.

Default no as-path-ignore

Parameters **ipv4** — Specifies that the AS-path length will be ignored for all unlabeled unicast IPv4 routes.

label-ipv4 — Specifies that the AS-path length will be ignored for all labeled-unicast IPv4 routes.

vpn-ipv4 — Specifies that the length AS-path will be ignored for all VPN IPv4 (SAFI 128) routes.

ipv6 — Specifies that the AS-path length will be ignored for all unlabeled unicast IPv6 routes.

label-ipv6 — Specifies that the AS-path length will be ignored for all labeled-unicast IPv6 routes.

vpn-ipv6 — Specifies that the AS-path length will be ignored for all VPN IPv6 (SAFI 128) routes.

mcast-ipv4 — Specifies that the AS-path length will be ignored for all IPv4 multicast routes.

mcast-ipv6 — Specifies that the AS-path length will be ignored for all IPv6 multicast routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mvpn-ipv4 — Specifies that the AS-path length will be ignored for all IPv4 MVPN routes.

mvpn-ipv6 — Specifies that the AS-path length will be ignored for all IPv6 MVPN routes.

l2-vpn — Specifies that the AS-path length will be ignored for all L2-VPN NLRIs.

Platforms All

5.300 as-path-length

as-path-length

Syntax **as-path-length** *length* [**equal** | **or-higher** | **or-lower**] [**unique**]
no as-path-length

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from as-path-length)

Full Context configure router policy-options policy-statement entry from as-path-length

Description This command matches BGP routes based on their AS path length (the number of AS numbers in the AS_PATH).

If no comparison qualifiers are present (**equal**, **or-higher**, **or-lower**), then **equal** is the implied default.

Confederation member AS numbers in the AS_PATH do not count towards the total. An AS_SET element is considered to have a length of 1.

The **unique** option counts.

A non-BGP route does not match a policy entry if it contains the **as-path-length** command.

Default no as-path-length

Parameters *length* — Specifies the length of the AS path.

Values 0 to 255, or a parameter name delimited by starting and ending at-sign (@) characters

equal — Specifies that matched routes should have the same number of AS path elements as the value specified.

or-higher — Specifies that matched routes should have the same or a greater number of AS path elements as the value specified.

or-lower — Specifies that matched routes should have the same or a lower number of AS path elements as the value specified.

unique — Specifies that only the unique AS numbers should be counted (that is, multiple occurrences of the same AS number in the sequence count as one).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

5.301 as-path-prepend

as-path-prepend

Syntax **as-path-prepend** *as-path* [*repeat*]
as-path-prepend most-recent [*repeat*]
no as-path-prepend

Context **[Tree]** (config>router>policy-options>policy-statement>default-action as-path-prepend)
[Tree] (config>router>policy-options>policy-statement>entry>action as-path-prepend)

Full Context configure router policy-options policy-statement default-action as-path-prepend
configure router policy-options policy-statement entry action as-path-prepend

Description The command prepends a BGP AS number once or numerous times to the AS path attribute of routes matching the route policy statement entry.

If an AS number is not configured, the AS path is not changed.

If the optional *number* is specified, then the AS number is prepended as many times as indicated by the number.

The **no** form of this command disables the AS path prepend action from the route policy entry.

Default no as-path-prepend

Parameters *as-path* — Specifies the AS number to prepend expressed as a decimal integer.

Values 1 to 4294967295

param-name — Specifies the AS path parameter variable name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

repeat — Specifies the number of times to prepend the specified AS number expressed as a decimal integer.

Values 1 to 50

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

param-name — Specifies the AS path parameter variable name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

most-recent — Specifies that the most recent AS number must be prepended to the AS-Path attribute of the route.

Platforms All

5.302 asbr

asbr

Syntax [**no**] **asbr** [**trace-path** *domain-id*]
no asbr
[**no**] **asbr**

Context **[Tree]** (config>router>ospf asbr)
[Tree] (config>router>ospf3 asbr)

Full Context configure router ospf asbr
configure router ospf3 asbr

Description This command configures the router as an Autonomous System Boundary Router (ASBR) if the router is to be used to export routes from the Routing Table Manager (RTM) into this instance of OSPF. After a router is configured as an ASBR, the export policies into this OSPF domain take effect. If no policies are configured, no external routes are redistributed into the OSPF domain.

The **no** form of this command removes the ASBR status and withdraws the routes redistributed from the Routing Table Manager into this instance of OSPF from the link state database.

When configuring multiple instances of OSPF, there is a risk of loops because networks are advertised by multiple domains configured with multiple interconnections to one another. To prevent this from happening, all routers in a domain should be configured with the same domain ID. Each domain (OSPF-instance) should be assigned a specific bit value in the 32-bit tag mask.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an external route is originated by an ASBR using an internal OSPF route in a given domain, the corresponding bit is set in the AS-external LSA. As the route gets redistributed from one domain to another, more bits are set in the tag mask, each corresponding to the OSPF domain the route visited. Route redistribution looping is prevented by checking the corresponding bit as part of the export policy; if the bit corresponding to the announcing OSPF process is already set, the route is not exported there.

Domain IDs are incompatible with any other use of normal tags. The domain ID should be configured with a value between 1 and 31 by each router in a given OSPF domain (OSPF Instance).

When an external route is originated by an ASBR using an internal OSPF route in a given domain, the corresponding (1-31) bit is set in the AS-external LSA.

As the route gets redistributed from one domain to another, more bits are set in the tag mask, each corresponding to the OSPF domain the route visited. Route redistribution looping is prevented by checking the corresponding bit as part of the export policy; if the bit corresponding to the announcing OSPF process is already set, the route is not exported there.

Default no asbr

Parameters *domain-id* — Specifies the domain ID.

Values 1 to 31

Default 0

Platforms All

5.303 assert

assert

Syntax **assert** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no assert

Context **[Tree]** (debug>router>pim assert)

Full Context debug router pim assert

Description This command enables debugging for PIM assert mechanism.

The **no** form of this command disables PIM assert debugging.

Parameters *grp-ip-address* — Debugs information associated with the PIM assert mechanism.

Values multicast group address (ipv4, ipv6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address — Debugs information associated with the PIM assert mechanism.

Values source address (ipv4, ipv6)

detail — Debugs detailed information on the PIM assert mechanism.

Platforms All

5.304 assert-period

assert-period

Syntax **assert-period** *assert-period*
no assert-period

Context **[Tree]** (config>service>vprn>pim>if assert-period)

Full Context configure service vprn pim interface assert-period

Description This command configures the period in seconds for periodic refreshes of PIM Assert messages on an interface.

The **no** form of this command reverts to the default.

Default assert-period 60

Parameters *assert-period* — Specifies the period, in seconds, for periodic refreshes of PIM Assert messages on an interface.

Values 1 to 300

Platforms All

assert-period

Syntax **assert-period** *assert-period*
no assert-period

Context **[Tree]** (config>router>pim>interface assert-period)

Full Context configure router pim interface assert-period

Description This command configures the period for periodic refreshes of PIM Assert messages on an interface.

The **no** form of this command removes the assert-period from the configuration.

Default no assert-period

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *assert-period* — Specifies the period, in seconds, for periodic refreshes of PIM Assert messages on an interface.

Values 1 to 300

Platforms All

5.305 assignment

assignment

Syntax **assignment** {**port** *port-id* | **card** *slot-number*}
no assignment

Context **[Tree]** (config>service>cust>multi-service-site assignment)

Full Context configure service customer multi-service-site assignment

Description This command assigns a multi-service customer site to a specific chassis slot, port, or channel. This allows the system to allocate the resources necessary to create the virtual schedulers defined in the ingress and egress scheduler policies as they are specified. This also verifies that each SAP assigned to the site exists within the context of the proper customer ID and that the SAP was configured on the proper slot, port, or channel. The assignment must be given prior to any SAP associations with the site.

The **no** form of this command removes the port, channel, or slot assignment. If the customer site has not yet been assigned, the command has no effect and returns without any warnings or messages.

Default no assignment

Parameters *port-id* — Assigns the multi-service customer site to the port-id or port-id.channel-id given. When the multi-service customer site is assigned to a specific port or channel, all SAPs associated with this customer site must be on a service owned by the customer and created on the defined port or channel. The defined port or channel must already have been pre-provisioned on the system but need not be installed when the customer site assignment is made.

Syntax: *port-id*[:encap-val]

Values For the 7950 XRS:

port-id	slot/mda/port [.channel]		
	eth-tunnel-id - eth-tunnel-<id>		
		eth-tunnel	keyword
		id	[1..1024]
	lag-id	lag-id	

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	lag	keyword
	id	1 to 800
gtg-id	gmpls-tun-grp-<id>	
	gmpls-tun-grp	keyword
	id	[1..1024]
eth-sat-id	esat-id/slot/port	
	esat	keyword
	id: 1 to 20	
	u	keyword
pxc-id	pxc-<id>.<sub-port>	
	pxc	keyword
	id: 1 to 64	
	sub-port	a, b
lag		keyword
id	1 to 800	1 to 800
pw-id	pw-<id>	
	pw	keyword
	id	1 to 32767

For the 7750 SR and the 7450 ESS:

port-id	slot/mda/port[.channel]		
	bundle-id	bundle-<type>-slot/mda.<bundle-num>	
		bundle	keyword
		type	ima, ppp
		bundle-num	1 to 256
	bpgrp-id:	bpgrp-type-bpgrp-num	
		bpgrp	keyword
		type	ima
		bpgrp-num	1 to 1280
	aps-id	aps-group-id[.channel]	
		aps keyword	
		group-id	1 to 128
	eth-tunnel-id	eth-tunnel-<id>	
		eth-tunnel	keyword
		id	1 to 1024
	lag-id	lag-id	
		lag	keyword
		id	1 to 800

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	gtg-id	gmpls-tun-grp-<id>	
		gmpls-tun-grp	keyword
		id	1 to 1024
	eth-sat-id	esat-<id>/<slot>/[u]<port>	
		esat	keyword
		id	1 to 20
		u	keyword for up-link port
	tdm-sat-id	tsat-<id>/<slot>/[<u>]<port>.<channel>	
		tsat	keyword
		id	1 to 20
		u	keyword for up-link port
	pxc-id	psc-id.sub-port	
		pxc psc-id.sub-port	
		pxc	keyword
		id: 1 to 64	
		sub-port: a, b	
	pw-id	pw-<id>	
		pw	keyword
		id	1 to 32767
slot-number	1 to 10		
fpe-id	1 to 64		

slot-number — Assigns the multi-service customer site to the slot-number given. When the multi-service customer site is assigned to a specific slot in the chassis, all SAPs associated with this customer site must be on a service owned by the customer and created on the defined chassis slot. The defined slot must already be pre-provisioned on the system but need not be installed when the customer site assignment is made.

Values Any pre-provisioned slot number for the chassis type that allows SAP creation.

1 to 20

fpe-id — Specifies the multi-service-site (MSS) assignment to an FPE object for the purpose of controlling aggregated bandwidth across a set of PW SAPs.

Values 1 to 64

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.306 assignment-id

assignment-id

Syntax **assignment-id** *assignment-id*

Context **[Tree]** (debug>router>l2tp assignment-id)

Full Context debug router l2tp assignment-id

Description This command enables and configures debugging for the L2TP tunnel with a given assignment ID.

Parameters *assignment-id* — Specifies a string that distinguishes this L2TP tunnel, up to 63 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.307 assisted-replication

assisted-replication

Syntax **assisted-replication** {**replicator** | **leaf**} [**replicator-activation-time** *seconds*]
no assisted-replication

Context **[Tree]** (config>service>vpls>vxlan assisted-replication)

Full Context configure service vpls vxlan assisted-replication

Description This command enables the Assisted Replication (AR) function for VXLAN tunnels in the service. The execution of this command triggers the BGP EVPN to send an update containing the inclusive multicast route for the service and the AR type=AR Replicator (AR-R) or AR Leaf (AR-L).

The Replicators switch the VXLAN traffic back to VXLAN destinations when the IP destination address matches their own AR-IP address. Leaf nodes select a Replicator node and send all the Broadcast or Multicast frames to it so that the Replicator can replicate the traffic on their behalf.

Enabling or disabling the AR function, or changing the role between the replicator and leaf requires the BGP EVPN MPLS to be shutdown.

If the **leaf** parameter is configured, the system creates a Broadcast or Multicast (BM) destination to the selected AR-R and Unknown Unicast (U) destinations to the rest of the VTEPs. If no replicator exists, the leaf creates BUM bindings to all the VTEPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the **replicator** parameter is configured, the system will create BUM destinations to the remote leafs, Regular Network Virtualization Edge routers (RNVE), and other AR-Rs. The system will perform assisted replication for traffic from known VTEPs only (that is, where the routes have been received and programmed toward a VTEP).

The **no** version of this command removes the AR function from the service.

Default no assisted-replication

Parameters **replicator-activation-time** *seconds* — Optional parameter that can be added to the leaf parameter. It specifies the wait time before the leaf can begin sending traffic to a new replicator and is used to allow some time for the replicator to learn about the leaf.

Values 1 to 255

Default 0 seconds (indicates **no replicator-activation-time** and no delay in sending packets to the AR-R)

replicator | leaf — Selects the AR role of the router for the service.

Platforms All

5.308 assisted-replication-ip

assisted-replication-ip

Syntax **assisted-replication-ip** *ip-address*
no assisted-replication-ip

Context **[Tree]** (config>service>system>vxlan assisted-replication-ip)

Full Context configure service system vxlan assisted-replication-ip

Description The assisted-replication-ip (AR-IP) command defines the IP address that supports the AR-R function in the router. The AR-IP address must also be defined as a loopback address in the base router and advertised in the IGP/BGP so that it is accessible to the remote NVE/PEs in the Overlay network.

If the AR-R function is enabled in a service, the Broadcast and Multicast frames encapsulated in VXLAN packets arriving at the router are replicated to the other VXLAN destinations within the service (except the destination pointing at the originator of the packet).

The **no** version of this command removes the AR IP address.

Default no assisted-replication-ip

Parameters *ip-address* — Specifies the assisted replication IP address.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.309 assistive-address-resolution

assistive-address-resolution

Syntax [**no**] **assistive-address-resolution**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext assistive-address-resolution)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext assistive-address-resolution)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext assistive-address-resolution
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext assistive-address-resolution

Description This command enables assistive address resolution (AAR) for HLE services.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.310 association

association

Syntax **association** *name*
no association

Context **[Tree]** (config>service>vpls>sap>pfcp association)

Full Context configure service vpls sap pfcp association

Description This command links this capture SAP to a PFCP association. This command enables CUPS for this capture SAP and makes any trigger packets eligible for forwarding to the BNG CUPS CPF.

The **no** form of this command disables CUPS for this capture SAP.

Parameters *name* — Specifies the name of the association, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

association

Syntax **association** *ma-index* [**format** {*format*}] **name** *ma-name* [**admin-name** *admin-name*]
association *ma-index*
no association *ma-index*

Context **[Tree]** (config>eth-cfm>domain association)

Full Context configure eth-cfm domain association

Description This command configures the Maintenance Association (MA) for the domain.

Parameters *ma-index* — Specifies the MA index value.

Values 1 to 4294967295

format — Specifies a value that represents the type (format).

Values icc-based, integer, string, vid, vpn-id

icc-based: Only applicable to a Y.1731 context where the domain format is configured as none. Allows for exactly a 13 character name.

integer 0 to 65535 (integer value 0 means the MA is not attached to a VID.)

string: raw ascii

vid: 0 to 4095

vpn-id: RFC 2685, *Virtual Private Networks Identifier*
xxx:xxxx, where x is a value between 00 and FF.
for example 00164D:AABBCCDD

Default integer

ma-name — Specifies the part of the maintenance association identifier which is unique within the maintenance domain name.

Values 1 to 45 characters

admin-name *admin-name* — Specifies a creation time required parameter that allows the operator to assign a name value to the domain container. This is used for information and migration purposes. This value cannot be modified without destroying the domain. If no **admin-name** exists, the configured *md-index* value will be converted into a character string to become the **admin-name** reference. When upgrading from a release that does not include the **admin-name** configuration option, the *md-index* will be converted into a character string. Once a value is assigned to this *admin-name* value it cannot be modified.

Values 1 to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.311 association-setup-retry

association-setup-retry

Syntax **association-setup-retry** *seconds*

Context **[Tree]** (config>subscr-mgmt>pfcp-association association-setup-retry)

Full Context configure subscriber-mgmt pfcp-association association-setup-retry

Description This command configures how frequently the association setup is retried until the setup is completed.

Default association-setup-retry 10

Parameters *seconds* — Specifies the time frame, in seconds, for association setup retries.

Values 1 to 36000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.312 async-mapping

async-mapping

Syntax [**no**] **async-mapping**

Context **[Tree]** (config>port>otu async-mapping)

Full Context configure port otu async-mapping

Description This command allows the user to configure the port to support asynchronous mapping of the payload inside the OTU. If the port is configured for async-mapping and the payload clock is asynchronous to the OTU clock, there will be positive or negative pointer justification that will show up in the OTU statistics and the data will be received error free. If the port is configured for synchronous mapping and the received data is asynchronously mapped, there will be errors in the received data.

async-mapping is the only mode of operation that is supported on the OTU3 encapsulated 40-Gigabit Ethernet and therefore the 'no async-mapping' is not supported on that port type and the default on the is async-mapping.

The **no** form of this command configures the port to receive synchronously mapped data.

Default no async-mapping

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.313 asynchronous-execution

asynchronous-execution

Syntax **asynchronous-execution** *seconds*
asynchronous-execution never

Context **[Tree]** (config>system>management-interface>ops>global-timeout asynchronous-execution)

Full Context configure system management-interface operations global-timeouts asynchronous-execution

Description This command configures the period of time that operations launched as “asynchronous” are allowed to execute before being automatically stopped by the SR OS.

An asynchronous operation is not deleted from the system when it is stopped. See the **asynchronous-retention** command.

If a specific execution timeout is not included in the request for a particular asynchronous operation, this system-level timeout applies.

Note: This execution timeout is part of the general global operations infrastructure and is separate and independent from any operation-specific timeouts (for example, the **ping** operation also has its own **timeout** parameter).

Default asynchronous-execution 3600

Parameters *seconds* — Specifies the period of time, in seconds, that asynchronous operations are allowed to execute.

Values 1 to 604800

never — Keyword to specify that an execution timeout is not applied to asynchronous operations.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.314 asynchronous-retention

asynchronous-retention

Syntax **asynchronous-retention** *seconds*
asynchronous-retention never

Context **[Tree]** (config>system>management-interface>ops>global-timeout asynchronous-retention)

Full Context configure system management-interface operations global-timeouts asynchronous-retention

Description This command configures the period of time that data related to operations launched as “asynchronous” is retained in the system. After the retention timeout expires, all information related to the operation is deleted, including any status information and result data.

If a specific retention timeout is not included in the request for a particular asynchronous operation, this system-level timeout applies.

Default asynchronous-retention 86400

Parameters *seconds* — Specifies the period of time, in seconds, that data related to asynchronous operations is retained in the system.

Values 1 to 604800

never — Keyword to specify that data related to asynchronous operations will persist in memory until explicitly deleted.

Platforms All

5.315 atm

atm

Syntax **atm**

Context **[Tree]** (config>service>ies>if>sap atm)
[Tree] (config>service>ies>sub-if>grp-if>sap atm)
[Tree] (config>service>vpls>sap atm)
[Tree] (config>service>vprn>if>sap atm)
[Tree] (config>service>vprn>sub-if>grp-if>sap atm)

Full Context configure service ies interface sap atm
configure service ies subscriber-interface group-interface sap atm
configure service vpls sap atm
configure service vprn interface sap atm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap atm

Description This command the context to configure ATM-related parameters. This command can only be used when a given context (for example, a channel or SAP) supports ATM functionality such as:

- Configuring ATM port or ATM port-related functionality on MDAs supporting ATM functionality
- Configuring ATM-related configuration for ATM-based SAPs that exist on MDAs supporting ATM functionality.

If ATM functionality is not supported for a given context, the command returns an error.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service vprn subscriber-interface group-interface sap atm
- configure service ies subscriber-interface group-interface sap atm

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service vprn interface sap atm
- configure service vpls sap atm
- configure service ies interface sap atm

atm

Syntax **atm**

Context **[Tree]** (config>service>vpls>sap atm)

Full Context configure service vpls sap atm

Description This command enables access to the context to configure ATM-related attributes. This command can only be used when a specified context (for example, a channel or SAP) supports ATM functionality such as:

- Configuring ATM port or ATM port-related functionality on MDAs supporting ATM functionality
- Configuring ATM-related configuration for ATM-based SAPs that exist on MDAs supporting ATM functionality.

If ATM functionality is not supported for a specified context, the command returns an error.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

atm

Syntax **atm**

Context **[Tree]** (config>port>sonet-sdh>path atm)
[Tree] (config>port>tdm>ds1>channel-group atm)
[Tree] (config>port>tdm>ds3 atm)
[Tree] (config>port>tdm>e1>channel-group atm)
[Tree] (config>port>tdm>e3 atm)
[Tree] (config>port>ml-bundle>ima atm)

Full Context configure port multilink-bundle ima atm
configure port sonet-sdh path atm
configure port tdm ds1 channel-group atm
configure port tdm ds3 atm
configure port tdm e1 channel-group atm
configure port tdm e3 atm

Description Commands in this context configure ATM interface properties.

Platforms 7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle ima atm

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 atm
- configure port tdm e1 channel-group atm
- configure port tdm ds1 channel-group atm
- configure port tdm ds3 atm

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure port sonet-sdh path atm

atm

Syntax [**no**] **atm**

Context **[Tree]** (debug atm)

Full Context debug atm

Description This command enables, disables and configures debugging for the ATM.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

atm

Syntax **atm**

Context **[Tree]** (config>service>apipe>sap atm)
[Tree] (config>service>epipe>sap atm)
[Tree] (config>service>ipipe>sap atm)

Full Context configure service apipe sap atm
configure service epipe sap atm
configure service ipipe sap atm

Description This command enables access to the context to configure ATM-related attributes. This command can only be used when a specified context (for example, a channel or SAP) supports ATM functionality such as:

- Configuring ATM port or ATM port-related functionality on MDAs supporting ATM functionality.
- Configuring ATM-related configuration for ATM-based SAPs that exist on MDAs supporting ATM functionality.

If ATM functionality is not supported for a specified context, the command returns an error.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

atm

Syntax **atm**

Context **[Tree]** (config>system atm)

Full Context configure system atm

Description Commands in this context configure system-wide ATM parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

atm

Syntax **atm**

Context **[Tree]** (config>subscr-mgmt>msap-policy atm)

Full Context configure subscriber-mgmt msap-policy atm

Description Commands in this context configure system-wide ATM parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.316 atm-location-id

atm-location-id

Syntax **atm-location-id** *location-id*
no atm-location-id

Context **[Tree]** (config>system>atm atm-location-id)

Full Context configure system atm atm-location-id

Description This command indicates the location ID for ATM OAM.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Services Overview Guide* for information about ATM QoS policies and ATM-related service parameters.

Default no atm-location-id

Parameters *location-id* — Specifies the 16 octets that identifies the system loopback location ID as required by the ATM OAM Loopback capability. This textual convention is defined in ITU-T standard I.610. The loopback location ID should be entered in the following format: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.

Invalid values include a location ID where the first octet is: 00, FF, 6A Acceptable *location-ids* include values where the first octet is: 01, 03 Other values are not accepted.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

5.317 atm-ping

atm-ping

Syntax **atm-ping** {*port-id* | *bundle-id* | *aps-id* | *bpgrp-id* [{:**vpi/vci** | **vpi**}]} [{**end-to-end** | **segment**}] [**dest** *destination-id*] [**send-count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam atm-ping)

Full Context oam atm-ping

Description This command tests ATM path connectivity and round trip time on an ATM VCC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id*[{*:* **vpi/vci** | **vpi**}] — Specifies the ID of the access port of the target VC. This parameter is required.

Values		
port-id	*slot*/*mda*/*port*	
bundle-id	bundle-<*type*>-*slot/mda*.<*bundle-num*>	
	bundle	keyword
	type	ima
	bundle-num	1 to 336
bpgrp-id	bpgrp-<*type*>-<*bpgrp-num*>	
	bpgrp	keyword
	type	ima
	bpgrp-num	1 to 2000
aps-id	*aps-group-id*	
	aps	keyword
	group-id	1 to 128
vpi	0 to 4095 (NNI)	
	0 to 255 (UNI)	
vci	1, 2, 5 to 65535	

end-to-end | segment — Specifies whether the ATM OAM loopback cell is destined to the first segment point in the line direction or the PVCC's connection endpoint.

Default end-to-end

destination-id — Specifies the LLID field in an OAM loopback cell. If set to all 1s, only the connection end (end-to-end ping) or segment end (segment ping) responds to the ping. If the **segment** parameter is specified and **dest** is set to a specific destination, only the destination responds to the ping.

Values xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

A 16 byte octet string, with each octet separated by a colon. If not specified, then the values of 0x11 are used.

Default FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF

send-count — Specifies the number of messages to send, expressed as a decimal integer. The **send-count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must have expired before the next message request is sent.

Values 1 to 100

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded.

Values 1 to 10

Default 5

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

5.318 atm-td-profile

atm-td-profile

Syntax **atm-td-profile** *traffic-desc-profile-id* [**create**]
no atm-td-profile *traffic-desc-profile-id*

Context **[Tree]** (config>qos atm-td-profile)

Full Context configure qos atm-td-profile

Description This command is used to configure an ATM traffic descriptor profile.

Traffic descriptor profiles are used to:

1. Define traffic management capabilities for ATM PVCCs.
2. Calculate the total bandwidth consumed on a given port by all ATM PVCC(s). The BW taken by a PVCC is equal to:
   a. PIR for CBR PVCCs
   b. SIR for rt-vbr and nrt-vbr PVCCs
   c. MIR for UBR PVCC
3. Define ATM-level SAR scheduling

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default traffic descriptor is preconfigured and non-modifiable. It cannot be deleted. All other traffic descriptor profiles must be explicitly created before use. The create keyword must follow each new profile configuration.

Any changes made to the existing profile, using any of the sub-commands, are applied immediately to all objects where this profile is applied (a small traffic interruption in data traffic will occur during the data plane reprogramming with the newly modified profile).

When many changes are required on a profile, it is recommended that the profile be copied to a work area profile ID. That work-in progress profile can be modified until complete, then written over the original profile-id. Use the config qos copy command to maintain profiles in this manner.

The weight assigned to each non-shaped PVCC in the Deficit Round Robin Scheduler depends on the service category and traffic rates (see the **config>qos>atm-td-profile traffic** command for more details).

The **no** form of this command deletes a given traffic profile. The profile to be deleted must not be associated with any object (for example, a SAP). If this condition is not met, the command will return an error.

Default atm-td-profile 1 — Default Traffic Descriptor (UBR, no traffic, no shaping)

Parameters *traffic-desc-profile-id* — Index identifier for a traffic descriptor profile

Values 1 to 1000

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

atm-td-profile

Syntax **atm-td-profile** *src-prof dst-prof* [**overwrite**]

Context **[Tree]** (config>qos>copy atm-td-profile)

Full Context configure qos copy atm-td-profile

Description This command copies the source atm profile into the destination atm profile. If the destination profile was already defined, the keyword 'overwrite' must be appended for the copy to complete.

The **copy** command is a configuration-level maintenance tool used to create new profiles using existing profiles. It also allows bulk modifications to an existing profile with the use of the **overwrite** keyword.

Parameters **atm-td-profile** *src-prof dst-prof* — Indicates that the source profile ID and the destination profile ID are atm-td-profile IDs. Specify the source ID that the copy command will copy and specify the destination ID to which the command will duplicate the profile to a new or different profile ID.

Values 1 to 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

overwrite — Specifies to replace the existing destination profile. Everything in the existing destination policy will be overwritten with the contents of the source policy. If **overwrite** is not specified, an error will occur if the destination profile ID exists.

```
A:ALA-48>config>qos# copy atm-td-profile 2 10
MINOR: CLI destination (10) exists use {overwrite}.
A:ALA-48>config>qos# copy atm-td-profile 2 10 overwrite
A:ALA-48>config>qos#
```

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

5.319 atm-vci

atm-vci

Syntax **atm-vci** *vci-value*
no atm-vci

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match atm-vci)

Full Context configure qos sap-ingress mac-criteria entry match atm-vci

Description This command configures a VCI based filter entry in the SAP ingress QoS policy.

This new criterion only takes effect when applied to a VPI SAP of an Apipe VLL service of type atm-vpc. The application of this criterion to the ATM SAP of any other ATM VLL service, any other VLL service, VPLS service, or IES/VPRN service has no effect.

The user is not allowed to configure a MAC matching criterion other than atm-vci when a MAC criteria filter entry that includes the frame type of atm has been configured.

When the policy is applied to the ingress ATM VPI SAP of an atm-vpc VLL service and a received packet matches the VCI value configured in the atm-vci parameter, it is assigned the FC in the fc option of the action part of the filter. This determines in which forwarding class queue this packet will be stored. If the user entered a priority value in the priority option, it is ignored as the priority and profile of ATM VLL service packets are solely determined based on the ATM conformance definition configured in the ATM QoS traffic descriptor profile applied to this ATM SAP.

On egress ATM SAP, the Q-chip will queue the packet on the egress SAP queue corresponding to the packet's FC and forward the packet to the ATM MDA. The ATM MDA stores the individual cells in the VP queue corresponding to the SAP.

It is strongly recommended that the user does not enable cell-concatenation on the spoke-SDP when a VCI QoS filter is applied to the SAP. The filter will match against the VCI in the header of the first cell in the concatenated packet. Cell concatenation is disabled by default on a spoke-SDP of all ATM VLL service types.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the VCI value as the match criterion.

Parameters *vci-value* — The value of the VCI field in the received ATM cell header.

Values 1, 2, 5 to 65535

Platforms All

5.320 attempts

attempts

Syntax **attempts** *count* [**time** *minutes1* [**lockout** *minutes2*]
no attempts

Context **[Tree]** (config>system>security>password attempts)

Full Context configure system security password attempts

Description This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.

If the threshold is exceeded, the user is locked out for a specified time period.

If multiple **attempts** commands are entered, each command overwrites the previously entered command.

The **no attempts** command resets all values to default.

Note: This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

Default attempts 3 time 5 lockout 10

Parameters *count* — Specifies the number of unsuccessful login attempts allowed for the specified **time**. This is a mandatory value that must be explicitly entered.

Values 1 to 64

minutes — Specifies the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.

Values 0 to 60

minutes — Specifies the lockout period, in minutes, during which the user is not allowed to login.

Values 0 to 1440, or infinite

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the user exceeds the attempted **count** times in the specified **time**, then that user is locked out from any further login attempts for the configured lockout time period.

Values 0 to 1440

Values infinite; user is locked out and must wait until manually unlocked before any further attempts.

Platforms All

attempts

Syntax **attempts** [*count*] [**time** *minutes1*] [**lockout** *minutes2*]
no attempts

Context **[Tree]** (config>system>security>snmp attempts)

Full Context configure system security snmp attempts

Description This command configures a threshold value of unsuccessful SNMP connection attempts allowed in a specified time frame. The command parameters are used to counter denial of service (DoS) attacks through SNMP.

If the threshold is exceeded, the host is locked out for the lockout time period.

If multiple **attempts** commands are entered, each command overwrites the previously entered command.

The **no** form of the command restores the default values, in which 20 failed SNMP attempts are allowed in a 5 minute period with a 10 minute lockout for the host if exceeded.

Default attempts 20 time 5 lockout 10

Parameters *count* — Specifies the number unsuccessful SNMP attempts allowed for the specified **time**.

Values 1 to 64

minutes1 — Specifies period of time, in minutes, that a specified number of unsuccessful attempts can be made before the host is locked out.

Values 0 to 60

minutes2 — Specifies the lockout period in minutes where the host is not allowed to login. When the host exceeds the attempted count times in the specified time, then that host is locked out from any further login attempts for the configured time period.

Values 0 to 144**0**

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.321 attrib

attrib

Syntax **attrib** [**+r** | **-r**] *file-url*
attrib

Context **[Tree]** (file attrib)

Full Context file attrib

Description This command sets or clears/resets the read-only attribute for a file in the local file system. To list all files and their current attributes enter **attrib** or **attrib x** where **x** is either the filename or a wildcard (*).

When an **attrib** command is entered to list a specific file or all files in a directory, the file's attributes are displayed with or without an "R" preceding the filename. The "R" implies that the **+r** is set and that the file is read-only. Files without the "R" designation implies that the **-r** is set and that the file is read-write-all. For example:

```
ALA-1>file cf3:\ # attrib
cf3:\bootlog.txt
cf3:\bof.cfg
cf3:\boot.ldr
cf3:\sr1.cfg
cf3:\test
cf3:\bootlog_prev.txt
cf3:\BOF.SAV
```

Parameters *file-url* — Specifies the URL for the local file.

Values

local-url	[*cflash-id*/][*file-path*] up to 200 characters, including cflash-id directory length 99 chars max each
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 199 characters
remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

+r — Sets the read-only attribute on the specified file.

-r — Clears/resets the read-only attribute on the specified file.

Platforms All

5.322 attribute

attribute

Syntax **attribute** [**vendor** *vendor-id*] **attribute-type** *attribute-type*
no attribute

Context **[Tree]** (config>router>nat>inside>subscriber-identification attribute)
[Tree] (config>service>vprn>nat>inside>subscriber-identification attribute)

Full Context configure router nat inside subscriber-identification attribute
configure service vprn nat inside subscriber-identification attribute

Description This command defines the attribute that will in addition to framed-ip-address (inside IP address) and service-id be used for correlating BNG subscriber with the NAT subscriber.

Only a single attribute at the time can be configured. The attribute will be extracted from the BNG accounting start and/or interim-update messages via RADIUS accounting proxy server. This attribute can be then optionally passed to the Large Scale NAT44 accounting server. User-name attribute (if included) in Large Scale NAT44 accounting messages will be automatically set to the subscriber-id string.

The attribute parameter can be changed at any given time and the change will be reflected automatically when the next interim-update message from the BNG host is received by the RADIUS accounting proxy.

In case that the BNG accounting message in RADIUS accounting proxy does not contain this attribute, subscriber aware Large Scale NAT44 functionality for this particular subscriber will be disabled.

Default attribute vendor "nokia" attribute-type "alc-sub-string"

Parameters **vendor** *vendor-id* — specifies the RADIUS vendor ID.

Values standard, nokia (6527), 3gpp

Default nokia

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

attribute-type *attribute-type* — Specifies the RADIUS attribute to be used as subscriber. identifier

Values

alc-sub-string (nokia) — Subscriber-id string (Alc-Subsc-ID-Str) is cached in Large Scale NAT44 application and used to correlate Large Scale NAT44 subscriber to BNG subscriber.

user-name (stnd) — User-Name standard RADIUS attribute is cached in Large Scale NAT44 application and is used to correlate Large Scale NAT44 subscriber to BNG subscriber.

class (stnd) — Class standard RADIUS attribute is cached in Large Scale NAT44 application and is used to correlate Large Scale NAT44 subscriber to BNG subscriber. Class attribute is initially set and send by RADIUS server. As such it must be echoed by BNG in all accounting messages.

station-id (stnd) — Calling-Station-Id RADIUS attribute is cached in Large Scale NAT44 application and is used to correlate Large Scale NAT44 subscriber to BNG subscriber.

imsi (3gpp) — International Mobile Subscriber Identification is used in WiFi Offload applications as a SIM card identifier.

imei (3gpp) — International Mobile Equipment Identification is used in WiFi Offload applications as a physical phone device identifier.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.323 attribute-matching

attribute-matching

Syntax **attribute-matching**

Context [Tree] (config>router>radius-proxy>server attribute-matching)
[Tree] (config>service>vprn>radius-proxy>server attribute-matching)

Full Context configure router radius-proxy server attribute-matching
configure service vprn radius-proxy server attribute-matching

Description Commands in this context select the RADIUS policy for authentication and accounting based on the RADIUS attribute. This feature is supported for both the ESM RADIUS proxy and the ISA RADIUS proxy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.324 attribute-table-high-wmark

attribute-table-high-wmark

Syntax **no attribute-table-high-wmark** *high-water-mark*
no attribute-table-high-wmark

Context **[Tree]** (config>service>vpls>mrp>mmrp attribute-table-high-wmark)
[Tree] (config>service>vpls>mrp>mvrp attribute-table-high-wmark)

Full Context configure service vpls mrp mmrp attribute-table-high-wmark
configure service vpls mrp mvrp attribute-table-high-wmark

Description This command specifies the percentage filling level of the MMRP attribute table where logs and traps are sent.

Default attribute-table-high-wmark 95

Parameters *high-water-mark* — Specifies the utilization of the MRP attribute table of this service at which a table full alarm will be raised by the agent, as a percentage.

Values 0 to 100

Platforms All

5.325 attribute-table-low-wmark

attribute-table-low-wmark

Syntax **attribute-table-low-wmark** *low-water-mark*
no attribute-table-low-wmark

Context **[Tree]** (config>service>vpls>mrp>mmrp attribute-table-low-wmark)
[Tree] (config>service>vpls>mrp>mvrp attribute-table-low-wmark)

Full Context configure service vpls mrp mmrp attribute-table-low-wmark
configure service vpls mrp mvrp attribute-table-low-wmark

Description This command specifies the MMRP attribute table low watermark as a percentage. When the percentage filling level of the MMRP attribute table drops below the configured value, the corresponding trap is cleared and/or a log entry is added.

Default attribute-table-low-wmark 90

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *low-water-mark* — Specifies utilization of the MRP attribute table of this service at which a table full alarm will be cleared by the agent, as a percentage.

Values 0 to 100

Platforms All

5.326 attribute-table-size

attribute-table-size

Syntax **attribute-table-size** *max-attributes*
no attribute-table-size

Context **[Tree]** (config>service>vpls>mrp>mmrp attribute-table-size)

Full Context configure service vpls mrp mmrp attribute-table-size

Description This command controls the number of attributes accepted on a per B-VPLS basis. When the limit is reached, no new attributes will be registered.

If a new lower limit (smaller than the current number of attributes) from a local or dynamic I-VPLS is being provisioned, a CLI warning will be issued stating that the system is currently beyond the new limit. The value will be accepted, but any creation of new attributes will be blocked under the attribute count drops below the new limit; the software will then start enforcing the new limit.

Default maximum number of attributes

Parameters *value* — The maximum number of attributes accepted per B-VPLS.

Values 1 to 2048 (Full participants)
1 to 8191 (End-Station-Only participants)

Platforms All

attribute-table-size

Syntax [**no**] **attribute-table-size** *value*

Context **[Tree]** (config>service>vpls>mrp>mvrp attribute-table-size)

Full Context configure service vpls mrp mvrp attribute-table-size

Description This command controls the number of attributes accepted on a per M-VPLS basis. When the limit is reached, no new attributes will be registered.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a new lower limit (smaller than the current number of attributes) is being provisioned, a CLI warning will be issued stating that the system is currently beyond the new limit. The value will be accepted, but any creation of new attributes will be blocked under the attribute count drops below the new limit; the software will then start enforcing the new limit.

Default maximum number of attributes

Parameters *value* — Specifies the number of attributes accepted on a per M-VPLS basis

Values 1 to 4095 for MVRP

Platforms All

5.327 audio-template

audio-template

Syntax **audio-template**

Context **[Tree]** (config>app-assure>group>cflowd>rtp-perf audio-template)

Full Context configure application-assurance group cflowd rtp-performance audio-template

Description Commands in this context configure the audio template for cflowd fields.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.328 augment-route-table

augment-route-table

Syntax [**no**] **augment-route-table**

Context **[Tree]** (config>router>isis>loopfree-alternates augment-route-table)

Full Context configure router isis loopfree-alternates augment-route-table

Description This command enables IS-IS to attach Remote LFA specific information to RTM entries for use by other protocols. This command requires **configure router isis lfa remote-lfa** to be enabled. Currently only LDP makes use of this additional information.

The **no** form of this command disables IS-IS to attach Remote LFA specific information to RTM entries for use by other protocols.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

augment-route-table

Syntax [**no**] **augment-route-table**

Context **[Tree]** (config>router>ospf>loopfree-alternates augment-route-table)

Full Context configure router ospf loopfree-alternates augment-route-table

Description This command enables OSPF to attach Remote LFA (rLFA) information to RTM entries for use by other protocols. Before this command is configured, the **configure router ospf lfa remote-lfa** command, must be enabled on the system. Currently, only LDP makes use of this additional information.

The **no** form of this command disables the attachment of rLFA-specific information to RTM entries for use by other protocols.

Default no augment-route-table

Platforms All

5.329 auth

auth

Syntax [**no**] **auth**

Context **[Tree]** (debug>router>rsvp>event auth)

Full Context debug router rsvp event auth

Description This command debugs auth events.

The **no** form of the command disables the debugging.

Platforms All

auth

Syntax [**no**] **auth** [**neighbor** *ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>rip auth)

Full Context debug router rip auth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for RIP authentication.

Parameters *ip-int-name* | *ip-address* — Debugs the RIP authentication for the neighbor IP address or interface.

Platforms All

5.330 auth-domain-name

auth-domain-name

Syntax **auth-domain-name** *domain-name*
no auth-domain-name

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host auth-domain-name)

Full Context configure subscriber-mgmt local-user-db ipoe host auth-domain-name

Description This command sets the domain name which can be appended to user-name in RADIUS-authentication-request message for the given host.

The **no** form of this command removes the domain name from the host configuration.

Parameters *domain-name* — Specifies the domain name, up to 32 characters, to be appended to user-name in RADIUS-authentication-request message for the given host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.331 auth-include-attributes

auth-include-attributes

Syntax [**no**] **auth-include-attributes**

Context **[Tree]** (config>aaa>isa-radius-plcy auth-include-attributes)

Full Context configure aaa isa-radius-policy auth-include-attributes

Description This command configures attributes to be included in RADIUS authentication messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.332 auth-keychain

auth-keychain

Syntax **auth-keychain** *name*
no auth-keychain

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy auth-keychain)

Full Context configure subscriber-mgmt bgp-peering-policy auth-keychain

Description This command configures the BGP authentication key for all peers.

The keychain allows the rollover of authentication keys during the lifetime of a session.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies the name of an existing keychain, up to 32 characters, to use for the specified TCP session or sessions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>service>vprn>bgp auth-keychain)
[Tree] (config>service>vprn>bgp>group auth-keychain)
[Tree] (config>service>vprn>bgp>group>neighbor auth-keychain)

Full Context configure service vprn bgp auth-keychain
configure service vprn bgp group auth-keychain
configure service vprn bgp group neighbor auth-keychain

Description This command configures the BGP authentication key for all peers.

The keychain allows the rollover of authentication keys during the lifetime of a session.

Default no auth-keychain

Parameters *name* — Specifies the name of an existing keychain, up to 32 characters, to use for the specified TCP session or sessions.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>service>vprn>isis auth-keychain)
[Tree] (config>service>vprn>isis>level auth-keychain)

Full Context configure service vprn isis auth-keychain
configure service vprn isis level auth-keychain

Description This command configures an authentication keychain to use for the protocol interface for the VPRN instance. The keychain allows the rollover of authentication keys during the lifetime of a session.

Default no auth-keychain

Parameters *name* — Specifies the name of the keychain, up to 32 characters, to use for the specified protocol session or sessions.

Platforms All

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>router>isis auth-keychain)
[Tree] (config>router>isis>level auth-keychain)

Full Context configure router isis auth-keychain
configure router isis level auth-keychain

Description This command configures an authentication keychain to use for the protocol interface. The keychain allows the rollover of authentication keys during the lifetime of a session.

Parameters *name* — Specifies the name of the keychain, up to 32 characters, to use for the specified protocol session or sessions.

Platforms All

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>service>vprn>ospf>area>if auth-keychain)
[Tree] (config>service>vprn>ospf>area>sham-link auth-keychain)
[Tree] (config>service>vprn>ospf>area>virtual-link auth-keychain)

Full Context configure service vprn ospf area interface auth-keychain
configure service vprn ospf area sham-link auth-keychain

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ospf area virtual-link auth-keychain

Description This command enables the authentication keychain.

Parameters *name* — Specifies the name of the authentication keychain, up to 32 characters.

Platforms All

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>router>ldp>tcp-session-params>peer-transport auth-keychain)
[Tree] (config>router>ldp>tcp-session-params auth-keychain)

Full Context configure router ldp tcp-session-parameters auth-keychain
configure router ldp tcp-session-parameters peer-transport auth-keychain

Description This command configures the TCP authentication keychain to use for the TCP session. The per-peer authentication configuration takes precedence over the global authentication configuration.

Parameters *name* — Specifies the name of the keychain, up to 32 characters. This keychain is used for the specified TCP session or sessions, and allows the rollover of authentication keys during the lifetime of a session. The peer address used must be the TCP session transport address.

Platforms All

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>router>rsvp>interface auth-keychain)

Full Context configure router rsvp interface auth-keychain

Description This command configures an authentication keychain to use for authentication of protocol messages sent and received over the associated interface. The keychain must include a valid entry to properly authenticate protocol messages, including a key, specification of a supported authentication algorithm, and beginning time. Each entry may also include additional options to control the overall lifetime of each entry to allow for the seamless rollover of without affecting the protocol adjacencies.

The **no** form of the auth-keychain command removes the association between the routing protocol and any keychain currently used.

Default no auth-keychain

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters name — Specifies the name of the keychain, up to 32 characters, to use for the specified protocol session or sessions.

Platforms All

auth-keychain

Syntax **auth-keychain** *name*

Context **[Tree]** (config>router>bgp auth-keychain)
[Tree] (config>router>bgp>group auth-keychain)
[Tree] (config>router>bgp>group>neighbor auth-keychain)

Full Context configure router bgp auth-keychain
configure router bgp group auth-keychain
configure router bgp group neighbor auth-keychain

Description This command configures a TCP authentication keychain to use for the session. The keychain allows the rollover of authentication keys during the lifetime of a session.

Default no auth-keychain

Parameters *name* — Specifies the name of the keychain, up to 32 characters, to use for the specified TCP session or sessions.

Platforms All

auth-keychain

Syntax **auth-keychain**

Context **[Tree]** (config>router>ospf>area>interface auth-keychain)
[Tree] (config>router>ospf>area>virtual-link auth-keychain)

Full Context configure router ospf area interface auth-keychain
configure router ospf area virtual-link auth-keychain

Description This command configures an authentication keychain to use for the protocol interface. The keychain allows the rollover of authentication keys during the lifetime of a session.

Default no auth-keychain

Parameters *name* — Specifies the name of the keychain, up to 32 characters, to use for the specified protocol session or sessions.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.333 auth-method

auth-method

Syntax **auth-method** {**psk** | **plain-psk-xauth** | **cert-auth** | **psk-radius** | **cert-radius** | **eap** | **auto-eap-radius** | **auto-eap**}
no auth-method

Context **[Tree]** (config>ipsec>ike-policy auth-method)

Full Context configure ipsec ike-policy auth-method

Description This command specifies the authentication method used with this IKE policy.

The **no** form of this command removes the parameter from the configuration.

Default no auth-method

Parameters **psk** — Both client and gateway authenticate each other by a hash derived from a pre-shared secret. Both client and gateway must have the PSK. This work with both IKEv1 and IKEv2

plain-psk-xauth — Both client and gateway authenticate each other by pre-shared key and RADIUS. This work with IKEv1 only.

psk-radius — Use the pre-shared-key and RADIUS to authenticate. IKEv2 remote-access tunnel only.

cert-radius — Use the certificate, public/private key and RADIUS to authenticate. IKEv2 remote-access tunnel only.

eap — Use the EAP to authenticate peer. IKEv2 remote-access tunnel only

auto-eap-radius — Use EAP or potentially other method to authenticate the peer. IKEv2 remote-access tunnel only. Also see **config>ipsec>ike-policy auto-eap-method** and **config>ipsec>ike-policy auto-eap-own-method**.

auto-eap — Use the EAP or potentially other RADIUS-related method to authenticate the peer. IKEv2 remote-access tunnel only. Also see **config>ipsec>ike-policy auto-eap-method** and **config>ipsec>ike-policy auto-eap-own-method**.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.334 auth-policy

auth-policy

Syntax **auth-policy** *policy-name*
no auth-policy

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host auth-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host auth-policy)

Full Context configure subscriber-mgmt local-user-db ipoe host auth-policy
configure subscriber-mgmt local-user-db ppp host auth-policy

Description This command configures the authentication policy of this host and PPPoE hosts. This authentication policy is only used if no authentication policy is defined at the interface level. For DHCP hosts, the host entry should not contain any other information needed for setup of the host (IP address, ESM strings, and so on.). For PPPoE hosts, the authentication policy configured here must have its PPPoE authentication method set to **pap-chap**, otherwise the request is dropped.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the authentication policy name, up to 32 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.335 auth-port

auth-port

Syntax **auth-port** *port*
no auth-port

Context **[Tree]** (config>router>radius-server>server auth-port)
[Tree] (config>service>vprn>radius-server>server auth-port)

Full Context configure router radius-server server auth-port
configure service vprn radius-server server auth-port

Description This command specifies the UDP listening port for RADIUS authentication requests.

The **no** form of this commands resets the UDP port to its default value (1812)

Default auth-port 1812

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port* — Specifies the UDP listening port for accounting requests of the external RADIUS server.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.336 auth-request-script-policy

auth-request-script-policy

Syntax **auth-request-script-policy** *policy-name*
no auth-request-script-policy

Context **[Tree]** (config>aaa>radius-srv-plcy auth-request-script-policy)

Full Context configure aaa radius-server-policy auth-request-script-policy

Description This command specifies the name of the RADIUS script policy used to change the RADIUS attributes of the Access-Request messages.

Parameters *policy-name* — Specifies the name of the Python script to modify Access-Request messages, up to 32 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.337 authenticate

authenticate

Syntax [**no**] **authenticate**

Context **[Tree]** (config>service>vprn>ntp authenticate)

Full Context configure service vprn ntp authenticate

Description This command enables authentication for the NTP server.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.338 authenticate-client

authenticate-client

Syntax **authenticate-client**

Context **[Tree]** (config>system>security>tls>server-tls-profile authenticate-client)

Full Context configure system security tls server-tls-profile authenticate-client

Description Commands in this context configure client authentication parameters.

Platforms All

5.339 authenticate-on-dhcp

authenticate-on-dhcp

Syntax [**no**] **authenticate-on-dhcp**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range authenticate-on-dhcp)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range authenticate-on-dhcp)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range authenticate-on-dhcp
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range authenticate-on-dhcp

Description This command enables initial authentication (when there is no state for the UE on the ISA), to be triggered by DHCP DISCOVER or REQUEST. The default behavior is authentication based on first Layer 3 packet.

The **no** form of this command reverts to the default.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.340 authenticated-brg-only

authenticated-brg-only

Syntax [**no**] **authenticated-brg-only**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>brg authenticated-brg-only)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-ranges>range>vrgw>brg authenticated-brg-only)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>brg authenticated-brg-only)
[Tree] (config>service>vprn>sub-if>grp-if>brg authenticated-brg-only)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>brg authenticated-brg-only)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-ranges>range>vrgw>brg authenticated-brg-only)

Full Context configure service ies subscriber-interface group-interface brg authenticated-brg-only
configure service ies subscriber-interface group-interface wlan-gw ranges range brg authenticated-brg-only
configure service ies subscriber-interface group-interface wlan-gw vlan-ranges range vrgw brg authenticated-brg-only
configure service vprn subscriber-interface group-interface brg authenticated-brg-only
configure service vprn subscriber-interface group-interface wlan-gw ranges range brg authenticated-brg-only
configure service vprn subscriber-interface group-interface wlan-gw vlan-ranges range vrgw brg authenticated-brg-only

Description This command indicates that only BRGs that are pre-authenticated using the RADIUS proxy are allowed in this context.

The **no** form of this command removes the restriction.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.341 authentication

authentication

Syntax **authentication** {**chap** | **pap** | **pref-chap** | **prep-pap**}

Context [Tree] (config>router>l2tp>group>ppp authentication)
[Tree] (config>router>l2tp>group>tunnel>ppp authentication)
[Tree] (config>service>vprn>l2tp>group>ppp authentication)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp authentication)

Full Context configure router l2tp group ppp authentication
configure router l2tp group tunnel ppp authentication
configure service vprn l2tp group ppp authentication
configure service vprn l2tp group tunnel ppp authentication

Description This command configures the PPP authentication protocol to negotiate authentication.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default authentication pref-chap

Parameters **chap** — Specifies to always use CHAP for authentication.

pap — Specifies to always use PAP for authentication.

pref-chap — Specifies to use CHAP as the preferred authentication method, and to use PAP if that attempt fails.

pref-pap — Specifies to use PAP as the preferred authentication method, and to use CHAP if that attempt fails.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication

Syntax **authentication**

Context **[Tree]** (config>service>dynsvc>policy authentication)

Full Context configure service dynamic-services dynamic-services-policy authentication

Description Commands in this context configure authentication parameters for data-triggered dynamic services.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication

Syntax **authentication** [**policy** *policy-name*] [**mac-addr** *ieee-address*] [**circuit-id** *circuit-id*]

Context **[Tree]** (debug>subscr-mgmt authentication)

Full Context debug subscriber-mgmt authentication

Description This command debugs subscriber authentication.

Parameters *policy-name* — Specifies an existing subscriber management authentication policy name.

ieee-address — Specifies the 48-bit MAC address xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

circuit-id — Specify the circuit-id, up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication

Syntax **authentication**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range authentication)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range authentication)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication

Description Commands in this context create configuration for authenticating a user from the WLAN-GW ISA.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

authentication

Syntax **authentication bidirectional** *sa-name*
authentication inbound *sa-name* **outbound** *sa-name*
no authentication

Context [Tree] (config>service>vprn>ospf3>area>if authentication)
[Tree] (config>service>vprn>ospf3>area>virtual-link authentication)

Full Context configure service vprn ospf3 area interface authentication
configure service vprn ospf3 area virtual-link authentication

Description This command configures OPSFv3 confidentiality authentication.

The **no** form of this command removes the SA name from the configuration.

Parameters **bidirectional** *sa-name* — Specifies the IPsec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

inbound *sa-name* — Specifies the IPsec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

outbound *sa-name* — Specifies the IPsec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

Platforms All

authentication

Syntax **authentication** *ascii-algorithm* **ascii-key** *ascii-string* [**hash** | **hash2** | **custom**]
authentication *auth-algorithm* **hex-key** *hex-string* [**hash** | **hash2** | **custom**]
no authentication

Context [Tree] (config>ipsec>static-sa authentication)

Full Context configure ipsec static-sa authentication

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the authentication algorithm to use for an IPsec manual SA.

Default no authentication

Parameters *auth-algorithm* — Specifies the authentication algorithm to be used.

Values mda5, sha1

ascii-string — Specifies an ASCII key; 16 characters for **md5** and 20 characters for **sha1**.

hex-string — Specifies a HEX key; 32 hex nibbles for **md5** and 40 hex nibbles for **sha1**.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication

Syntax **authentication** [**port** *udp-port*]
no authentication

Context **[Tree]** (config>aaa>isa-radius-plcy>servers>server authentication)

Full Context configure aaa isa-radius-policy servers server authentication

Description This command configures authentication for this server.

Default no authentication

Parameters *udp-port* — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

authentication

Syntax [**no**] **authentication**

Context **[Tree]** (config>li>x-interfaces>lics>lic authentication)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure li x-interfaces lics lic authentication

Description This command configures the parameters for authentication of INE and LIC on the X1 and X2 interfaces.

The **no** form of this command removes the configured parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

authentication

Syntax **authentication none**
authentication *authentication-protocol authentication-key* [**privacy-none**] [**hash** | **hash2** | **custom**]
authentication *authentication-protocol authentication-key* **privacy** *privacy-protocol privacy-key* [**hash** | **hash2** | **custom**]
no authentication

Context **[Tree]** (config>system>security>user>snmp authentication)

Full Context configure system security user snmp authentication

Description This command configures the SNMPv3 authentication and privacy protocols for the user to communicate with the router. The keys are stored in an encrypted format in the configuration.

The keys configured with these commands must be localized keys, which are a hash of the SNMP engine ID and a password. The password is not entered directly in this command. Use the **tools perform system management-interface snmp generate-key** command to generate localized authentication and privacy keys.

Default authentication none

Parameters **none** — Keyword to specify that no authentication protocol is used. If **none** is specified, privacy cannot be configured.

authentication-protocol — Specifies the SNMPv3 authentication protocol.

Values **hmac-md5-96** — Specifies use of the HMAC-MD5-96 authentication protocol.

hmac-sha1-96 — Specifies use of the HMAC-SHA-96 authentication protocol.

hmac-sha2-224 — Specifies use of the HMAC-SHA-224 authentication protocol.

hmac-sha2-256 — Specifies use of the HMAC-SHA-256 authentication protocol.

hmac-sha2-384 — Specifies use of the HMAC-SHA-384 authentication protocol.

hmac-sha-512 — Specifies use of the HMAC-SHA-512 authentication protocol.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

authentication-key — Specifies the localized authentication key, which is entered as a hexadecimal string; the character length depends on the specified authentication protocol. The following table lists the authentication protocol key lengths.

Table 28 **Authentication protocol key lengths**

Authentication protocol	Character lengths
HMAC-MD5-96	32
HMAC-SHA-96	40
HMAC-SHA-224	56
HMAC-SHA-256	64
HMAC-SHA-384	96
HMAC-SHA-512	128

privacy-none — Keyword to specify that a privacy protocol is not used in the communication.

Default privacy none

privacy-protocol — Specifies the SNMPv3 privacy protocol.

Values **cbc-des** — Specifies the use of the CBC-DES privacy protocol. This parameter is not available in FIPS-140-2 mode.

cfb128-aes-128 — Specifies the use of the CFB128-AES-128 privacy protocol.

cfb128-aes-192 — Specifies the use of the CFB128-AES-192 privacy protocol.

cfb128-aes-256 — Specifies the use of the CFB128-AES-256 privacy protocol.

privacy-key — Specifies the localized privacy key, which is entered as a hexadecimal string; the character length depends on the specified privacy protocol. The following table lists the privacy protocol key lengths.

Table 29 **Privacy protocol key lengths**

Privacy protocol	Character length
CBC-DES	32
CFB128-AES-128	32
CFB128-AES-192	48
CFB128-AES-256	64

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash — Keyword that specifies the key is entered in an encrypted form. If the **hash** or **hash2** keyword is not specified, the key is assumed to be in an unencrypted, cleartext form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Keyword that specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone; that is, the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** keyword is not specified, the key is assumed to be in an unencrypted, cleartext form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Keyword that specifies the custom encryption to the management interface.

Platforms All

authentication

Syntax **authentication bidirectional** *sa-name*
authentication [**inbound** *sa-name* **outbound** *sa-name*]
no authentication

Context **[Tree]** (config>router>ospf3>area>interface authentication)
[Tree] (config>router>ospf3>area>virtual-link authentication)

Full Context configure router ospf3 area interface authentication
configure router ospf3 area virtual-link authentication

Description This command configures the password used by the OSPF3 interface or virtual-link to send and receive OSPF3 protocol packets on the interface when simple password authentication is configured.

All neighboring routers must use the same type of authentication and password for proper protocol communication.

By default, no authentication key is configured.

The **no** form of this command removes the authentication.

Default no authentication

Parameters **bidirectional** *sa-name* — Specifies bidirectional OSPF3 authentication.

inbound *sa-name* — Specifies the inbound security association (SA) name for OSPF3 authentication.

outbound *sa-name* — Specifies the outbound SA name for OSPF3 authentication.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.342 authentication-check

authentication-check

Syntax [**no**] **authentication-check**

Context **[Tree]** (config>service>vprn>isis authentication-check)

Full Context configure service vprn isis authentication-check

Description This command sets an authentication check to reject PDUs that do not match the type or key requirements for the VPRN instance.

The default behavior when authentication is configured is to reject all IS-IS protocol PDUs that have a mismatch in either the authentication type or authentication key.

When **no authentication-check** is configured, authentication PDUs are generated and IS-IS PDUs are authenticated on receipt. However, mismatches cause an event to be generated and will not be rejected.

The **no** form of this command allows authentication mismatches to be accepted and generates a log event.

Default authentication-check — Rejects authentication mismatches.

Platforms All

authentication-check

Syntax [**no**] **authentication-check**

Context **[Tree]** (config>service>vprn>ntp authentication-check)

Full Context configure service vprn ntp authentication-check

Description This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key-id, type or key requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type or key.

When **authentication-check** is enabled, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for type and one for key-id, one for type, value mismatches. These counters are visible in a show command.

The **no** form of this command allows authentication mismatches to be accepted; the counters however are maintained.

Default authentication-check — Rejects authentication mismatches.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

authentication-check

Syntax [**no**] **authentication-check**

Context **[Tree]** (config>system>time>ntp authentication-check)

Full Context configure system time ntp authentication-check

Description This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key-id, type or key requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type or key.

When **authentication-check** is enabled, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for type and one for key-id, one for type, value mismatches. These counters are visible in a show command.

The **no** form of this command allows authentication mismatches to be accepted; the counters however are maintained.

Default authentication-check

Platforms All

authentication-check

Syntax [**no**] **authentication-check**

Context **[Tree]** (config>router>isis authentication-check)

Full Context configure router isis authentication-check

Description This command sets an authentication check to reject PDUs that do not match the type or key requirements.

The default behavior when authentication is configured is to reject all IS-IS protocol PDUs that have a mismatch in either the authentication type or authentication key.

When **no authentication-check** is configured, authentication PDUs are generated and IS-IS PDUs are authenticated on receipt. However, mismatches cause an event to be generated and will not be rejected.

The **no** form of this command allows authentication mismatches to be accepted and generates a log event.

Default authentication-check

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

5.343 authentication-key

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy authentication-key)

Full Context configure subscriber-mgmt bgp-peering-policy authentication-key

Description This command configures the BGP authentication key.

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest. The authentication key can be any combination of letters or numbers from 1 to 16.

The **no** form of this command removes the authentication password from the configuration and effectively disables authentication.

Parameters *authentication-key* — Specifies an authentication key. The key can be any combination of ASCII characters, up to 255 characters (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Species the hash key. The key can be any combination of ASCII characters up to 342 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>redundancy>multi-chassis>peer authentication-key)

Full Context configure redundancy multi-chassis peer authentication-key

Description This command configures the authentication key used between this node and the multi-chassis peer. The authentication key can be any combination of letters or numbers. The **no** form of the command removes the authentication key.

Default no authentication-key

Parameters *authentication-key* — Specifies the authentication key. Allowed values are any string up to 20 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 33 (hash1-key) or 55 (hash2-key) characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>subscr-mgmt>rip-policy authentication-key)

Full Context configure subscriber-mgmt rip-policy authentication-key

Description This command configures the BGP authentication key.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest. The authentication key can be any combination of letters or numbers from 1 to 16.

The **no** form of this command removes the authentication password from the configuration and effectively disables authentication.

Default Authentication is disabled and the authentication password is empty.

Parameters *authentication-key* — Specifies the authentication key. The key can be any combination of ASCII characters up to 255 characters (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 342 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2**| **custom**]
no authentication-key

Context **[Tree]** (config>service>ies>if>vrrp authentication-key)

Full Context configure service ies interface vrrp authentication-key

Description The **authentication-key** command, within the **vrrp** *virtual-router-id* context, is used to assign a simple text password authentication key to generate master VRRP advertisement messages and validating received VRRP advertisement messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The authentication-key command is one of the few commands not affected by the presence of the owner keyword. If simple text password authentication is not required, the authentication-key command is not required. If the command is re-executed with a different password key defined, the new key will be used immediately. If a no authentication-key command is executed, the password authentication key is restored to the default value. The authentication-key command may be executed at any time.

To change the current in-use password key on multiple virtual router instances:

- Identify the current master
- Shutdown the virtual router instance on all backups
- Execute the authentication-key command on the master to change the password key
- Execute the authentication-key command and no shutdown command on each backup key

The **no** form of the command removes the authentication key.

Default No default. The authentication data field contains the value 0 in all 16 octets.

Parameters *authentication-key* — The *key* parameter identifies the simple text password used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses a string eight octets long that is inserted into all transmitted VRRP advertisement messages and compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the key.

The *key* parameter is expressed as a string consisting up to eight alpha-numeric characters. Spaces must be contained in quotation marks (“ ”). The quotation marks are not considered part of the string.

The string is case sensitive and is left-justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with the value 0 in the corresponding octet.

Values Any 7-bit printable ASCII character.

Exceptions:	Double quote (")	ASCII 34
	Carriage Return	ASCII 13
	Line Feed	ASCII 10
	Tab	ASCII 9
	Backspace	ASCII 8

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>service>vprn>bgp authentication-key)
[Tree] (config>service>vprn>bgp>group authentication-key)
[Tree] (config>service>vprn>bgp>group>neighbor authentication-key)

Full Context configure service vprn bgp authentication-key
configure service vprn bgp group authentication-key
configure service vprn bgp group neighbor authentication-key

Description This command configures the BGP authentication key.

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest. The authentication key can be any combination of letters or numbers from 1 to 16.

The **no** form of this command removes the authentication password from the configuration and effectively disables authentication.

Default no authentication-key

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 255 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>service>vprn>if>vrrp authentication-key)

Full Context configure service vprn interface vrrp authentication-key

Description The **authentication-key** command, within the **vrrp** *virtual-router-id* context, is used to assign a simple text password authentication key to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

The **authentication-key** command is one of the few commands not affected by the presence of the **owner** keyword. If simple text password authentication is not required, this command is not required. If the command is re-executed with a different password key defined, the new key will be used immediately. If a no **authentication-key** command is executed, the password authentication key is restored to the default value. The **authentication-key** command may be executed at any time.

To change the current in-use password key on multiple virtual router instances:

- Identify the current master
- Shut down the virtual router instance on all backups
- Execute the **authentication-key** command on the master to change the password key
- Execute the **authentication-key** command and the **no shutdown** command on each backup key

The **no** form of this command restores the default null string to the value of key.

Parameters *authentication-key* — The *key* parameter identifies the simple text password used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses a string eight octets long that is inserted into all transmitted VRRP advertisement messages and compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the key.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The *key* parameter is expressed as a string consisting of up to eight alpha-numeric characters. Spaces must be contained in quotation marks (“ ”). The quotation marks are not considered part of the string.

The string is case sensitive and is left-justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with the value 0 in the corresponding octet.

Values Any 7-bit printable ASCII character.

Exceptions:	Double quote (")	ASCII 34
	Carriage Return	ASCII 13
	Line Feed	ASCII 10
	Tab	ASCII 9
	Backspace	ASCII 8

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”)

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>service>vprn>isis authentication-key)
[Tree] (config>service>vprn>isis>level authentication-key)

Full Context configure service vprn isis authentication-key
configure service vprn isis level authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the authentication key used to verify PDUs sent by neighboring routers on the interface for the VPRN instance.

Neighboring routers use passwords to authenticate PDUs sent from an interface. For authentication to work, both the authentication *key* and the authentication *type* on a segment must match. The OSPF Commands statement must also be included.

To configure authentication on the global level, configure this command in the **config>router>isis** context. When this parameter is configured on the global level, all PDUs are authenticated including the Hello PDU.

To override the global setting for a specific level, configure the **authentication-key** command in the **config>router>isis>level** context. When configured within the specific level, hello PDUs are not authenticated.

The **no** form of this command removes the authentication key.

Default no authentication-key — No authentication key is configured.

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 255 characters in length (un-encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>service>vprn>msdp>group>peer authentication-key)
[Tree] (config>service>vprn>msdp>peer authentication-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn msdp group peer authentication-key
configure service vprn msdp peer authentication-key

Description This command configures a Message Digest 5 (MD5) authentication key to be used with a specific Multicast Source Discovery Protocol (MSDP) peering session. The authentication key must be configured per peer as such no global or group configuration is possible.

The **no** form of this command removes the authentication key.

Default no authentication-key (All MSDP messages are accepted and the MD5 signature option authentication key is disabled.)

Parameters *authentication-key* — Specifies the authentication key. Allowed values are any string up to 256 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 451 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** *key-id* **key** *key* [**hash** | **hash2** | **custom**] **type** {**des** | **message-digest**}
no authentication-key *key-id*

Context **[Tree]** (config>service>vprn>ntp authentication-key)

Full Context configure service vprn ntp authentication-key

Description This command sets the authentication key-id, type and key used to authenticate NTP PDUs sent by the broadcast server function toward external clients or to authenticate NTP PDUs received from external unicast clients within the VPRN routing instance. For authentication to work, the authentication key-id, type, and key value must match.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the authentication key.

Parameters *key-id* — Configure the authentication key-id that will be used by the node when transmitting or receiving Network Time Protocol packets.

Entering the authentication-key command with a key-id value that matches an existing configuration key will result in overriding the existing entry.

Recipients of the NTP packets must have the same authentication key-id, type, and key value in order to use the data transmitted by this node. This is an optional parameter.

Values 1 to 255

key — The authentication key associated with the configured key-id, the value configured in this parameter is the actual value used by other network elements to authenticate the NTP packet.

The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“.”).

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

type — This parameter determines if DES or message-digest authentication is used.

This is a required parameter; either DES or message-digest must be configured.

Values des — Specifies that DES authentication is used for this key. The des value is not supported in FIPS-140-2 mode.

message-digest — Specifies that MD5 authentication in accordance with RFC 2104 is used for this key.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>service>vprn>ospf>area>if authentication-key)
[Tree] (config>service>vprn>ospf>area>virtual-link authentication-key)
[Tree] (config>service>vprn>ospf>area>sham-link authentication-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ospf area interface authentication-key
configure service vprn ospf area sham-link authentication-key
configure service vprn ospf area virtual-link authentication-key

Description This command configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.

This command is not valid in the OSPF3 context.

All neighboring routers must use the same type of authentication and password for proper protocol communication. If the **authentication-type** is configured as password, then this key must be configured.

By default, no authentication key is configured.

This command is not supported in the OSPF context.

The **no** form of this command removes the authentication key.

Default no authentication-key — No authentication key is defined.

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>rip authentication-key)
[Tree] (config>service>vprn>rip>group authentication-key)
[Tree] (config>service>vprn>rip>group>neighbor authentication-key)

Full Context configure service vprn rip authentication-key
configure service vprn rip group authentication-key
configure service vprn rip group neighbor authentication-key

Description This command sets the authentication password to be passed between RIP neighbors.

The authentication type and authentication key must match exactly to authenticate and then process the RIP message.

The **no** form of this command removes the authentication password from the configuration and disables authentication.

Default no authentication-key

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 16 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 33 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context [Tree] (config>router>ldp>tcp-session-params>peer-transport authentication-key)
[Tree] (config>router>ldp>tcp-session-params authentication-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ldp tcp-session-parameters authentication-key
configure router ldp tcp-session-parameters peer-transport authentication-key

Description This command specifies the authentication key used to establish a session between LDP peers. Authentication uses the MD-5 message-based digest. The peer address used in authentication must be the TCP session transport address. If one or more transport addresses used in the Hello adjacencies to the same peer LSR are different from the LSR-ID value, the user must add each transport address to the authentication-key configuration as a separate peer. As a result, when the TCP connection is bootstrapped by a specific Hello adjacency, the authentication can operate over that TCP connection by using its specific transport address. The per peer authentication configuration takes precedence over global authentication configuration, and authentication keychain configuration takes precedence over authentication key configuration.

The **no** form of this command disables authentication.

Parameters *authentication-key* — Specifies the authentication key. The key can be any combination of ASCII characters, up to 255 characters (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of up to 33 alphanumeric characters. If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex, encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to the management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>router>rsvp>interface authentication-key)

Full Context configure router rsvp interface authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the authentication key to be used between RSVP neighbors to authenticate RSVP messages. Authentication uses the MD-5 message-based digest.

When enabled on an RSVP interface, authentication of RSVP messages operates in both directions of the interface.

A node maintains a security association using one authentication key for each interface to a neighbor. The following items are stored in the context of this security association:

- The HMAC-MD5 authentication algorithm.
- Key used with the authentication algorithm.
- Lifetime of the key. The user-entered key is valid until the user deletes it from the interface.
- Source Address of the sending system.
- Latest sending sequence number used with this key identifier.

A router RSVP sender transmits an authenticating digest of the RSVP message, computed using the shared authentication key and a keyed-hash algorithm. The message digest is included in an integrity object which also contains a flags field, a key identifier field, and a sequence number field. The RSVP sender complies to the procedures for RSVP message generation in RFC 2747, *RSVP Cryptographic Authentication*.

A RSVP receiver uses the key together with the authentication algorithm to process received RSVP messages.

When a PLR node switches the path of the LSP to a bypass LSP, it does not send the Integrity object in the RSVP messages sent over the bypass tunnel. If the PLR receives an RSVP message with an Integrity object, it will perform the digest verification for the key of the interface over which the packet was received. If this fails, the packet is dropped. If the received RSVP message is a RESV message and does not have an Integrity object, then the PLR node will accept it only if it originated from the MP node.

An MP node will accept RSVP messages received over the bypass tunnel with and without the Integrity object. If an Integrity object is present, the proper digest verification for the key of the interface over which the packet was received is performed. If this fails, the packet is dropped.

The MD5 implementation does not support the authentication challenge procedures in RFC 2747.

The **no** form of this command disables authentication.

Default no authentication-key - The authentication key value is the null string.

Parameters *authentication-key* — Specifies the authentication key. The key can be any combination of ASCII characters up to 16 characters in length (unencrypted). If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash-key — Specifies the hash key. The key can be any combination of up 33 alphanumeric characters. If spaces are used in the string, enclose the entire string in quotation marks (“ ”)

This is useful when a user must configure the parameter, but for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no authentication-key

Context **[Tree]** (config>router>msdp>peer authentication-key)
[Tree] (config>router>msdp>group>peer authentication-key)

Full Context configure router msdp group peer authentication-key
configure router msdp peer authentication-key

Description This command configures a Message Digest 5 (MD5) authentication key to be used with a specific Multicast Source Discovery Protocol (MSDP) peering session. The authentication key must be configured per peer as such no global or group configuration is possible.

The **no** form of the command configures acceptance of all MSDP messages and disables the MD5 signature option authentication key.

Default no authentication-key

Parameters *authentication-key* — Specifies the authentication key. The key can be any combination of printable, 7-bit ASCII characters, up to 255 characters long in the config>router>msdp>peer context, or up to 127 characters long in the config>router>msdp>group>peer context. If the string contains special characters (#, $, spaces, and so on), enclose the entire string in quotation marks (“ ”).

hash-key — Specifies a hash key. The key can be any combination of ASCII characters up to 451 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This is useful when a user must configure the parameter, although, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies that the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [{**hash** | **hash2** | **custom**}]
no authentication-key

Context **[Tree]** (config>router>if>vrrp authentication-key)

Full Context configure router interface vrrp authentication-key

Description This command sets the simple text authentication key used to generate master VRRP advertisement messages and validates VRRP advertisements.

If simple text password authentication is not required, the **authentication-key** command is not required.

The command is configurable in both non-owner and owner **vrrp** nodal contexts.

The *key* parameter identifies the simple text password to be used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses an eight octet long string that is inserted into all transmitted VRRP advertisement messages and is compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the *key*.

The *key* string is case sensitive and is left justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field similarly holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with a 0 value in the corresponding octet.

If the command is re-executed with a different password key defined, the new key is used immediately.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **authentication-key** command can be executed at anytime.

To change the current in-use password key on multiple virtual router instances:

Identify the current master.

1. Shutdown the virtual router instance on all backups.
2. Execute the **authentication-key** command on the master to change the password key.
3. Execute the **authentication-key** command and **no shutdown** command on each backup.

The **no** form of the command reverts to the default value.

Default no authentication-key — The authentication key value is the null string.

Parameters *authentication-key* — The authentication key. Allowed values are any string up to 8 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 (hash-key1) or 121 (hash-key2) characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** *key-id* **key** *key* [**hash** | **hash2** | **custom**] **type** {**des** | **message-digest**}
no authentication-key *key-id*

Context **[Tree]** (config>system>time>ntp authentication-key)

Full Context configure system time ntp authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the authentication key-id, type and key used to authenticate NTP PDUs sent to or received by other network elements participating in the NTP protocol. For authentication to work, the authentication key-id, type and key value must match.

The **no** form of the command removes the authentication key.

Parameters *key-id* — Configures the authentication key-id that will be used by the node when transmitting or receiving Network Time Protocol packets

Entering the authentication-key command with a key-id value that matches an existing configuration key will result in overriding the existing entry.

Recipients of the NTP packets must have the same authentication key-id, type, and key value in order to use the data transmitted by this node. This is an optional parameter.

Values 1 to 255

key — Specifies the authentication key associated with the configured key-id, the value configured in this parameter is the actual value used by other network elements to authenticate the NTP packet.

The key can be any combination of ASCII characters up to 32 characters for message-digest (md5) or 8 characters for des (length limits are unencrypted lengths). If spaces are used in the string, enclose the entire string in quotation marks (“.”).

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

type — Determines if DES or message-digest authentication is used.

This is a required parameter; either DES or message-digest must be configured.

des — Specifies that DES authentication is used for this key. The des option is not permitted in FIPS-140-2 mode.

message-digest — Specifies that MD5 authentication in accordance with RFC 2104 is used for this key.

Platforms All

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no authentication-key

Context [Tree] (config>router>bgp authentication-key)
[Tree] (config>router>bgp>group authentication-key)
[Tree] (config>router>bgp>group>neighbor authentication-key)

Full Context configure router bgp authentication-key
configure router bgp group authentication-key
configure router bgp group neighbor authentication-key

Description This command configures the BGP authentication key.

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message based digest.

The **no** form of this command reverts to the default value.

Default no authentication-key

Parameters *authentication-key* — Specifies the authentication key. The key can be any combination of ASCII characters up to 255 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no authentication-key

Context [Tree] (config>router>isis authentication-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>isis>level authentication-key)

Full Context
configure router isis authentication-key
configure router isis level authentication-key

Description
This command sets the authentication key used to verify PDUs sent by neighboring routers on the interface.

Neighboring routers use passwords to authenticate PDUs sent from an interface. For authentication to work, both the authentication *key* and the authentication *type* on a segment must match. The **authentication-type** command must also be included.

To configure authentication on the global level, configure this command in the **config>router>isis** context. When this parameter is configured on the global level, all PDUs are authenticated including the hello PDU.

To override the global setting for a specific level, configure the **authentication-key** command in the **config>router>isis>level** context. When configured within the specific level, hello PDUs are not authenticated.

The **no** form of this command removes the authentication key.

Parameters
authentication-key — Specifies the authentication key. The key can be any combination of ASCII characters up to 255 characters in length (un-encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms
All

authentication-key

Syntax
authentication-key [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no authentication-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ospf>area>interface authentication-key)
[Tree] (config>router>ospf>area>virtual-link authentication-key)

Full Context configure router ospf area interface authentication-key
configure router ospf area virtual-link authentication-key

Description This command configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.

All neighboring routers must use the same type of authentication and password for proper protocol communication. If the **authentication-type** is configured as **password**, then this key must be configured.

By default, no authentication key is configured.

The **no** form of this command removes the authentication key.

Default no authentication-key

Parameters *authentication-key* — Specifies the authentication key. The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 22 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

authentication-key

Syntax **authentication-key** {*authentication-key* | *hash-key*} [{**hash** | **hash2** | **custom**}]
no authentication-key

Context [Tree] (config>router>rip authentication-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>rip>group authentication-key)
[Tree] (config>router>rip>group>neighbor authentication-key)

Full Context
configure router rip authentication-key
configure router rip group authentication-key
configure router rip group neighbor authentication-key

Description
This command sets the authentication password to be passed between RIP neighbors.

The authentication type and authentication key must match exactly for the RIP message to be considered authentic and processed.

The **no** form of the command removes the authentication password from the configuration and disables authentication.

Default
no authentication-key

Parameters
authentication-key — Specifies the authentication key. Allowed values are any string up to 16 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hash-key — Specifies the hash key. The key can be any combination of ASCII characters up to 33 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms
All

5.344 authentication-order

authentication-order

Syntax
authentication-order [*method-1*] [*method-2*] [*method-3*] [*method-4*] [**exit-on-reject**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no authentication-order

Context **[Tree]** (config>system>security>password authentication-order)

Full Context configure system security password authentication-order

Description This command configures the sequence in which password authentication, authorization, and accounting is attempted among local passwords, RADIUS, TACACS+, and LDAP.

The authentication order should be from the most preferred authentication method to the least preferred. The presence of all methods in the command line does not guarantee that they are all operational. Specifying options that are not available delays user authentication.

If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log documents the failed attempt. Both the attempted login identification and originating IP address are logged with a timestamp.

The **no** form of this command reverts to the default authentication sequence.

Note: This command applies to a local user, in addition to users on RADIUS, TACACS, and LDAP.

Default authentication-order radius tacplus ldap local - The preferred order for password authentication is 1. local passwords, 2. RADIUS, 3. TACACS+, and 4. LDAP.

Parameters *method-1* — Specifies the first password authentication method to attempt.

Values local, radius, tacplus, ldap

method-2 — Specifies the second password authentication method to attempt.

Values local, radius, tacplus, ldap

method-3 — Specifies the third password authentication method to attempt.

Values local, radius, tacplus, ldap

method-4 — Specifies the fourth password authentication method to attempt.

Values local, radius, tacplus, ldap

local — Specifies the password authentication based on the local password database.

radius — Specifies RADIUS authentication.

tacplus — Specifies TACACS+ authentication.

ldap — Specifies LDAP authentication.

exit-on-reject — When enabled and if one of the AAA methods configured in the authentication order sends a reject, then the next method in the order will not be tried. If the **exit-on-reject** keyword is not specified and if one AAA method sends a reject, the next AAA method will be attempted. If in this process, all the AAA methods are exhausted, it will be considered as a reject.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A rejection is distinct from an unreachable authentication server. When the **exit-on-reject** keyword is specified, authorization and accounting will only use the method that provided an affirmation authentication; only if that method is no longer readable or is removed from the configuration will other configured methods be attempted. If the **local** keyword is the first authentication and:

- **exit-on-reject** is configured and the user does not exist, the user is not authenticated
- the user is authenticated locally, then other methods, if configured, it is used for authorization and accounting
- the user is configured locally but without console access, login is denied

Platforms All

5.345 authentication-origin

authentication-origin

Syntax **authentication-origin**

Context **[Tree]** (config>subscr-mgmt authentication-origin)

Full Context configure subscriber-mgmt authentication-origin

Description Commands in this context configure a subscriber's authentication origin.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.346 authentication-policy

authentication-policy

Syntax **authentication-policy** *auth-policy-name*
no authentication-policy

Context **[Tree]** (config>router>l2tp>group>ppp authentication-policy)
[Tree] (config>router>l2tp>group>tunnel>ppp authentication-policy)
[Tree] (config>service>vprn>l2tp>group>ppp authentication-policy)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp authentication-policy)

Full Context configure router l2tp group ppp authentication-policy
configure router l2tp group tunnel ppp authentication-policy
configure service vprn l2tp group ppp authentication-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn l2tp group tunnel ppp authentication-policy

Description This command configures the RADIUS authentication policy that will be used to authenticate PPP sessions on the LNS.

The **no** form of this command reverts to the default value.

Default no authentication-policy

Parameters *auth-policy-name* — Specifies the authentication policy name.

Values 32 chars max

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication-policy

Syntax **authentication-policy** *name* [**create**]
no authentication-policy

Context **[Tree]** (config>subscr-mgmt authentication-policy)

Full Context configure subscriber-mgmt authentication-policy

Description This command creates a RADIUS authentication policy containing parameters to authenticate subscriber sessions. The policies can be applies to an IES or VPRN interface or group interface, or a VPLS SAP.

The **no** form of this command removes the policy from the configuration.

Parameters *name* — Specifies the name of the authentication profile. The string is case sensitive and limited to 32 ASCII 7-bit printable characters.

create — Keyword used to create the authentication policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication-policy

Syntax **authentication-policy** *name*
no authentication-policy

Context **[Tree]** (config>service>ies>if authentication-policy)
[Tree] (config>service>ies>sub-if>grp-if authentication-policy)
[Tree] (config>service>vprn>if authentication-policy)
[Tree] (config>service>vprn>sub-if>grp-if authentication-policy)

Full Context configure service ies interface authentication-policy
configure service ies subscriber-interface group-interface authentication-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface authentication-policy
configure service vprn subscriber-interface group-interface authentication-policy

Description This command assigns a RADIUS authentication policy to the interface.

The **no** form of this command removes the policy from the interface configuration.

Parameters *name* — Specifies the authentication policy name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface authentication-policy
- configure service vprn subscriber-interface group-interface authentication-policy

All

- configure service ies interface authentication-policy
- configure service vprn interface authentication-policy

authentication-policy

Syntax **authentication-policy** *name*
no authentication-policy

Context **[Tree]** (config>service>vpls>sap authentication-policy)

Full Context configure service vpls sap authentication-policy

Description For a regular SAP (bridged CO model), this command defines which subscriber authentication policy must be applied when a DHCP message is received on the interface. The authentication policies must already be defined. The policy is only applied when DHCP snooping is enabled on the SAP.

For a capture SAP, this command specifies the RADIUS authentication policy to use for subscriber session authentication when a valid trigger packet is received. The same authentication policy must be assigned on the group-interface where the MSAP for the subscriber session is created.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication-policy

Syntax **authentication-policy** *policy-name*
no authentication-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>authentication authentication-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>authentication authentication-policy)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication authentication-policy
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication authentication-policy

Description This command assigns a RADIUS authentication policy configured under the **aaa** context for authenticating users on WLAN-GW ISA.

The **no** form of this command removes the policy from the configuration.

Parameters *policy-name* — Specifies the name of the authentication policy up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

authentication-policy

Syntax **authentication-policy** *name*
no authentication-policy

Context [Tree] (config>app-assure>group>transit-ip>radius authentication-policy)

Full Context configure application-assurance group transit-ip-policy radius authentication-policy

Description This command configures the RADIUS authentication-policy for the IP transit policy.

Default no authentication-policy

Parameters *name* — Specifies the authentication policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.347 authentication-type

authentication-type

Syntax **authentication-type** {**none** | **password** | **message-digest** | **message-digest-20**}
no authentication-type

Context [Tree] (config>subscr-mgmt>rip-plcy authentication-type)

Full Context configure subscriber-mgmt rip-policy authentication-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the type of authentication to be used between RIP neighbors. The type and password must match exactly for the RIP message to be considered authentic and processed.

The **no** form of this command removes the authentication type from the configuration and effectively disables authentication.

Parameters **none** — Disables authentication at a given level (global, group, neighbor). If the command does not exist in the configuration, the parameter is inherited.

password — Specifies enable simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple password authentication is enabled.

message-digest — Configures 16 byte message digest for MD5 authentication. If this option is configured, then at least one message-digest-key must be configured.

message-digest-20 — Configures 20 byte message digest for MD5 authentication in accordance with RFC 2082, RIP-2 MD5 Authentication. If this option is configured, then at least one message-digest-key must be configured.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

authentication-type

Syntax **authentication-type** {**password** | **message-digest**}
no authentication

Context **[Tree]** (config>service>vprn>isis authentication-type)
[Tree] (config>service>vprn>isis>level authentication-type)

Full Context configure service vprn isis authentication-type
configure service vprn isis level authentication-type

Description This command enables either simple password or message digest authentication or must go in either the global IS-IS or IS-IS level context.

Both the authentication key and the authentication type on a segment must match. The **authentication-key** statement must also be included.

Configure the authentication type on the global level in the **config>router>isis** context.

Configure or override the global setting by configuring the authentication type in the **config>router>isis>level** context.

The **no** form of this command disables authentication.

Default no authentication-type — No authentication type is configured and authentication is disabled.

Parameters **password** — Specifies that simple password (plain text) authentication is required.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

message-digest — Specifies that MD5 authentication in accordance with RFC2104 is required.

Platforms All

authentication-type

Syntax **authentication-type** {**password** | **message-digest**}
no authentication-type

Context **[Tree]** (config>service>vprn>ospf>area>if authentication-type)
[Tree] (config>service>vprn>ospf>area>sham-link authentication-type)
[Tree] (config>service>vprn>ospf>area>virtual-link authentication-type)

Full Context configure service vprn ospf area interface authentication-type
configure service vprn ospf area sham-link authentication-type
configure service vprn ospf area virtual-link authentication-type

Description This command enables authentication and specifies the type of authentication to be used on the OSPF interface, virtual-link, and sham-link.

This command is not valid in the OSPF3 context.

Both simple **password** and **message-digest** authentication are supported.

The **no** form of this command disables authentication on the interface.

Default no authentication-type — No authentication is enabled on an interface.

Parameters **password** — This keyword enables simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple **password** authentication is enabled.

message-digest — This keyword enables message digest MD5 authentication in accordance with RFC1321. If this option is configured, then at least one message-digest-key must be configured.

Platforms All

authentication-type

Syntax **authentication-type** {**none** | **password** | **message-digest** | **message-digest-20**}
no authentication-type

Context **[Tree]** (config>service>vprn>rip authentication-type)
[Tree] (config>service>vprn>rip>group authentication-type)
[Tree] (config>service>vprn>rip>group>neighbor authentication-type)

Full Context configure service vprn rip authentication-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn rip group authentication-type
configure service vprn rip group neighbor authentication-type

Description This command defines the type of authentication used between RIP neighbors. The type and password must match exactly to authenticate and then process the RIP message.

The **no** form of this command removes the authentication type from the configuration and effectively disables authentication.

Default no authentication-type

Parameters **none** — No authentication is used.

password — A simple clear-text password is sent.

message-digest — MD5 authentication is used.

message-digest-20 — MD20 authentication is used.

Platforms All

authentication-type

Syntax **authentication-type** {**password** | **message-digest**}
no authentication

Context **[Tree]** (config>router>isis authentication-type)
[Tree] (config>router>isis>level authentication-type)

Full Context configure router isis authentication-type
configure router isis level authentication-type

Description This command enables either simple password or message digest authentication or must go in either the global IS-IS or IS-IS level context.

Both the authentication key and the authentication type on a segment must match. The **authentication-key** statement must also be included.

Configure the authentication type on the global level in the **config>router>isis** context.

Configure or override the global setting by configuring the authentication type in the **config>router>isis>level** context.

The **no** form of this command disables authentication.

Parameters **password** — Specifies that simple password (plain text) authentication is required.

message-digest — Specifies that MD5 authentication in accordance with RFC2104 is required.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

authentication-type

Syntax **authentication-type** {**password** | **message-digest**}
no authentication-type

Context **[Tree]** (config>router>ospf>area>interface authentication-type)
[Tree] (config>router>ospf>area>virtual-link authentication-type)

Full Context configure router ospf area interface authentication-type
configure router ospf area virtual-link authentication-type

Description This command enables authentication and specifies the type of authentication to be used on the OSPF interface.

Both simple **password** and **message-digest** authentication are supported.

By default, authentication is not enabled on an interface.

The **no** form of this command disables authentication on the interface.

Default no authentication-type

Parameters **password** — Enables the simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple **password** authentication is enabled.

message-digest — Enables message digest MD5 authentication in accordance with RFC1321. If this option is configured, then at least one message-digest-key must be configured.

Platforms All

authentication-type

Syntax **authentication-type** {**none** | **password** | **message-digest** | **message-digest-20**}
no authentication-type

Context **[Tree]** (config>router>rip authentication-type)
[Tree] (config>router>rip>group authentication-type)
[Tree] (config>router>rip>group>neighbor authentication-type)

Full Context configure router rip authentication-type
configure router rip group authentication-type
configure router rip group neighbor authentication-type

Description This command sets the type of authentication to be used between RIP neighbors.

The type and password must match exactly for the RIP message to be considered authentic and processed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the authentication type from the configuration and effectively disables authentication.

Default no authentication-type

Parameters **none** — The **none** parameter explicitly disables authentication at a given level (global, group, neighbor). If the command does not exist in the configuration, the parameter is inherited.

password — Specifies that the password enables simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple **password** authentication is enabled.

message-digest — Configures 16 byte message digest for MD5 authentication. If this option is configured, then at least one **message-digest-key must** be configured.

message-digest-20 — Configures 20 byte message digest for MD5 authentication in accordance with RFC 2082, *RIP-2 MD5 Authentication*. If this option is configured, then at least one **message-digest-key** must be configured.

Platforms All

5.348 authenticator-init

authenticator-init

Syntax [**no**] **authenticator-init**

Context **[Tree]** (config>port>ethernet>dot1x>per-host-authentication authenticator-init)

Full Context configure port ethernet dot1x per-host-authentication authenticator-init

Description This command configures the authenticator-initiated mode of the host.

The **no** form of this command disables the authenticator-initiated mode of the host.

Default authenticator-init

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.349 authorization

authorization

Syntax **authorization**

Context **[Tree]** (config>system>security>cli-script authorization)

Full Context configure system security cli-script authorization

Description Commands in this context authorize CLI script execution.

Platforms All

authorization

Syntax [**no**] **authorization**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius authorization)

Full Context configure service vprn aaa remote-servers radius authorization

Description This command configures RADIUS authorization parameters for the system.

Default no authorization

Platforms All

authorization

Syntax [**no**] **authorization**

Context **[Tree]** (config>system>security>radius authorization)

Full Context configure system security radius authorization

Description This command configures RADIUS authorization parameters for the system.

Default no authorization

Platforms All

authorization

Syntax [**no**] **authorization** [**use-priv-lvl**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>security>tacplus authorization)
[Tree] (config>service>vprn>aaa>remote-servers>tacplus authorization)

Full Context configure service vprn aaa remote-servers tacplus authorization
configure system security tacplus authorization

Description This command controls how TACACS+ is used for command authorization.

If this command is enabled without the **use-priv-lvl** option, then each command is sent to the TACACS+ server for authorization (this is true whether the **tacplus use-default-template** setting is enabled or not).

If the **tacplus authorization** command is disabled, and the **tacplus use-default-template** setting is enabled, then the local profile in the **user-template tacplus_default** is used for command authorization.

Default no authorization

Parameters *use-priv-lvl* — Automatically performs a single authorization request to the TACACS+ server for cmd* (all commands) immediately after login, and then use the local profile associated (via the **priv-lvl-map**) with the priv-lvl returned by the TACACS+ server for all subsequent authorization (except **enable-admin**). After the initial authorization for cmd*, no further authorization requests are sent to the TACACS+ server (except **enable-admin**). If the TACACS+ server does not return a priv-lvl for a user, the profile from the **user-template tacplus_default** is used for command authorization (as long as **tacplus use-default-template** is enabled, otherwise all commands are rejected).

Platforms All

5.350 authorized-only

authorized-only

Syntax [**no**] **authorized-only**

Context [Tree] (config>subscr-mgmt>wlan-gw>ue-query>state authorized-only)

Full Context configure subscriber-mgmt wlan-gw ue-query state authorized-only

Description This command enables matching on UEs in an authorized state.

The **no** form of this command disables matching on UEs in an authorized state, unless all state matching is disabled.

Default no authorized-only

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.351 auto-bandwidth

auto-bandwidth

Syntax [**no**] **auto-bandwidth**

Context **[Tree]** (config>router>mpls>lsp auto-bandwidth)
[Tree] (config>router>mpls>lsp-template auto-bandwidth)

Full Context configure router mpls lsp auto-bandwidth
configure router mpls lsp-template auto-bandwidth

Description This command enables (and the no form disables) automatic adjustments of LSP bandwidth.

Auto-bandwidth at the LSP level cannot be executed unless **adaptive** is configured in the **config**>**router**>**mpls**>**lsp** context.

Default no auto-bandwidth

Platforms All

5.352 auto-bandwidth-multipliers

auto-bandwidth-multipliers

Syntax **auto-bandwidth-multipliers sample-multiplier** *number1* **adjust-multiplier** *number2*
no auto-bandwidth-multipliers

Context **[Tree]** (config>router>mpls auto-bandwidth-multipliers)

Full Context configure router mpls auto-bandwidth-multipliers

Description This command specifies the number of collection intervals in the adjust interval.

Default auto-bandwidth-multipliers sample-multiplier 1 adjust-multiplier 288

Parameters **sample-multiplier** *number1* — Specifies the multiplier for collection intervals in a sample interval.

Values 1 to 511

adjust-multiplier *number2* — Specifies the number of collection intervals in the adjust interval.

Values 1 to 16383

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.353 auto-bind-tunnel

auto-bind-tunnel

Syntax **auto-bind-tunnel**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls auto-bind-tunnel)
[Tree] (config>service>vpls>bgp-evpn>mpls auto-bind-tunnel)
[Tree] (config>service>vprn>bgp-evpn>mpls auto-bind-tunnel)
[Tree] (config>service>vprn>bgp-ipvpn>mpls auto-bind-tunnel)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel
configure service vpls bgp-evpn mpls auto-bind-tunnel
configure service vprn bgp-evpn mpls auto-bind-tunnel
configure service vprn bgp-ipvpn mpls auto-bind-tunnel

Description Commands in this context configure automatic binding of a VPRN service using tunnels to MP-BGP peers.

The **auto-bind-tunnel** node is simply a context to configure the binding of BGP IPVPN or EVPN routes to tunnels. The user must configure the **resolution** option to enable auto-bind resolution to tunnels in TTM. If the **resolution** option is explicitly set to **disabled**, the auto-binding to tunnel is removed.

If resolution is set to **any**, any supported tunnel type in the Epipe/VPRN/VPLS context is selected following TTM preference. If one or more explicit tunnel types are specified using the **resolution-filter** option, then only these tunnel types are selected again following the TTM preference.

The user must set **resolution** to **filter** in order to activate the list of tunnel-types configured under resolution-filter.

In VPRN services and for BGP-IPVPN, when an explicit SDP to a BGP next hop is configured (**config**>**service**>v**prn**>**spoke-sdp**), it overrides the auto-bind-tunnel selection for that BGP next hop only. There is no support for reverting automatically to the auto-bind-tunnel selection if the explicit SDP goes down. The user must delete the explicit spoke-sdp in the VPRN service context to resume using the auto-bind-tunnel selection for the BGP next hop.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.354 auto-boot

auto-boot

Syntax **auto-boot** [**management-port**] [**inband** [**vlan** *vlan-id* | **vlan-discovery**]] [**ipv4**] [**ipv6**] [**client-identifier** {**string** *ascii-string* | **hex** *hex-string* | **chassis-mac**}] [**include-user-class**]
auto-boot ospf [**neid** *neid-hex-string*] [**vendor-id** *vendor-id*] [**neip-ipv4** *ip-address*] [**neip-ipv6** *ipv6-address*] [**port-mtu** *mtu-bytes*] [**ospf-mtu** *ip-mtu-bytes*] [**vlan** *vlan-id*]
no auto-boot

Context **[Tree]** (bof auto-boot)

Full Context bof auto-boot

Description This command enables the **auto-boot** flag in the BOF and configures the **auto-boot** options for ZTP. When modifying **auto-boot** options using CLI, all required options must be explicitly configured as the default cases will no longer be used.

The **no** form of this command disables the **auto-boot** flag.

Default no auto-boot

Parameters **management-port** — Specifies that the out-of-band management port (Mgmt port) should be used for ZTP.

inband — Specifies that in-band management through an Ethernet port should be used for ZTP. Unless the **vlan-discovery** flag is used, the **inband** option disables VLAN discovery.

vlan-id — Specifies an in-band VLAN to use for the auto-boot process.

Values 1 to 4094

vlan-discovery — Floods all VLANs (1 to 4094) with DHCP discovery messages and is supported only on **inband** ports. The first offer received on a specific VLAN is processed.

ipv4 — Enables IPv4 DHCP discovery. This parameter is mandatory if the **ipv6** parameter is not specified.

ipv6 — Enables IPv6 DHCP solicitation. This parameter is mandatory if the **ipv4** parameter is not specified.

ascii-string — Specifies a DHCP client identification string, up to 58 ASCII characters, to be used for Option 61 (IPv4) or Option 1 (IPv6).

hex-string — Specifies a DHCP client identification string, up to 116 hexadecimal nibbles, to be used for Option 61 (IPv4) or Option 1 (IPv6).

Values 0x0 to 0xFFFFFFFF

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

chassis-mac — Specifies that the chassis MAC address should be used as the DHCP client identification string for Option 61 (IPv4) or Option 1 (IPv6).

include-user-class — Specifies that Option 77 should be included in DHCP messages.

client-identifier — Specifies that a custom client ID should be used in network discovery requests.

minutes — Specifies the time interval after which, if the auto-boot process is not successful (in the case of auto-boot using OSPF, if no OSPF adjacency is found), the node is rebooted and the auto-boot process is retried.

Values 30 to 1440

ospf — Specifies that OSPF auto-discovery should be used.

neid-hex-string — Specifies a hexadecimal network element identification string.

Values 0x10101to 0xFEFEFE

ip-address — Specifies the IPv4 address for the network element.

Values a.b.c.d

Default *vendor-id.neid-hex-string*

ipv6-address — Specifies the IPv6 address for the network element.

Values

x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0 to FFFF]H
d [0 to 255]D

Default The IPv6 version of *vendor-id.neid-hex-string*

vendor-id — Specifies the vendor identification number. The number 140 corresponds to “Nokia”.

Values 1 to 254

Default 140

ip-mtu-bytes — Specifies the OSPF MTU in bytes.

Values 512 to 9786

Default 1500

mtu-bytes — Specifies the port MTU in bytes.

Values 512 to 9800

Default The default MTU of the port type.

Platforms 7450 ESS-7, 7750 SR-1, 7750 SR-1e, 7750 SR-7, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.355 auto-config

auto-config

Syntax [**no**] **auto-config**

Context **[Tree]** (config>service>epipe>spoke-sdp-fec auto-config)

Full Context configure service epipe spoke-sdp-fec auto-config

Description This command enables single sided automatic endpoint configuration of the spoke SDP. The router acts as the passive T-PE for signaling this MS-PW.

Automatic Endpoint Configuration allows the configuration of a spoke SDP endpoint without specifying the TAII associated with that spoke SDP. It allows a single-sided provisioning model where an incoming label mapping message with a TAII that matches the SAII of that spoke SDP to be automatically bound to that endpoint. In this mode, the far end T-PE actively initiates MS-PW signaling and will send the initial label mapping message using T-LDP, while the router T-PE for which auto-config is specified will act as the passive T-PE.

The **auto-config** command is blocked in CLI if signaling active has been enabled for this spoke SDP. It is only applicable to spoke SDPs configured under the Epipe, IES and VPRN interface context.

The **no** form of this command means that the router T-PE either acts as the active T-PE (if signaling active is configured) or automatically determines which router will initiate MS-PW signaling based on the prefix values configured in the SAII and TAII of the spoke SDP. If the SAII has the greater prefix value, then the router will initiate MS-PW signaling without waiting for a label mapping message from the far end. However, if the TAII has the greater value prefix, then the router will assume that the far end T-PE will initiate MS-PW signaling and will wait for that label mapping message before responding with a T-LDP label mapping message for the MS-PW in the reverse direction.

Default no auto-config

Platforms All

5.356 auto-config-save

auto-config-save

Syntax [**no**] **auto-config-save**

Context **[Tree]** (config>system>management-interface>cli>md-cli auto-config-save)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system management-interface cli md-cli auto-config-save

Description This command enables the functionality to automatically save the configuration as part of a commit operation.

The **no** form of the command disables this function.

Platforms All

auto-config-save

Syntax [**no**] **auto-config-save**

Context **[Tree]** (config>system>netconf auto-config-save)

Full Context configure system netconf auto-config-save

Description This command controls whether committed changes are automatically persistent (that is, copied to the <startup> datastore) or not, when a commit is successful.

Default no auto-config-save

Platforms All

auto-config-save

Syntax [**no**] **auto-config-save**

Context **[Tree]** (config>system>grpc>gnmi auto-config-save)

Full Context configure system grpc gnmi auto-config-save

Description This command enables automatic saving of the configuration as part of the commit operation.

The **no** form of this command disables automatic saving.

Platforms All

5.357 auto-creation

auto-creation

Syntax **[no] auto-creation**

Context **[Tree]** (config>qos>fp-resource-policy>aggregate-shapers auto-creation)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos fp-resource-policy aggregate-shapers auto-creation

Description This command enables the auto-creation of hardware aggregate shapers on the specified FP. After enabling, the corresponding FP is rebooted.

The **no** version of this command disables auto-creation of hardware aggregate shapers.

Default no auto-creation

Platforms 7750 SR-1, 7750 SR-s

5.358 auto-crl-update

auto-crl-update

Syntax **auto-crl-update** [**create**]
no auto-crl-update

Context **[Tree]** (config>system>security>pki>ca-prof auto-crl-update)

Full Context configure system security pki ca-profile auto-crl-update

Description This command creates an auto CRL update configuration context with the **create** parameter, or enters the auto-crl-update configuration context without the **create** parameter.

This mechanism auto downloads a CRL file from a list of configured HTTP URLs either periodically or before existing CRL expires. If the downloaded CRL is more recent than the existing one, then the existing one will be replaced.

Note: The configured URL must point to a DER encoded CRL file.

Parameters **create** — Creates an auto CRL update for the ca-profile.

Platforms All

auto-crl-update

Syntax [**no**] **auto-crl-update**

Context **[Tree]** (debug>certificate auto-crl-update)

Full Context debug certificate auto-crl-update

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables trace for automated and manual CRL updates.

Platforms All

5.359 auto-disc-route-advertisement

auto-disc-route-advertisement

Syntax [**no**] **auto-disc-route-advertisement**

Context **[Tree]** (config>service>vpls>bgp-evpn>vxlan auto-disc-route-advertisement)

Full Context configure service vpls bgp-evpn vxlan auto-disc-route-advertisement

Description This command enables sending route advertisements on auto-discovery.

The **no** form of this command disables sending route advertisements on auto-discovery.

Default no auto-disc-route-advertisement

Platforms All

5.360 auto-discovery

auto-discovery

Syntax **auto-discovery** [**default** | **mdt-safi**] [**source-address** *ip-address*]

Context **[Tree]** (config>service>vprn>mvpn auto-discovery)

Full Context configure service vprn mvpn auto-discovery

Description This command enables MVPN membership auto-discovery through BGP. When auto-discovery is enabled, PIM peering on the inclusive provider tunnel is disabled. Changing auto-discovery configuration requires shutdown of this VPRN instance.

The **no** form of this command disables MVPN membership auto-discovery through BGP.

Default auto-discovery default

Parameters **default** — Enables AD route exchange based on format defined in NG-MVPN (RFC6514).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mdt-safi — Enables AD route exchange based on mdt-safi format defined in *draft-rosen-vpn-mcast.*

This command optionally specifies a **source-address** - an IP address to be used by Rosen MVPN or NG-MVPN for core diversity, non-default IGP instances (not using system IP). Two unique IP addresses for PIM or GRE MVPNs are supported. The two unique IP address restriction does not apply to MVPNs with MPLS tunnels (for example, RSVP and MLDP). For instances using default System IP, source address configuration should not be specified to avoid consuming one of the addresses.

Explicitly defining a **source-address** allows GRE-encapsulated Rosen MVPN or NG-MVPN multicast traffic (Default and Data MDT) to originate from a configured IP address, so the source IP address of the GRE packets will not be the default system IP address.

Value:

ip-address — An IPv4 address. To achieve the desired functionality the address should be a pre-configured non-default ISIS or OSPF loopback address for an IGP instance using loopback address different from the system IP loopback.

Platforms All

auto-discovery

Syntax **auto-discovery** [**default**]
no auto-discovery

Context **[Tree]** (config>router>pim>gtm auto-discovery)

Full Context configure router pim gtm auto-discovery

Description This command enables multicast auto-discovery over BGP for GTM.

The **no** form of this command disables auto-discovery.

Default no auto-discovery

Parameters **default** — Enables the default auto-discovery mode.

Platforms All

5.361 auto-discovery-disable

auto-discovery-disable

Syntax [**no**] **auto-discovery-disable**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>mvpn>pt>selective auto-discovery-disable)

Full Context configure service vprn mvpn provider-tunnel selective auto-discovery-disable

Description This command disables C-trees to P-tunnel binding auto-discovery through BGP so it is signaled using PIM join TLVs.

This command requires the **c-mcast-signaling** parameter to be set to PIM.

For multi-stream S-PMSI, this command must be enabled for BGP auto-discovery to function.

The **no** form of this command enables multicast VPN membership auto-discovery through BGP.

Default auto-discovery-disable

Platforms All

5.362 auto-eap-method

auto-eap-method

Syntax **auto-eap-method** {**psk** | **cert** | **psk-or-cert**}

Context [Tree] (config>ipsec>ike-policy auto-eap-method)

Full Context configure ipsec ike-policy auto-eap-method

Description This command enables following behavior for IKEv2 remote-access tunnel when auth-method is configured as auto-eap-radius:

- If there is no AUTH payload in IKE_AUTH request, then system use EAP to authenticate client and also will own-auth-method to generate AUTH payload.
- If there is AUTH payload in IKE_AUTH request:
  - if auto-eap-method is psk, then system proceed as auth-method:psk-radius
  - if auto-eap-method is cert, then system proceed as auth-method:cert-radius
  - if auto-eap-method is psk-or-cert, then:
    - if the "Auth Method" field of AUTH payload is PSK, then system proceed as auth-method:psk-radius
    - if the "Auth Method" field of AUTH payload is RSA or DSS, then system proceed as auth-method:cert-radius
  - The system will use **auto-eap-own-method** to generate AUTH payload.

This command only applies when **auth-method** is configured as **auto-eap-radius**.

Default auto-eap-method cert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **psk** — Uses the pre-shared-key as the authentication method.

cert — Uses the certificate as the authentication method.

psk-or-cert — Uses either the pre-shared-key or certificate based on the “Auth Method” field of the received AUTH payload.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

5.363 auto-eap-own-method

auto-eap-own-method

Syntax **auto-eap-own-method** {**psk** | **cert**}

Context **[Tree]** (config>ipsec>ike-policy auto-eap-own-method)

Full Context configure ipsec ike-policy auto-eap-own-method

Description This command enables following behavior for IKEv2 remote-access tunnel when auth-method is configured as auto-eap-radius:

- If there is no AUTH payload in IKE_AUTH request, then system use EAP to authenticate client and also will own-auth-method to generate AUTH payload.
- If there is AUTH payload in IKE_AUTH request:
  - if auto-eap-method is psk, then system proceed as auth-method:psk-radius.
  - if auto-eap-method is cert, then system proceed as auth-method:cert-radius.
  - if auto-eap-method is psk-or-cert, then:
    - if the "Auth Method" field of AUTH payload is PSK, then system proceed as auth-method:psk-radius.
    - if the "Auth Method" field of AUTH payload is RSA or DSS, then system proceed as auth-method:cert-radius.
  - The system will use **auto-eap-own-method** to generate AUTH payload.

This command only applies when **auth-method** is configured as **auto-eap-radius**.

Default auto-eap-own-method cert

Parameters **psk** — Uses a pre-shared-key to generate AUTH payload.

cert — Uses a public/private key to generate AUTH payload.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.364 auto-edge

auto-edge

Syntax [**no**] **auto-edge**

Context **[Tree]** (config>service>vpls>sap>stp auto-edge)
[Tree] (config>service>template>vpls-sap-template>stp auto-edge)
[Tree] (config>service>vpls>spoke-sdp>stp auto-edge)

Full Context configure service template vpls-sap-template stp auto-edge
configure service vpls sap stp auto-edge
configure service vpls spoke-sdp stp auto-edge

Description This command configures automatic detection of the edge port characteristics of the SAP or spoke-SDP.

If auto-edge is enabled, and STP concludes there is no bridge behind the spoke-SDP, the OPER_EDGE variable will dynamically be set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable will dynamically be set to true (see **edge-port** [**config>service>vpls>sap>stp edge-port**, **config>service>template>vpls-sap-template>stp edge-port**, **config>service>vpls>spoke-sdp>stp edge-port**]).

The **no** form of this command returns the auto-detection setting to the default value.

Default auto-edge

Platforms All

auto-edge

Syntax [**no**] **auto-edge**

Context **[Tree]** (config>service>pw-template>stp auto-edge)

Full Context configure service pw-template stp auto-edge

Description This command configures automatic detection of the edge port characteristics of the SAP or spoke SDP.

If auto-edge is enabled, and STP concludes there is no bridge behind the spoke SDP, the OPER_EDGE variable will dynamically be set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable will dynamically be set to true (see **config>service>pw-template>stp edge-port**).

The **no** form of this command returns the auto-detection setting to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default auto-edge

Platforms All

5.365 auto-esi

auto-esi

Syntax **auto-esi** {**none** | **type-1**}

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg auto-esi)

Full Context configure service system bgp-evpn ethernet-segment auto-esi

Description This command configures the auto-ESI type to use in the Ethernet segment (ES).

The default mode is **none** and forces the user to configure a manual ESI. When **type-1** is configured, a manual ESI cannot be configured and the ESI is auto-derived in accordance with the RFC 7432 ESI type 1 definition.

An ESI type 1 encodes 0x01 in the ESI type octet (T=0x01) and indicates that IEEE 802.1AX LACP is used between the PEs and CEs.

The ESI is auto-derived from the LACP PDUs by concatenating the following parameters:

- CE LACP system MAC address (6 octets)
  The CE LACP system MAC address is encoded in the high-order 6 octets of the ESI value field.
- CE LACP port Key (2 octets)
  The CE LACP port key is encoded in the 2 octets next to the system MAC address.
- the remaining octet is set to 0x00.

Parameters **type-1** — Specifies an auto-generated ESI value.

none — Specifies the configuration of a manual ESI.

Platforms All

5.366 auto-establish

auto-establish

Syntax [**no**] **auto-establish**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>l2tp>group>tunnel auto-establish)

Full Context configure router l2tp group tunnel auto-establish

Description This command specifies if this tunnel is to be automatically set up by the system.

Default no auto-establish

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

auto-establish

Syntax [**no**] **auto-establish**

Context [Tree] (config>service>vprn>l2tp>group>tunnel auto-establish)

Full Context configure service vprn l2tp group tunnel auto-establish

Description This command specifies if this tunnel is to be automatically set up by the system.

Default no auto-establish

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

auto-establish

Syntax [**no**] **auto-establish**

Context [Tree] (config>ipsec>trans-mode-prof>dyn auto-establish)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn auto-establish)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>dyn auto-establish)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn auto-establish)
[Tree] (config>service>vprn>if>sap>ipsec-tun>dyn auto-establish)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying auto-establish
configure router interface ipsec ipsec-tunnel dynamic-keying auto-establish
configure service ies interface ipsec ipsec-tunnel dynamic-keying auto-establish
configure service vprn interface ipsec ipsec-tunnel dynamic-keying auto-establish
configure service vprn interface sap ipsec-tunnel dynamic-keying auto-establish

Description This command enables automatic attempts to establish a phase 1 exchange.

The system automatically establishes a phase 1 SA as soon as the tunnel is provisioned and enabled (**no shutdown**). This option should only be configured on one side of the tunnel.

Any associated static routes remains up as long as the tunnel is up, even though it may actually be operationally down according to the CLI.

The **no** form of this command disables the automatic attempts to establish a phase 1 exchange.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no auto-establish

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel dynamic-keying auto-establish
- configure ipsec ipsec-transport-mode-profile dynamic-keying auto-establish

VSR

- configure router interface ipsec ipsec-tunnel dynamic-keying auto-establish
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying auto-establish
- configure service ies interface ipsec ipsec-tunnel dynamic-keying auto-establish

5.367 auto-learn-mac-protect

auto-learn-mac-protect

Syntax [**no**] **auto-learn-mac-protect**

Context **[Tree]** (config>service>vpls>endpoint auto-learn-mac-protect)
[Tree] (config>service>pw-template>split-horizon-group auto-learn-mac-protect)

Full Context configure service pw-template split-horizon-group auto-learn-mac-protect
configure service vpls endpoint auto-learn-mac-protect

Description This command enables the automatic protection of source MAC addresses learned on the associated object. MAC protection is used in conjunction with the **restrict-protected-src**, **restrict-unprotected-dst**, and **mac-protect** commands. When **auto-learn-mac-protect** command is applied or removed, the MAC addresses are cleared from the related object.

When the **auto-learn-mac-protect** is enabled on an SHG the action only applies to the associated SAPs (no action is taken by default for spoke SDPs in the SHG). To enable this function for spoke SDPs within a SHG, the **auto-learn-mac-protect** command must be enabled explicitly under the spoke SDP. If required, the **auto-learn-mac-protect** command can also be enabled explicitly under specific SAPs within the SHG.

The **no** form of the command reverts to the default.

Default no auto-learn-mac-protect

Platforms All

auto-learn-mac-protect

Syntax **auto-learn-mac-protect** [**exclude-list** *name*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no auto-learn-mac-protect

Context [Tree] (config>service>pw-template auto-learn-mac-protect)
[Tree] (config>service>vpls>mesh-sdp auto-learn-mac-protect)
[Tree] (config>service>vpls>sap auto-learn-mac-protect)
[Tree] (config>service>vpls>split-horizon-group auto-learn-mac-protect)
[Tree] (config>service>vpls>spoke-sdp auto-learn-mac-protect)

Full Context configure service pw-template auto-learn-mac-protect
configure service vpls mesh-sdp auto-learn-mac-protect
configure service vpls sap auto-learn-mac-protect
configure service vpls split-horizon-group auto-learn-mac-protect
configure service vpls spoke-sdp auto-learn-mac-protect

Description This command specifies whether to enable automatic population of the MAC protect list with source MAC addresses learned on the associated object under which the command is configured.

When configured, dynamically learned MAC Source Addresses (SA) are protected only if they are learned on an object with ALMP configured and there is no exclude list associated to the same object or if there is an exclude list but the MAC does not match any entry.

The same list can be used in multiple objects of the same or different service. If the list is empty, ALMP does not exclude any learned MAC from protection on the object.

The **no** form of the command disables the automatic population of the MAC protect list.

Default auto-learn-mac-protect

Parameters *name* — Specifies the name of the exclude list, up to 32 characters.

Platforms All

5.368 auto-lifetimes

auto-lifetimes

Syntax [**no**] **auto-lifetimes**

Context [Tree] (config>subscr-mgmt>rtr-adv-plcy>pfx-opt>stateful auto-lifetimes)

Full Context configure subscriber-mgmt router-advertisement-policy prefix-options stateful auto-lifetimes

Description This command adjusts the valid and preferred lifetime values of the router advertisement from the DHCP lease of the subscriber. Every router advertisement sent to the subscriber is derived from the DHCP lease in real time. The route advertisement is always sent on a DHCP Renew.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.369 auto-lsp

auto-lsp

Syntax **auto-lsp lsp-template** *template-name* {**policy** *peer-prefix-policy* [**peer-prefix-policy**] | **one-hop**}
no auto-lsp lsp-template *template-name*

Context **[Tree]** (config>router>mpls auto-lsp)

Full Context configure router mpls auto-lsp

Description This command enables the automatic creation of an RSVP point-to-point LSP to a destination node whose router ID matches a prefix in the specified peer prefix policy. This LSP type is referred to as auto-LSP of type mesh.

The user can associate multiple templates with same or different peer prefix policies. Each application of an LSP template with a given prefix in the prefix list results in the instantiation of a single CSPF computed LSP primary path using the LSP template parameters as long as the prefix corresponds to a router ID for a node in the TE database. This command does not support the automatic signaling of a secondary path for an LSP. If the signaling of multiple LSPs to the same destination node is required, the user must apply a separate LSP template to the same or different prefix list that contains the same destination node. Each instantiated LSP will have a unique LSP ID and a unique tunnel ID. This command also does not support the signaling of a non-CSPF LSP. The selection of the **no cspf** option in the LSP template is blocked.

Up to five peer prefix policies can be associated with a given LSP template at all times. Each time the user runs the **auto-lsp** command with the same or different prefix policy associations, or the user changes a prefix policy associated with an LSP template, the system re-evaluates the prefix policy. The outcome of the re-evaluation tells MPLS if an existing LSP needs to be torn down or if a new LSP needs to be signaled to a destination address that is already in the TE database.

If a /32 prefix is added to (removed from) or if a prefix range is expanded (shrunk) in a prefix list associated with an LSP template, the preceding prefix policy re-evaluation is performed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The user must perform a **no shutdown** of the template before the template takes effect. After a template is in use, the user must shut down the template before effecting any changes to the parameters, except for those LSP parameters for which the change can be handled with the Make-Before-Break (MBB) procedures. These parameters are **bandwidth** and enabling **fast-reroute** with or without the **hop-limit** or **node-protect** options. For all other parameters, the user must shut down the template, makes the change, and perform a **no shutdown**. This results in the existing instances of the LSP using this template to be torn down and re-signaled.

When a router with a router ID that matches a prefix in the prefix list appears in the TE database, it is a trigger to signal the LSP. The signaled LSP is installed in the Tunnel Table Manager (TTM) and is available to applications such as LDP-over-RSVP, resolution of BGP label routes, resolution of BGP, IGP, and static routes. It is, however, not available for use as a provisioned SDP for explicit binding or auto-binding by services.

Except for the MBB limitations to the configuration parameter change in the LSP template, MBB procedures for manual and timer based re-signaling of the LSP, for TE Graceful Shutdown and for soft preemption are supported.

The **one-to-one** option under **fast-reroute**, the LSP Diff-Serv **class-type** and **backup-class-type** parameters are not supported. If **diffserv-te** is enabled under RSVP, the auto-created LSP is still signaled but with the default LSP class type.

If the **one-hop** option is specified instead of a prefix list, this command enables the automatic signaling of one-hop point-to-point LSPs using the specified template to all directly connected neighbors. This LSP type is referred to as auto-LSP of type one-hop. Although the provisioning model and CLI syntax differ from that of a mesh LSP only by the absence of a prefix list, the actual behavior is quite different. When this command is executed, the TE database keeps track of each TE link that comes up to a directly connected IGP neighbor whose router ID is discovered. It then instructs MPLS to signals an LSP with a destination address matching the router ID of the neighbor and with a strict hop consisting of the address of the interface used by the TE link. Thus, the **auto-lsp** command with the **one-hop** option results in one or more LSPs signaled to the neighboring router.

An auto-created mesh or one-hop LSP can collect egress statistics at the ingress LER by adding the **egress-statistics** node configuration into the LSP template. The user can also collect ingress statistics at the egress LER by using the same **ingress-statistics** node configuration. The user must specify the full LSP name as signaled by the ingress LER in the RSVP session name field of the Session Attribute object in the received Path message.

This feature also provides for the auto-creation of an SR-TE mesh LSP and for an SR-TE one-hop LSP.

The SR-TE mesh LSP feature specifically binds a **mesh-p2p-srte** LSP template with one or more prefix lists. When the TE database discovers a router that has a router ID matching an entry in the prefix list, it triggers MPLS to instantiate an SR-TE LSP to that router using the LSP parameters in the LSP template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SR-TE one-hop LSP feature specifically activates a **one-hop-p2p-srte** LSP template. In this case, the TE database keeps track of each TE link that comes up to a directly connected IGP neighbor. It then instructs MPLS to instantiate a SR-TE LSP with the following parameters:

- the source address of the local router
- an outgoing interface matching the interface index of the TE-link
- a destination address matching the router ID of the neighbor on the TE link

In both types of SR-TE auto-LSP, the router's hop-to-label translation computes the label stack required to instantiate the LSP.

Note: An SR-TE auto-LSP can be reported to a PCE but cannot be delegated or have its paths computed by PCE.

The **no** form of this command deletes all LSPs signaled using the specified template and prefix policy. When the **one-hop** option is used, it deletes all one-hop LSPs signaled using the specified template to all directly-connected neighbors.

Parameters **lsp-template** *template-name* — Specifies an LSP template name, up to 32 characters in length.

policy *peer-prefix-policy* — Specifies an peer prefix policy name, up to 32 characters in length.

one-hop — Enables the automatic signaling of one-hop point-to-point LSPs.

Platforms All

5.370 auto-mep-discovery

auto-mep-discovery

Syntax [**no**] **auto-mep-discovery**

Context **[Tree]** (config>eth-cfm>domain>assoc auto-mep-discovery)

Full Context configure eth-cfm domain association auto-mep-discovery

Description This command enables the ability to auto-discover remote MEPs from a peer MEP sending ETH-CC.

The **no** form of this command disables the ability to auto-discover remote MEPs from a peer MEP sending ETH-CC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no auto-mep-discovery

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

5.371 auto-reply

auto-reply

Syntax [**no**] **auto-reply**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6 auto-reply)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 auto-reply)

Full Context configure service ies subscriber-interface group-interface ipv6 auto-reply
configure service vprn subscriber-interface group-interface ipv6 auto-reply

Description This command assists IP-only static hosts to resolve their default gateway and MAC. By default, the BNG anti-spoof filter drops packets from unknown hosts. The auto-reply features first allow hosts to resolve their default gateway and afterwards allow them to forward traffic. Using the data traffic, the BNG can utilize the data-trigger mechanism to learn the host's MAC and populate the full IP+MAC static host entry.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.372 auto-rp

auto-rp

Syntax **auto-rp** [**detail**]
no auto-rp

Context **[Tree]** (debug>router>pim auto-rp)

Full Context debug router pim auto-rp

Description This command enables debugging for PIM auto-RP.

The **no** form of this command disables PIM auto-RP debugging.

Parameters **detail** — Debugs detailed information on the PIM auto-RP mechanism.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.373 auto-rp-discovery

auto-rp-discovery

Syntax **auto-rp-discovery** [**candidate**] [**mapping-agent**]
no auto-rp-discovery

Context **[Tree]** (config>service>vprn>pim>rp auto-rp-discovery)

Full Context configure service vprn pim rp auto-rp-discovery

Description This command enables the auto-RP protocol in discovery mode. In discovery mode, RP-mapping and RP-candidate messages are received and forwarded to downstream nodes. RP-mapping messages are received locally to learn the availability of RP nodes present in the network. In a VPRN configuration, Nokia recommends that a local loopback interface should be created with the same IP address as the system IP address.

The following configuration guidelines apply.

- Either **bsr-candidate** for IPv4 or **auto-rp-discovery** can be configured; the two mechanisms cannot be enabled together.
- **bsr-candidate** for IPv6 and **auto-rp-discovery** for IPv4 can be enabled together.
- **auto-rp-discovery** cannot be enabled together with **mdt-type sender-only** or **mdt-type receiver-only**, or **wildcard-spmsi** configurations.

This command also enables the auto-RP listener functionality. The auto-RP listener forwards the candidate 224.0.1.39 and mapping 224.0.1.40 messages over the PIM interfaces.

The **no** form of this command disables auto-RP discovery, auto-RP listener, candidate, and mapping-agent.

Default no auto-rp-discovery

Parameters **candidate** — Specifies that the RP is a candidate RP. The auto-RP C-RP announces the candidate RP messages on the 224.0.1.39 multicast address. This functionality is in addition to the listener functionality enabled by the auto RP discovery.

The default value is **no candidate**.

mapping agent — Specifies the mapping agent on the node. The auto-RP MA observes the **auto-rp-announcement** messages, selects the RP, and generates the RP discovery 224.0.1.40 messages. This functionality is in addition to the auto RP discovery functionality.

The default value is **no mapping-agent**.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

auto-rp-discovery

Syntax **auto-rp-discovery** [**candidate**] [**mapping-agent**]
no auto-rp-discovery

Context **[Tree]** (config>router>pim>rp auto-rp-discovery)

Full Context configure router pim rp auto-rp-discovery

Description This command enables the auto-RP protocol in discovery mode. In discovery mode, RP-mapping and RP candidate messages are received and forwarded to downstream nodes. RP-mapping messages are received locally to learn the availability of RP nodes present in the network.

The following configuration guidelines apply.

- Either **bsr-candidate** for IPv4 or **auto-rp-discovery** can be configured; the two mechanisms cannot be enabled together.
- **bsr-candidate** for IPv6 and **auto-rp-discovery** for IPv4 can be enabled together.

This command also enables the auto-RP listener functionality. The auto-RP listener forwards the candidate 224.0.1.39 and mapping 224.0.1.40 messages over the PIM interfaces.

The **no** form of this command disables auto-RP discovery, auto-RP listener, candidate, and mapping-agent.

Default no auto-rp-discovery

Parameters **candidate** — Specifies that the RP is a candidate RP. The auto-RP C-RP announces the candidate RP messages on the 224.0.1.39 multicast address. This functionality is in addition to the listener functionality enabled by the auto RP discovery.

The default value is **no candidate**.

mapping agent — Specifies the mapping agent on the node. The auto-RP MA observes the **auto-rp-announcement** messages, selects the RP, and generates the RP discovery 224.0.1.40 messages. This functionality is in addition to the auto RP discovery functionality.

The default value is **no mapping-agent**.

Platforms All

5.374 auto-rx

auto-rx

Syntax **auto-rx**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ldp>targeted-session auto-rx)

Full Context configure router ldp targeted-session auto-rx

Description Commands in this context configure an automatic targeted LDP session and accept targeted Hello messages from any peer.

Platforms All

5.375 auto-srrp-id-range

auto-srrp-id-range

Syntax **auto-srrp-id-range start** *start-id* **end** *end-id*
no auto-srrp-id-range

Context [Tree] (config>redundancy>srrp auto-srrp-id-range)

Full Context configure redundancy srrp auto-srrp-id-range

Description This command reserves IDs for internal SRRP objects created for inter-UPF resiliency. Manually provisioned SRRP instances cannot use these reserved IDs.

The **no** form of this command removes the reservation of IDs.

Parameters *start-id* — Specifies the lower bound of the ID range.

Values 1 to 4294967294

end-id — Specifies the upper bound of the ID range.

Values 2 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.376 auto-sub-id-key

auto-sub-id-key

Syntax **auto-sub-id-key**

Context [Tree] (config>subscr-mgmt auto-sub-id-key)

Full Context configure subscriber-mgmt auto-sub-id-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure auto-generated subscriber identification key parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.377 auto-tx

auto-tx

Syntax **auto-tx**

Context **[Tree]** (config>router>ldp>targeted-session auto-tx)

Full Context configure router ldp targeted-session auto-tx

Description Commands in this context configure an automatic targeted LDP session and send targeted Hello messages towards PQ nodes determined by the rLFA algorithm.

Platforms All

5.378 autoconfigure

autoconfigure

Syntax **autoconfigure**

Context **[Tree]** (bof autoconfigure)

Full Context bof autoconfigure

Description Commands in this context autoconfigure the IP address for the BOF. The IPv4 DHCP client, IPv6 DHCP client, and NDP/RA can be configured on the management interface.

Default no autoconfigure

Platforms 7450 ESS-7, 7750 SR-1, 7750 SR-1e, 7750 SR-7, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.379 autonegotiate

autonegotiate

Syntax **autonegotiate** [**limited**]
no autonegotiate

Context **[Tree]** (config>port>ethernet autonegotiate)

Full Context configure port ethernet autonegotiate

Description This command enables speed and duplex autonegotiation on Fast Ethernet ports and enables far-end fault indicator support on Gb ports.

There are three possible settings for autonegotiation:

- “on” or enabled with full port capabilities advertised
- “off” or disabled where there are no autonegotiation advertisements
- “limited” where a single speed/duplex is advertised.

When autonegotiation is enabled on a port, the link attempts to automatically negotiate the link speed and duplex parameters. If autonegotiation is enabled, the configured duplex and speed parameters are ignored.

When autonegotiation is disabled on a port, the port does not attempt to autonegotiate and will only operate at the **speed** and **duplex** settings configured for the port. Note that disabling autonegotiation on Gb ports is not allowed as the IEEE 802.3 specification for Gb Ethernet requires autonegotiation be enabled for far end fault indication.

If the **autonegotiate limited** keyword option is specified the port will auto-negotiate but will only advertise a specific speed and duplex. The speed and duplex advertised are the **speed** and **duplex** settings configured for the port. One use for limited mode is for multi-speed Gb ports to force Gb operation while keeping autonegotiation enabled for compliance with IEEE 802.3.

Router requires that autonegotiation be disabled or limited for ports in a Link Aggregation Group to guarantee a specific port speed.

The **no** form of this command disables autonegotiation on this port.

Default autonegotiate

Parameters **limited** — The Ethernet interface will automatically negotiate link parameters with the far end, but will only advertise the speed and duplex mode specified by the Ethernet **config>port>ethernet speed** and **config>port>ethernet duplex** commands.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

autonegotiate

Syntax [**no**] **autonegotiate**

Context **[Tree]** (bof autonegotiate)

Full Context bof autonegotiate

Description This command enables speed and duplex autonegotiation on the management Ethernet port in the running configuration and the Boot Option File (BOF).

When **autonegotiation** is enabled, the link attempts to automatically negotiate the link speed and duplex parameters. If **autonegotiation** is enabled, then the configured duplex and speed parameters are ignored.

The **no** form of this command disables the autonegotiate feature on this port.

Platforms All

5.380 autonomous

autonomous

Syntax [**no**] **autonomous**

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv>pfx-opt autonomous)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv>pfx-opt autonomous)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv>pfx-op autonomous)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv>pfx-opt autonomous)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements prefix-options autonomous
configure service ies subscriber-interface ipv6 router-advertisements prefix-options autonomous
configure service vprn subscriber-interface group-interface ipv6 router-advertisements prefix-options autonomous
configure service vprn subscriber-interface ipv6 rtr-adv pfx-op autonomous

Description This command enables the option that determines whether or not the prefix can be used for stateless address autoconfiguration.

The **no** form of this command disables the option.

Default no autonomous

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

autonomous

Syntax [**no**] **autonomous**

Context **[Tree]** (config>service>vprn>router-advert>if>prefix autonomous)

Full Context configure service vprn router-advertisement interface prefix autonomous

Description This command specifies whether the prefix can be used for stateless address autoconfiguration.

Default autonomous

Platforms All

autonomous

Syntax [**no**] **autonomous**

Context **[Tree]** (config>router>router-advert>if>prefix autonomous)

Full Context configure router router-advertisement interface prefix autonomous

Description This command specifies whether the prefix can be used for stateless address autoconfiguration.

Default autonomous

Platforms All

5.381 autonomous-system

autonomous-system

Syntax **autonomous-system** *as-number*
no autonomous-system

Context **[Tree]** (config>service>vprn autonomous-system)

Full Context configure service vprn autonomous-system

Description This command defines the autonomous system (AS) to be used by this VPN routing/forwarding (VRF). This command defines the autonomous system to be used by this VPN routing

The **no** form of this command removes the defined AS from this VPRN context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no autonomous-system

Parameters *as-number* — Specifies the AS number for the VPRN service.

Values 1 to 4294967295

Platforms All

autonomous-system

Syntax **autonomous-system** *autonomous-system*
no autonomous-system

Context **[Tree]** (config>router autonomous-system)

Full Context configure router autonomous-system

Description This command configures the autonomous system (AS) number for the router. A router can only belong to one AS. An AS number is a globally unique number with an AS. This number is used to exchange exterior routing information with neighboring ASs and as an identifier of the AS itself.

If the AS number is changed on a router with an active BGP instance, the new AS number is not used until the BGP instance is restarted either by administratively disabling/enabling (**shutdown**/**no shutdown**) the BGP instance or rebooting the system with the new configuration.

Default no autonomous-system

Parameters *autonomous-system* — Specifies the autonomous system number expressed as a decimal integer.

Values 1 to 4294967295

Platforms All

5.382 autonomous-system-type

autonomous-system-type

Syntax **autonomous-system-type** {**origin** | **peer**}

Context **[Tree]** (config>cflowd>collector autonomous-system-type)

Full Context configure cflowd collector autonomous-system-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines whether the autonomous system (AS) information included in the flow data is based on the originating AS or external peer AS of the routes.

This option is only allowed if the collector is configured as Version 5 or Version 8.

Default autonomous-system-type origin

Parameters **origin** — Specifies that the AS information included in the flow data is based on the originating AS.

peer — Specifies that the AS information included in the flow data is based on the peer AS.

Platforms All

5.383 aux-channel-enable

aux-channel-enable

Syntax [**no**] **aux-channel-enable**

Context **[Tree]** (config>open-flow>of-switch aux-channel-enable)

Full Context configure open-flow of-switch aux-channel-enable

Description This command enables auxiliary connections for the given H-OFS instance. If enabled, the H-OFS switch sets up a statistics auxiliary channel (Auxiliary ID 1) and a packet-in auxiliary channel (Auxiliary ID 2) for the main connection to every configured OpenFlow controller.

The **no** form of this command disables auxiliary connections.

Default no aux-channel-enable

Platforms All

5.384 aux-stats

aux-stats

Syntax [**no**] **aux-stats sr**

Context **[Tree]** (config>router>mpls aux-stats)

Full Context configure router mpls aux-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables and configures counters for the specified labeled traffic type in an auxiliary MPLS statistics table. The **sr** keyword indicates to the system to increment packet and octet counters of that table for any type of Segment Routing traffic (SR-OSPF, SR-ISIS, SR-TE, and so on). This command cannot be used in specific system configurations. This command does not impact the overall counting of MPLS packets and octets shown, for example, by the **show router mpls interface** [*ip-int-name* | *ip-address*] **statistics** command.

The **no** form of this command disables the counters of the auxiliary MPLS statistics table. The **no** form of this command cannot be used if dark bandwidth accounting is enabled (**config>router>rsvp>dbw-accounting**).

Default aux-stats sr

Parameters **sr** — Specifies the type of traffic to count in the auxiliary MPLS statistics table. Refers to any type of Segment Routing traffic (SR-OSPF, SR-ISIS, SR-TE, and so on).

5.385 availability

availability

Syntax **availability**

Context **[Tree]** (config>oam-pm>session>ethernet>lmm availability)

Full Context configure oam-pm session ethernet lmm availability

Description Commands in this context activate, collect, and record availability statistics for LMM tests. These computations are not enabled by default. In order to modify parameters within a session, including these availability parameters, the LMM test must be shut down.

Platforms All

5.386 avg-flr-event

avg-flr-event

Syntax **avg-flr-event** {**forward** | **backward**} **threshold** *raise-threshold-percentage* [**clear** *clear-threshold-percentage*]
no avg-flr-event {**forward** | **backward**}

Context **[Tree]** (config>oam-pm>session>ethernet>slm>loss-events avg-flr-event)
[Tree] (config>oam-pm>session>ethernet>lmm>loss-events avg-flr-event)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>oam-pm>session>ip>twamp-light>loss-events avg-flr-event)

Full Context
configure oam-pm session ethernet lmm loss-events avg-flr-event
configure oam-pm session ethernet slm loss-events avg-flr-event
configure oam-pm session ip twamp-light loss-events avg-flr-event

Description
This command sets the frame loss ratio threshold configuration to be applied and checked at the end of the measurement interval for the specified direction. This is a percentage based on average frame loss ratio over the entire measurement interval. If the *clear-threshold-percent* value is not specified, the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and without regard to any previous window. Each unique event can only be raised once within measurement interval. If the optional *clear-threshold-percent* value is specified, the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is carried forward to following measurement intervals. If a threshold crossing event is raised another is not raised until a measurement interval completes and the clear threshold has not been exceeded. A clear event is raised under that condition.

The **no** form of this command removes the event threshold for frame loss ratio. The direction must be included with the **no** command.

Default
no avg-flr-event forward

no avg-flr-event backward

Parameters
forward — Specifies the threshold is applied to the forward direction value.

backward — Specifies the threshold is applied to the backward direction value.

raise-threshold-percentage — Specifies the rising percentage that determines when the event is to be generated.

Values 0.001 to 100.000

clear-threshold-percentage — Specifies an optional value used for stateful behavior that allows the operator to configure a percentage of loss value lower than the rising percentage to indicate when the clear event should be generated.

Values 0.000 to 99.999
A value 0.000 means that the FLR must be 0.000.

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events avg-flr-event

All

- configure oam-pm session ethernet lmm loss-events avg-flr-event
- configure oam-pm session ethernet slm loss-events avg-flr-event

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.387 avg-frame-overhead

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue avg-frame-overhead)

Full Context configure subscriber-mgmt sla-profile egress qos queue avg-frame-overhead

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a SONET or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.
- Frame encapsulation overhead — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queues current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- Frame based offered-load — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queues offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead is the same as the packet to frame factor making this calculation unnecessary.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queues configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.
- Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a policer, queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-cir pass.

- Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue's configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.
- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to determine the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command reverts to the default. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default avg-frame-overhead 0

Parameters *percent* — Specifies the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0.00 to 100.00, default

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue avg-frame-overhead)

Full Context configure service ies interface sap egress queue-override queue avg-frame-overhead
configure service ies interface sap ingress queue-override queue avg-frame-overhead
configure service ies subscriber-interface group-interface sap egress queue-override queue avg-frame-overhead
configure service vpls sap ingress queue-override queue avg-frame-overhead

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue expands during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-Load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet-based offered-load.
- Frame-encapsulation overhead — Using the avg-frame-overhead parameter, the frame-encapsulation overhead is simply the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10,000 octets and the avg-frame-overhead equals 10%, the frame-encapsulation overhead would be 10,000 x 0.1 or 1,000 octets.

For egress Ethernet queues, the frame-encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame-encapsulation overhead would be 50 x 20 or 1,000 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame-based offered-load — The frame-based offered-load is calculated by adding the offered-load to the frame-encapsulation overhead. If the offered-load is 10,000 octets and the encapsulation overhead was 1,000 octets, the frame-based offered-load would equal 11,000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame-encapsulation overhead by the queue's offered-load (packet-based). If the frame-encapsulation overhead is 1,000 octets and the offered-load is 10,000 octets then the packet to frame factor would be 1,000 / 10,000 or 0.1. When in use, the avg-frame-overhead is the same as the packet to frame factor making this calculation unnecessary.
- Frame-based CIR — The frame-based CIR is calculated by multiplying the packet to frame factor with the queue's configured CIR, then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame-based CIR would be 500 x 1.1 or 550 octets.
- Frame-based within-CIR offered-load — The frame-based within-CIR offered-load is the portion of the frame-based offered-load considered to be within the frame-based CIR. The frame-based within-CIR offered-load is the lesser of the frame-based offered-load and the frame-based CIR. If the frame-based offered-load equaled 11000 octets and the frame-based CIR equaled 550 octets, the frame-based within-CIR offered-load would be limited to 550 octets. If the frame-based offered-load equaled 450 octets and the frame-based CIR equaled 550 octets, the frame-based within-CIR offered-load would equal 450 octets (or the entire frame-based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame-based within-CIR offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-CIR pass.

- Frame-based PIR — The frame-based PIR is calculated by multiplying the packet to frame factor with the queue's-configured PIR, then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame-based PIR would be 7,500 x 1.1 or 8,250 octets.
- Frame-based within-pir offered-load — The frame-based within-pir offered-load is the portion of the frame-based offered-load considered to be within the frame-based PIR. The frame-based within-pir offered-load is the lesser of the frame-based offered-load and the frame-based PIR. If the frame-based offered-load equaled 11,000 octets and the frame-based PIR equaled 8250 octets, the frame-based within-pir offered-load would be limited to 8,250 octets. If the frame-based offered-load equaled 7,000 octets and the frame-based PIR equaled 8,250 octets, the frame-based within-pir offered load would equal 7,000 octets.

Port Scheduler Operation Using Frame Transformed Rates — The port scheduler uses the frame-based rates to figure the maximum rates that each queue may receive during the within-CIR and above-CIR bandwidth allocation passes. During the within-CIR pass, a queue may receive up to its frame-based within-CIR offered-load. The maximum it may receive during the above-CIR pass is the difference between the frame-based within-pir offered load and the amount of actual bandwidth allocated during the within-CIR pass.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

SAP and Subscriber SLA-Profile Average Frame Overhead Override — The average frame overhead parameter on a sap-egress may be overridden on an individual egress queue basis; on each SAP and within the sla-profile policy used by subscribers. An avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance uses its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet-based queue statistics for calculating port scheduler priority bandwidth allocation. If the **no avg-frame-overhead** command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default avg-frame-overhead 0

Parameters *percent* — Sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues. This parameter only applies to the 7450 ESS and 7750 SR.

Values 0.00 to 100.00

Platforms All

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue avg-frame-overhead)

Full Context configure service vpls sap egress queue-override queue avg-frame-overhead

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a SONET or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame encapsulation overhead — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- Frame based offered-load — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue's offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.
- Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queue's configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.
- Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-cir pass.

- Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue's configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to calculate the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default avg-frame-overhead 0

Parameters *percent* — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0 to 100

Platforms All

avg-frame-overhead

Syntax **avg-frame-overhead** *percentage*
no avg-frame-overhead

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>epipe>sap>egress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue avg-frame-overhead)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue avg-frame-overhead)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context

configure service apipe sap egress queue-override queue avg-frame-overhead
configure service cpipe sap egress queue-override queue avg-frame-overhead
configure service epipe sap egress queue-override queue avg-frame-overhead
configure service fpipe sap egress queue-override queue avg-frame-overhead
configure service ipipe sap egress queue-override queue avg-frame-overhead

Description

This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a SONET or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.
- Frame encapsulation overhead — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

  For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets, then the frame encapsulation overhead would be 50 x 20 or 1000 octets.
- Frame based offered-load — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue's offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets, then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.
- Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queue's configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

  As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-cir pass.
- Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue's configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.
- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to figure the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

On the 7450 ESS and 7750 SR, SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default avg-frame-overhead 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent* — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress queue-override queue avg-frame-overhead
- configure service cpipe sap egress queue-override queue avg-frame-overhead

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue avg-frame-overhead

All

- configure service epipe sap egress queue-override queue avg-frame-overhead
- configure service ipipe sap egress queue-override queue avg-frame-overhead

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue avg-frame-overhead)

Full Context configure service vprn interface sap egress queue-override queue avg-frame-overhead

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.
- Frame encapsulation overhead — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- Frame based offered-load — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue's offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.
- Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queue's configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.
- Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-cir pass.

- Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue's configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.
- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to determine the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default 0

Parameters *percent* — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0 to 100

Platforms All

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context **[Tree]** (config>qos>sap-egress>queue avg-frame-overhead)

Full Context configure qos sap-egress queue avg-frame-overhead

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Offered-Load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet-based offered-load.
- Frame-encapsulation overhead — Using the avg-frame-overhead parameter, the frame-encapsulation overhead is simply the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10,000 octets and the avg-frame-overhead equals 10%, the frame-encapsulation overhead would be 10,000 x 0.1 or 1,000 octets.

For egress Ethernet queues, the frame-encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets, then the frame-encapsulation overhead would be 50 x 20 or 1,000 octets.

- Frame-based offered-load — The frame-based offered-load is calculated by adding the offered-load to the frame-encapsulation overhead. If the offered-load is 10,000 octets and the encapsulation overhead was 1,000 octets, the frame-based offered-load would equal 11,000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame-encapsulation overhead by the queue's offered-load (packet-based). If the frame-encapsulation overhead is 1,000 octets and the offered-load is 10,000 octets, then the packet to frame factor would be 1,000 / 10,000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.
- Frame-based CIR — The frame-based CIR is calculated by multiplying the packet to frame factor with the queue's configured CIR, then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame-based CIR would be 500 x 1.1 or 550 octets.
- Frame-based within-CIR offered-load — The frame-based within-CIR offered-load is the portion of the frame-based offered-load considered to be within the frame-based CIR. The frame-based within-CIR offered-load is the lesser of the frame-based offered-load and the frame-based CIR. If the frame-based offered-load equaled 11000 octets and the frame-based CIR equaled 550 octets, the frame-based within-CIR offered-load would be limited to 550 octets. If the frame-based offered-load equaled 450 octets and the frame-based CIR equaled 550 octets, the frame-based within-CIR offered-load would equal 450 octets (or the entire frame-based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame-based within-CIR offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-CIR pass.

- Frame-based PIR — The frame-based PIR is calculated by multiplying the packet to frame factor with the queue's-configured PIR, then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame-based PIR would be 7,500 x 1.1 or 8,250 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame-based within-pir offered-load — The frame-based within-pir offered-load is the portion of the frame-based offered-load considered to be within the frame-based PIR. The frame-based within-pir offered-load is the lesser of the frame-based offered-load and the frame-based PIR. If the frame-based offered-load equaled 11,000 octets and the frame-based PIR equaled 8250 octets, the frame-based within-pir offered-load would be limited to 8,250 octets. If the frame-based offered-load equaled 7,000 octets and the frame-based PIR equaled 8,250 octets, the frame-based within-pir offered load would equal 7,000 octets.

Port Scheduler Operation Using Frame Transformed Rates — The port scheduler uses the frame-based rates to figure the maximum rates that each queue may receive during the within-CIR and above-CIR bandwidth allocation passes. During the within-CIR pass, a queue may receive up to its frame-based within-CIR offered-load. The maximum it may receive during the above-CIR pass is the difference between the frame-based within-pir offered load and the amount of actual bandwidth allocated during the within-CIR pass.

SAP and Subscriber SLA-Profile Average Frame Overhead Override — The average frame overhead parameter on a sap-egress may be overridden on an individual egress queue basis; on each SAP and within the sla-profile policy used by subscribers. An avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet-based queue statistics for calculating port scheduler priority bandwidth allocation. If the **no avg-frame-overhead** command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default no avg-frame-overhead

Parameters *percent* — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues. This parameter only applies to the 7450 ESS and 7750 SR.

Values 0.00 to 100.00

Platforms All

avg-frame-overhead

Syntax **avg-frame-overhead** *percent*
no avg-frame-overhead

Context **[Tree]** (config>qos>network-queue>queue avg-frame-overhead)

Full Context configure qos network-queue queue avg-frame-overhead

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a SONET or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- Offered-Load — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet-based offered-load.
- Frame-encapsulation overhead — Using the avg-frame-overhead parameter, the frame-encapsulation overhead is the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10 000 octets and the avg-frame-overhead equals 10%, the frame-encapsulation overhead would be 10 000 x 0.1 or 1000 octets.

For egress Ethernet queues, the frame-encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets, the frame-encapsulation overhead would be 50 x 20 or 1000 octets.

- Frame-based offered-load — The frame-based offered-load is calculated by adding the offered-load to the frame-encapsulation overhead. If the offered-load is 10,000 octets and the encapsulation overhead was 1000 octets, the frame-based offered-load would equal 11 000 octets.
- Packet to frame factor — The packet to frame factor is calculated by dividing the frame-encapsulation overhead by the queue's offered-load (packet-based). If the frame-encapsulation overhead is 1000 octets and the offered-load is 10 000 octets, then the packet to frame factor would be 1000 / 10 000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor, making this calculation unnecessary.
- Frame-based CIR — The frame-based CIR is calculated by multiplying the packet to frame factor with the queue's-configured CIR, then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame-based CIR would be 500 x 1.1 or 550 octets.
- Frame-based within-CIR offered-load — The frame-based within-CIR offered-load is the portion of the frame-based offered-load considered to be within the frame-based CIR. The frame-based within-CIR offered-load is the lesser of the frame-based offered-load and the frame-based CIR. If the frame-based offered-load equaled 11 000 octets and the frame-based CIR equaled 550 octets, the frame-based within-CIR offered-load would be limited to 550 octets. If the frame-based offered-load equaled 450 octets and the frame-based CIR equaled 550 octets, the frame-based within-CIR offered-load would equal 450 octets (or the entire frame-based offered-load).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue's frame-based within-CIR offered-load to 0, preventing it from receiving bandwidth during the port scheduler's within-CIR pass.

- Frame-based PIR — The frame-based PIR is calculated by multiplying the packet to frame factor with the queue's-configured PIR, then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame-based PIR would be 7500 x 1.1 or 8250 octets.
- Frame-based within-pir offered-load — The frame-based within-pir offered-load is the portion of the frame-based offered-load considered to be within the frame-based PIR. The frame-based within-pir offered-load is the lesser of the frame-based offered-load and the frame-based PIR. If the frame-based offered-load equaled 11,000 octets and the frame-based PIR equaled 8250 octets, the frame-based within-pir offered-load would be limited to 8,250 octets. If the frame-based offered-load equaled 7,000 octets and the frame-based PIR equaled 8,250 octets, the frame-based within-pir offered load would equal 7,000 octets.

Port Scheduler Operation Using Frame Transformed Rates — The port scheduler uses the frame-based rates to figure the maximum rates that each queue may receive during the within-CIR and above-CIR bandwidth allocation passes. During the within-CIR pass, a queue may receive up to its frame-based within-CIR offered load. The maximum it may receive during the above-CIR pass is the difference between the frame-based within-PIR offered load and the amount of actual bandwidth allocated during the within-CIR pass.

SAP and Subscriber SLA-Profile Average Frame Overhead Override (applies only to the 7450 ESS and 7750 SR) — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers, an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress-defined overhead.

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0%. When set to 0, the system uses the packet-based queue statistics for calculating port scheduler priority bandwidth allocation. If the **no avg-frame-overhead** command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default no avg-frame-overhead

Parameters *percent* — This parameter sets the average number of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0.00 to 100.00

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.388 avp

avp

Syntax **avp** *avp-id* **type** *type* [**ascii** | **hex**] **value** *value*
no avp *avp-id*

Context **[Tree]** (debug>diam>diam-peer-plcy>avp-match avp)

Full Context debug diameter diameter-peer-policy avp-match avp

Description This command specifies an AVP match criteria for AVP value matching. At least one and up to five AVP match criteria can be specified in an **avp-match** *id* command. When multiple AVP match criteria are specified, they must all match to be successful and result in a diameter session ID learning. (AND function between **avp** *avp-id* commands.)

The AVP in an AVP match criteria is identified by its AVP ID. The AVP ID is specified as [*vendor-id*-]*avp-code*[.*avp-id*] with nesting up to five levels deep.

The format type of the AVP should match the standard documents in which the AVP is specified. Any AVP can be specified as an octet string in hex format.

Parameters *avp-id* — Specifies that an AVP is a [*vendor-id*-]*avp-code*[.*avp-id*], up to five levels deep. For example to specify the Multiple-Services-Credit-Control.Quota-Holding-Time AVP, use *avp-id* = 456.10415-871.

Values *vendor-id*: [1 to 4294967295]
avp-code: [1 to 4294967295]

type — Specifies the format type of the AVP as octets string, integer32, integer64, unsigned32, unsigned64 or address. The type should match the format as specified in the corresponding standard documents. Any AVP can be specified as octet string in hex.

ascii | hex — Specifies the value format. The ASCII format is default. The hexadecimal format value should start with "0x". For example: 0x0000000a to specify a 4 byte integer value in hexadecimal format.

value — Specifies the actual value of the AVP that should be matched against (up to 256 characters or up to 127 characters when specified in hex).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

5.389 avp-hiding

avp-hiding

Syntax **avp-hiding** {**sensitive** | **always**}
no avp-hiding

Context **[Tree]** (config>router>l2tp avp-hiding)
[Tree] (config>service>vprn>l2tp avp-hiding)

Full Context configure router l2tp avp-hiding
configure service vprn l2tp avp-hiding

Description This command configures Attribute Value Pair (AVP) hiding. This capability can be used to avoid the passing of sensitive data, such as user passwords, as cleartext in an AVP.

The **no** form of this command reverts to the default value.

Default no avp-hiding

Parameters **sensitive** — AVP hiding is used only for sensitive information (such as username/password).

always — AVP hiding is always used.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

avp-hiding

Syntax **avp-hiding** {**sensitive** | **always**}
no avp-hiding

Context **[Tree]** (config>service>vprn>l2tp>group avp-hiding)

Full Context configure service vprn l2tp group avp-hiding

Description This command configures Attribute Value Pair (AVP) hiding. This capability can be used to avoid the passing of sensitive data, such as user passwords, as clear text in an AVP.

The **no** form of this command returns the value to **never** allow AVP hiding.

Default no avp-hiding

Parameters *avp-hiding* — Specifies the method to be used for the authentication of the tunnels in this L2TP group.

Values sensitive — AVP hiding is used only for sensitive information (such as username/password).

always — AVP hiding is always used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

avp-hiding

Syntax **avp-hiding** {**never** | **sensitive** | **always**}
no avp-hiding

Context **[Tree]** (config>service>vprn>l2tp>group>tunnel avp-hiding)

Full Context configure service vprn l2tp group tunnel avp-hiding

Description This command configures Attribute Value Pair (AVP) hiding. This capability can be used to avoid the passing of sensitive data, such as user passwords, as clear text in an AVP.

Caution: Nokia recommends that sensitive information not be sent in clear text.

The **no** form of this command removes the parameter of the configuration and indicates that the value on group level will be taken.

Default no avp-hiding

Parameters *avp-hiding* — Specifies the method to be used for the authentication of the tunnel.

Values never — AVP hiding is not used.
sensitive — AVP hiding is used only for sensitive information (such as username/password).
always — AVP hiding is always used.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.390 avp-match

avp-match

Syntax **avp-match** *id*
no avp-match *id*

Context **[Tree]** (debug>diam>diam-peer-plcy avp-match)

Full Context debug diameter diameter-peer-policy avp-match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command restricts the debug output to messages within the diameter peer policy that belong to a diameter session identified based on the AVP value matching in a diameter application message. At least the message type and one AVP match criteria must be specified in an **avp-match** *id* command.

If a diameter application message matches all criteria within one AVP match ID, then the session ID is learned and all subsequent messages of that diameter session are shown until a relearning occurs. (OR function between **avp-match** *id* commands.)

When the session ID is learned in an Answer message, an attempt is made to include the corresponding Request message in the debug output: The Request message should still be available in the system and must pass all debug filters (such as **message-type**).

By default an **avp-match** *id* is disabled and must be configured with the **debug>diam>diam-peer-plcy>avp-match no shutdown** to activate.

Parameters *id* — Specifies the AVP match ID, up to five per diameter peer policy.

Values 1 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

5.391 avp-subscription-id

avp-subscription-id

Syntax **avp-subscription-id** *origin* [**type** *type*]
no avp-subscription-id

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx avp-subscription-id)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy avp-subscription-id)

Full Context configure subscriber-mgmt diameter-application-policy gx avp-subscription-id
configure subscriber-mgmt diameter-application-policy gy avp-subscription-id

Description This command is used to provide identification information to the PCRF for the end user. Subscription-id is a grouped AVP. In case that parameter designated to be the subscription-id is not available, the subscription-avp will not be sent.

The **no** form of this command returns the command to the default setting.

Default avp-subscription-id subscriber-id type private

Parameters *origin* — Specifies the origin of the information to send in the Subscription-Id data AVP.

Values **circuit-id** — Specifies the circuit ID. For Gy, the circuit id is an ASCII- converted value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dual-stack-remote-id — Specifies the remote ID for IPv4 and IPv6. The enterprise-id field is stripped off from IPv6 remote ID. For Gy, the remote id is an ascii-converted value.

imei — Specifies the physical ID of the end device.

imsi — Specifies the SIM ID.

mac — Specifies the MAC address of the end device.

msisdn — Specifies the phone number of the end device.

nas-port-id — Specifies the NAS port ID which can be a prefix or suffix with a custom string to make it unique network wide.

subscriber-id — Specifies the subscriber ID.

username — Specifies that the username identifier can be of type **private** or **nai** which specifies the username is a PPP username (PAP/CHAP). When the PPP username is not available, the string in the Username attribute returned by RADIUS or NASREQ is used.

type — Specifies the type of the identifier stored in the Subscription-Id data AVP.

Values **e164** — Specifies the identifier is in international E.164 format (such as MSISDN).

imsi — Specifies the identifier is in international IMSI format according to the ITU-T E.212 numbering plan.

nai — Specifies the identifier is in the form of a Network Access Identifier as defined in RFC 2486.

private — Specifies the identifier is a private type identifier.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6 b Commands

6.1 back

back

Syntax **back**

Context **[Tree]** (global back)

Full Context global back

Description This command moves the context back one level of the command hierarchy. For example, if the current level is the **config router ospf** context, the **back** command moves the cursor to the **config router** context level.

6.2 backbone-vpls

backbone-vpls

Syntax **backbone-vpls** *service-id* [**isid** *isid*]
no backbone-vpls

Context **[Tree]** (config>service>vpls>pbb backbone-vpls)

Full Context configure service vpls pbb backbone-vpls

Description This command configures B-VPLS service associated with the I-VPLS.

Parameters *service-id* — Specifies the service ID.

Values 1 to 2147483648

isid — Specifies the ISID.

Values 0 to 16777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.3 backup

backup

Syntax [**no**] **backup** *ip-address*

Context **[Tree]** (config>service>ies>if>ipv6>vrrp backup)

Full Context configure service ies interface ipv6 vrrp backup

Description This command configures virtual router IP addresses for the interface.

Platforms All

backup

Syntax [**no**] **backup** *ip-address*

Context **[Tree]** (config>service>ies>if>vrrp backup)

Full Context configure service ies interface vrrp backup

Description This command configures virtual router IP addresses for the interface.

Platforms All

backup

Syntax [**no**] **backup** *ip-address*

Context **[Tree]** (config>service>vprn>if>vrrp backup)

Full Context configure service vprn interface vrrp backup

Description This command configures virtual router IP addresses for the interface.

Platforms All

backup

Syntax [**no**] **backup** *ipv6-address*

Context **[Tree]** (config>service>vprn>if>ipv6>vrrp backup)

Full Context configure service vprn interface ipv6 vrrp backup

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures virtual router IP addresses for the interface.

Platforms All

backup

Syntax [**no**] **backup** [*mda-id* | *esa-vm-id*]

Context **[Tree]** (config>isa>aa-grp backup)

Full Context configure isa application-assurance-group backup

Description This command assigns an AA ISA or ESA-VM configured in the specified location to this application assurance group. The backup module provides the application assurance group with warm redundancy when the primary module in the group is configured. Primary and backup modules have equal operational status and when both module are coming up, the ones that becomes operational first becomes the active module. A module can serve as a backup for multiple AA ISA cards but only one can fail to it at one time.

On an activity switch from the primary module, configurations are already on the backup MDA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When the AA service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When AA redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an AA activity switch occurred.

The **no** form of this command removes the specified module from the application assurance group.

Parameters *mda-id* — Specifies the slot and MDA, identifying a provisioned module to use as a backup module.

Values

slot/*mda*	
slot	1 to 10, depending on chassis model
mda	1 to 2

esa-vm-id — Specifies the ESA and VM, identifying a provisioned module to use as a backup module; for example, an ESA 1 with VM2 would be referred to as **esa-1/2**.

Values

esa-*esa-id*/*vm-id*	
esa-id	1 to 16

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vm-id 1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

backup

Syntax **backup** *mda-id*
no backup

Context **[Tree]** (config>isa>tunnel-grp backup)

Full Context configure isa tunnel-group backup

Description This command assigns a tunnel ISA configured in the specified slot to this IPsec group. The backup module provides the IPsec group with warm redundancy when the primary module in the group is configured. An IPsec group must always have a primary configured.

Primary and backup modules have equal operational status and when both modules are coming up, the one that becomes operational first becomes the active module. An IPsec module can serve as a backup for multiple IPsec groups but the backup can become active for only one ISA IPsec group at a time.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPsec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPsec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPsec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPsec activity switch took place.

The **no** form of this command removes the specified module from the IPsec group.

Default no backup

Parameters *mda-id* — Specifies the card/slot identifying a provisioned module to be used as a backup module.

Values mda-id:*slot*/*mda*slot 1 to up to 10 depending on chassis model mda 1 to 2

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

backup

Syntax [**no**] **backup** *ip-address*

Context **[Tree]** (config>router>if>vrrp backup)

Full Context configure router interface vrrp backup

Description This command associates router IP addresses with the parental IP interface IP addresses.

The **backup** command has two distinct functions when used in an **owner** or a **non-owner** context of the virtual router instance.

Non-owner virtual router instances actually create a routable IP interface address that is operationally dependent on the virtual router instance mode (master or backup). The **backup** command in **owner** virtual router instances does not create a routable IP interface address; it simply defines the existing parental IP interface IP addresses that are advertised by the virtual router instance.

For **owner** virtual router instances, the **backup** command defines the IP addresses that are advertised within VRRP advertisement messages. This communicates the IP addresses that the master is representing to backup virtual routers receiving the messages. Advertising a correct list is important. The specified *ip-address* must be equal to one of the existing parental IP interface IP addresses (primary or secondary) or the **backup** command fails.

For non-owner virtual router instances, the **backup** command actually creates an IP interface IP address used for routing IP packets and communicating with the system when the access commands are defined (**ntp-reply, ping-reply**, **telnet-reply**, and **ssh-reply**). The specified *ip-address* must be an IP address that is within one of the parental IP interface local subnets created with the **address** or **secondary** commands. If a local subnet does not exist that includes the specified *ip-address* or if *ip-address* is the same IP address as the parental IP interface IP address, the **backup** command fails.

The new interface IP address created with the **backup** command assumes the mask and parameters of the corresponding parent IP interface IP address. The *ip-address* is only active when the virtual router instance is operating in the master state. When not operating as master, the virtual router instance acts as if it is operationally down. It does not respond to ARP requests to *ip-addr*ess, nor does it route packets received with its *vrid* derived source MAC address. A non-master virtual router instance always silently discards packets destined to *ip-address*. A single virtual router instance may only have a single virtual router IP address from a given parental local subnet. Multiple virtual router instances can define a virtual router IP address from the same local subnet as long as each is a different IP address.

In IPv4, up to sixteen **backup** *ip-address* commands can be executed within the same virtual router instance. Executing **backup** multiple times with the same *ip-addr*ess results in no operation performed and no error generated. At least one successful **backup** *ip-address* command must be executed before the virtual router instance can enter the operational state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When operating as (non-owner) master, the default functionality associated with *ip-address* is ARP response to ARP requests to *ip-address*, routing of packets destined to the virtual router instance source MAC address and silently discarding packets destined to *ip-address*. Enabling the non-owner-access parameters selectively allows ping, Telnet and SSH connectivity to *ip-address* when the virtual router instance is operating as master.

The **no** form of the command removes the specified virtual router IP address from the virtual router instance. For non-owner virtual router instances, this causes all routing and local access associated with the *ip-address* to cease. For **owner** virtual router instances, the **no backup** command only removes *ip-addr*ess from the list of advertised IP addresses. If the last *ip-address* is removed from the virtual router instance, the virtual router instance will enter the operationally down state

Default no backup — No virtual router IP address is assigned.

Special Cases

Assigning the Virtual Router ID IP Address — Once the *vrid* is created on the parent IP interface, IP addresses need to be assigned to the virtual router instance. If the *vrid* was created with the keyword **owner**, the virtual router instance IP addresses must have one or more of the parent IP interface defined IP addresses (primary and secondary). For non-owner virtual router instances, the virtual router IP addresses each must be within one of the parental IP interface IP address defined local subnets. For both **owner** and non-owner virtual router instances, the virtual router IP addresses must be explicitly defined using the **backup** *ip-addr* command.

Virtual Router Instance IP Address Assignment Conditions — The RFC does not specify that the assigned IP addresses to the virtual router instance must be in the same subnet as the parent IP interface primary IP address or secondary IP addresses. The only requirement is that all virtual routers participating in the same virtual router instance have the same virtual router IP addresses assigned. To avoid confusion, the assigned virtual router IP addresses must be in a local subnet of one of the parent IP interfaces IP addresses. For **owner** virtual router instances the assigned virtual router IP address must be the same as one of the parental IP interface primary or secondary IP addresses.

The following rules apply when adding, changing, or removing parental and virtual router IP addresses:

Owner Virtual Router IP Address Parental Association — When an IP address is assigned to an **owner** virtual router instance, it must be associated with one of the parental IP interface-assigned IP addresses. The virtual router IP address must be equal to the primary or one of the secondary IP addresses within the parental IP interface.

Table 30 **Example - Owner Virtual Router Instance**

Parent IP addresses:	10.10.10.10/24 11.11.11.11/24	
Virtual router IP addresses:	10.10.10.11	Invalid (not equal to parent IP address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 30 **Example - Owner Virtual Router Instance**

	10.10.10.10	Associated (same as parent IP address 10.10.10.10)
	10.10.11.11	Invalid (not equal to parent IP address)
	11.11.11.254	Invalid (not equal to parent IP address)
	11.11.11.255	Invalid (not equal to parent IP address)

Non-Owner Virtual Router IP Address Parental Association — When an IP address is assigned to a non-owner virtual router instance, it must be associated with one of the parental IP interface assigned IP addresses. The virtual router IP address must be a valid IP address within one of the parental IP interfaces local subnet. Local subnets are created by the primary or secondary IP addresses in conjunction with the IP addresses mask. If the defined virtual router IP address is equal to the associated subnet's broadcast address, it is invalid. Virtual router IP addresses for non-owner virtual router instances that are equal to a parental IP interface IP address are also invalid.

The same virtual router IP address may not be assigned to two separate virtual router instances. If the virtual router IP address already exists on another virtual router instance, the virtual router IP address assignment will fail.

Table 31 **Example - Non-Owner Virtual Router Instance**

Parent IP addresses:	10.10.10.10/24 11.11.11.11/24	
Virtual router IP addresses:	10.10.10.11	Associated with 10.10.10.10 (in subnet)
	10.10.10.10	Invalid (same as parent IP address)
	10.10.11.11	Invalid (outside of all Parent IP subnets)
	11.11.11.254	Associated with 11.11.11.11 (in subnet)
	11.11.11.255	Invalid (broadcast address of 11.11.11.11/24)

Virtual Router IP Address Assignment without Parent IP Address — When assigning an IP address to a virtual router instance, an associated IP address (see backup) on the parental IP interface must already exist. If an associated IP address on the parental IP interface is not configured, the virtual router IP address assignment fails.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parent Primary IP Address Changed — When a virtual router IP address is set and the associated parent IP interface IP address is changed, the new parent IP interface IP address is evaluated to ensure it meets the association rules defined in backup (**config>router>if>vrrp backup**) or **config>router>if>ipv6>vrrp backup**. If the association check fails, the parental IP address change is not allowed. If the parental IP address change fails, the previously configured IP address definition remains in effect.

Only the primary parent IP address can be changed. Secondary addresses must be removed before the new IP address can be added. backup (**config>router>if>vrrp backup**) explains IP address removal conditions.

Parent Primary or Secondary IP Address Removal — When a virtual router IP address is successfully set, but removing the associated parent IP interface IP address is attempted and fails. All virtual router IP addresses associated with the parental IP interface IP address must be deleted prior to removing the parental IP address. This includes virtual router IP address associations from multiple virtual router instances on the IP interface.

Parameters *ip-address* — The virtual router IP address expressed in dotted decimal notation. The IP virtual router IP address must be in the same subnet of the parental IP interface IP address or equal to one of the primary or secondary IP addresses for **owner** virtual router instances.

Values 1.0.0.1 to 223.255.255.254

Platforms All

backup

Syntax [**no**] **backup** *ipv6-address*

Context **[Tree]** (config>router>if>ipv6>vrrp backup)

Full Context configure router interface ipv6 vrrp backup

Description This command associates router IPv6 addresses with the parental IP interface IP addresses.

The **backup** command has two distinct functions when used in an **owner** or a **non-owner** context of the virtual router instance.

Non-owner virtual router instances actually create a routable IP interface address that is operationally dependent on the virtual router instance mode (master or backup). The **backup** command in **owner** virtual router instances does not create a routable IP interface address; it simply defines the existing parental IP interface IP addresses that are advertised by the virtual router instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For **owner** virtual router instances, the **backup** command defines the IP addresses that are advertised within VRRP advertisement messages. This communicates the IP addresses that the master is representing to backup virtual routers receiving the messages. Advertising a correct list is important. The specified *ipv6-addr* must be equal to one of the existing parental IP interface IP addresses (link-local or global) or the **backup** command will fail.

For non-owner virtual router instances, the **backup** command actually creates an IP interface IP address used for routing IP packets and communicating with the system when the access commands are defined (**ntp-reply, ping-reply**, **telnet-reply**, and **ssh-reply**). The specified *ipv6-addr* must be an IP address that is within one of the parental IP interface local subnets created with the **link-local-address or address** commands. If a local subnet does not exist that includes the specified *ipv6-addr* or if *ipv6-addr* is the same IP address as the parental IP interface IP address, the **backup** command will fail.

The new interface IP address created with the **backup** command assumes the mask and parameters of the corresponding parent IP interface IP address. The *ipv6-addr* is only active when the virtual router instance is operating in the master state. For IPv6 VRRP, the parental interface's IP address that is in the same subnet as the backup address must be manually-configured, non EUI-64 and configured to be in the preferred state.

When not operating as master, the virtual router instance acts as if it is operationally down. It will not respond to Neighbor Solicitation (NS) requests to *ipv6-addr*, nor will it route packets received with its *vrid* derived source MAC address. A non-master virtual router instance always silently discards packets destined to *ipv6-addr*.

IPv6 allows the configuration of a link-local IPv6 address and multiple global IPv6 addresses on an interface. For each of these configured subnets, a virtual router IP address can be configured. Each IPv6 enabled device on a particular IPv6 subnet dynamically learns the connected IPv6 routers and correlated subnets in addition to the IPv6 default gateway using IPv6 neighbor discovery protocol (RFC4861). This protocol behavior is revised from IPv4 where the default gateway is manually configured or derived from supporting protocols (for example, DHCP). During the IPv6 neighbor discovery process, VRRP enabled routers will use backup IPv6 addresses and correlated derived virtual MAC addresses. Multiple virtual router instances can define a virtual router IP address from the same local subnet as long as each is a different IP address.

Executing **backup** multiple times with the same *ipv6-addr* results in no operation performed and no error generated. At least one successful **backup** *ipv6-addr* command must be executed before the virtual router instance can enter the operational state.

When operating as (non-owner) master, the default functionality associated with *ipv6-addr* results in the IPv6 Neighbor Advertisement response to IPv6 Neighbor Solicitation requests to *ip-addr*, routing of packets destined to the virtual router instance source MAC address, and silently discarding packets destined to *ipv6-addr*. An IPv6 virtual router instance can enter the operational state only if one of the configured backup addresses is a link-local address and the router advertisement of the interface is configured to use the virtual MAC address. Enabling the non-owner-access parameters selectively allows ping, Telnet, and traceroute connectivity to *ipv6-addr* when the virtual router instance is operating as master.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the specified virtual router IP address from the virtual router instance. For non-owner virtual router instances, this causes all routing and local access associated with the *ipv6-addr* to cease. For **owner** virtual router instances, the **no backup** command only removes *ipv6-addr* from the list of advertised IP addresses. If the last *ipv6-addr or the link-local address* is removed from the virtual router instance, the virtual router instance will enter the operationally down state

Default no backup — No virtual router IP address is assigned.

Special Cases **Assigning the Virtual Router ID Address —** Once the *vrid* is created on the parent IP interface, IP addresses need to be assigned to the virtual router instance. If the *vrid* was created with the keyword **owner**, the virtual router instance IP addresses must have one or more of the parent IP interface defined IP addresses. For non-owner virtual router instances, the virtual router IP addresses each must be within one of the parental IP interface IP address defined local subnets. For both **owner** and non-owner virtual router instances, the virtual router IP addresses must be explicitly defined using the **backup** *ipv6-addr* command.

The following rules apply when adding, changing, or removing parental and virtual router IP addresses:

Owner Virtual Router IP Address Parental Association — When an IP address is assigned to an **owner** virtual router instance, it must be associated with one of the parental IP interface-assigned IP addresses.

Table 32 **Example - Owner Virtual Router Instance**

Parent IP addresses	2001:db8:1::2/64 fe80::1:2/64	
Virtual router IP addresses	2001:db8:1::23	Invalid (not equal to parent IP address)
	2001:db8:1::2	Associated (same as parent IP address)
	2001:db8:2::23	Invalid (not equal to parent IP address)

Non-Owner Virtual Router IP Address Parental Association — When an IP address is assigned to a non-owner virtual router instance, it must be associated with one of the parental IP interface assigned IP addresses. The virtual router IP address must be a valid IP address within one of the parental IP interfaces local subnet. Local subnets are created by the link-local or global IP addresses in conjunction with the IP addresses mask. Virtual router IP addresses for non-owner virtual router instances that are equal to a parental IP interface IP address are also invalid.

The same virtual router IP address may not be assigned to two separate virtual router instances. If the virtual router IP address already exists on another virtual router instance, the virtual router IP address assignment will fail.

One exception to this rule is for the IPv6 link-local address that is configured as a backup address. The same link-local address can be configured in all virtual routers that use the same vrid.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 33 **Example - Non-Owner Virtual Router Instance**

Parent IP addresses:	2001:db8:1::2/64 fe80::1:2/64	
Virtual router IPv6 addresses:	2001:db8:1::23	Associated with 2001:db8:1::2 (in subnet)
	2001:db8:1::2	Invalid (same as parent IP address)
	2001:db8:2::2	Invalid (outside of all Parent IP subnets)
	fe80::1:23	Associated with fe80::1:2 (in subnet)

Virtual Router IP Address Assignment without Parent IP Address — When assigning an IP address to a virtual router instance, an associated IP address (see **config>router>if>vrrp backup** and **config>router>if>ipv6>vrrp backup** [this command]) on the parental IP interface must already exist. If an associated IP address on the parental IP interface is not configured, the virtual router IP address assignment fails.

Virtual Router IPv6 Address Assignment — An IPv6 backup address requires that the parental IP address that is in the same subnet as the backup address must be manually configured, non-EUI-64 and configured to be in the preferred state. A configured IPv6 address is manually set in preferred state by using the **dad-disable** command. A configured IPv6 address on an interface with DAD disabled, immediately enters preferred state, without checking for uniqueness on the interface.

Parameters *ipv6-address* — The virtual router IP address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). The IP virtual router IP address must be in the same subnet of the parental IP interface IP address or equal to one of the parent interface addresses for **owner** virtual router instances.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x::d.d.d.d x: [0..FFFF]H d: [0..255]D

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.4 backup-class-type

backup-class-type

Syntax **backup-class-type ct-number**
no backup-class-type

Context **[Tree]** (config>router>mpls>lsp>primary backup-class-type)

Full Context configure router mpls lsp primary backup-class-type

Description This command enables the use of the Diff-Serv backup Class-Type (CT), instead of the Diff-Serv main CT, to signal the LSP primary path when it fails and goes into retry. The Diff-Serv main CT is configured at the LSP level or at the primary path level using the following commands:

config>router>mpls>lsp>class-type *ct-number*

config>router>mpls>lsp>primary>class-type *ct-numbe*r

When an LSP primary path retries due a failure, for example, it fails after being in the UP state, or undergoes any type of Make-Before-Break (MBB), MPLS will retry a new path for the LSP using the main CT. If the first attempt failed, the head-end node performs subsequent retries using the backup CT. This procedure must be followed regardless if the currently used CT by this path is the main or backup CT. This applies to both CSPF and non-CSPF LSPs.

The triggers for using the backup CT after the first retry attempt are:

1. A local interface failure or a control plane failure (hello timeout and so on).
2. Receipt of a PathErr message with a notification of a FRR protection becoming active downstream and/or Receipt of a Resv message with a ‘Local-Protection-In-Use’ flag set. This invokes the FRR Global Revertive MBB.
3. Receipt of a PathErr message with error code=25 (“Notify”) and sub-code=7 (“Local link maintenance required”) or a sub-code=8 (“Local node maintenance required”). This invokes the TE Graceful Shutdown MBB.
4. Receipt of a Resv refresh message with the ‘Preemption pending’ flag set or a PathErr message with error code=34 (“Reroute”) and a value=1 (“Reroute request soft preemption”). This invokes the soft preemption MBB.
5. Receipt of a ResvTear message.
6. A configuration change MBB.
7. The user executing the **clear**>**router**>**mpls**>**lsp** command.

When an unmapped LSP primary path goes into retry, it uses the main CT until the number of retries reaches the value of the new **main-ct-retry-limit** parameter. If the path did not come up, it must start using the backup CT at that point in time. By default, this parameter is set to infinite value. The new main-ct-retry-limit parameter has no effect on an LSP primary path which retries due to a failure event.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An unmapped LSP primary path is a path which has never received a Resv in response to the first Path message sent. This can occur when performing a 'shut/no-shut' on the LSP or LSP primary path or when the node reboots. An unmapped LSP primary path goes into retry if the retry timer expired or the head-end node received a PathErr message before the retry timer expired.

When the re-signal timer expires, CSPF will try to find a path with the main CT. The head-end node must re-signal the LSP even if the new path found by CSPF is identical to the existing one since the idea is to restore the main CT for the primary path. A path with main CT is not found, the LSP remains on its current primary path using the backup CT.

When the user performs a manual re-signal of the primary path, CSPF will try to find a path with the main CT. The head-end node must re-signal the LSP as in current implementation.

The **no** form of this command disables the use of the Diff-Serv backup CT.

Default no backup-class-type

Parameters *ct-number* — Specifies the Diff-Serv Class Type number. One or more system forwarding classes can be mapped to a CT.

Values 0 to 7, integer

Platforms All

6.5 backup-next-hop

backup-next-hop

Syntax [**no**] **backup-next-hop**

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy>nh-grp backup-next-hop)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group backup-next-hop

Description Commands in this context configure the backup next hop of an NHG entry in a forwarding policy.

The **no** form of this command removes the backup next hop context from an NHG entry in a forwarding policy.

Platforms All

backup-next-hop

Syntax **backup-next-hop**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>static-route-entry>next-hop backup-next-hop)
[Tree] (config>service>vprn>static-route-entry>next-hop backup-next-hop)

Full Context configure router static-route-entry next-hop backup-next-hop
configure service vprn static-route-entry next-hop backup-next-hop

Description Commands in this context configure static route entry fast failover.

Platforms All

6.6 backup-node-sid

backup-node-sid

Syntax **backup-node-sid** *ip-prefix/prefix-length* **index** *index*
backup-node-sid *ip-prefix/prefix-length* **label** *label*
no backup-node-sid

Context [Tree] (config>router>ospf>segm-rtng backup-node-sid)

Full Context configure router ospf segment-routing backup-node-sid

Description This command enables LFA Protection using segment routing backup node SID.

The objective of this feature is to reduce the label stack pushed in a LFA tunnel next hop of inter-area and inter-domain prefixes. This is applicable in MPLS deployments across multiple IGP areas or domains such in seamless MPLS design.

The user enables the feature by configuring a backup node SID at an ABR/ASBR that is acting as a backup to the primary exit ABR/ASBR of inter-area or inter-as routes learned as BGP labeled routes. The user can enter either a label or an index for the backup node SID.

When a node in a IGP domain resolves a BGP label route for an inter-area or inter-domain prefix via the primary ABR exit router, it will use the backup node SID of this router, which is advertised by the backup ABR/ABR, as the LFA backup instead of the SID to the remote LFA PQ node to save on the pushed label stack.

This feature only allows the configuration of a single backup node SID per IGP instance and per ABR/ASBR. In other words, only a pair of ABR/ASBR nodes can back up each other in an IGP domain. Each time the user invokes the above command within the same IGP instance, it will override any previous configuration of the backup node SID. The same ABR/ASBR can, however, participate in multiple IGP instances and provide backup support within each instance.

Default no backup-node-sid

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix/prefix-length* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ip-prefix/mask:

- ip-prefix a.b.c.d (host bits must be 0)

ipv6-prefix:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

prefix-length: 0 to 128

index — Specifies the index for this backup node SID.

Values 0 to 4294967295

label — Specifies the SID value for this backup node SID.

Values 1 to 4294967295

Platforms All

6.7 backup-path

backup-path

Syntax [**no**] **backup-path** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**]

Context **[Tree]** (config>service>vprn>bgp backup-path)

Full Context configure service vprn bgp backup-path

Description This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP-learned prefixes belonging to the base router or a particular VPRN. Multiple paths must be received for a prefix to take advantage of this feature. When a prefix has a backup path and its primary paths fail, the affected traffic is rapidly diverted to the backup path without waiting for control plane reconvergence to occur. When many prefixes share the same primary paths, and in some cases also the same backup path, the time to failover traffic to the backup path is independent of the number of prefixes.

By default, IPv4 and IPv6 prefixes do not have a backup path installed in the IOM.

Default no backup-path

Parameters **ipv4** — Keyword that enables the use of a backup path for BGP-learned unlabeled IPv4 prefixes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6 — Keyword that enables the use of a backup path for BGP-learned unlabeled IPv6 prefixes.

label-ipv4 — Keyword that enables the use of a backup path for BGP-learned labeled-IPv4 prefixes.

label-ipv6 — Keyword that enables support for labeled-unicast IPv6 routes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

backup-path

Syntax [**no**] **backup-path** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**]

Context **[Tree]** (config>router>bgp backup-path)

Full Context configure router bgp backup-path

Description This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP-learned prefixes belonging to the base router. Multiple paths must be received for a prefix to take advantage of this feature. When a prefix has a backup path and its primary paths fail, the affected traffic is rapidly diverted to the backup path without waiting for control plane reconvergence to occur. When many prefixes share the same primary paths, and in some cases also the same backup path, the time to failover traffic to the backup path is independent of the number of prefixes.

By default, IPv4 and IPv6 prefixes do not have a backup path installed in the IOM.

Default no backup-path

Parameters **ipv4** — Keyword that enables BGP fast reroute for unlabeled unicast IPv4 routes.

ipv6 — Keyword that enables BGP fast reroute for unlabeled unicast IPv6 routes.

label-ipv4 — Keyword that enables BGP fast reroute for labeled-unicast IPv4 routes.

label-ipv6 — Keyword that enables BGP fast reroute for labeled-unicast IPv6 routes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.8 backup-remote-ip

backup-remote-ip

Syntax **backup-remote-ip** *ip-address*
no backup-remote-ip

Context **[Tree]** (config>service>ies>if>sap>ip-tunnel backup-remote-ip)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>sap>ip-tunnel backup-remote-ip)

Full Context configure service ies interface sap ip-tunnel backup-remote-ip
configure service vprn interface sap ip-tunnel backup-remote-ip

Description This command configures the alternate destination IPv4 or IPv6 address to use for an IP tunnel. This destination address is used only if the primary destination configured with the **remote-ip** command is unreachable in the delivery service. The **source** address, **remote-ip** address and **backup-remote-ip** address of a tunnel must all belong to the same address family (IPv4 or IPv6). When the backup-remote-ip address contains an IPv6 address it must be a global unicast address.

The **no** form of this command deletes the backup-destination address from the tunnel configuration.

Default no backup-remote-ip

Parameters *ip-address* — Specifies the destination IPv4 address or IPv6 address of the tunnel.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

6.9 backup-tag

backup-tag

Syntax **backup-tag** *tag-id*
no backup-tag

Context [Tree] (config>router>static-route-entry backup-tag)
[Tree] (config>service>vprn>static-route-entry backup-tag)

Full Context configure router static-route-entry backup-tag
configure service vprn static-route-entry backup-tag

Description This command associates a 4-byte backup route tag with the static route when the **backup-next-hop** command is activated. The tag value is an identifier that can be used in route policies to control distribution of the static route into other protocols when the backup-next-hop is activated for the associated static route.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The tag specified at this level of the static route causes the tag values that are configured under the **next-hop**, **black-hole**, and **indirect** contexts of the static route to be ignored.

The **no** form of this command removes the tag association.

Default no backup-tag

Parameters *tag-id* — Specifies an integer tag value.

Values 1 to 4294967295

Platforms All

6.10 bandwidth

bandwidth

Syntax **bandwidth** *bandwidth*
no bandwidth

Context **[Tree]** (config>lag>access bandwidth)
[Tree] (config>port>ethernet>access bandwidth)

Full Context configure lag access bandwidth
configure port ethernet access bandwidth

Description This command specifies the admin bandwidth assigned to SAPs, ports and LAGs which is used by SAP bandwidth CAC. The admin bandwidth on a port or LAG can be over or under booked using the **booking-factor** command.

Port or LAG: Increasing the port or LAG admin bandwidth will increase the available admin bandwidth on that port or LAG. Reducing the port or LAG admin bandwidth will reduce the available admin bandwidth on that port or LAG, however, if the reduction of available admin bandwidth would cause it to be insufficient to cover the sum of the current SAP admin bandwidth on the port or LAG then the command will fail.

The **no** version of the command reverts to the default value.

Default no bandwidth

Parameters *bandwidth* — Specifies the administrator bandwidth assigned to the SAP, port or LAG, in kb/s.

Values 1 to 6400000000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bandwidth

Syntax **bandwidth** *bandwidth*
no bandwidth

Context **[Tree]** (config>service>apipe>sap bandwidth)
[Tree] (config>service>epipe>sap bandwidth)
[Tree] (config>service>fpipe>sap bandwidth)
[Tree] (config>service>ipipe>sap bandwidth)

Full Context configure service apipe sap bandwidth
configure service epipe sap bandwidth
configure service fpipe sap bandwidth
configure service ipipe sap bandwidth

Description This command specifies the admin bandwidth assigned to SAPs, ports and LAGs which is used by SAP bandwidth CAC.

SAP: Attempts to increase the SAP admin bandwidth will fail if there is insufficient available admin bandwidth on its port or LAG, otherwise the port or LAG available admin bandwidth will be reduced by the incremental SAP admin bandwidth. Reducing the SAP admin bandwidth will increase the available admin bandwidth on its port or LAG. This is not supported for PW-SAPs, Ethernet tunnels or subscriber group interface SAPs.

The **no** version of the command reverts to the default value.

Default no bandwidth

Parameters *bandwidth* — Specifies the admin bandwidth assigned to the SAP, port or LAG, in kb/s.

Values 1 to 6400000000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap bandwidth

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap bandwidth

All

- configure service ipipe sap bandwidth
- configure service epipe sap bandwidth

bandwidth

Syntax **bandwidth** *bw-value*
bandwidth max
no bandwidth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>service>apipe>spoke-sdp bandwidth)
[Tree] (config>service>cpipe>spoke-sdp bandwidth)
[Tree] (config>service>epipe>spoke-sdp bandwidth)
[Tree] (config>service>fpipe>spoke-sdp bandwidth)
[Tree] (config>service>ipipe>spoke-sdp bandwidth)

Full Context
configure service apipe spoke-sdp bandwidth
configure service cpipe spoke-sdp bandwidth
configure service epipe spoke-sdp bandwidth
configure service fpipe spoke-sdp bandwidth
configure service ipipe spoke-sdp bandwidth

Description
This command specifies the bandwidth to be used for VLL bandwidth accounting by the VLL CAC feature.

The service manager keeps track of the available bandwidth for each SDP. The maximum value is the sum of the bandwidths of all constituent LSPs in the SDP. The SDP available bandwidth is adjusted by the user configured booking factor.

If an LSP consists of a primary and many secondary standby LSPs, then the bandwidth used in the maximum SDP available bandwidth is that of the active path. Any change to and LSP active path bandwidth will update the maximum SDP available bandwidth. Note however that a change to any constituent LSP bandwidth due to re-signaling of the primary LSP path or the activation of a secondary path which causes overbooking of the maximum SDP available bandwidth causes a warning and a trap to be issued but no further action is taken. The activation of a bypass or detour LSP in the path of the primary LSP does not change the maximum SDP available bandwidth.

When the user binds a VLL service to this SDP, an amount of bandwidth equal to bandwidth is subtracted from the SDP available bandwidth adjusted by the booking factor. When the user deletes this VLL service binding from this SDP, an amount of bandwidth equal to bandwidth is added back into the SDP available bandwidth.

If the total SDP available bandwidth when adding this VLL service is about to overbook, a warning is issued and the binding is rejected. This means that the spoke SDP bandwidth does not update the maximum SDP available bandwidth. In this case, the spoke SDP is put in operational down state and a status message of “pseudowire not forwarding” is sent to the remote SR-series PE node. A trap is also generated. The service manager will not put the spoke SDP into an operationally up state until the user executes a **shutdown** command and then a **no-shutdown** command of the spoke SDP and the bandwidth check succeeds. Therefore, the service manager will not automatically audit spoke SDPs subsequently to their creation to check if bandwidth is available.

If the VLL service contains an endpoint with multiple redundant spoke SDPs, each spoke SDP will have its bandwidth checked against the available bandwidth of the corresponding SDP.

If the VLL service performs a pseudowire switching (VC switching) function, each spoke SDP is separately checked for bandwidth against the corresponding SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This feature does not alter the way service packets are sprayed over multiple RSVP LSPs, which are part of the same SDP. That is, by default load balancing of service packets occurs over the SDP LSPs based on service-id, or based on a hash of the packet header if ingress SAP shared queuing is enabled. In both cases, the VLL bandwidth is not checked against the available bandwidth of the selected LSPs but on the total SDP available bandwidth. Therefore, if there is a single LSP per SDP, these two matches.

If class-forwarding is enabled on the SDP, VLL service packets are forwarded to the SDP LSP which the packet forwarding class maps to, or if this is down to the default LSP. However, the VLL bandwidth is not checked against the selected LSP available bandwidth but on the total SDP available bandwidth. If there is a single LSP per SDP, these two matches.

If a non-zero bandwidth is specified for a VLL service and attempts to bind the service to an LDP or a GRE SDP, a warning is issued that CAC failed but the VLL is established. A trap is also generated.

The **no** form of this command reverts to the default value.

Parameters *bw-value* — The bandwidth to be used for VLL bandwidth accounting by the VLL CAC feature, in kilobits per second.

Values 0 to 100000000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp bandwidth
- configure service fpipe spoke-sdp bandwidth

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp bandwidth

All

- configure service ipipe spoke-sdp bandwidth
- configure service epipe spoke-sdp bandwidth

bandwidth

Syntax **bandwidth** *bandwidth*
no bandwidth

Context **[Tree]** (config>service>vpls>sap bandwidth)

Full Context configure service vpls sap bandwidth

Description This command specifies the admin bandwidth assigned to SAPs, ports and LAGs which is used by SAP bandwidth CAC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

SAP: Attempts to increase the SAP admin bandwidth will fail if there is insufficient available admin bandwidth on its port or LAG, otherwise the port or LAG available admin bandwidth will be reduced by the incremental SAP admin bandwidth. Reducing the SAP admin bandwidth will increase the available admin bandwidth on its port or LAG. This is not supported for PW-SAPs, Ethernet tunnels or subscriber group interface SAPs.

The **no** version of the command reverts to the default value.

Default no bandwidth

Parameters *bandwidth* — Specifies the admin bandwidth assigned to the SAP, port or LAG, in kb/s.

Values 1 to 6400000000

Platforms All

bandwidth

Syntax **bandwidth** *bandwidth*
no bandwidth

Context **[Tree]** (config>service>ies>if>sap bandwidth)

Full Context configure service ies interface sap bandwidth

Description This command specifies the admin bandwidth assigned to SAPs, ports and LAGs which is used by SAP bandwidth CAC.

SAP: Attempts to increase the SAP admin bandwidth will fail if there is insufficient available admin bandwidth on its port or LAG, otherwise the port or LAG available admin bandwidth will be reduced by the incremental SAP admin bandwidth. Reducing the SAP admin bandwidth will increase the available admin bandwidth on its port or LAG. This is not supported for PW-SAPs, Ethernet tunnels or subscriber group interface SAPs.

The **no** version of the command reverts to the default value.

Default no bandwidth

Parameters *bandwidth* — Specifies the admin bandwidth assigned to the SAP, port or LAG, in kb/s.

Values 1 to 6400000000

Platforms All

bandwidth

Syntax **bandwidth** *bandwidth*
no bandwidth

Context **[Tree]** (config>service>vprn>if>sap bandwidth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap bandwidth

Description This command specifies the admin bandwidth assigned to SAPs, ports and LAGs which is used by SAP bandwidth CAC.

SAP: Attempts to increase the SAP admin bandwidth will fail if there is insufficient available admin bandwidth on its port or LAG, otherwise the port or LAG available admin bandwidth will be reduced by the incremental SAP admin bandwidth. Reducing the SAP admin bandwidth will increase the available admin bandwidth on its port or LAG. This is not supported for PW-SAPs, Ethernet tunnels or subscriber group interface SAPs.

The **no** version of the command reverts to the default value.

Default no bandwidth

Parameters *bandwidth* — Specifies the admin bandwidth assigned to the SAP, port or LAG, in kb/s.

Values 1 to 6400000000

Platforms All

bandwidth

Syntax **bandwidth signal-type** *signal-type*
no bandwidth

Context **[Tree]** (config>router>gmpls>lsp>working-path bandwidth)
[Tree] (config>router>gmpls>lsp>protect-path bandwidth)

Full Context configure router gmpls lsp protect-path bandwidth
configure router gmpls lsp working-path bandwidth

Description This command specifies the bandwidth to be signaled for the path of the GMPLS LSP. Bandwidth is specified in terms of the RFC 3471 signal type name.

If an empty path is configured or the first hop TE Link is not configured, the system will automatically select a TE Link to use for a GMPLS LSP path based on the lowest available TE Link ID with a matching bandwidth (if a bandwidth is configured for the GMPLS LSP). During a data-bearer link allocation request, an RSVP-requested GMPLS LSP BW can be either a non-zero value as per RFC 3471 signal-type, or it can be zero). There are the following cases:

- Case 1 — The requested BW is non-zero as per RFC 3471 Signal-type config:

  a) When a TE (or TE/DB) Link is configured in the related hop, LMP checks whether the related port BW is the same (exact match) as the requested BW, and allocates the port (provided any other checks are OK).

  b) When the related Hop is empty: LMP finds a db-link port to the peer node matching the requested BW, and allocates it.
- Case 2 — Requested BW is zero:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

a) When a TE (or TE/DB) Link is configured in the related hop, LMP allocates the port (provided the other checks are OK), and provides the port BW to RSVP to use in signaling.

b) When the related Hop is empty, LMP finds the first available db-link to the peer (based on lower db-link Id), and allocates it and provides the port BW to RSVP to use in signaling.

The **no** form of the command updates the bandwidth to zero.

Default no bandwidth

Parameters *signal-type* — Specifies the RFC 3471 name of the signal type representing the requested bandwidth for the GMPLS LSP path.

Values {ds0 | ds1 | e1 | ds2 | e2 | ethernet | e3 | ds3 | sts-1 | fast-ethernet | e4 | fc-0-133m | oc-3/stm1 | fc-0-266m | fc-0-531m | oc-12/stm-4 | gige | fc-0-1062m | oc-48/stm-16 | oc-192/stm-64 | 10gige-ieee | oc-768/stm-256 | 100gige-ieee}

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bandwidth

Syntax **bandwidth** *bandwidth-in-mbps*
no bandwidth

Context **[Tree]** (config>router>mpls>lsp>primary-p2mp-instance bandwidth)
[Tree] (config>router>mpls>lsp-template bandwidth)

Full Context configure router mpls lsp primary-p2mp-instance bandwidth
configure router mpls lsp-template bandwidth

Description This command specifies the amount of bandwidth to be reserved for the P2MP instance.

The **config**>**router**>**mpls**>**lsp**>**primary-p2mp-instance**>**bandwidth** command is not supported on the 7450 ESS.

Parameters *bandwidth-in-mbps* — Specifies the bandwidth, in Mb/s.

Values 0 to 6400000

Platforms All

bandwidth

Syntax **bandwidth** *bandwidth-in-mbps*
no bandwidth

Context **[Tree]** (config>router>mpls>lsp>primary bandwidth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>mpls>lsp>secondary bandwidth)

Full Context configure router mpls lsp primary bandwidth
configure router mpls lsp secondary bandwidth

Description This command specifies the amount of bandwidth to be reserved for the LSP path.

The **no** form of this command resets bandwidth parameters (no bandwidth is reserved).

Default no bandwidth (bandwidth setting in the global LSP configuration)

Parameters *bandwidth-in-mbps* — Specifies the amount of bandwidth reserved for the LSP path in Mb/s.

Values 0 to 6400000

Platforms All

bandwidth

Syntax **bandwidth**

Context **[Tree]** (config>isa>video-group>watermark bandwidth)

Full Context configure isa video-group watermark bandwidth

Description Commands in this context configure watermark parameters based on the bandwidth.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

bandwidth

Syntax **bandwidth** *bandwidth-in-kbps*
no bandwidth

Context **[Tree]** (config>router>mcac>policy>bundle bandwidth)

Full Context configure router mcac policy bundle bandwidth

Description This command configures the MCAC policy bundle maximum bandwidth.

Parameters *bandwidth-in-kbps* — Specifies the MCAC policy bandwidth.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bandwidth

Syntax **bandwidth** *gbps*
no bandwidth

Context **[Tree]** (config>card>mda>xcon>mac>lpbk bandwidth)
[Tree] (config>card>xiom>mda>xcon>mac>lpbk bandwidth)

Full Context configure card mda xconnect mac loopback bandwidth
configure card xiom mda xconnect mac loopback bandwidth

Description This command defines the bandwidth for a maximum Layer 2 rate for the MAC loopback. This is equivalent to a faceplate port rate with the difference that the bandwidth of a faceplate port is a Layer 1 rate, which on Ethernet- based ports includes 20B per frame (preamble and inter-packet gap).

The **no** form of this command reverts to the default value.

Default bandwidth 100

Parameters *gbps* — Specifes the bandwidth in Gb/s.

Values 10, 25, 40, 100, 400

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

- configure card mda xconnect mac loopback bandwidth

7750 SR-s

- configure card xiom mda xconnect mac loopback bandwidth

6.11 bandwidth-distribution

bandwidth-distribution

Syntax **bandwidth-distribution**

Context **[Tree]** (config>qos>adv-config-policy>child-control bandwidth-distribution)

Full Context configure qos adv-config-policy child-control bandwidth-distribution

Description This command modifies or controls the bandwidth distribution phase of the parent virtual scheduler.

This command edits the parameters that control the child given bandwidth for all policers and queues associated with the policy.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.12 bandwidth-policer

bandwidth-policer

Syntax **bandwidth-policer** *policer-name*
no bandwidth-policer

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action bandwidth-policer)

Full Context configure application-assurance group policy app-qos-policy entry action bandwidth-policer

Description This command assigns an existing bandwidth policer as an action on flows matching this AQP entry. The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worst case of all policer outcomes (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of this command removes bandwidth policer from actions on flows matching this AQP entry.

Default no bandwidth-policer

Parameters *policer-name* — Specifies the name of the existing flow setup rate policer for this application assurance profile. The *policer-name* is configured in the **config>app-assure>group>policer** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.13 bandwidth-policy

bandwidth-policy

Syntax **bandwidth-policy** *policy-name* [**create**]
no bandwidth-policy *policy-name*

Context **[Tree]** (config>mcast-mgmt bandwidth-policy)

Full Context configure mcast-management bandwidth-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a multicast bandwidth policy. Bandwidth policies are used to manage the ingress multicast path bandwidth. Each forwarding plane supports multicast forwarding paths into the switch fabric. By default, two paths are available; the multicast high priority path and the multicast low priority path. Multicast packets are forwarded on either path based on the expedited or non-expedited (best-effort) nature of the queue the packets are scheduled from. The ingress forwarding plane uses the classification rules to determine the forwarding class of each multicast packet and uses the forwarding class to queue mapping to decide which ingress multipoint queue forwards the packet.

When multicast path management is enabled, the ingress forwarding plane allows IP multicast snooped or routed packets to be placed on to the two multicast paths independently of the ingress classification rules. The high priority multicast path is treated as the primary path and the low priority multicast path is treated as the secondary path. The ingress bandwidth manager evaluates each multicast FIB (M-FIB) record to determine which path is best based on ingress bandwidth, number of switch fabric destinations and the fill level of each path. Explicit path association is also supported.

Dynamic Bandwidth Activity Monitoring

When ingress multicast path management is enabled on an MDA, the system monitors the in-use bandwidth associated with each Layer 2 and Layer 3 ingress multicast record. When records are first populated by static, snooping or routing protocols, they are first assumed to be inactive. An inactive record is not considered to be currently consuming ingress multicast path bandwidth.

Within the multicast-info-policy, the bandwidth activity of the new record was configured to be either managed based on an administrative bandwidth, or based on the dynamic bandwidth rate table. The bandwidth-policy associated with ingress MDA contains the configuration parameters for creating the dynamic bandwidth rate table. The purpose of the table is to allow for the system to monitor the bandwidth activity associated with a multicast record and compare the current rate against several rate thresholds. Rate thresholds are used to allow a multicast streams rate to fluctuate between a given range while keeping the managed rate at a certain level. Multiple dynamic managed rates are supported in the table to allow monitoring of different types of multicast traffic. Each rate threshold is associated with a rising and falling threshold that defines when the specified rate should be used and when the next lower rate should be used.

Once a record’s monitored current rate rises to the first dynamic rising threshold, the record is active and the system then manages the bandwidth the record represents based on the parameters associated with the record in the records multicast-info-policy and the configured path information in the MDAs associated bandwidth-policy.

Ingress Multicast Path Parameters

The bandwidth-policy also contains the configuration parameters for each of the managed ingress multicast paths. The queue default parameters can be overridden for each primary and secondary path. In addition, the number of secondary paths (and by implication the number of primary paths) can be overridden.

Default Bandwidth Policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A bandwidth policy with the name ‘default’ always exists and is used as the default bandwidth policy when ingress multicast path management is enabled without an explicit bandwidth policy defined on an FP. The default policy cannot be deleted or edited.

The **no** form of this command removes the specified bandwidth policy from the system. The bandwidth policy associations must be removed from MDA configurations before it can be removed.

Default bandwidth-policy “default”

Parameters *policy-name* — Specifies the name of the bandwidth policy, up to 32 characters. Each bandwidth policy must be uniquely named within the system. 32 policies can be configured per system.

create — This keyword is required if creating a new bandwidth policy when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the bandwidth policy name already exists.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

bandwidth-policy

Syntax **bandwidth-policy** *policy-name*
no bandwidth-policy

Context **[Tree]** (config>card>fp>ingress>mcast-path-management bandwidth-policy)

Full Context configure card fp ingress mcast-path-management bandwidth-policy

Description This command explicitly associates a bandwidth policy to a forwarding plane. The bandwidth policy defines the dynamic rate table and the multicast paths bandwidth and queuing parameters.

If a bandwidth policy is not explicitly associated with a forwarding plane, the default bandwidth policy is used when ingress multicast path management is enabled.

The **no** form of this command removes an explicit bandwidth policy from a forwarding plane or MDA and restores the default bandwidth policy.

Parameters *policy-name* — The policy-name parameter is required and defines the bandwidth policy that should be associated with the MDA or forwarding plane for ingress multicast path management. If the policy name does not exist, the bandwidth-policy command will fail. The name can be up to 32 characters long.

Values Any existing bandwidth policy name.

Default default

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.14 base-op-authorization

base-op-authorization

Syntax **base-op-authorization**

Context **[Tree]** (config>system>security>profile>netconf base-op-authorization)

Full Context configure system security profile netconf base-op-authorization

Description Commands in this context configure the permission to use NETCONF operations at the base operation level for the specified profile.The NETCONF operations are authorized by default in the built-in system-generated administrative profile.

Platforms All

6.15 base-r13-modules

base-r13-modules

Syntax [**no**] **base-r13-modules**

Context **[Tree]** (config>system>management-interface>yang-modules base-r13-modules)

Full Context configure system management-interface yang-modules base-r13-modules

Description This command enables or disables support of the Base-R13 YANG modules in the SR OS NETCONF server. If the Base-R13 modules are disabled, then the NETCONF requests, which reference the Base-R13 modules, return an error, and when a NETCONF client establishes a new session, the Base-R13 modules are not advertised in the SR OS *hello*. When **management-interface configuration-mode** is set to **model-driven**, attempts to modify the configuration using the Base-13 configuration modules or namespace via NETCONF results in errors, even if **base-r13-modules** is enabled.

The **no** form of this command disables support of the Base-R13 YANG modules in the SR OS NETCONF server.

Default no base-r13-modules

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.16 base-routing-instance

base-routing-instance

Syntax **base-routing-instance**

Context **[Tree]** (config>router>segment-routing>srv6 base-routing-instance)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance

Description Commands in this context configure the function value for End SID, End.X SID, and service SID of an IPv4 or an IPv6 prefix in the global routing instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

6.17 base-user-name

base-user-name

Syntax **base-user-name** *user-name*
no base-user-name

Context **[Tree]** (config>aaa>route-downloader base-user-name)

Full Context configure aaa route-downloader base-user-name

Description This command sets the prefix for the user name that shall be used as access requests. The actual name used is a concatenation of this string, the “-” (dash) character and a monotonically increasing integer.

The **no** form of this command removes the *user-name* from the configuration.

Default The system’s configured name (system name).

Parameters *user-name* — Specifies the prefix of the username that is used in the RADIUS access requests. The username used in the RADIUS access requests is a concatenation of this string, the dash character and an increasing integer.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.18 bd

bd

Syntax **bd** *identifier*

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query bd)

Full Context configure subscriber-mgmt wlan-gw ue-query bd

Description This command enables matching on UEs that are part of the specified BD.

The **no** form of this command disables matching on the BD.

Default no bd

Parameters *identifier* — Specifies the BD identifier.

Values 0 to 4294967294

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.19 bd-mac-prefix

bd-mac-prefix

Syntax **bd-mac-prefix** *mac-prefix*
no bd-mac-prefix

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext bd-mac-prefix)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext bd-mac-prefix)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext bd-mac-prefix
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext bd-mac-prefix

Description This command specifies the prefix of the HLE BD MAC address.

The **no** form of this command removes the MAC prefix from the configuration.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.20 bearer-fteid

bearer-fteid

Syntax [**no**] **bearer-fteid**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute bearer-fteid)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute bearer-fteid

Description This command, in the case of ESM over GTP access includes the Alc-Bearer-Fteid VSA in accounting. This VSA contains the fully qualified TEID of the current GTP-U tunnel, including the bearer ID, endpoint IP addresses and TEIDs for both local and remote endpoints.

The **no** version of this command disables inclusion of the Alc-Bearer-Fteid VSA.

Default no bearer-fteid

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.21 begin

begin

Syntax **begin**

Context **[Tree]** (config>app-assure>group>policy begin)

Full Context configure application-assurance group policy begin

Description This command begins a policy editing session.

The editing session continues until one of the following conditions takes place:

- Abort or commit is issued.
- Control complex resets.

The editing session is not interrupted by:

- HA activity switch.
- CLI session termination (for example, as result of closing a Telnet session).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

begin

Syntax **begin**

Context **[Tree]** (config>router>bfd begin)

Full Context configure router bfd begin

Description This command switches to edit mode for a BFD template. Changes are not activated until the **commit** command is issued for the BFD template changes.

Platforms All

begin

Syntax **begin**

Context **[Tree]** (config>router>route-next-hop-policy begin)

Full Context configure router route-next-hop-policy begin

Description This command switches to edit mode for route next-hop templates. Changes are not activated until the **commit** command is issued for the route next-hop templates changes.

Default begin

Platforms All

begin

Syntax **begin**

Context **[Tree]** (config>system>sync-if-timing begin)

Full Context configure system sync-if-timing begin

Description This command is required in order to enter the mode to create or edit the system synchronous interface timing configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

begin

Syntax **begin** {**exclusive**}

Context **[Tree]** (config>router>policy-options begin)

Full Context configure router policy-options begin

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is required in order to enter the mode to create or edit route policies.

Parameters **exclusive** — Specifies an exclusive lock on the policy configuration. Other CLI and SNMP users will be unable to edit the policy configuration until the lock is removed (via commit, abort, a timeout occurring, or a forced override).

Platforms All

6.22 begin-time

begin-time

Syntax **begin-time** *date hours-minutes* [**UTC**]
begin-time {**now** | **forever**}
no begin-time

Context **[Tree]** (config>system>security>keychain>direction>bi>entry begin-time)
[Tree] (config>system>security>keychain>direction>uni>receive>entry begin-time)
[Tree] (config>system>security>keychain>direction>uni>send>entry begin-time)

Full Context configure system security keychain direction bi entry begin-time
configure system security keychain direction uni receive entry begin-time
configure system security keychain direction uni send entry begin-time

Description This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and/or authenticate the protocol stream.

If no date and time is set, the begin-time is represented by a date and time string with all NULLs and the key is not valid by default.

Default begin-time forever

Parameters *date hours-minutes* — Specifies the date and time for the key to become active.

Values date: YYYY/MM/DD hours-minutes: hh:mm[:ss]

now — Specifies the key should become active immediately.

forever — Specifies that the key is always inactive.

UTC — Indicates that time is given with reference to Coordinated Universal Time in the input.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.23 ber-sf-link-down

ber-sf-link-down

Syntax [**no**] **ber-sf-link-down**

Context **[Tree]** (config>port>tdm>ds1>channel-group>ppp ber-sf-link-down)
[Tree] (config>port>tdm>e1>channel-group>ppp ber-sf-link-down)

Full Context configure port tdm ds1 channel-group ppp ber-sf-link-down
configure port tdm e1 channel-group ppp ber-sf-link-down

Description This command enables the port down on BER-SF alarm. When enabled, the link will be placed out of service once ber-sf is detected.

The **no** form of this command reverts to normal operation where the link remains in-service when ber-sf is encountered.

Default no ber-sf-link-down

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

6.24 bert

bert

Syntax **bert** {**2e3** | **2e9** | **2e11** | **2e15** | **2e20** | **2e20q** | **2e23** | **ones** | **zeros** | **alternating**} **duration** *duration*
no bert

Context **[Tree]** (config>port>tdm>ds1 bert)
[Tree] (config>port>tdm>ds3 bert)
[Tree] (config>port>tdm>e1 bert)
[Tree] (config>port>tdm>e3 bert)

Full Context configure port tdm ds1 bert
configure port tdm ds3 bert
configure port tdm e1 bert
configure port tdm e3 bert

Description This command initiates or restarts a Bit Error Rate Test (BERT) on the associated DS-1/E-1 or DS-3/E-3 circuit.

The associated DS-1, E-1, DS-3, or E-3 must be in a shutdown (admin down) state to initiate this test.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command terminates the BERT test if it has not yet completed.

Notes:

- This command is not saved in the router configuration between boots.
- The 4-port OC-3/STM-1 and the 1-port OC-12/STM-4 ASAP MDA supports up to 28 concurrent BERT tests per MDA. The 4-port and 12-port DS-3/E-3 ASAP MDAs support a single BERT test per MDA. An attempt to configure more BERT tests can result in an error indicating an operation failure due to resource exhaustion.
- If the ASAP MDA BERT error insertion **rate** command is executed when tests are running, it will not take effect until test is restarted.

Default bert 2e3

Parameters *duration* — Sets the duration for the BERT test.

Values Up to 24 hours, in seconds or hh:mm:ss format

ones — Sends an all ones pattern.

zeros — Sends an all zeros pattern.

alternating — Sends an alternating ones and zeros pattern.

2e3 — Sends a pseudo-random 2^3 -1 pattern.

2e9 — Sends a pseudo-random 2^9 -1 pattern.

2e15 — Sends a pseudo-random 2^15 -1 pattern.

2e20 — Sends a pseudo-random 2^20 -1 pattern. Not available on channelized ASAP MDAs.

2e23 — Sends a pseudo-random 2^23 -1 pattern.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

6.25 best-path-selection

best-path-selection

Syntax **best-path-selection**

Context **[Tree]** (config>service>vprn>bgp best-path-selection)

Full Context configure service vprn bgp best-path-selection

Description This command enables path selection configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

best-path-selection

Syntax **best-path-selection**

Context **[Tree]** (config>router>bgp best-path-selection)

Full Context configure router bgp best-path-selection

Description Commands in this context configure path selection parameters.

Platforms All

6.26 bfd

bfd

Syntax **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier* [**echo-receive** *echo-interval*] [**type cpm-np**]
no bfd

Context **[Tree]** (config>service>ies>if bfd)
[Tree] (config>service>ies>if>ipv6 bfd)
[Tree] (config>service>vprn>if bfd)
[Tree] (config>service>vprn>if>ipv6 bfd)
[Tree] (config>service>vprn>nw-if bfd)

Full Context configure service ies interface bfd
configure service ies interface ipv6 bfd
configure service vprn interface bfd
configure service vprn interface ipv6 bfd
configure service vprn network-interface bfd

Description This command specifies the BFD parameters for the associated IP interface. If no parameters are defined the default value are used.

The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocols (OSPF, IS-IS, BGP or PIM) is notified of the fault.

The **no** form of this command removes BFD from the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: On the 7750 SR, the *transmit-interval,* **receive** *receive-interval, and* **echo-receive** *echo-interval* values can only be modified to a value less than 100 when:

1. The **type cpm-np option** is explicitly configured.
2. The service is shut down (**shutdown**)
3. The interval is specified 10 to 100000.
4. The service is re-enabled (**no shutdown**)

To remove the **type cpm-np** option, re-issue the **bfd** command without specifying the **type** parameter.

Parameters *transmit-interval* — Sets the transmit interval for the BFD session.

Values 100 to 100000
10 to 100000 (for the 7750 SR only; see the note above)

Default 100

receive *receive-interval* — Sets the receive interval for the BFD session.

Values 100 to 100000
10 to 100000 (for the 7750 SR only; see the note above)

Default 100

multiplier *multiplier* — Sets the multiplier for the BFD session.

Values 3 to 20

Default 3

echo-receive *echo-interval* — Sets the minimum echo receive interval, in milliseconds, for the BFD session.

Values 100 to 100000
10 to 100000 (for the 7750 SR only; see the Note above)

Default 100

type cpm-np — For the 7750 SR only, specifies that BFD sessions associated with this interface is created on the CPM network processor to allow for fast timers down to 10 ms granularity.

Platforms All

bfd

Syntax **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier* [**echo-receive** *echo-interval*] [**type cpm-np**]
no bfd

Context **[Tree]** (config>service>vprn>sub-if bfd)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if bfd)
[Tree] (config>service>vprn>sub-if>ipv6 bfd)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 bfd)

Full Context

configure service vprn subscriber-interface bfd
configure service vprn subscriber-interface group-interface bfd
configure service vprn subscriber-interface group-interface ipv6 bfd
configure service vprn subscriber-interface ipv6 bfd

Description

This command specifies the BFD attributes for the associated retail subscriber interface or group interface. If no parameters are defined the default value are used.

The **no** form of this command removes BFD from the interface.

To remove the **type cpm-np** option, re-issue the **bfd** command without specifying the **type** parameter.

Default

no bfd

Parameters

transmit-interval — Sets the transmit interval for the BFD session.

Values 10 to 100000

Default 100

Note: On the 7750 SR, the *transmit-interval* can only be modified to a value less than 100 when the **type cpm-np option** is explicitly configured.

receive-interval — Sets the receive interval for the BFD session.

Values 10 to 100000

Default 100

Note: On the 7750 SR, the *receive-interval* can only be modified to a value less than 100 when the **type cpm-np option** is explicitly configured.

multiplier — Sets the multiplier for the BFD session. A multiplier of less than 3 should not be used in production environments. The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocol (BGP) is notified of the fault.

Values 1 to 20

Default 3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

echo-interval — Sets the minimum echo receive interval, in milliseconds, for the BFD session.

Values 100 to 100000

Default 0

type cpm-np — Sets the CPM network processor as the local termination point for the BFD session to allow for fast timers down to 10ms granularity.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

bfd

Syntax **bfd**

Context **[Tree]** (config>lag bfd)

Full Context configure lag bfd

Description This command creates the bfd context and enables BFD over the associated LAG links.

Platforms All

bfd

Syntax **bfd**

Context **[Tree]** (config>router>mpls>lsp bfd)
[Tree] (config>router>mpls>lsp>primary bfd)
[Tree] (config>router>mpls>lsp>secondary bfd)
[Tree] (config>router>mpls>lsp-template bfd)

Full Context configure router mpls lsp bfd
configure router mpls lsp primary bfd
configure router mpls lsp secondary bfd
configure router mpls lsp-template bfd

Description Commands in this context configure LSP BFD commands on RSVP LSPs or seamless BFD commands on SR-TE LSPs.

Platforms All

bfd

Syntax **bfd**

Context **[Tree]** (config bfd)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure bfd

Description This command specifies the context for the configuration of BFD parameters global to a specific router.

The **no** form of this command removes the context.

Platforms All

bfd

Syntax **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier*] [**echo-receive** *echo-interval*] [**type cpm-np**]
no bfd

Context **[Tree]** (config>router>if bfd)
[Tree] (config>router>if>ipv6 bfd)

Full Context configure router interface bfd
configure router interface ipv6 bfd

Description This command specifies the bidirectional forwarding detection (BFD) parameters for the associated IP interface. If no parameters are defined the default values are used.

The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocols (OSPF, IS-IS, BGP or PIM) is notified of the fault.

The **no** form of this command removes BFD from the router interface regardless of the IGP/RSVP.

Important notes: On the 7750 SR and 7950 XRS SR OS, the *transmit-interval* and **receive receive-interval** values can only be modified to a value less than 100 ms when:

1. The **type cpm-np option** is explicitly configured.
2. The service is shut down (**shutdown**)
3. The interval is specified 10 to 100000.
4. The service is re-enabled (**no shutdown**)

To remove the **type cpm-np** option, re-issue the **bfd** command without specifying the **type** parameter.

Default no bfd

Parameters *transmit-interval* — Sets the transmit interval, in milliseconds, for the BFD session.

Values 10 to 100000 (see Important Notes above) The minimum value is 300 msec for central BFD sessions in the 7950 XRS.

Default 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

receive-interval — Sets the receive interval, in milliseconds, for the BFD session.

Values 10 to 100000 (see Important Notes above)

Default 100

multiplier — Sets the multiplier for the BFD session. A multiplier of less than 3 should not be used in production environments.

Values 1 to 20

Default 3

echo-interval — Sets the minimum echo receive interval, in milliseconds, for the session.

Values 100 to 100000

Default 0

cpm-np — Selects the CPM network processor type as the local termination point for the BFD session for the 7750 SR and 7950 XRS. See Important Notes, above.

Platforms All

bfd

Syntax **bfd**

Context **[Tree]** (config>service>apipe>spoke-sdp bfd)
[Tree] (config>service>cpipe>spoke-sdp bfd)
[Tree] (config>service>epipe>spoke-sdp bfd)
[Tree] (config>service>fpipe>spoke-sdp bfd)
[Tree] (config>service>ies>if>spoke-sdp bfd)
[Tree] (config>service>ipipe>spoke-sdp bfd)
[Tree] (config>service>vpls>mesh-sdp bfd)
[Tree] (config>service>vpls>spoke-sdp bfd)
[Tree] (config>service>vprn>if>spoke-sdp bfd)

Full Context configure service apipe spoke-sdp bfd
configure service cpipe spoke-sdp bfd
configure service epipe spoke-sdp bfd
configure service fpipe spoke-sdp bfd
configure service ies interface spoke-sdp bfd
configure service ipipe spoke-sdp bfd
configure service vpls mesh-sdp bfd
configure service vpls spoke-sdp bfd
configure service vprn interface spoke-sdp bfd

Description This command creates a context for the configuration of VCCV BFD.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp bfd

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe spoke-sdp bfd

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp bfd

All

- configure service vpls spoke-sdp bfd
- configure service vpls mesh-sdp bfd
- configure service ies interface spoke-sdp bfd
- configure service epipe spoke-sdp bfd
- configure service ipipe spoke-sdp bfd
- configure service vprn interface spoke-sdp bfd

6.27 bfd-designate

bfd-designate

Syntax [**no**] **bfd-designate**

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel bfd-designate)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel bfd-designate)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel bfd-designate)
[Tree] (config>router>if>ipsec>ipsec-tunnel bfd-designate)

Full Context configure router interface ipsec ipsec-tunnel bfd-designate
configure service ies interface ipsec ipsec-tunnel bfd-designate
configure service vprn interface ipsec ipsec-tunnel bfd-designate
configure service vprn interface sap ipsec-tunnel bfd-designate

Description This command specifies whether this IPsec tunnel is the BFD designated tunnel.

Default no bfd-designate

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel bfd-designate

VSR

- configure router interface ipsec ipsec-tunnel bfd-designate
- configure service ies interface ipsec ipsec-tunnel bfd-designate
- configure service vprn interface ipsec ipsec-tunnel bfd-designate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.28 bfd-enable

bfd-enable

Syntax [**no**] **bfd-enable** *service-id* **interface** *interface-name* **dst-ip** *ip-address*
[**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address* **name** *service-name*
[**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address*

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp bfd-enable)
[Tree] (config>service>vprn>sub-if>grp-if>srrp bfd-enable)

Full Context configure service ies subscriber-interface group-interface srrp bfd-enable
configure service vprn subscriber-interface group-interface srrp bfd-enable

Description This commands assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP/SRRP instance. There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session. If the interface configured with BFD is using a LAG or a spoke-SDP, the BFD transmit and receive intervals need to be set to a minimum of 300 ms.

BFD control the state of the associated interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The specified interface may not be configured with BFD; when it is, the virtual router will then initiate the BFD session.

The **no** form of this command removes BFD from the configuration.

Parameters *service-id* — Specifies the service ID of the interface running BFD. If no *svc-id* is specified then it indicates that the interface is a network interface in the Base router instance.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **bfd-enable interface** *interface-name* **dst-ip** *ip-address* **name** *name* variant can be used in all configuration modes.

Values {*id* | *svc-name*}

id:	1 to 2147483647
svc-name:	Specifies an existing service name up to 64 characters (*svc-name* is an alias for input only. The *svc-name* gets replaced with an id automatically by SR OS in the configuration)

interface *interface-name* — Specifies the name of the interface running BFD, up to 32 characters.

dst-ip *ip-address* — Specifies the destination address for the BFD session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name *service-name* — Specifies a service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ep bfd-enable)
[Tree] (config>router>bgp bfd-enable)
[Tree] (config>router>bgp>group bfd-enable)
[Tree] (config>router>bgp>group>neighbor bfd-enable)

Full Context configure redundancy multi-chassis peer mc-endpoint bfd-enable
configure router bgp bfd-enable
configure router bgp group bfd-enable
configure router bgp group neighbor bfd-enable

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command disables BFD.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>service>apipe>spoke-sdp>bfd bfd-enable)
[Tree] (config>service>cpipe>spoke-sdp>bfd bfd-enable)
[Tree] (config>service>epipe>spoke-sdp>bfd bfd-enable)
[Tree] (config>service>fpipe>spoke-sdp>bfd bfd-enable)
[Tree] (config>service>ipipe>spoke-sdp>bfd bfd-enable)

Full Context configure service apipe spoke-sdp bfd bfd-enable
configure service cpipe spoke-sdp bfd bfd-enable
configure service epipe spoke-sdp bfd bfd-enable
configure service fpipe spoke-sdp bfd bfd-enable
configure service ipipe spoke-sdp bfd bfd-enable

Description This command enables VCCV BFD on the PW associated with the VLL, BGP VPWS, or VPLS service. The parameters for the BFD session are derived from the named BFD template, which must have been first configured using the **bfd-template** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables VCCV BFD on the spoke-SDP.

Default no bfd-enable

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp bfd bfd-enable
- configure service fpipe spoke-sdp bfd bfd-enable

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp bfd bfd-enable

All

- configure service epipe spoke-sdp bfd bfd-enable
- configure service ipipe spoke-sdp bfd bfd-enable

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>service>epipe>bgp>pw-template-binding bfd-enable)

Full Context configure service epipe bgp pw-template-binding bfd-enable

Description This command enables VCCV BFD on the PW associated with the VLL, BGP VPWS, or VPLS service. The parameters for the BFD session are derived from the named BFD template, which must have been first configured using the **bfd-template** command.

The **no** form of this command disables VCCV BFD.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>service>vpls>mesh-sdp>bfd bfd-enable)
[Tree] (config>service>vpls>spoke-sdp>bfd bfd-enable)

Full Context configure service vpls mesh-sdp bfd bfd-enable
configure service vpls spoke-sdp bfd bfd-enable

Description This command enables VCCV BFD on the PWs associated with the VPLS service's spoke or mesh SDPs. The parameters for the BFD session are derived from the named BFD template, which must have been first configured using the **bfd-template** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables VCCV BFD on the mesh-SDP or spoke-SDP.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>service>vpls>bgp>pw-template-binding bfd-enable)
[Tree] (config>service>vpls>bgp-ad>pw-template-binding bfd-enable)

Full Context configure service vpls bgp pw-template-binding bfd-enable
configure service vpls bgp-ad pw-template-binding bfd-enable

Description This command enables VCCV BFD on the PWs associated with the BGP AD VPLS service. The parameters for the BFD session are derived from the named BFD template, which must have been first configured using the **bfd-template** command.

The **no** form of this command disables VCCV BFD.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>service>ies>if>spoke-sdp>bfd bfd-enable)

Full Context configure service ies interface spoke-sdp bfd bfd-enable

Description This command enables VCCV BFD on the PW associated with the spoke-SDP terminated on the IES interface. The parameters for the BFD session are derived from the named BFD template, which must have been first configured using the **bfd-template** command.

The **no** form of this command disables VCCV BFD on the spoke-SDP.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable** [*service-id*] **interface** *interface-name* **dst-ip** *ip-address*
[**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address* **name** *name*

Context **[Tree]** (config>service>ies>if>vrrp bfd-enable)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>if>ipv6>vrrp bfd-enable)

Full Context configure service ies interface ipv6 vrrp bfd-enable
configure service ies interface vrrp bfd-enable

Description This commands assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP/SRRP instance. There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session.

BFD control the state of the associated interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The specified interface may not be configured with BFD; however, when it is, the virtual router will then initiate the BFD session.

The **no** form of this command removes BFD from the configuration.

Parameters *service-id* — Specifies the service ID of the interface running BFD.

Values service-id: 1 to 2147483648
No service ID indicates a network interface.

interface *interface-name* — Specifies the name of the interface running BFD.

dst-ip *ip-address* — Specifies the destination address to be used for the BFD session.

name *name* — Specifies the name, up to 64 characters.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context [Tree] (config>service>vprn>static-route-entry>next-hop bfd-enable)

Full Context configure service vprn static-route-entry next-hop bfd-enable

Description This command associates the static route state to a BFD session between the local system and the configured nexthop.

The remote end of the BFD session must also be configured to originate or accept the BFD session controlling the static route state.

The **no** form of this command removes the association of the static route state to that of the BFD session.

Default no bfd-enable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>service>vprn>if>spoke-sdp>bfd bfd-enable)

Full Context configure service vprn interface spoke-sdp bfd bfd-enable

Description This command enables VCCV BFD on the PW associated with the spoke-SDP terminated on the VPRN interface service. The parameters for the BFD session are derived from the named BFD template, which must have been first configured using the **bfd-template** command.

The **no** form of this command disables VCCV BFD on the spoke-SDP.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address*
[**no**] **bfd-enable** *service-id* **interface** *interface-name* **dst-ip** *ip-address*
[**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address* **name** *service-name*

Context **[Tree]** (config>service>vprn>if>vrrp bfd-enable)
[Tree] (config>service>vprn>if>ipv6>vrrp bfd-enable)

Full Context configure service vprn interface ipv6 vrrp bfd-enable
configure service vprn interface vrrp bfd-enable

Description This commands assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP/SRRP instance. There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session. If the interface used is configured with centralized BFD, the BFD transmit and receive intervals need to be set to at least 300 ms.

BFD control the state of the associated interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The specified interface may not be configured with BFD; when it is, the virtual router will then initiate the BFD session.

The **no** form of this command removes BFD from the configuration.

Parameters *svc-id* — Specifies the service ID of the interface running BFD. If no *svc-id* is specified then it indicates that the interface is a network interface in the Base router instance.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **bfd-enable interface** *interface-name* **dst-ip** *ip-address* **name** *name* variant can be used in all configuration modes.

Values {*id* | *svc-name*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

id:	1 to 2147483647
svc-name:	Specifies an existing service name up to 64 characters (*svc-name* is an alias for input only. The *svc-name* gets replaced with an id automatically by SR OS in the configuration)

interface *interface-name* — Specifies the name of the interface running BFD, up to 32 characters.

dst-ip *ip-address* — Specifies the destination address to be used for the BFD session.

name *name* — Specifies a service name, up to 64 characters.

Platforms All

bfd-enable

Syntax **bfd-enable** {**ipv4** | **ipv6**} [**include-bfd-tlv**]
no bfd-enable {**ipv4** | **ipv6**}

Context **[Tree]** (config>service>vprn>isis>if bfd-enable)

Full Context configure service vprn isis interface bfd-enable

Description This command enables the use of bi-directional forwarding (BFD) to control IPv4 or adjacencies. By enabling BFD on an IPv4 or IPv6 protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set by the BFD command under the IP interface. This command must be given separately to enable or disable BFD for IPv4 and IPv6.

The **no** form of this command removes BFD from the associated adjacency.

Default no bfd-enable ipv4

no bfd-enable ipv6

Parameters **ipv4** — Keyword to enable BFD to control IPv4 adjacencies.

ipv6 — Keyword to enable BFD to control IPv6 adjacencies.

include-bfd-tlv — Enables support for the IS-IS BFD TLV options in accordance with RFC 6213, which specifies that a BFD session must be established before an IS-IS adjacency can transition to the established state. This option must be enabled on all IS-IS neighbors on a shared interface.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax **bfd-enable** [**remain-down-on-failure**]
no bfd-enable

Context **[Tree]** (config>service>vprn>ospf>if bfd-enable)
[Tree] (config>service>vprn>ospf3>area>if bfd-enable)

Full Context configure service vprn ospf interface bfd-enable
configure service vprn ospf3 area interface bfd-enable

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set using the **bfd** command in the associated IP interface context.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default no bfd-enable

Parameters **remain-down-on-failure** — Forces adjacency down on BFD failure.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable** [**ipv4** | **ipv6**]

Context **[Tree]** (config>service>vprn>pim>if bfd-enable)

Full Context configure service vprn pim interface bfd-enable

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>bgp bfd-enable)
[Tree] (config>service>vprn>bgp>group bfd-enable)
[Tree] (config>service>vprn>bgp>group>neighbor bfd-enable)

Full Context configure service vprn bgp bfd-enable
configure service vprn bgp group bfd-enable
configure service vprn bgp group neighbor bfd-enable

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. The parameters used for the BFD are set with the BFD command under the IP interface.

The **no** form of this command disables bfd-enable on the VPRN service.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context [Tree] (config>service>vprn>rip bfd-enable)
[Tree] (config>service>vprn>rip>group bfd-enable)
[Tree] (config>service>vprn>rip>group>neighbor bfd-enable)
[Tree] (config>service>vprn>ripng bfd-enable)
[Tree] (config>service>vprn>ripng>group bfd-enable)
[Tree] (config>service>vprn>ripng>group>neighbor bfd-enable)

Full Context configure service vprn rip bfd-enable
configure service vprn rip group bfd-enable
configure service vprn rip group neighbor bfd-enable
configure service vprn ripng bfd-enable
configure service vprn ripng group bfd-enable
configure service vprn ripng group neighbor bfd-enable

Description This command enables bi-directional forwarding (BFD) to control the state of the associated protocol adjacency. By enabling BFD on a given protocol interface, the state of the RIP neighbor is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set using the **bfd** command under the IP interface configuration context.

The **no** form of this command removes BFD from the associated protocol adjacency.

Default no bfd-enable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>ldp>lsp-bfd bfd-enable)

Full Context configure router ldp lsp-bfd bfd-enable

Description This command enables BFD on LDP LSPs with FECs that match the prefix list specified using the **lsp-bfd** command. A named BFD template must be configured and applied prior to enabling BFD.

The **no** form of this command disables BFD.

Default no bfd-enable

Platforms All

bfd-enable

Syntax **bfd-enable** [**ipv4**][**ipv6**]
no bfd-enable

Context **[Tree]** (config>router>ldp>if-params>if bfd-enable)

Full Context configure router ldp interface-parameters interface bfd-enable

Description This command enables tracking of the Hello adjacency to an LDP peer using BFD.

The **ipv6** option for this command is not supported on the 7450 ESS.

When this command is enabled on an LDP interface, LDP registers with BFD and starts tracking the LSR-id of all peers it formed Hello adjacencies with over that LDP interface. The LDP hello mechanism is used to determine the remote address to be used for the BFD session. The parameters used for the BFD session, that is, transmit-interval, receive-interval, and multiplier are those configured under the IP interface in existing implementation: **config>router>if>bfd**.

The operation of BFD over an LDP interface tracks the next-hop of the IPv4 and IPv6 prefixes in addition to tracking the LDP peer address of the Hello adjacency over that link. This is required since LDP can resolve both IPv4 and IPv6 prefix FECs over a single IPv4 or IPv6 LDP session and as such the next-hop of a prefix will not necessarily match the LDP peer source address of the Hello adjacency.

The failure of either or both of the BFD session tracking the FEC next-hop and the one tracking the Hello adjacency will cause the LFA backup NHLFE for the FEC to be activated or the FEC to be re-resolved if there is no FRR backup.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When multiple links exist to the same LDP peer, a Hello adjacency is established over each link and a separate BFD session is enabled on each LDP interface. If a BFD session times out on a specific link, LDP will immediately associate the LDP session with one of the remaining Hello adjacencies and trigger the LDP FRR procedures. As soon as the last Hello adjacency goes down due to BFD timing out, the LDP session goes down and the LDP FRR procedures will be triggered.

The **no** form of this command disables BFD on the LDP interface.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>ldp>targ-session>peer bfd-enable)
[Tree] (config>router>ldp>targ-session>peer-template bfd-enable)

Full Context configure router ldp targeted-session peer bfd-enable
configure router ldp targeted-session peer-template bfd-enable

Description This command enables the bidirectional forwarding detection (BFD) session for the selected TLDP session. By enabling BFD for a selected targeted session, the state of that session is tied to the state of the underneath BFD session between the two nodes.

The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes the TLDP session operational state binding to the central BFD session one.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>mpls>lsp>bfd bfd-enable)
[Tree] (config>router>mpls>lsp>primary>bfd bfd-enable)
[Tree] (config>router>mpls>lsp>secondary>bfd bfd-enable)
[Tree] (config>router>mpls>lsp-template>bfd bfd-enable)

Full Context configure router mpls lsp bfd bfd-enable
configure router mpls lsp primary bfd bfd-enable
configure router mpls lsp secondary bfd bfd-enable
configure router mpls lsp-template bfd bfd-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables LSP BFD on the RSVP LSP or S-BFD for the SR-TE LSP. LSP BFD must also be configured under **config>router** to enable LSP BFD. The parameters for the BFD session are derived from the named BFD Template, which must have been configured prior to the **bfd-enable** command and associated with the service using the **bfd-template** command.

The **no** form of this command disables LSP BFD on the RSVP LSP or S-BFD on the SR-TE LSP.

Default no bfd-enable

Platforms All

bfd-enable

Syntax **bfd-enable** [**cc** | **cc_cv**]
no bfd-enable

Context **[Tree]** (config>router>mpls>lsp>working-tp-path>mep bfd-enable)
[Tree] (config>router>mpls>lsp>protect-tp-path>mep bfd-enable)

Full Context configure router mpls lsp protect-tp-path mep bfd-enable
configure router mpls lsp working-tp-path mep bfd-enable

Description The command associates the operational state of an MPLS-TP path with a BFD session whose control packets flow on the path. The BFD packets are encapsulated in a generic associated channel (G-ACh) on the path. The timer parameters of the BFD session are taken from the OAM template of the MEP.

A value of **cc** means that the BFD session is only used for continuity check of the MPLS-TP path. In this case, the CC timer parameters of the OAM template apply. A value of **cv** means that the BFD session is used for both continuity checking and connectivity verification, and the CV timers of the OAM template apply.

This form of the **bfd-enable** command is only applicable when it is configured under a MEP used on an MPLS-TP working or protection path.

Default no bfd-enable

Parameters **cc** — Indicates that BFD runs in CC only mode. This mode uses G-ACh channel type 0x07.

cc_cv — Indicates that BFD runs in combined CC and CV mode. This mode uses channel type 0x22 for MPLS-TP CC packets, and 0x23 for MPLS-TP CV packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>rsvp>interface bfd-enable)

Full Context configure router rsvp interface bfd-enable

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated RSVP interface. This causes RSVP to register the interface with the BFD session on that interface.

The user configures the BFD session parameters, such as, **transmit-interval**, **receive-interval**, and **multiplier**, under the IP interface in the **config>router> if>bfd** context.

Note: It is possible that the BFD session on the interface was started because of a prior registration with another protocol, for example, OSPF or IS-IS.

The registration of an RSVP interface with BFD is performed at the time of neighbor gets its first session. This means when this node sends or receives a new Path message over the interface. If however the session did not come up, due to not receiving a Resv for a new path message sent after the maximum number of re-tries, the LSP is shutdown and the node de-registers with BFD. In general, the registration of RSVP with BFD is removed as soon as the last RSVP session is cleared.

The registration of an RSVP interface with BFD is performed independent of whether RSVP hello is enabled on the interface or not. However, hello timeout will clear all sessions towards the neighbor and RSVP de-registers with BFD at clearing of the last session.

An RSVP session is associated with a neighbor based on the interface address the path message is sent to. If multiple interfaces exist to the same node, each interface is treated as a separate RSVP neighbor. The user will have to enable BFD on each interface and RSVP will register with the BFD session running with each of those neighbors independently

Similarly the disabling of BFD on the interface results in removing registration of the interface with BFD.

When a BFD session transitions to DOWN state, the following actions are triggered. For RSVP signaled LSPs, this triggers activation of FRR bypass/detour backup (PLR role), global revertive (head-end role), and switchover to secondary if any (head-end role) for affected LSPs with FRR enabled. It triggers switchover to secondary if any and scheduling of re-tries for signaling the primary path of the non-FRR affected LSPs (head-end role).

The **no** form of this command removes BFD from the associated RSVP protocol adjacency.

Default no bfd-enable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax **bfd-enable service-name** *service-name* **interface-name** *interface-name* **dst-ip** *ip-address*
no bfd-enable

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel bfd-enable)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel bfd-enable)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel bfd-enable)
[Tree] (config>router>if>ipsec>ipsec-tunnel bfd-enable)

Full Context configure router interface ipsec ipsec-tunnel bfd-enable
configure service ies interface ipsec ipsec-tunnel bfd-enable
configure service vprn interface ipsec ipsec-tunnel bfd-enable
configure service vprn interface sap ipsec-tunnel bfd-enable

Description This command assigns a BFD session to provide a heart-beat mechanism for a given IPsec tunnel. There can be only one BFD session assigned to any given IPsec tunnel, but there can be multiple IPsec tunnels using same BFD session. BFD controls the state of the associated tunnel. If the BFD session goes down, the system will also bring down the associated non-designated IPsec tunnel.

Parameters *service-name* — Specifies the service name, up to 64 characters, on which the BFD session resides.

interface-name — Specifies the name, up to 32 characters, of the interface used by the BFD session.

ip-address — Specifies the destination address to be used for the BFD session.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel bfd-enable

VSR

- configure router interface ipsec ipsec-tunnel bfd-enable
- configure service vprn interface ipsec ipsec-tunnel bfd-enable
- configure service ies interface ipsec ipsec-tunnel bfd-enable

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ipsec bfd-enable)

Full Context configure redundancy multi-chassis peer mc-ipsec bfd-enable

Description This command enables tracking a central BFD session, if the BFD session goes down, then system consider the peer is down and change the mc-ipsec status of configured tunnel-group accordingly.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The BFD session uses specified the loopback interface (in the specified service) address as the source address and uses specified dst-ip as the destination address. Other BFD parameters are configured with the **bfd** command on the specified interface.

Default no bfd-enable

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

bfd-enable

Syntax [**no**] **bfd-enable** [**ipv4** | **ipv6**]

Context **[Tree]** (config>router>pim>interface bfd-enable)

Full Context configure router pim interface bfd-enable

Description This command enables the use of IPv4 or IPv6 bidirectional forwarding detection (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default no bfd-enable

Parameters **ipv4** — Enables the use of IPv4 BFD.

ipv6 — Enables the use of IPv6 BFD.

Platforms All

bfd-enable

Syntax **bfd-enable** [**ipv4**] [**ipv6**]
no bfd-enable

Context **[Tree]** (config>router>p2mp-sr-tree bfd-enable)

Full Context configure router p2mp-sr-tree bfd-enable

Description This command enables BFD tracking at the P2MP SR tree level, which causes all next-hops of the replication segments that use a BFD-enabled Layer 3 interface to register with the BFD module.

The **no** form of this command disables BFD tracking of the P2MP SR tree.

Default no bfd-enable

Parameters **ipv4** — Enables the use of IPv4 BFD tracking.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6 — Enables the use of IPv6 BFD tracking.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>static-route-entry>next-hop bfd-enable)

Full Context configure router static-route-entry next-hop bfd-enable

Description This command associates the static route state to a BFD session between the local system and the configured nexthop.

The remote end of the BFD session must also be configured to originate or accept the BFD session controlling the static route state.

The **no** form of this command removes the association of the static route state to that of the BFD session.

Default no bfd-enable

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address*
[**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address* **name** *name*
[**no**] **bfd-enable** *svc-id* **interface** *interface-name* **dst-ip** *ip-address*

Context **[Tree]** (config>router>if>vrrp bfd-enable)
[Tree] (config>router>if>ipv6>vrrp bfd-enable)

Full Context configure router interface ipv6 vrrp bfd-enable
configure router interface vrrp bfd-enable

Description This commands assigns a bidirectional forwarding detect (BFD) session to a specific VRRP/SRRP instance. This BFD sessions provided a heartbeat mechanism that can be used to speed up the transition of the standby VRRP router to an active state. If the associated BFD session fails, the VRRP routers will immediately send a VRRP Advertisement message. In addition, the standby VRRP router(s) will transition to a Master state to speed convergence. The normal VRRP election process will then take place based on the Advertisement messages sent by all VRRP routers.

There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The parameters used for the BFD sessions are set by the BFD command under the IP interface.

The **no** form of this command removes BFD from the configuration.

Parameters *interface-name* — Specifies the name of the interface running BFD. The specified interface may not yet be configured with BFD. However, when it is, this virtual router will then initiate the BFD session.

ip-address — Specifies the destination address to be used for the BFD session.

svc-id — Specifies the service ID of the interface running BFD.

Values *service-id*:1 to 2147483647
svc-name: 64 characters maximum

Platforms All

bfd-enable

Syntax **bfd-enable interface** *interface-name* **dest-ip** *ipv4-address* [**service** *service-id*]
no bfd-enable

Context **[Tree]** (config>service>oper-group bfd-enable)

Full Context configure service oper-group bfd-enable

Description This command associates a BFD sessions with the named oper-group so that if the BFD session fails then the oper-group is changed to operationally down and all monitoring interfaces should also be brought operationally down.

Parameters *interface-name* — Specifies the source interface, up to 32 characters in length, for the BFD sessions to be monitored for the associated oper-group.

ipv4-address — Specifies the destination IPv4 address for the BFD sessions to be monitored for the associated oper-group.

service-id — Specifies the service ID, up to 64 characters in length, in which the BFD session exists if it is not in the base routing context.

Platforms All

bfd-enable

Syntax **bfd-enable** {**ipv4** | **ipv6**} [**include-bfd-tlv**]
no bfd-enable {**ipv4** | **ipv6**}

Context **[Tree]** (config>router>isis>if bfd-enable)

Full Context configure router isis interface bfd-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the use of bidirectional forwarding detection (BFD) to control IPv4 or IPv6 adjacencies. By enabling BFD on an IPv4 or IPv6 protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set by the BFD command under the IP interface. This command must be given separately to enable or disable BFD for both IPv4 and IPv6.

The **no** form of this command removes BFD from the associated adjacency.

Default no bfd-enable ipv4

no bfd-enable ipv6

Parameters **ipv4** — Keyword to enable BFD to control IPv4 adjacencies.

ipv6 — Keyword to enable BFD to control IPv6 adjacencies.

include-bfd-tlv — Enables support for the IS-IS BFD TLV options in accordance with RFC 6213, which specifies that a BFD session must be established before an IS-IS adjacency can transition to the established state. This option must be enabled on all IS-IS neighbors on a shared interface.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable** [**remain-down-on-failure**]

Context **[Tree]** (config>router>ospf>area>interface bfd-enable)
[Tree] (config>router>ospf3>area>interface bfd-enable)

Full Context configure router ospf area interface bfd-enable
configure router ospf3 area interface bfd-enable

Description This command enables the use of bidirectional forwarding detection (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated OSPF protocol adjacency.

Default no bfd-enable

Parameters **remain-down-on-failure** — If the BFD session does not come back up within 10 seconds, then OSPF brings down the adjacency and wait on BFD again. This can cause OSPF neighbors to flap, because OSPF will form the adjacency and then bring it down if the BFD session is still down. If this parameter is not configured, the OSPF adjacency will form even if the BFD adjacency does not come back up after a failure.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>rip bfd-enable)
[Tree] (config>router>rip>group bfd-enable)
[Tree] (config>router>rip>group>neighbor bfd-enable)
[Tree] (config>router>ripng bfd-enable)
[Tree] (config>router>ripng>group bfd-enable)
[Tree] (config>router>ripng>group>neighbor bfd-enable)

Full Context configure router rip bfd-enable
configure router rip group bfd-enable
configure router rip group neighbor bfd-enable
configure router ripng bfd-enable
configure router ripng group bfd-enable
configure router ripng group neighbor bfd-enable

Description This command enables bidirectional forwarding detection (BFD) to control the state of the associated protocol adjacency. By enabling BFD on a given protocol interface, the state of the RIP neighbor is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set using the **bfd** command under the IP interface configuration context.

The **no** form of this command removes BFD from the associated protocol adjacency.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>router>segment-routing>maintenance-policy bfd-enable)

Full Context configure router segment-routing maintenance-policy bfd-enable

Description This command enables seamless BFD on every programmed segment list of an SR policy candidate path to which the maintenance policy is applied. BFD session parameters are taken from the BFD template that is configured for the maintenance policy.

The **no** form of this command disables seamless BFD on every segment list of an SR policy.

Default no bfd-enable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-enable

Syntax **bfd-enable** [**ipv4**]
no bfd-enable

Context **[Tree]** (config>router>bier bfd-enable)

Full Context configure router bier bfd-enable

Description This command configures BFD tracking for BIER, which means that all next-hops that use a BFD-enabled interface register with the BFD module.

The **no** form of this command disables BFD tracking under BIER.

Default no bfd-enable

Parameters **ipv4** — Enables the use of IPv4 BFD tracking.

Platforms All

bfd-enable

Syntax [**no**] **bfd-enable**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy bfd-enable)

Full Context configure subscriber-mgmt bgp-peering-policy bfd-enable

Description This command enables bi-directional forwarding (BFD) to control the state of an ESM dynamic BGP peer that is setup with this BGP peering policy. The parameters used for the BFD session are configured in the **bfd** context of the **group-interface** or retail **subscriber-interface**.

The **no** form of this command disables BFD for new ESM dynamic BGP peers that are setup with this BGP peering policy.

Default no bfd-enable

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

6.29 bfd-on-distributing-only

bfd-on-distributing-only

Syntax [**no**] **bfd-on-distributing-only**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>lag>bfd>family bfd-on-distributing-only)

Full Context configure lag bfd family bfd-on-distributing-only

Description This command enables standardized implementation for interworking with other vendors by restricting micro-BFD sessions to links in LACP state distributing.

The **no** form of this command disables restricting micro-BFD sessions, which is an enhanced proprietary solution.

Default no bfd-on-distributing-only

Platforms All

6.30 bfd-sessions

bfd-sessions

Syntax **bfd-sessions** *max-limit*
no bfd-sessions

Context [Tree] (config>router>lsp-bfd bfd-sessions)

Full Context configure router lsp-bfd bfd-sessions

Description This command enables or disables LSP BFD at the tail end of LSPs on the system. It is also used to limit the maximum number of LSP BFD sessions that may be established at the tail-end of LSPs on a node to *max-limit*. It has no impact on the number of LSP BFD sessions that may be configured at the head end.

The **no** version of this command disables the creation of LSP BFD sessions by the node at the tail end of LSPs.

Default no bfd-sessions

Parameters *max-limit* — Specifies the maximum number of LSP BFD sessions at the tail end of LSPs that can be established on a system. The maximum value that can be entered is constrained by the system wide limit for centralized BFD sessions.

Values 1- max, where max is the platform specific limit on centralized BFD sessions.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.31 bfd-template

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context **[Tree]** (config>service>apipe>spoke-sdp>bfd bfd-template)
[Tree] (config>service>cpipe>spoke-sdp>bfd bfd-template)
[Tree] (config>service>epipe>spoke-sdp>bfd bfd-template)
[Tree] (config>service>fpipe>spoke-sdp>bfd bfd-template)
[Tree] (config>service>ipipe>spoke-sdp>bfd bfd-template)

Full Context configure service apipe spoke-sdp bfd bfd-template
configure service cpipe spoke-sdp bfd bfd-template
configure service epipe spoke-sdp bfd bfd-template
configure service fpipe spoke-sdp bfd bfd-template
configure service ipipe spoke-sdp bfd bfd-template

Description This command configures a named BFD template to be used by VCCV BFD on PWs belonging to the VLL service. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, used by the BFD session. Template parameters are configured under the **config>router>bfd** context.

The **no** form of this command removes the binding of the BFD template to the spoke-SDP.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string, up to 32 characters, in printable 7-bit ASCII, enclosed in double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp bfd bfd-template
- configure service cpipe spoke-sdp bfd bfd-template

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp bfd bfd-template

All

- configure service epipe spoke-sdp bfd bfd-template
- configure service ipipe spoke-sdp bfd bfd-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context **[Tree]** (config>service>epipe>bgp>pw-template-binding bfd-template)

Full Context configure service epipe bgp pw-template-binding bfd-template

Description This command configures a named BFD template to be used by VCCV BFD on PWs belonging to the BGP VPWS service. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, to be used by the BFD session. Template parameters are configured under the **config>router>bfd** context.

The **no** form of this command removes the binding of the BFD template to the BGP VPWS.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string, up to 32 characters, in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context **[Tree]** (config>service>vpls>mesh-sdp>bfd bfd-template)
[Tree] (config>service>vpls>spoke-sdp>bfd bfd-template)

Full Context configure service vpls mesh-sdp bfd bfd-template
configure service vpls spoke-sdp bfd bfd-template

Description This command configures a named BFD template to be used by VCCV BFD on the PW belonging to the VPLS spoke-SDP or mesh-SDP. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, to be used by the BFD session. Template parameters are configured under the **config>router>bfd** context.

The **no** form of this command removes the binding of the BFD template to the spoke-SDP.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string, up to 32 characters, in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context **[Tree]** (config>service>vpls>bgp-ad>pw-template-binding bfd-template)
[Tree] (config>service>vpls>bgp>pw-template-binding bfd-template)

Full Context configure service vpls bgp pw-template-binding bfd-template
configure service vpls bgp-ad pw-template-binding bfd-template

Description This command configures a named BFD template to be used by VCCV BFD on PWs belonging to the BGP VPWS, or BGP AD VPLS service. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, to be used by the BFD session. Template parameters are configured under the **config>router>bfd** context.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string, up to 32 characters, in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context **[Tree]** (config>service>ies>if>spoke-sdp>bfd bfd-template)

Full Context configure service ies interface spoke-sdp bfd bfd-template

Description This command configures a named BFD template to be used by VCCV BFD on the PW belonging to the spoke-SDP that is terminated on the IES interface. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, to be used by the BFD session. Template parameters are configured under the **config>router>bfd** context.

The **no** form of this command removes the binding of the BFD template to the spoke-SDP.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string, up to 32 characters, in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context **[Tree]** (config>service>vprn>if>spoke-sdp>bfd bfd-template)

Full Context configure service vprn interface spoke-sdp bfd bfd-template

Description This command configures a named BFD template to be used by VCCV BFD on the PW belonging to spoke-SDP that is terminated on the VPRN interface. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, to be used by the BFD session. Template parameters are configured under the **config>router>bfd** context.

The **no** form of this command removes the binding of the BFD template to the spoke-SDP.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string, up to 32 characters, in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

bfd-template

Syntax **bfd-template** *bfd-template-name*
no bfd-template

Context **[Tree]** (config>router>ldp>lsp-bfd bfd-template)

Full Context configure router ldp lsp-bfd bfd-template

Description This command applies the specified BFD template to the BFD sessions for LDP LSPs with FECs that match the prefix list. The specified BFD template must exist prior to its application to LSP BFD.

The **no** form of this command removes the application of the BFD template.

Default no bfd-template

Parameters *bfd-template-name* — Specifies the name of the BFD template configured using the **config**>**router**>**bfd**>**bfd-template** command, up to 32 characters maximum.

Platforms All

bfd-template

Syntax **bfd-template** *name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no bfd-template

Context [Tree] (config>router>mpls>mpls-tp>oam-template bfd-template)

Full Context configure router mpls mpls-tp oam-template bfd-template

Description This command configures a named BFD template to be referenced by an OAM template.

Default no bfd-template

Parameters *name* — Specifies the BFD template name as a text string up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context [Tree] (config>router>mpls>lsp>bfd bfd-template)
[Tree] (config>router>mpls>lsp>primary>bfd bfd-template)
[Tree] (config>router>mpls>lsp>secondary>bfd bfd-template)
[Tree] (config>router>mpls>lsp-template>bfd bfd-template)

Full Context configure router mpls lsp bfd bfd-template
configure router mpls lsp primary bfd bfd-template
configure router mpls lsp secondary bfd bfd-template
configure router mpls lsp-template bfd bfd-template

Description This command references a named BFD template to be used by LSP BFD. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, to be used by the BFD session. Templates are configured under the **config>router>bfd** context.

The **no** form of this command removes the association of the named BFD template to the LSP.

Default no bfd-template

Parameters *name* — Specifies a text string name for the template of up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

bfd-template

Syntax [**no**] **bfd-template** *name*

Context [Tree] (config>router>bfd bfd-template)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bfd bfd-template

Description This command configures a BFD template. A BFD template defines the set of configurable parameters used by a BFD session. These include the transmit and receive timer intervals used for BFD CC packets, the transmit timer interval used when the session is providing a CV function, the multiplier value, the echo-receive interval, and whether the BFD session terminates in the CPM network processor.

The **no** form of this command reverts to the default value.

Default no bfd-template

Parameters *name* — Specifies a text string name for the template, up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms All

bfd-template

Syntax **bfd-template** *bfd-template*
no bfd-template

Context **[Tree]** (config>router>segment-routing>maintenance-policy bfd-template)

Full Context configure router segment-routing maintenance-policy bfd-template

Description This command references a named BFD template that is used by seamless BFD. The template specifies parameters, such as the minimum transmit and receive control packet timer intervals, that are used by the BFD session. Templates are configured under the **config**>**router**>**bfd** context.

A BFD template must exist on the system before being referenced from a maintenance policy.

The **no** form of this command removes the configured template.

Parameters *bfd-template* — Specifies the name of the BFD template, up to 32 characters.

Platforms All

6.32 bfd-trap-suppression

bfd-trap-suppression

Syntax [**no**] **bfd-trap-suppression**

Context **[Tree]** (config>router>mpls>lsp>protect-tp-path>mep bfd-trap-suppression)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>mpls>lsp>working-tp-path>mep bfd-trap-suppression)

Full Context configure router mpls lsp protect-tp-path mep bfd-trap-suppression
configure router mpls lsp working-tp-path mep bfd-trap-suppression

Description This command enables AIS packets on a working or protection path of an MPLS-TP LSP to suppress BFD Down traps if a BFD session goes down on that path. It also causes BFD Up traps to be suppressed, and enables the 2.5 s hold-down timer.

Suppression only occurs as a result of a received AIS packet. Traps generated as a result of a local failure at an LER are not suppressed.

The **no** form of this command disables BFD Down/Up trap suppression when AIS packets are received.

Default no bfd-trap-suppression

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.33 bfr-id

bfr-id

Syntax **bfr-id** *bfr-id*
no bfr-id

Context **[Tree]** (config>router>bier>template>sub-domain bfr-id)

Full Context configure router bier template sub-domain bfr-id

Description This command specifies the BIER-ID for this sub-domain. BIER-IDs should be assigned sequentially as the SI and BIER bit position are driven by the IDs. The equation used to drive BIER SI and bit positions from the ID is as follows:

SI = (BFR-id -1) /BitStringLength

bit position = ((BFR-id -1) modulo BitStringLength) +1

If the BIER-ID is sequential then the all bit positions in a bit string length will be utilized before moving on to the next SetID (SI).

BFR ID configuration is only necessary for BFIR and BFER, and not for transit BFRs

The **no** form of this command removes the BIER-ID.

Parameters *bfr-id* — The BIER-ID of the router.

Values 1 to 4096

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

6.34 bgp

bgp

Syntax [**no**] **bgp**

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>evpn bgp)

Full Context configure subscriber-mgmt isa-service-chaining evpn bgp

Description Commands in this context configure EVPN BGP-specific information.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

bgp

Syntax [**no**] **bgp**

Context **[Tree]** (config>service>epipe bgp)

Full Context configure service epipe bgp

Description Commands in this context configure the BGP related parameters BGP used for multi-homing and BGP VPWS.

The **no** form of this command removes the string from the configuration.

Platforms All

bgp

Syntax [**no**] **bgp**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter bgp)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter bgp)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter bgp)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter bgp)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter bgp
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter bgp
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter bgp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter bgp

Description This command selects the BGP tunnel type.

This command instructs BGP EVPN to search for a BGP LSP to the address of the BGP next hop. If the user does not enable the BGP tunnel type, inter-area or inter-as prefixes are not resolved.

The **no** form of this command removes the BGP tunnel type configuration.

Default bgp

Platforms All

bgp

Syntax **bgp** *bgp-instance*
no bgp *bgp-instance*

Context **[Tree]** (config>service>vpls bgp)

Full Context configure service vpls bgp

Description Commands in this context configure the BGP related parameters for BGP VPLS.

A maximum of two BGP instances can be configured in a VPLS service. The *bgp-instance* parameter value can be configured as 1 or 2. If it is not specified, the parameter value is configured as 1 by default.

The **route-distinguisher** configured in BGP instance 1 and 2 must be different. However, the route-target value may be configured the same or different for the two instances.

Only BGP-EVPN MPLS is allowed to be assigned to instance 2. Instance 1 must be used for the VXLAN and L2VPN address families.

BGP-EVPN VXLAN and BGP-EVPN MPLS can only be configured as **no shutdown** in the same service if they are associated with different instances (When the two BGP instances are created, the **bgp-instance** command must be configured in the **bgp-evpn mpls** context).

The **evi** value in **bgp-evpn** can be used to auto-derive the route distinguisher in instance 1 only. However, the **evi** value can be used to auto-derive the **route-target** in both instances.

The **no** version of the command removes the BGP instance.

Parameters *bgp-instance* — Specifies the value associated with the BGP instance.

Values 1 to 2

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bgp

Syntax [**no**] **bgp**

Context **[Tree]** (config>router bgp)

Full Context configure router bgp

Description This command creates the BGP protocol instance and BGP configuration context. BGP is administratively enabled upon creation.

The **no** form of this command deletes the BGP protocol instance and removes all configuration parameters for the BGP instance. BGP must be **shutdown** before deleting the BGP instance. An error occurs if BGP is not **shutdown** first.

Platforms All

bgp

Syntax [**no**] **bgp**

Context **[Tree]** (config>service>vprn bgp)

Full Context configure service vprn bgp

Description This command enables the BGP protocol with the VPRN service.

The **no** form of this command disables the BGP protocol from the given VPRN service.

Default no bgp

Platforms All

bgp

Syntax **bgp** [**source** *src-Addr*] [**group** *grpAddr*] [**peer** *peerAddr*]
no bgp

Context **[Tree]** (debug>router>pim bgp)

Full Context debug router pim bgp

Description This command enables debugging for PIM/BGP-specific interoperation.

The **no** form of this command disables debugging for PIM/BGP-specific interoperation.

Parameters *src-Addr* — Debugs BGP information associated with the specified source.

Values source address (ipv4, ipv6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

grp-Addr — Debugs BGP information associated with the specified group.

Values group address (ipv4, ipv6)

PeerAddr — Debugs BGP information associated with the specified peer.

Values peer address (ipv4, ipv6)

Platforms All

bgp

Syntax [**no**] **bgp**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter bgp)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter bgp)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter bgp
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter bgp

Description This command selects BGP tunneling for next-hop resolution and specifies the IPv4 tunnels created by receiving BGP label-unicast IPv4 routes for /32.

The **no** form of this command disables the selection of BGP tunneling for next-hop resolution.

Platforms All

6.35 bgp-ad

bgp-ad

Syntax [**no**] **bgp-ad**

Context **[Tree]** (config>service>vpls bgp-ad)

Full Context configure service vpls bgp-ad

Description This command configures BGP auto-discovery.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.36 bgp-auto-rd-range

bgp-auto-rd-range

Syntax **bgp-auto-rd-range** *ip-address* **comm-val** *comm-val* **to** *comm-val*
no bgp-auto-rd-range

Context **[Tree]** (config>service>system bgp-auto-rd-range)

Full Context configure service system bgp-auto-rd-range

Description This command defines the type-1 route-distinguisher IPv4 address and community value range within which the system will select a route-distinguisher for the **bgp-enabled** services using **auto-rd**.

Interactions:

This command is used along with the **route-distinguisher auto-rd** command supported in VPLS, VPRN and Epipe services. The system forces the user to create a **bgp-auto-range** before the **auto-rd** option can be used in the services.

The system will keep allocating values for services configured with **route-distinguisher auto-rd** as long as there are available community values within the configured range. After the command is added, the following changes are allowed:

- The ip-address can be changed without modifying the *comm-val* range, even if services using **auto-rd** are present. The affected routes will be withdrawn and re-advertised with the new route-distinguishers.
- The *comm-val* range can be modified as long as no conflicting values are present in the new range. For example, the user may expand the range as long as the new range does not overlap with existing manual route-distinguishers. The user may also reduce the range as long as the new range can accommodate the already allocated auto-RDs.

Parameters *ip-address* — Specifies the IPv4 address used in the first 4 octets of all the type-1 auto route-distinguishers selected by the system.

comm-val — Specifies the community value of the type-1 auto route-distinguisher.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.37 bgp-evpn

bgp-evpn

Syntax [**no**] **bgp-evpn**

Context **[Tree]** (config>service>epipe bgp-evpn)
[Tree] (config>service>system bgp-evpn)
[Tree] (config>service>vpls bgp-evpn)

Full Context configure service epipe bgp-evpn
configure service system bgp-evpn
configure service vpls bgp-evpn

Description Commands in this context configure the BGP EVPN parameters in the base instance.

Platforms All

bgp-evpn

Syntax **bgp-evpn**

Context **[Tree]** (config>service>vprn bgp-evpn)

Full Context configure service vprn bgp-evpn

Description Commands in this context configure the BGP EVPN parameters.

Platforms All

6.38 bgp-evpn-multi-homing

bgp-evpn-multi-homing

Syntax **bgp-evpn-multi-homing**

Context **[Tree]** (config>redundancy bgp-evpn-multi-homing)

Full Context configure redundancy bgp-evpn-multi-homing

Description Commands in this context configure the BGP-EVPN global timers

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.39 bgp-high-priority

bgp-high-priority

Syntax [**no**] **bgp-high-priority**

Context **[Tree]** (config>router>policy-options>policy-statement>default-action bgp-high-priority)
[Tree] (config>router>policy-options>policy-statement>entry>action bgp-high-priority)

Full Context configure router policy-options policy-statement default-action bgp-high-priority
configure router policy-options policy-statement entry action bgp-high-priority

Description This command enables eligible BGP routes matched by the policy entry or policy default-action that are tagged for faster route table updates.

This action applies only when the policy is applied as a BGP import policy to a base router BGP peer or VPRN BGP peer and applies only to the following route types:

- IPv4
- label-IPv4
- IPv6
- label-IPv6

This command is useful when the BGP RIB contains a large number of routes and quick routing table updates are needed for a small subset of these routes. The effectiveness of this command decreases as the subset becomes a larger proportion of the total RIB.

The **no** form of this command disables the routes that are tagged for faster route table updates.

Default no bgp-high-priority

Platforms All

6.40 bgp-ipvpn

bgp-ipvpn

Syntax **bgp-ipvpn**

Context **[Tree]** (config>service>vprn bgp-ipvpn)

Full Context configure service vprn bgp-ipvpn

Description Commands in this context configure the BGP IPVPN parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

6.41 bgp-labels-hold-timer

bgp-labels-hold-timer

Syntax **bgp-labels-hold-timer** *seconds*
no bgp-labels-hold-timer

Context **[Tree]** (config>router>mpls-labels bgp-labels-hold-timer)

Full Context configure router mpls-labels bgp-labels-hold-timer

Description This command configures the BGP labels hold timer on the ingress router.

Default bgp-labels-hold-timer 0

Parameters *seconds* — Specifies the seconds

Values 0 to 255

Platforms All

6.42 bgp-leak

bgp-leak

Syntax [**no**] **bgp-leak**

Context **[Tree]** (config>router>policy-options>policy-statement>default-action bgp-leak)
[Tree] (config>router>policy-options>policy-statement>entry>action bgp-leak)

Full Context configure router policy-options policy-statement default-action bgp-leak
configure router policy-options policy-statement entry action bgp-leak

Description This command causes qualifying matched BGP routes to be marked as leakable, meaning they are candidates to be leaked into other routing instances (copied with their complete set of path attributes). A BGP route is a qualifying route if it is an IPv4 route (unlabeled), IPv6 route (unlabeled) or a label-IPv4 route.

Note: A leakable BGP route is not actually leaked into another routing instance unless it is accepted by a leak-import policy of that other routing instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **bgp-leak** command has an effect only when the policy is applied as a BGP import policy in the base router or a VPRN context.

Default no bgp-leak

Platforms All

6.43 bgp-med

bgp-med

Syntax **bgp-med adjust** *expression*
bgp-med set {**igp** | **min-igp**}
bgp-med set *med-value*
no bgp-med

Context **[Tree]** (config>router>policy-options>policy-statement>default-action bgp-med)
[Tree] (config>router>policy-options>policy-statement>entry>action bgp-med)

Full Context configure router policy-options policy-statement default-action bgp-med
configure router policy-options policy-statement entry action bgp-med

Description This command changes the BGP MED attribute value in BGP routes matched by the route policy entry (or the policy default action).

If the matched route already has a MED attribute, this command overwrites the existing value. If the matched route does not have a MED attribute, then one is added and the value is set based on the parameters of this command.

This command has no effect on non-BGP routes. The default, **no bgp-med**, does not modify MED values.

Default no bgp-med

Parameters *expression* — Specifies a logical expression parsed as a string. The string can contain:

- parentheses () to change the order of operations
- mathematical operators: + (addition), - (subtraction) and * (multiplication)
- directly entered decimal values that act as operands of the mathematical operators. Each decimal value supports up to three decimal places precision in the range of 0.000 to 4294967295.000
- decimal values represented by parameter names (using the usual @parameter-name@ syntax) that act as operands of the mathematical operators. Each parameterized decimal value supports up to three decimal places precision in the range of 0.000 to 4294967295.000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

igp — Instructs the policy to set the MED based on the current route table or tunnel table cost to resolve the BGP next-hop address.

min-igp — Instructs the policy to set the MED based on the minimum route table or tunnel table cost to resolve the BGP next-hop of the route, over its lifetime in the local RIB.

med-value — Specifies a new MED value (or parameter name to use for the new MED value) to use with the route.

Values *value*
- 0 to 4294967295

param-name
- up to 32 characters
- Must start and end with an at-sign (@)

Platforms All

6.44 bgp-multi-homing

bgp-multi-homing

Syntax **bgp-multi-homing**

Context **[Tree]** (config>redundancy bgp-multi-homing)

Full Context configure redundancy bgp-multi-homing

Description This command configures BGP multi-homing parameters.

Platforms All

6.45 bgp-peering-policy

bgp-peering-policy

Syntax **bgp-peering-policy** *policy-name* [**create**]
no bgp-peering-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt bgp-peering-policy)

Full Context configure subscriber-mgmt bgp-peering-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the name of the BGP peering policy.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the BGP peer policy name, up to 32 characters.

create — Keyword used to create the peering policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

6.46 bgp-peers

bgp-peers

Syntax **bgp-peers** *criterion-index* **group** *reg-exp* **neighbor** *reg-exp*
bgp-peers *criterion-index* **router** *router-instance* **group** *reg-exp* **neighbor** *reg-exp*
bgp-peers *criterion-index* **router service-name** *service-name* **group** *reg-exp* **neighbor** *reg-exp*
no bgp-peers *criterion-index*

Context **[Tree]** (config>filter>match-list>ip-prefix-list>apply-path bgp-peers)
[Tree] (config>filter>match-list>ipv6-prefix-list>apply-path bgp-peers)

Full Context configure filter match-list ip-prefix-list apply-path bgp-peers
configure filter match-list ipv6-prefix-list apply-path bgp-peers

Description This command configures auto-generation of IPv4 or IPv6 address prefixes (as required by the context that the command is executed within) based on the base router BGP instance configuration.

The **no** form of this command removes the bgp-peers configuration for auto-generation of address prefixes for the specified index value.

Parameters *service-name* — Specifies the service name, up to 64 characters in length.

group — Configures a match against the base router BGP instance group configuration.

Regex match (.*) can be used to match against any group.

neighbor — Configures a match against the base router BGP instance neighbor configuration.

Regex match (.*) can be used to match against any neighbor.

criterion-index — Specifies an integer from 1 to 255 enumerating BGP peers auto-generation configuration within this list.

router-instance — Specifies the router name or service ID.

Values router-instance: *router-name* or *vprn-svc-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-name: "Base"

vprn-svc-id: 1 to 2147483647

service-name: Specifies the service name, up to 64 characters in length.

router — Configures a match against the base router BGP instance configuration.

reg-exp — Specifies a regular expression that defines a match string, up to 255 characters in length, to be used to auto-generate address prefixes. Matching is performed from the least-significant digit. For example, a string **10.0** matches all neighbors with addresses starting with **10**, such as **10.0.x.x** or **10.0xx.x.x**.

Platforms All

6.47 bgp-shared-queue

bgp-shared-queue

Syntax **bgp-shared-queue** [**cir** *rate*] [**pir** *rate*]
no bgp-shared-queue

Context **[Tree]** (config>service>vprn bgp-shared-queue)

Full Context configure service vprn bgp-shared-queue

Description This command enables all BGP peers within a VPRN instance to share a single CPM queue. This command takes effect on new BGP connections established; already established BGP peers continue to use their own CPM queue. Any changes to PIR/CIR of the shared queue takes effect only after BGP connections are re-established.

Parameters **cir** *rate* — Specifies the CIR rate for the shared queue.

pir *rate* — Specifies the PIR rate for the shared queue.

Platforms All

6.48 bgp-shortcut

bgp-shortcut

Syntax [**no**] **bgp-shortcut**

Context **[Tree]** (config>router>mpls>lsp bgp-shortcut)
[Tree] (config>router>mpls>lsp-template bgp-shortcut)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls lsp bgp-shortcut
configure router mpls lsp-template bgp-shortcut

Description This command enables the use of RSVP LSP for IPv4 BGP routes.

Platforms All

6.49 bgp-transport-tunnel

bgp-transport-tunnel

Syntax **bgp-transport-tunnel** [**include** | **exclude**]

Context **[Tree]** (config>router>mpls>lsp bgp-transport-tunnel)
[Tree] (config>router>mpls>lsp-template bgp-transport-tunnel)

Full Context configure router mpls lsp bgp-transport-tunnel
configure router mpls lsp-template bgp-transport-tunnel

Description This command allows or blocks RSVP-TE LSP to be used as a transport LSP for BGP tunnel routes.

Default bgp-transport-tunnel include

Parameters **include** — Allows RSVP-TE LSP to be used as transport LSP from the ASBR to local PE router, from ingress PE to ASBR in the local AS or between multi-hop External Border Gateway Protocol (EBGP) peers with ASBR to ASBR adjacency.

exclude — Blocks RSVP-TE LSP to be used as transport LSP from the ASBR to local PE router, from ingress PE to ASBR in the local AS or between multi-hop EBGP peers with ASBR to ASBR adjacency.

Platforms All

6.50 bgp-tunnel

bgp-tunnel

Syntax [**no**] **bgp-tunnel**

Context **[Tree]** (config>service>sdp bgp-tunnel)

Full Context configure service sdp bgp-tunnel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the use of BGP route tunnels available in the tunnel table to reach SDP far-end nodes. Use of BGP route tunnels are only available with MPLS-SDP. Only one of the transport methods is allowed per SDP - LDP, RSVP-LSP BGP, SR-ISIS, or SR-OSPF. This restriction is relaxed for some combinations of the transport methods when the mixed-lsp-mode option is enabled within the SDP.

The **no** form of the command disables resolving BGP route tunnel LSP for SDP far-end.

Default no bgp-tunnel (BGP tunnel route to SDP far-end is disabled)

Platforms All

6.51 bgp-tunnel-metric

bgp-tunnel-metric

Syntax **bgp-tunnel-metric** [*value*] **prefer-aigp**
bgp-tunnel-metric [*value*] [**prefer-aigp**]
no bgp-tunnel-metric

Context **[Tree]** (config>router>bgp bgp-tunnel-metric)

Full Context configure router bgp bgp-tunnel-metric

Description This command sets the TTM metric of all BGP tunnels to a fixed value or a value derived from the AIGP metric of the BGP-LU route, if the BGP-LU route has an AIGP path attribute; otherwise, it is set to the number specified by *value*. The effect of this command can be overridden by BGP import policies.

By default, BGP tunnels are installed with a fixed cost of 1000 in the tunnel table. This can overstate or understate their true cost when compared to other tunnels with IGP-derived costs.

The **no** form of this command reverts to the default.

Default no bgp-tunnel-metric

Parameters *value* — Specifies the BGP tunnel metric.

Values 0 to 4294967295

prefer-aigp — Specifies that the TTM metric be based on the Accumulated IGP (AIGP) metric if the route has the path attribute. When **prefer-aigp** is configured and a BGP-LU route is selected for installation in TTM and it is not matched by a BGP import policy entry that overrides the **bgp-tunnel-metric** action, the TTM metric of the tunnel is set to the AIGP metric value of the BGP-LU route, plus the resolved cost to the BGP next-hop of the route if the tunnel has the AIGP path attribute. Otherwise, the number in *value* is set as the metric.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

bgp-tunnel-metric

Syntax **bgp-tunnel-metric** [*value* | *param-name*] [**prefer-aigp**]
no bgp-tunnel-metric

Context **[Tree]** (config>router>policy-options>policy-statement>default-action bgp-tunnel-metric)
[Tree] (config>router>policy-options>policy-statement>entry>action bgp-tunnel-metric)

Full Context configure router policy-options policy-statement default-action bgp-tunnel-metric
configure router policy-options policy-statement entry action bgp-tunnel-metric

Description This command provides the ability to set the TTM metric of all BGP tunnels, matched by the policy entry or the policy default action, to a fixed value or a value derived from the AIGP metric of the BGP-LU route, if the BGP-LU route has an AIGP path attribute, otherwise it reverts to the *value* parameter.

The **no** form of this command reverts to the default.

Default no bgp-tunnel-metric

Parameters *value* — Specifies the BGP tunnel metric.

Values 0 to 4294967295

param-name — Specifies the parameter name, up to 32 characters that starts and ends with an at-sign (@).

prefer-aigp — Specifies that the TTM metric be based on the Accumulated IGP (AIGP) metric if the route has the path attribute.

Platforms All

6.52 bgp-tunnel-preference

bgp-tunnel-preference

Syntax **bgp-tunnel-preference** [*preference*]
no bgp-tunnel-preference

Context **[Tree]** (config>router>bgp bgp-tunnel-preference)

Full Context configure router bgp bgp-tunnel-preference

Description This command configures the tunnel table preference for BGP-LU tunnel type away from its default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The tunnel table preference applies to the next-hop resolution of BGP routes of the following families: EVPN, IPv4, IPv6, VPN-IPv4, VPN-IPv6, label-IPv4, and label-IPv6 in the tunnel table.

This feature does not apply to a VPRN, VPLS, or VLL service with explicit binding to an SDP which enabled the **mixed-lsp-mode** option. The tunnel preference, in such an SDP, is fixed and is controlled by the service manager. The configuration of the tunnel table preference parameter does not modify the behavior of such an SDP and the services that bind to it.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

The **no** form of this command reverts to the default value.

Default bgp-tunnel-preference 12

Parameters *preference* — Specifies the BGP tunnel preference.

Values 1 to 255

Default 12

Platforms All

6.53 bgp-vpls

bgp-vpls

Syntax **bgp-vpls**

Context **[Tree]** (config>service>vpls bgp-vpls)

Full Context configure service vpls bgp-vpls

Description Commands in this context configure the BGP-VPLS parameters and addressing.

Platforms All

6.54 bgp-vpls-mh-ve-id

bgp-vpls-mh-ve-id

Syntax **bgp-vpls-mh-ve-id** *number*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no bgp-vpls-mh-ve-id

Context [Tree] (config>service>vpls>sap bgp-vpls-mh-ve-id)

Full Context configure service vpls sap bgp-vpls-mh-ve-id

Description This command upon the configuration of the ve-id under the SAP and if BGP-VPLS is configured and is operationally up, causes the PE to advertise a bgp-mh route for the ve-id (the route does not contain label information). The bgp-mh route contains the F and D flags properly set based on the SAP operational state. Upon switchover, the former active PE (DF in case of EVPN-MH) sends an update with a transition of the F bit from 1 to 0. This is an indication for the remote PEs to flush their MACs associated to the advertising PE.

This command is required when MC-LAG or EVPN-MH is used for multi-homing redundancy and mac-flush is required at remote BGP-VPLS PEs when there is a failure in the active PE.

The **no** form of this command withdraws the L2 VPN route.

Parameters *number* — Specifies the BGP-VPLS multi-homing virtual-edge identifier.

Values 1 to 65535

Platforms All

6.55 bgp-vpws

bgp-vpws

Syntax [**no**] **bgp-vpws**

Context [Tree] (config>service>epipe bgp-vpws)

Full Context configure service epipe bgp-vpws

Description Commands in this context configure BGP-VPWS parameters and addressing.

Default no bgp-vpws

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.56 bi

bi

Syntax **bi**

Context **[Tree]** (config>system>security>keychain>direction bi)

Full Context configure system security keychain direction bi

Description This command configures keys for both send and receive stream directions.

Platforms All

6.57 bier

bier

Syntax [**no**] **bier**

Context **[Tree]** (config>service>vprn>mvpn>provider-tunnel>inclusive bier)
[Tree] (config>service>vprn>mvpn>provider-tunnel>selective bier)

Full Context configure service vprn mvpn provider-tunnel inclusive bier
configure service vprn mvpn provider-tunnel selective bier

Description This command creates a BIER inclusive or selective provider tunnel.

The **no** form of this command deletes the tunnel.

Platforms All

bier

Syntax [**no**] **bier**

Context **[Tree]** (config>router bier)

Full Context configure router bier

Description Commands in this context configure BIER.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bier

Syntax [**no**] **bier**

Context **[Tree]** (config>router>isis>level bier)

Full Context configure router isis level bier

Description This command enables BIER capabilities.

The **no** form of this command disables BIER capabilities.

Platforms All

bier

Syntax [**no**] **bier**

Context **[Tree]** (config>router>ospf>area bier)

Full Context configure router ospf area bier

Description This command enables BIER capabilities.

The **no** form of this command disables BIER capabilities.

Default no bier

Platforms All

6.58 bier-ping

bier-ping

Syntax **bier-ping** [**sub-domain** *sub-domain-id*] **bfr-id** *bfr-id* [**detail**] [**fc** *fc-name*] [**profile** {**in**| **out**}] [**timeout** *timeout*] [**ttl** *ttl*]
bier-ping [**sub-domain** *sub-domain-id*] **bfr-id-start** *bfr-id* **bfr-id-end** *bfr-id* [**detail**] [**fc** *fc-name*] [**profile** {**in**| **out**}] [**timeout** *timeout*] [**ttl** *ttl*]
bier-ping [**sub-domain** *sub-domain-id*] **bfr-prefix** *ipv4-address* [*ipv4-address*] [**detail**] [**fc** *fc-name*] [**profile** {**in**| **out**}] [**timeout** *timeout*] [**ttl** *ttl*]

Context **[Tree]** (oam bier-ping)

Full Context oam bier-ping

Description This command performs connectivity tests on the BIER data plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sub-domain-id* — Specifies the ID of the sub-domain where the BIER OAM packet is generated.

Values 0 to 255

Default 0

bfr-id — Specifies the BIER-ID of the router.

Values 1 to 4096

ipv4-address — Specifies the routable IPv4 address of the BFR, used by BIER to identify the BFR. Up to 16 IPv4 addresses can be specified.

Values a.b.c.d

detail — Keyword to display more information.

fc-name — Specifies the FC and profile parameters that are used to indicate the forwarding class and profile of the BIER echo request packet.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

{**in** | **out**} — Specifies the profile state of the BIER echo request packet.

Default out

timeout — Specifies the number, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the timeout, the test is marked complete and no more packets are processed.

Values 1 to 120

Default 10

ttl — Specifies the TTL value for the BIER ping test, expressed as a decimal integer.

Values 1 to 255

Default 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.59 bier-signaling

bier-signaling

Syntax [**no**] **bier-signaling** [**detail**]

Context **[Tree]** (debug>router>pim bier-signaling)

Full Context debug router pim bier-signaling

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for bier inband.

The **no** form of this command disables debugging for bier inband.

Parameters **detail** — Debugs detailed information on the bier inband.

bier-signaling

Syntax [**no**] **bier-signaling** [**ipv4**] [**ipv6**]

Context **[Tree]** (config>router>pim>interface bier-signaling)

Full Context configure router pim interface bier-signaling

Description This commands enables PIM signaling through a BIER domain. PIM signaling only functions in the context of SD0. PIM signaling can signal PIM IPv4 and IPv6 over a BIER IPV4 core.

The **no** form of this command disables PIM signaling through a BIER domain.

Default no bier-signaling

Parameters **ipv4** — Enables the use of IPv4 PIM signaling through a BIER domain.

ipv6 — Enables the use of IPv6 PIM signaling through a BIER domain.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.60 bier-trace

bier-trace

Syntax **bier-trace** [**sub-domain** *sub-domain-id*] **bfr-id** *bfr-id* [**detail**] [**fc** *fc-name*] [**profile** {**in**| **out**}] [**min-ttl** *min-ttl*] [**max-ttl** *max-ttl*] [**probe-count** *probes-per-hop*] [**timeout** *timeout*]

bier-trace [**sub-domain** *sub-domain-id*] **bfr-prefix** *ipv4-address* [**detail**] [**fc** *fc-name*] [**profile** {**in**| **out**}] [**min-ttl** *min-ttl*] [**max-ttl** *max-ttl*] [**probe-count** *probes-per-hop*] [**timeout** *timeout*]

Context **[Tree]** (oam bier-trace)

Full Context oam bier-trace

Description This command performs trace tests on the BIER data plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sub-domain-id* — Specifies the ID of the sub-domain where the BIER OAM packet is generated.

Values 0 to 255

Default 0

bfr-id — Specifies the BIER-ID of the router.

Values 1 to 4096

ipv4-address — Specifies the routable IPv4 address of the BFR, used by BIER to identify the BFR.

Values a.b.c.d

detail — Keyword to display more information.

fc-name — Specifies the FC and profile parameters that are used to indicate the forwarding class and profile of the BIER OAM packet.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

{**in** | **out**} — Specifies the profile state of the BIER echo request packet.

Default out

min-ttl — Specifies the minimum TTL value for the BIER trace test, expressed as a decimal integer.

Values 1 to 255

Default 1

max-ttl — Specifies the maximum TTL value for the BIER trace test, expressed as a decimal integer.

Values 1 to 255

Default 30

probes-per-hop — Specifies the probes-per-hop count, expressed as number of packets.

Values 1 to 10

Default 1

timeout — Specifies the number, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending each probe for a specific test. Upon the expiration of the timeout, the test is marked complete and no more packets are processed for the request probe.

When the test consists of multiple probes, the timeout is the interval, in seconds, between request probes.

A BIER trace test terminates after five consecutive timeouts.

Values 1 to 60

Default 3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.61 bin

bin

Syntax **bin** *bin-number*

Context **[Tree]** (config>oam-pm>bin-group>bin-type bin)

Full Context configure oam-pm bin-group bin-type bin

Description Commands in this context configure the thresholds for the specified bin.

Parameters *bin-number* — Specifies bin to configure.

Values 1 to 9

Platforms All

6.62 bin-group

bin-group

Syntax **bin-group** *bin-group-number* [**fd-bin-count** *fd-bin-count* **fdr-bin-count** *fdr-bin-count* **ifdv-bin-count** *ifdv-bin-count* **create**]
no bin-group *bin-group-number*

Context **[Tree]** (config>oam-pm bin-group)

Full Context configure oam-pm bin-group

Description This command allows the operator to configure the parameters for a specific bin group. Bin-group 1 is a default **bin-group** and cannot be modified. If no bin group is assigned to an oam-pm session, this is assigned by default. The default values for bin-group 1 are (fd-bin-count 3 bin 1 lower-bound 5000us, bin 2 lower-bound 10000us fdr-bin-count 2 bin 1lower-bound 5000us and ifdv-bin-count 2 bin 1lower-bound 5000us)

The **no** form of this command disables the OAM Performance Monitoring bin group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *bin-group-number* — Specifies an identifier for a bin-group that is referenced by oam-pm sessions. A bin group can only shutdown and modified when all the PM Sessions referencing the bin group have been shutdown. The only exception is the description parameter.

Values 1 to 255

fd-bin-count — Specifies the number of frame delay bins that are created.

Values 2 to 10

fdr-bin-count — Specifies the number of frame delay range bins that are created.

Values 2 to 10

ifdv-bin-count — Specifies the number of inter-frame delay variation bins that are created.

Values 2 to 10

create — Keyword that creates the bin group.

Platforms All

bin-group

Syntax **bin-group** *bin-group-number*
no bin-group

Context **[Tree]** (config>oam-pm>session bin-group)

Full Context configure oam-pm session bin-group

Description This command links the individual test to the group of bins that map the probe responses.

The **no** form of this command installs the default bin-group 1 as the bin-group for the session.

Parameters *bin-group-number* — Specifies the number that was used to create the specific **bin-group** that is referenced for this session.

Values 1 to 255

Default 1

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.63 bin-type

bin-type

Syntax **bin-type** {**fd** | **fdr** | **ifdv**}

Context **[Tree]** (config>oam-pm>bin-group bin-type)

Full Context configure oam-pm bin-group bin-type

Description This command is the start of the hierarchy where the specific delay metric bin structure isis defined.

Parameters **fd** — Keyword to enter the frame delay bin threshold configuration.

fdr — Keyword to enter the frame delay range bin threshold configuration.

ifdv — Keyword to enter the inter-frame delay variation bin thresholds configuration.

Platforms All

6.64 bind-authentication

bind-authentication

Syntax **bind-authentication** *root-dn* [**password** *password*] [**hash** | **hash2** | **custom**]
no bind-authentication

Context **[Tree]** (config>system>security>ldap>server bind-authentication)

Full Context configure system security ldap server bind-authentication

Description This command configures the LDAP binding used to log into LDAP server. A string of domain components (DC) and common names (CN) can be programmed to identify the user in addition to the password field. The password is hashed. For example, “cn=admin,dc=nokia,dc=com” indicates the user admin in domain nokia.com. Table 34 lists the LDAP attributes.

The **no** version of this command removes the bind-authentication.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 34 **LDAP Attributes**

Object Class	Naming Attribute Display Name	Naming Attribute LDAP Name
user	Common-Name	cn
organizationalUnit	Organizational-Unit-Name	ou
domain	Domain-Component	dc

Parameters *root-dn* — Up to 512 characters.

password — Configures the password which enables a user to bind to the LDAP server. The maximum length is 128 characters.

hash — Specifies that the password is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the password is assumed to be in an unencrypted, clear text form. For security, all passwords are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the password is entered in a more complex encrypted form that involves more variables than the password value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the password is assumed to be in an unencrypted, clear text form. For security, all passwords are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

6.65 binding

binding

Syntax **binding**

Context **[Tree]** (config>service>sdp binding)

Full Context configure service sdp binding

Description Commands in this context configure SDP bindings.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.66 binding-label

binding-label

Syntax **binding-label** *label-number*
no binding-label

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy binding-label)

Full Context configure router mpls forwarding-policies forwarding-policy binding-label

Description This command configures a binding label for the MPLS forwarding policy.

The policy associates an incoming label, referred to as a binding label, to an NHG in which the primary and backup direct or indirect next hops are defined. This type of MPLS forwarding policy is referred to as a label-binding policy.

The **no** form of the command removes the binding label from the MPLS forwarding policy.

Parameters *label-number* — Specifies the label number.

Values 32 to 1048575

Platforms All

6.67 binding-operator

binding-operator

Syntax **binding-operator** {**and** | **or**}
no binding-operator

Context **[Tree]** (config>filter>redirect-policy-binding binding-operator)

Full Context configure filter redirect-policy-binding binding-operator

Description This command configures the logical operator to use with the destinations test results to obtain the master test result (the redirect-policy binding test result). A change in this configuration results in the re-evaluation of the master test result.

The **no** version of this command sets the value to its default

Default binding-operator and

Parameters **and | or** — Keyword to specify the type of logical or boolean operation to perform between the individual destinations test results to obtain the master result.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

6.68 binding-sid

binding-sid

Syntax **binding-sid** *number*
no binding-sid

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy binding-sid)

Full Context configure router segment-routing sr-policies static-policy binding-sid

Description This command associates a binding SID with a statically defined segment routing policy. This is a mandatory parameter and configuration command to enable the segment routing policy; if the binding SID label value is not configured, the execution of the **no shutdown** command on the static segment routing policy fails.The BSID label should be an available label in the **reserved-label-block** range.

The **no** form of this command removes the BSID association.

Default no binding-sid

Parameters *number* — Specifies the binding SID label value.

Values 32 to 1048575

Platforms All

6.69 bindings

bindings

Syntax [**no**] **bindings**

Context **[Tree]** (debug>router>ldp>peer>event bindings)

Full Context debug router ldp peer event bindings

Description This command displays debugging information about addresses and label bindings learned from LDP peers for LDP bindings.

The **no** form of the command disables the debugging output.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

6.70 bit-error-insertion

bit-error-insertion

Syntax **bit-error-insertion** *rate*
no bit-error-insertion

Context **[Tree]** (config>port>tdm>ds1 bit-error-insertion)
[Tree] (config>port>tdm>ds3 bit-error-insertion)
[Tree] (config>port>tdm>e1 bit-error-insertion)
[Tree] (config>port>tdm>e3 bit-error-insertion)

Full Context configure port tdm ds1 bit-error-insertion
configure port tdm ds3 bit-error-insertion
configure port tdm e1 bit-error-insertion
configure port tdm e3 bit-error-insertion

Description This command inserts bit errors into a running BERT test. The number of errors inserted corresponds to 10^(-rate). A rate of 0 will cause 1 error in every bit transmitted. A rate of 7 will cause an error rate of 10^(-7), or 1 error in every one billion bits transmitted.

The no command disables the insertion of bit errors into the bit error rate test stream.

Note that this command is not saved in the router configuration between boots.

Default no bit-error-insertion

Parameters *rate* — Specifies the bit error rate, expressed as an integer.

Values 2 to 7

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

6.71 bit-error-threshold

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>lag>eth-cfm>mep bit-error-threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure eth-tunnel path eth-cfm mep eth-test-enable bit-error-threshold
configure lag eth-cfm mep bit-error-threshold

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default bit-error-threshold 1

Parameters *bit-errors* — Specifies the lowest priority defect.

Values 0 to 11840

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bit-error-threshold

Syntax **bit-error-threshold** *errors*
no bit-error-threshold

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>eth-test-enable bit-error-threshold)

Full Context configure service epipe sap eth-cfm mep eth-test-enable bit-error-threshold
configure service epipe spoke-sdp eth-cfm mep eth-test-enable bit-error-threshold

Description This command is used to specify the threshold value of bit errors.

Parameters *errors* — The threshold value of bit errors.

Values 0 to 11840

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context **[Tree]** (config>service>vpls>sap>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>service>vpls>eth-cfm>mep>eth-test-enable bit-error-threshold)

Full Context configure service vpls eth-cfm mep eth-test-enable bit-error-threshold
configure service vpls mesh-sdp eth-cfm mep eth-test-enable bit-error-threshold
configure service vpls sap eth-cfm mep eth-test-enable bit-error-threshold
configure service vpls spoke-sdp eth-cfm mep eth-test-enable bit-error-threshold

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default bit-error-threshold 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *bit-errors* — Specifies the lowest priority defect.

Values 0 to 11840

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>eth-test-enable bit-error-threshold)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>eth-test-enable bit-error-threshold)

Full Context configure service ies interface sap eth-cfm mep eth-test-enable bit-error-threshold
configure service ies interface spoke-sdp eth-cfm mep eth-test-enable bit-error-threshold
configure service ies subscriber-interface group-interface sap eth-cfm mep eth-test-enable bit-error-threshold

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default bit-error-threshold 1

Parameters *bit-errors* — Specifies the lowest priority defect.

Values 0 to 11840

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep eth-test-enable bit-error-threshold

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep eth-test-enable bit-error-threshold
- configure service ies interface sap eth-cfm mep eth-test-enable bit-error-threshold

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep bit-error-threshold)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep bit-error-threshold)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm bit-error-threshold)

Full Context configure service vprn interface sap eth-cfm mep bit-error-threshold
configure service vprn interface spoke-sdp eth-cfm mep bit-error-threshold
configure service vprn subscriber-interface group-interface sap eth-cfm bit-error-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default bit-error-threshold 1

Parameters *bit-errors* — Specifies the lowest priority defect.

Values 0 to 11840

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context **[Tree]** (config>router>if>eth-cfm>mep>eth-test-enable bit-error-threshold)

Full Context configure router interface eth-cfm mep eth-test-enable bit-error-threshold

Description This command specifies the lowest priority defect that generates a fault alarm.

Default bit-error-threshold 1

Parameters *bit-errors* — Specifies the priority defect threshold.

Values 0 to 11840

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bit-error-threshold

Syntax **bit-error-threshold** *bit-errors*

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>eth-test-enable bit-error-threshold)

Full Context configure eth-ring path eth-cfm mep eth-test-enable bit-error-threshold

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default bit-error-threshold 1

Parameters *bit-errors* — Specifies the lowest priority defect.

Values 0 to 11840

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.72 bit-rate-high-wmark

bit-rate-high-wmark

Syntax **bit-rate-high-wmark** *high-watermark*

Context **[Tree]** (config>application-assurance bit-rate-high-wmark)

Full Context configure application-assurance bit-rate-high-wmark

Description This command configures the high watermark for bit rate alarms.

Default bit-rate-high-wmark max

Parameters *high-watermark* — Specifies the high watermark for bit rate alarms, in Mb/s. The value must be larger than or equal to the low watermark value.

Values 1 to 40000, **max** (disabled)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.73 bit-rate-low-wmark

bit-rate-low-wmark

Syntax **bit-rate-low-wmark** *low-watermark*
no bit-rate-low-wmark

Context **[Tree]** (config>application-assurance bit-rate-low-wmark)

Full Context configure application-assurance bit-rate-low-wmark

Description This command configures the utilization of the flow records on the ISA-AA Group when the full alarm will be cleared by the agent.

Default bit-rate-low-wmark 0

Parameters *low-watermark* — Specifies the low watermark for bit rate alarms, in Mb/s. The value must be lower than or equal to the high watermark value.

Values 0 to 39999

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.74 bits

bits

Syntax **bits**

Context **[Tree]** (config>system>sync-if-timing bits)

Full Context configure system sync-if-timing bits

Description Commands in this context configure parameters for the Building Integrated Timing Supply (BITS). The settings specified under this context apply to both the BITS input and BITS output ports.

The **bits** command subtree is only available on the 7450 ESS-7, 7450 ESS-12, 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7950 XRS-20, 7950 XRS-40, 7750 SR-a4, 7750 SR-a8, 7750 SR-1e, 7750 SR-2e, and 7750 SR-3e.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.75 bits-interface-type

bits-interface-type

Syntax **bits-interface-type** {**ds1** [{**esf** | **sf**}] | **e1** [{**pcm30crc** | **pcm31crc**}
no bits-interface-type

Context **[Tree]** (config>system>sync-if-timing>ref1 bits-interface-type)
[Tree] (config>system>sync-if-timing>ref2 bits-interface-type)

Full Context configure system sync-if-timing ref1 bits-interface-type
configure system sync-if-timing ref2 bits-interface-type

Description This command configures the interface type of the BITS timing reference.

The **no** form of the command reverts to the default configuration

Parameters **ds1 esf** — Specifies Extended Super Frame (ESF). This is a framing type used on DS1 circuits that consists of 24 192-bit frames, The 193rd bit provides timing and other functions.

ds1 sf — Specifies Super Frame (SF), also called D4 framing. This is a common framing type used on DS1 circuits. SF consists of 12 192-bit frames. The 193rd bit provides error checking and other functions. ESF supersedes SF.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

e1 pcm30crc — Specifies the pulse code modulation (PCM) type. PCM30CRC uses PCM to separate the signal into 30 user channels with CRC protection.

e1 pcm31crc — Specifies the pulse code modulation (PCM) type. PCM31CRC uses PCM to separate the signal into 31 user channels with CRC protection.

6.76 black-hole

black-hole

Syntax [**no**] **black-hole**

Context **[Tree]** (config>service>vprn>static-route-entry black-hole)

Full Context configure service vprn static-route-entry black-hole

Description This command specifies that the route is a black hole route. If the destination address on a packet matches this static route, it will be silently discarded.

Default no black-hole

Platforms All

black-hole

Syntax [**no**] **black-hole**

Context **[Tree]** (config>router>static-route-entry black-hole)

Full Context configure router static-route-entry black-hole

Description This command specifies that the route is a black hole route. If the destination address on a packet matches this static route, it will be silently discarded.

Default no black-hole

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.77 black-hole-dup-mac

black-hole-dup-mac

Syntax [**no**] **black-hole-dup-mac**

Context **[Tree]** (config>service>vpls>bgp-evpn>mac-duplication black-hole-dup-mac)

Full Context configure service vpls bgp-evpn mac-duplication black-hole-dup-mac

Description The **black-hole-dup-mac** command is disabled by default. If enabled, a duplicated MAC detected in the network is programmed as a black-hole MAC in the FDB and displayed in the **show service id fdb detail** command as follows:

- Source-Identifier—black-hole
- Type—EvpnD:P

Because the MAC is now programmed in the FDB as a black-hole, all received frames with MAC DA matching the duplicate MAC are discarded. The duplicate black-hole MACs are installed as Protected, therefore, all received frames with MAC SA matching the duplicate MAC are discarded by default.

A BGP-EVPN (MPLS or VXLAN) shutdown is required to add or remove the **black-hole-dup-mac** command.

The **no** form of the command removes the feature, and duplicate MACs are no longer programmed as black-hole MACs.

Default no black-hole-dup-mac

Platforms All

6.78 blackhole-aggregate

blackhole-aggregate

Syntax [**no**] **blackhole-aggregate**

Context **[Tree]** (config>service>vprn>ospf>area blackhole-aggregate)
[Tree] (config>service>vprn>ospf3>area blackhole-aggregate)

Full Context configure service vprn ospf area blackhole-aggregate
configure service vprn ospf3 area blackhole-aggregate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command installs a low priority blackhole route for the entire aggregate. Existing routes that make up the aggregate have a higher priority and only the components of the range for which no route exists are blackholed.

It is possible that when performing area aggregation, addresses may be included in the range for which no actual route exists. This can cause routing loops. To avoid this problem, configure the **blackhole-aggregate** command.

The **no** form of this command removes this configuration.

Default blackhole-aggregate

Platforms All

blackhole-aggregate

Syntax [**no**] **blackhole-aggregate**

Context **[Tree]** (config>router>ospf>area blackhole-aggregate)
[Tree] (config>router>ospf3>area blackhole-aggregate)

Full Context configure router ospf area blackhole-aggregate
configure router ospf3 area blackhole-aggregate

Description This command installs a low priority blackhole route for the entire aggregate. Existing routes that make up the aggregate will have a higher priority and only the components of the range for which no route exists are blackholed.

When performing area aggregation, addresses may be included in the range for which no actual route exists, which can cause routing loops. To avoid this problem, configure the **blackhole-aggregate** option.

The **no** form of this command removes this option.

Default blackhole-aggregate

Platforms All

6.79 block-length

block-length

Syntax **block-length** *block-length*
no block-length

Context **[Tree]** (config>router>segment-routing>srv6>locator block-length)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router segment-routing segment-routing-v6 locator block-length

Description This command configures the length of the block field of a SRv6 locator.

The **no** form of this command reverts to the default value.

Default block-length 0

Parameters *block-length* — Specifies the block length, in bits, for the SRv6 locator. This value must be less than the locator prefix length and is enforced by CLI validation.

Values 0 to 96

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

6.80 block-limit

block-limit

Syntax **block-limit** [**1..40**]
no block-limit

Context **[Tree]** (config>service>nat>nat-policy block-limit)

Full Context configure service nat nat-policy block-limit

Description This command configures the maximum number of port blocks per subscriber.

The **no** form of the command reverts to the default.

Default block-limit 1

Parameters *1..40* — Specifies the maximum number of port-blocks per NAT subscriber.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.81 block-on-mesh-failure

block-on-mesh-failure

Syntax [**no**] **block-on-mesh-failure**

Context **[Tree]** (config>service>vpls>endpoint block-on-mesh-failure)
[Tree] (config>service>vpls>spoke-sdp block-on-mesh-failure)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls endpoint block-on-mesh-failure
configure service vpls spoke-sdp block-on-mesh-failure

Description This command enables blocking (brings the entity to an operationally down state) after all configured SDPs or endpoints are in operationally down state. This event is signaled to corresponding T-LDP peer by withdrawing service label (status-bit-signaling non-capable peer) or by setting “PW not forwarding” status bit in T-LDP message (status-bit-signaling capable peer).

The **no** form of this command reverts to the default.

Default no block-on-mesh-failure

Platforms All

6.82 block-on-peer-fault

block-on-peer-fault

Syntax [**no**] **block-on-peer-fault**

Context **[Tree]** (config>service>epipe>spoke-sdp block-on-peer-fault)

Full Context configure service epipe spoke-sdp block-on-peer-fault

Description When enabled, this command blocks the transmit direction of a PW when any of the following PW status codes is received from the far end PE:

0x00000001	Pseudowire Not Forwarding
0x00000002	Local Attachment Circuit (ingress) Receive Fault
0x00000004	Local Attachment Circuit (egress) Transmit Fault
0x00000008	Local PSN-facing PW (ingress) Receive Fault
0x00000010	Local PSN-facing PW (egress) Transmit Fault

The transmit direction is unblocked when the following PW status code is received:

0x00000000	Pseudowire forwarding (clear all failures)

This command is mutually exclusive with **no pw-status-signaling**, and **standby-signaling-slave**. It is not applicable to spoke SDPs forming part of an MC-LAG or spoke SDPs in an endpoint.

Default no block-on-peer-fault

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

block-on-peer-fault

Syntax [**no**] **block-on-peer-fault**

Context **[Tree]** (config>service>pw-template block-on-peer-fault)

Full Context configure service pw-template block-on-peer-fault

Description When enabled, this command blocks the transmit direction of a pseudowire when any of the following pseudowire status codes is received from the far end PE:

0x00000001	Pseudowire Not Forwarding
0x00000002	Local Attachment Circuit (ingress) Receive Fault
0x00000004	Local Attachment Circuit (egress) Transmit Fault
0x00000008	Local PSN-facing PW (ingress) Receive Fault
0x00000010	Local PSN-facing PW (egress) Transmit Fault

The transmit direction is unblocked when the following pseudowire status code is received:

0x00000000	Pseudowire forwarding (clear all failures)

This command is mutually exclusive with **no pw-status-signaling**, and **standby-signaling-slave**. It is not applicable to spoke SDPs forming part of an MC-LAG or spoke SDPs in an endpoint.

Default no block-on-peer-fault

Platforms All

6.83 block-prefix-sid

block-prefix-sid

Syntax [**no**] **block-prefix-sid**

Context **[Tree]** (config>router>bgp block-prefix-sid)
[Tree] (config>router>bgp>group block-prefix-sid)
[Tree] (config>router>bgp>group>neighbor block-prefix-sid)

Full Context configure router bgp block-prefix-sid

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group block-prefix-sid
configure router bgp group neighbor block-prefix-sid

Description This command specifies whether all prefix SID attributes are removed from label IPv4 and label IPv6 routes when they are exchanges with EBGP and IBGP peers covered by the scope of the command. Even locally-imposed prefix SID attributes are removed.

A change of this configuration causes the affected BGP sessions to flap.

The **no** form of this command allows prefix SID attributes associated with label IPv4 and label IPv6 routes to be propagated without restriction.

Default no block-prefix-sid

Platforms All

6.84 bluetooth

bluetooth

Syntax **bluetooth**

Context **[Tree]** (config>system bluetooth)

Full Context configure system bluetooth

Description Commands in this context configure Bluetooth console attributes.

Platforms 7750 SR-1, 7750 SR-s

6.85 bmp

bmp

Syntax **bmp**

Context **[Tree]** (config bmp)

Full Context configure bmp

Description Commands in this context configure BGP Monitoring Protocol (BMP) parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bmp

Syntax **bmp**

Context **[Tree]** (debug>router bmp)

Full Context debug router bmp

Description Commands in this context debug BMP information.

Platforms All

6.86 bof

bof

Syntax **bof**

Context **[Tree]** (bof)

Full Context bof

Description This command creates or edits the boot option file (BOF) for the specified local storage device.

A BOF file specifies where the system searches for runtime images, configuration files, and other operational parameters during system initialization.

BOF parameters can be modified. Changes can be saved to a specified compact flash. The BOF must be located in the root directory of either an internal or external compact flash local to the system and have the mandatory filename of *bof.cfg*.

When modifications are made to in-memory parameters that are currently in use or operating, the changes are effective immediately. For example, if the IP address of the management port is changed, the change takes place immediately.

Only one entry of the BOF configuration command statement can be saved once the statement has been found to be syntactically correct.

When opening an existing BOF that is not the BOF used in the most recent boot, a message is issued notifying the user that the parameters will not affect the operation of the node.

No default boot option file exists. The router boots with the factory default boot sequence and options.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.87 bonding-active-connections

bonding-active-connections

Syntax [**no**] **bonding-active-connections**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute bonding-active-connections)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute bonding-active-connections

Description This command triggers the inclusion of the Alc-Bonding-Active-Connection VSA in accounting for bonding subscribers.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.88 bonding-id

bonding-id

Syntax [**no**] **bonding-id**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute bonding-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute bonding-id

Description This command triggers the inclusion of the Alc-Bonding-Id VSA in accounting for bonding subscribers.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.89 bonding-parameters

bonding-parameters

Syntax **bonding-parameters**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>sub-if>grp-if bonding-parameters)
[Tree] (config>service>ies>sub-if>grp-if bonding-parameters)

Full Context configure service ies subscriber-interface group-interface bonding-parameters
configure service vprn subscriber-interface group-interface bonding-parameters

Description Commands in this context configure ESM connection bonding parameters. The configuration of parameters under this context is only allowed when the group interface is created with the bonding parameter specified.

6.90 bonding-selection

bonding-selection

Syntax bonding-selection

Context [Tree] (config>subscr-mgmt>sla-profile>egress bonding-selection)

Full Context configure subscriber-mgmt sla-profile egress bonding-selection

Description Commands in this context configure parameters belonging to this node for link selection behavior in a bonding context. These parameters are ignored outside of bonding subscribers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.91 booking-factor

booking-factor

Syntax **booking-factor** *factor*
no booking-factor

Context [Tree] (config>lag>access booking-factor)
[Tree] (config>port>ethernet>access booking-factor)

Full Context configure lag access booking-factor
configure port ethernet access booking-factor

Description This command specifies the booking factor applied against the port or LAG administrator bandwidth by SAP administrator bandwidth CAC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The service manager keeps track of the available administrator bandwidth for each port or LAG configured with an administrator bandwidth. The port or LAG available administrator bandwidth is adjusted by the user configured booking factor, allowing the port or LAG bandwidth to be over or under booked.

If the booking factor is increased then available administrator bandwidth on the port or LAG increases. If the booking factor is decreased then available administrator bandwidth on the port or LAG decreases, however, if the reduction of available administrator bandwidth would cause it to be insufficient to cover the sum of the current SAP administrator bandwidth on the port or LAG then the command fails.

The **no** form of this command reverts to the default value.

Default booking-factor 100

Parameters *factor* — Specifies the percentage of the port or LAG admin bandwidth for SAP bandwidth CAC.

Values 1 to 1000

Platforms All

booking-factor

Syntax **booking-factor** *percentage*
no booking-factor

Context **[Tree]** (config>service>sdp booking-factor)

Full Context configure service sdp booking-factor

Description This command specifies the booking factor applied against the maximum SDP available bandwidth by the VLL CAC feature.

The service manager keeps track of the available bandwidth for each SDP. The maximum value is the sum of the bandwidths of all constituent LSPs in the SDP. The SDP available bandwidth is adjusted by the user configured booking factor. A value of 0 means no VLL can be admitted into the SDP.

The **no** form of the command reverts to the default value.

Default no booking-factor

Parameters *percentage* — Specifies the percentage of the SDP maximum available bandwidth for VLL call admission. When the value of this parameter is set to zero (0), no new VLL spoke SDP bindings with non-zero bandwidth are permitted with this SDP. Overbooking, >100% is allowed.

Values 0 to 1000%

Default 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

6.92 boot-bad-exec

boot-bad-exec

Syntax **boot-bad-exec** *file-url*
no boot-bad-exec

Context **[Tree]** (config>system boot-bad-exec)

Full Context configure system boot-bad-exec

Description Use this command to configure a URL for a CLI script to **exec** following a failure of a bootup configuration. The command specifies a URL for the CLI scripts to be run following the completion of the bootup configuration. A URL must be specified or no action is taken.

The commands are persistent between router (re)boots and are included in the configuration saves (**admin>save**).

Related Commands

exec — This command executes the contents of a text file as if they were CLI commands entered at the console.

Default no boot-bad-exec

Parameters *file-url* — Specifies the location and name of the CLI script file executed following failure of the bootup configuration file execution. When this parameter is not specified, no CLI script file is executed.

Ipv6-address only applies to the 7750 SR and 7950 XRS.

Values

file url	*local-url* | *remote-url*	255 chars max
local-url	[*cflash-id*/][*file-path*]	
remote-url	[{ftp://} *login:pswd@remote-locn*/][*file-path*]	
	remote-locn	[*hostname* | *ipv4-address* | [*ipv6- address*]]
	ipv4-address	*a.b.c.d*
	ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
		x:x:x:x:x:x:d.d.d.d[-*interface*]
		x - [0 to FFFF]H
		d - [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

		interface - 32 chars max, for link local addresses
	cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

6.93 boot-good-exec

boot-good-exec

Syntax **boot-good-exec** *file-url*
no boot-good-exec

Context **[Tree]** (config>system boot-good-exec)

Full Context configure system boot-good-exec

Description Use this command to configure a URL for a CLI script to **exec** following the success of a bootup configuration.

Related Commands

exec - This command executes the contents of a text file as if they were CLI commands entered at the console.

Default no boot-good-exec

Parameters *file-url* — Specifies the location and name of the file executed following successful completion of the bootup configuration file execution. When this parameter is not specified, no CLI script file is executed.

Ipv6-address only applies to the 7750 SR and 7950 XRS and ipv4-address applies to the 7450 ESS.

Values

file url	*local-url* | *remote-url*	255 chars max
local-url	[*cflash-id*/][*file-path*]	
remote-url	[{ftp://} *login:pswd@remote-locn*/][*file-path*]	
	remote-locn	[*hostname* | *ipv4-address* | [*ipv6- address*]]
	ipv4-address	*a.b.c.d*
	ipv6-address	*x:x:x:x:x:x:x:x*[*-interface*]
		x:x:x:x:x:x:d.d.d.d[*-interface*]
		x - [0 to FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

		d - [0 to 255]D *interface* - 32 chars max, for link local addresses
	cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

6.94 boot-timer

boot-timer

Syntax **boot-timer** *interval*
no boot-timer

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ep boot-timer)

Full Context configure redundancy multi-chassis peer mc-endpoint boot-timer

Description This command configures the boot timer interval. This command applies only when the node reboots. It specifies the time the MC-EP protocol keeps trying to establish a connection before assuming a failure of the remote peer. This is different from the keep-alive mechanism which is used just after the peer-peer communication was established. After this time interval passed all the mc-endpoints configured under services will revert to single chassis behavior, activating the best local PW.

The **no** form of this command sets the interval to default.

Default no boot-timer

Parameters *interval* — Specifies the boot timer interval.

Values 1 to 600

Platforms All

boot-timer

Syntax **boot-timer** *seconds*

Context **[Tree]** (config>redundancy>bgp-evpn-multi-homing boot-timer)

Full Context configure redundancy bgp-evpn-multi-homing boot-timer

Description This command allows the necessary time for the control plane protocols to come up upon PE boot-up before bringing up the ESs and running the DF algorithm.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The following considerations apply to this command:

- The **boot-timer** command must provide enough time to allow the IOMs and BGP sessions to come up before exchanging ES routes and running the DF election for each EVI or ISID.
- The boot-timer is synchronized across CPMs and is relative to the system up time; it is not changed or reset upon CPM switchover.
- The boot-timer is never interrupted (the e**s-activation-timer**, however, can be interrupted if there is a new event triggering the DF election).
- The boot-timer runs per EVI or ISID on the ESs in the system. If the system up time (time the system has been up since the last reboot) is less than the **boot-timer** value, the system does not run the DF election for any EVI or ISID. When the **boot-timer** value expires, the DF election runs, and if the system is elected DF for the EVI or ISID, the **es-activation-timer** is triggered.
- The system does not advertise ES routes until the boot timer expires, which guarantees that the peer ES PEs only run the DF election when the PE is ready to become the DF, if required.

Default boot-timer 10

Parameters *seconds* — Specifies the number of seconds for the boot-timer.

Values 0 to 1800

Platforms All

boot-timer

Syntax **boot-timer** *seconds*
no boot-timer

Context **[Tree]** (config>service>vpls>site boot-timer)

Full Context configure service vpls site boot-timer

Description This command configures for how long the service manager waits after a node reboot before running the DF election algorithm. The boot-timer value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed/exchanged.

The **no** form of this command reverts the default.

Default boot-timer 10

Parameters *seconds* — Specifies the site boot-timer in seconds.

Values 0 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

boot-timer

Syntax **boot-timer** *seconds*
no boot-timer

Context **[Tree]** (config>service>epipe>site boot-timer)

Full Context configure service epipe site boot-timer

Description This command configures for how long the service manager waits after a node reboot before running the DF election algorithm. The boot-timer value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed/exchanged.

The **no** form of this command reverts the default.

Default boot-timer 10

Parameters *seconds* — Specifies the site boot-timer in seconds.

Values 0 to 600

Platforms All

boot-timer

Syntax **boot-timer** *secs*
no boot-timer

Context **[Tree]** (config>service>pw-routing boot-timer)

Full Context configure service pw-routing boot-timer

Description This command configures a hold-off timer for MS-PW routing advertisements and signaling and is used at boot time.

The **no** form of this command removes a previously configured timer and restores it to its default.

Default no boot-timer

Parameters *timer-value* — Specifies the value of the boot timer in seconds.

Values 0 to 600

Platforms All

boot-timer

Syntax **boot-timer** *seconds*
no boot-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>redundancy>bgp-multi-homing boot-timer)

Full Context configure redundancy bgp-multi-homing boot-timer

Description This command configures the time the service manager waits after a node reboot before running the DF election algorithm. The **boot-timer** value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed or exchanged.

The **no** form of the command reverts the default.

Default no boot-timer

Parameters *seconds* — Specifies the BGP multi-homing boot-timer in seconds.

Values 0 to 600

Platforms All

6.95 bootstrap-export

bootstrap-export

Syntax **bootstrap-export** *policy-name* [*policy-name*]
no bootstrap-export

Context [Tree] (config>service>vprn>pim>rp bootstrap-export)

Full Context configure service vprn pim rp bootstrap-export

Description This command exports policies to control the flow of bootstrap messages from the RP. Up to five policies can be defined.

The **no** form of this command removes the specified policy names from the configuration.

Parameters *policy-name* — Specifies up to five policy names. The policy statement must already be configured in the **config>router>policy-options** context.

Platforms All

bootstrap-export

Syntax **bootstrap-export** *policy-name* [*policy-name*]
no bootstrap-export

Context [Tree] (config>router>pim>rp bootstrap-export)

Full Context configure router pim rp bootstrap-export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command applies export policies to control the flow of bootstrap messages from the RP, and apply them to the PIM configuration.

The **no** form of this command removes the policy name from the PIM RP configuration.

Default no bootstrap-export

Parameters *policy-name* — Specifies up to five export policy names, up to 32 characters.

Platforms All

6.96 bootstrap-import

bootstrap-import

Syntax **bootstrap-import** *policy-name* [*policy-name*... **up to five**]
no bootstrap-import *policy-name* [*policy-name*... **up to five**]

Context **[Tree]** (config>service>vprn>pim>rp bootstrap-import)

Full Context configure service vprn pim rp bootstrap-import

Description This command imports policies to control the flow of bootstrap messages into the RP. Up to five policies can be defined.

The **no** form of this command removes the specified policy names from the configuration.

Parameters *policy-name* — Specifies the policy name. The policy statement must already be configured in the config>router>policy-options context.

Platforms All

bootstrap-import

Syntax **bootstrap-import** *policy-name* [*policy-name*]
no bootstrap-import

Context **[Tree]** (config>router>pim>rp bootstrap-import)

Full Context configure router pim rp bootstrap-import

Description This command applies import policies to control the flow of bootstrap messages to the RP, and apply them to the PIM configuration.

The **no** form of this command removes the policy name from the

Default no bootstrap-import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies up to five import policy names, up to 32 characters.

Platforms All

6.97 boundary-type

boundary-type

Syntax **boundary-type** {**clock-aligned** | **test-relative**}
no boundary-type

Context **[Tree]** (config>oam-pm>session>meas-interval boundary-type)

Full Context configure oam-pm session meas-interval boundary-type

Description This command establishes the alignment of the start of the measurement interval with either the time of day clock or the start of the test. Alignment with the time of day clock always defaults to the representative top of the hour. Clock-aligned 15-minute measurement intervals divide the hour into four equal sections 00, 15, 30, 45. Clock-aligned 1-hour measurement intervals start at 00. Clock-aligned 1-day measurement intervals start at midnight. Test relative start times launches the measurement interval when the individual test enters the active (**no shutdown**) state. It is typical for the first measurement interval of a clock-aligned test to have the suspect flag set to yes because it is unlikely the **no shutdown** exactly corresponds to the clock based measurement interval start time. Clock-aligned measurement intervals can include an additional offset.

The **no** form of this command sets the boundary to the default clock-aligned.

Default boundary-type clock-aligned

Parameters **clock-aligned** — Aligns the start of the measurement interval with the time of day clock.

test-relative — Aligns the start of the measurement interval with the start of the test.

Platforms All

6.98 bpdu

bpdu

Syntax [**no**] **bpdu**

Context **[Tree]** (debug>service>id>stp bpdu)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug service id stp bpdu

Description This command enables STP debugging for received and transmitted BPDUs.

Platforms All

bpdu

Syntax [**no**] **bpdu**

Context **[Tree]** (debug>service>id>stp bpdu)

Full Context debug service id stp bpdu

Description This command enables STP debugging for received and transmitted BPDUs.

The **no** form of the command disables debugging.

Platforms All

6.99 bpdu-translation

bpdu-translation

Syntax **bpdu-translation** {**auto** | **auto-rw** | **pvst** | **pvst-rw** | **stp**}
no bpdu-translation

Context **[Tree]** (config>service>vpls>spoke-sdp bpdu-translation)
[Tree] (config>service>vpls>sap bpdu-translation)

Full Context configure service vpls sap bpdu-translation
configure service vpls spoke-sdp bpdu-translation

Description This command enables the translation of BPDUs to a specified format, meaning that all BPDUs transmitted on a specified SAP or spoke-SDP will have a specified format.

The **no** form of this command reverts to the default.

Default no bpdu-translation

Parameters **auto** — Specifies that appropriate format will be detected automatically, based on type of BPDUs received on such port.

auto-rw — Specifies that appropriate format will be detected automatically and the VLAN ID will be rewritten as follows:

- BPDU sent on egress of dot1q SAP will contain the VLAN ID of the SAP in BPDU-PVID TLV

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- BPDU sent on egress of default QinQ SAP will contain the outer VLAN ID of the SAP in BPDU-PVID TLV
- BPDU sent on egress of QinQ SAP will contain the inner VLAN ID of the SAP in BPDU-PVID TLV

pvst — Specifies the BPDU-format as PVST. Note: the correct VLAN tag is included in the payload (depending on encapsulation value of outgoing SAP).

pvst-rw — Specifies the BPDU-format as PVST. The VLAN ID will be rewritten as follows:

- BPDU sent on egress of dot1q SAP will contain the VLAN ID of the SAP in BPDU-PVID TLV
- BPDU sent on egress of default QinQ SAP will contain the outer VLAN ID of the SAP in BPDU-PVID TLV
- BPDU sent on egress of QinQ SAP will contain the inner VLAN ID of the SAP in BPDU-PVID TLV

stp — Specifies the BPDU-format as STP.

Platforms All

6.100 breakout

breakout

Syntax **breakout** *breakout*
no breakout

Context **[Tree]** (config>port>connector breakout)

Full Context configure port connector breakout

Description This command configures the transceiver port breakout for use in the connector. Specifying the breakout type triggers the creation of accessible ports for the connector.

When a QSFP28 connector uses an SFP+ optical module with the QSFP28-to-SFP+/SFP28 adapter, the user should set the *breakout* parameter to c1-10g, which indicates the presence of this adapter.

The **no** form of this command removes the ports under the connector.

Default no breakout

Parameters *breakout* — Specifies the breakout type.

Values c1-100g, c1-10g, c1-25g, c1-400g, c1-40g, c10-10g, c2-100g, c4-100g, c4-10g, c4-25g

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.101 brg

brg

Syntax **brg**

Context **[Tree]** (config>subscr-mgmt>vrgw brg)

Full Context configure subscriber-mgmt vrgw brg

Description Commands in this context configure Bridged Residential Gateway parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

brg

Syntax **brg**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw brg)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw brg)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range brg)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range brg)
[Tree] (config>service>ies>sub-if>grp-if brg)
[Tree] (config>service>vprn>sub-if>grp-if brg)

Full Context configure service ies subscriber-interface group-interface brg
configure service ies subscriber-interface group-interface wlan-gw ranges range brg
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw brg
configure service vprn subscriber-interface group-interface brg
configure service vprn subscriber-interface group-interface wlan-gw ranges range brg
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw brg

Description Commands in this context configure BRG parameters. In the **config>service>ies>sub-if>grp-if** and **config>service>vprn>sub-if>grp-if** contexts, these commands are only available in the **vlan-tag-ranges** level.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface brg
- configure service vprn subscriber-interface group-interface brg

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw brg
- configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw brg

6.102 brg-id

brg-id

Syntax [**no**] **brg-id** *brg-ident*

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg>pppoe-client brg-id)

Full Context debug subscriber-mgmt vrgw brg pppoe-client brg-id

Description This command enables debugging of PPPoE client messages linked to a BRG.

Parameters *brg-ident* — The string identifying the BRG.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

6.103 brg-num-active-sessions

brg-num-active-sessions

Syntax [**no**] **brg-num-active-sessions**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include brg-num-active-sessions)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute brg-num-active-sessions

Description This command indicates the number of IPoE sessions that are currently active on the BRG to which this accounting message relates. The **no** form of this command removes the attribute from inclusion.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.104 brg-profile

brg-profile

Syntax **brg-profile** *profile-name* [**create**]
no brg-profile *profile-name*

Context **[Tree]** (config>subscr-mgmt>vrgw>brg brg-profile)

Full Context configure subscriber-mgmt vrgw brg brg-profile

Description This command creates the profile for Bridged Residential Gateway (BRG) devices. The BRG profile specifies default parameters that are used for host management under a single BRG.

The **no** form of this command removes the profile name from the configuration.

Parameters *profile-name* — Specifies the name of the BRG profile.

create — Keyword used to create a BRG profile. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

6.105 bridge-identifier

bridge-identifier

Syntax **bridge-identifier** *bridge-id* **vlan** *vlan-id*

Context **[Tree]** (config>eth-cfm>default-domain bridge-identifier)

Full Context configure eth-cfm default-domain bridge-identifier

Description This command configures the cross-reference required to link the CFM function with the service context. The link is created when the **bridge-id**, **service-id**, and **vlan-id** (for a primary VLAN) match.

This command allows the entry of MIP-specific parameters for the index (**bridge-identifier** and **vlan**) in the default-domain table.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *bridge-id* — Specifies the ID for a link to a specific service. Note that there is no verification that a service has been created with a matching service ID.

Values 1 to 2147483647

vlan-id — Specifies the VLAN ID for the **default-domain** index. The complete index allows the user to reference specific MIP entries in the **default-domain** table. The *vlan-id* value must match the configured **primary-vlan-enable** *vlan-id* corresponding to the **bridge-identifier**. If the MIP does not have **primary-vlan-enable** configured, the *vlan-id* must be configured as "none". When the *vlan-id* is configured as none, the MIP relies on the service delineation for extraction and installs no additional VLAN in that portion of the index.

Values 1 to 4094 | none

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bridge-identifier

Syntax [**no**] **bridge-identifier** [*bridge-id* | **bridge-name** *bridge-name*]

Context **[Tree]** (config>eth-cfm>domain>assoc bridge-identifier)

Full Context configure eth-cfm domain association bridge-identifier

Description This command configures the cross-reference required to link the CFM function with the service context. The link is created when the *bridge-id*, or *bridge-name* matches the *service-id*, or *service-name*, respectively.

The **no** form of this command removes the bridge identifier and the link between the ETH-CFM configuration and the matching service.

There is no verification that any service has been created with a matching value. An existing bridge-identifier configuration can be overwritten with the alternate type, as long as the new reference does not change the existing service linkage.

Parameters *bridge-id* — Specifies the ID to link to a specific service. Note that there is no verification that a service has been created with a matching *service-id*.

This *bridge-id* variant of the command is only supported in classic configuration mode (**configure system management-interface configuration-mode classic**). The **bridge-identifier bridge-name** *bridge-name* variant can be used in all configuration modes. All references to **bridge-identifier** *bridge-id* must be changed to the **bridge-identifier bridge-name** *bridge-name* option as a prerequisite to model-driven mode.

Values 1 to 2147483647

bridge-name *bridge-name* — Specifies a link to a service with a matching *service-name*, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.106 bridge-priority

bridge-priority

Syntax **bridge-priority** *bridge-priority*
no bridge-priority

Context **[Tree]** (config>service>vpls>spb>level bridge-priority)

Full Context configure service vpls spb level bridge-priority

Description This command configures the four bit bridge priority for Shortest Path Bridging. This value is added to the 6 byte bridge Identifier (which is the system-id) in the top four bits of a two byte field. Note the actual value will be bit shifted 12 bits left effective putting this in the high bits of the 16 bits added to system ID.

The bridge priority is important in choosing the Root Bridge for the single tree algorithm (lowest value = best). Bridge priority also factors into the tie breaker for SPF algorithms as described in the SPB standard. The bridge-identifier (system-id) of the control B-VPLS determines the tiebreaker when the bridge-priorities are equal.

Default bridge-priority 8

Parameters *bridge-priority* — The bridge-priority value.

Values 0 to 15

Platforms All

6.107 broadcast

broadcast

Syntax **broadcast** {**interface** *ip-int-name*} [**key-id** *key-id*] [**version** *version*] [**ttl** *ttl*]
no broadcast {**interface** *ip-int-name*}

Context **[Tree]** (config>service>vprn>ntp broadcast)

Full Context configure service vprn ntp broadcast

Description This command configures the node to transmit NTP packets on a given interface. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended.

The **no** form of this command removes the address from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-int-name* — Specifies the local interface on which to transmit NTP broadcast packets. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Values 32 character maximum

key-id *key-id* — Identifies the configured authentication key and authentication type used by this node to receive and transmit NTP packets to and from an NTP server and peers. If an NTP packet is received by this node both authentication key and authentication type must be valid otherwise the packet will be rejected and an event/trap generated.

Values 1 to 255

version *version* — Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all versions will be accepted.

Values 2 to 4

Default 4

ttl *ttl* — Specifies the IP Time To Live (TTL) value.

Values 1 to 255

Platforms All

broadcast

Syntax **broadcast** [**router** *router-name*] {**interface** *ip-int-name*} [**key-id** *key-id*] [**version** *version*] [**ttl** *ttl*]
no broadcast [**router** *router-name*] {**interface** *ip-int-name*}

Context **[Tree]** (config>system>time>ntp broadcast)

Full Context configure system time ntp broadcast

Description This command configures the node to transmit NTP packets on a given interface. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended.

The **no** form of this command removes the address from the configuration.

Parameters *router-name* — Specifies the router name used to transmit NTP packets. Base is the default. Select management to use the management port (Ethernet port on the CPM). Note that broadcast server capability can also be enabled on an interface within a VPRN context. Refer to “NTP Within a VPRN Service” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* for more information.

Values Base | Management

Default Base

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-int-name — Specifies the local interface on which to transmit NTP broadcast packets, up to 32 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

key-id — Identifies the configured authentication key and authentication type used by this node to receive and transmit NTP packets to and from an NTP server and peers. If an NTP packet is received by this node both authentication key and authentication type must be valid otherwise the packet will be rejected and an event or trap generated.

Values 1 to 255

version — Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all versions will be accepted.

Values 2 to 4

Default 4

ttl — Specifies the IP Time To Live (TTL) value.

Values 1 to 255

Platforms All

6.108 broadcast-client

broadcast-client

Syntax [**no**] **broadcast-client**

Context **[Tree]** (config>system>time>sntp broadcast-client)

Full Context configure system time sntp broadcast-client

Description This command enables listening to SNTP/NTP broadcast messages on interfaces with **broadcast client** enabled at global device level.

SNTP must be shutdown prior to changing either to or from broadcast mode.

The **no** form of the command disables broadcast client mode.

Default no broadcast-client

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.109 broadcast-policer

broadcast-policer

Syntax **broadcast-policer** *policer-id* [**fp-redirect-group**]
no broadcast-policer

Context **[Tree]** (config>qos>sap-ingress>fc broadcast-policer)

Full Context configure qos sap-ingress fc broadcast-policer

Description Within a **sap-ingress** QoS policy forwarding class context, the **broadcast-policer** command is used to map packets that match the forwarding class and are considered broadcast in nature to the specified policer-id. The specified policer-id must already exist within the **sap-ingress** QoS policy. While the system is determining the forwarding class of a packet, it is also looking up its forwarding destination based on the ingress service type and the service instance forwarding records. If the service type is VPLS and the destination MAC address is the broadcast address (ff:ff:ff:ff:ff:ff), the packet is classified into the broadcast forwarding type.

Broadcast forwarding type packets are mapped to either an ingress multipoint queue (using the **broadcast** *queue-id* or **broadcast** *queue-id* **group** *ingress-queue-group* commands) or an ingress policer (**broadcast-policer** *policer-id*). The **broadcast** and **broadcast-policer** commands within the forwarding class context are mutually exclusive. By default, the broadcast forwarding type is mapped to the SAP ingress default multipoint queue. If the **broadcast-policer** *policer-id* command is executed, any previous policer mapping or queue mapping for the broadcast forwarding type within the forwarding class is overridden if the policer mapping is successful.

A policer defined within the **sap-ingress** policy is not actually created on an ingress SAP or a subscriber using an **sla-profile** where the policy is applied until at least one forwarding type (unicast, broadcast, unknown, or multicast) from one of the forwarding classes is mapped to the policer. If insufficient policer resources exist to create the policer for a SAP or subscriber or multiservice site, or ingress policing is not supported on the port associated with the SAP or subscriber or multiservice site, the initial forwarding class forwarding type mapping will fail.

The **broadcast-policer** command is ignored for instances of the policer applied to SAPs or subscribers' multiservice site where broadcast packets are not supported.

When the broadcast forwarding type within a forwarding class is mapped to a policer, the broadcast packets classified to the subclasses within the forwarding class are also mapped to the policer.

The **no** form of this command is used to restore the mapping of the broadcast forwarding type within the forwarding class to the default multipoint queue. If all forwarding class forwarding types had been removed from the default multipoint queue, the queue will not exist on the SAPs or subscribers or multiservice site associated with the QoS policy and the **no broadcast-policer** command will cause the system to attempt to create the default multipoint

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue on each object. If the system cannot create the queue on each instance, the **no broadcast-policer** command will fail and the broadcast forwarding type within the forwarding class will continue its mapping to the existing policer-id. If the **no broadcast-policer** command results in a policer without any current mappings, the policer will be removed from the SAPs and subscribers associated with the QoS policy. All statistics associated with the policer on each SAP and subscriber will be lost.

Parameters *policer-id* — When the forwarding class **broadcast-policer** command is executed, a valid *policer-id* must be specified. The parameter *policer-id* references a *policer-id* that has already been created within the sap-ingress QoS policy.

Values 1 to 63

fp-redirect-group — Redirects a forwarding class to a forwarding plane queue-group as specified in a SAP QoS policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

6.110 broadcast-queue

broadcast-queue

Syntax **broadcast-queue** *queue-id* [**group** *queue-group-name*]
no broadcast queue

Context **[Tree]** (config>qos>sap-ingress>fc broadcast-queue)

Full Context configure qos sap-ingress fc broadcast-queue

Description This command overrides the default broadcast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all broadcast traffic on a SAP using this policy will be forwarded using the *queue-id*.

The broadcast forwarding type usually tracks the multicast forwarding type definition. This command overrides that default behavior.

The **no** form of this command sets the broadcast forwarding type *queue-id* back to the default of tracking the multicast forwarding type queue mapping.

Parameters *queue-id* — The *queue-id* parameter must be an existing, multipoint queue defined in the config>qos>sap-ingress context.

Values Any valid multipoint queue ID in the policy including 2 through 32.

Default 11

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group *queue-group-name* — This optional parameter is used to redirect the forwarding type within the forwarding class to the specified queue-id within the queue-group-name. When the policy is applied, all packets matching the forwarding class and forwarding type will be redirected to the queue within the specified queue group. The *queue-group-name* are configured in the **config>qos>queue-group-templates** egress and ingress contexts.

Platforms All

broadcast-queue

Syntax **broadcast-queue** *queue-id*

Context **[Tree]** (config>qos>shared-queue>fc broadcast-queue)

Full Context configure qos shared-queue fc broadcast-queue

Description This command configures the broadcast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all broadcast traffic on a SAP using this policy will be forwarded using the *queue-id*.

The broadcast forwarding type usually tracks the multicast forwarding type definition. This command overrides that default behavior.

The **no** form of this command sets the broadcast forwarding type *queue-id* back to the default of tracking the multicast forwarding type queue mapping.

Parameters *queue-id* — The *queue-id* parameter must specify an existing multipoint queue defined in the **config>qos>sap-ingress** context policer-output-queues profile. For the 7950 XRS, this is not configurable in the policer-output-queues profile.

Values 17 to 24

Platforms All

6.111 broadcastclient

broadcastclient

Syntax **broadcastclient** [**router** *router-instance* | **service-name** *service-name*] {**interface** *ip-int-name*} [**authenticate**]
no broadcastclient [**router** *router-instance* | **service-name** *service-name*] {**interface** *ip-int-name*}

Context **[Tree]** (config>system>time>ntp broadcastclient)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system time ntp broadcastclient

Description When configuring NTP, the node can be configured to receive broadcast packets on a specified subnet. This command configures a specific interface to listen for broadcast NTP messages. The interface may exist within a VPRN service.

Broadcast and multicast messages can easily be spoofed, so authentication is strongly recommended. If broadcast is not configured, then any received NTP broadcast traffic will be ignored. Use the **show** command to view the state of the configuration.

The **no** form of this command removes the interface from the configuration.

Parameters *router-instance* — Specifies the routing context that contains the interface in the form of *router-name* or *service-id*.

Values *router-name* — Base | Management
service-id — 1 to 2147483647

Default Base

service name — Specifies the service name for the VPRN. The name can be up to 64 characters in length. Note that CPM routing instances are not supported.

ip-int-name — Specifies the VPRN interface on which to receive NTP broadcast packets. If the string contains special characters (such as #, $, or spaces) the entire string must be enclosed within double quotes.

authenticate — Specifies whether or not to require authentication of NTP PDUs. When enabled, NTP PDUs are authenticated upon receipt.

Platforms All

6.112 bsm-check-rtr-alert

bsm-check-rtr-alert

Syntax [**no**] **bsm-check-rtr-alert**

Context **[Tree]** (config>service>vprn>pim>if bsm-check-rtr-alert)

Full Context configure service vprn pim interface bsm-check-rtr-alert

Description This command enables the checking of router alert option in the bootstrap messages received on this interface.

Default no bsm-check-rtr-alert

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bsm-check-rtr-alert

Syntax [**no**] **bsm-check-rtr-alert**

Context **[Tree]** (config>router>pim>interface bsm-check-rtr-alert)

Full Context configure router pim interface bsm-check-rtr-alert

Description This command enables the checking of the router alert option in the bootstrap messages received on this interface.

The **no** form of this command disables accepting BSM packets without the router alert option.

Default no bsm-check-rtr-alert

Platforms All

6.113 bsr

bsr

Syntax **bsr** {**unicast** | **spmsi**}
no bsr

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive bsr)

Full Context configure service vprn mvpn provider-tunnel inclusive bsr

Description This command configures the type of BSR signaling used.

The no form of this command restores the default.

Default **no** bsr

Parameters **unicast** — BSR PDUs are sent/forwarded using unicast PDUs (default).

spmsi — BSR PDUs are sent/forwarded using S-PMSI full mesh.

Platforms All

bsr

Syntax **bsr** [**detail**]
no bsr

Context **[Tree]** (debug>router>pim bsr)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router pim bsr

Description This command enables/disables debugging for the PIM bootstrap mechanism.

The **no** form of the command disables debugging.

Parameters **detail** — Debugs detailed information on the PIM bootstrap mechanism.

Platforms All

6.114 bsr-candidate

bsr-candidate

Syntax **bsr-candidate**

Context **[Tree]** (config>service>vprn>pim>rp bsr-candidate)
[Tree] (config>service>vprn>pim>rp>ipv6 bsr-candidate)

Full Context configure service vprn pim rp bsr-candidate
configure service vprn pim rp ipv6 bsr-candidate

Description Commands in this context configure Candidate Bootstrap (BSR) parameters.

Either **bsr-candidate** for IPv4 or **auto-rp-discovery** can be configured; the two mechanisms cannot be enabled together. **bsr-candidate** for IPv6 and **auto-rp-discovery** for IPv4 can be enabled together.

The **no** form of this command disables BSR.

Default no bsr-candidate

Platforms All

bsr-candidate

Syntax **bsr-candidate**

Context **[Tree]** (config>router>pim>rp bsr-candidate)
[Tree] (config>router>pim>rp>ipv6 bsr-candidate)

Full Context configure router pim rp bsr-candidate
configure router pim rp ipv6 bsr-candidate

Description Commands in this context configure Candidate Bootstrap (BSR) parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Either **bsr-candidate** for IPv4 or **auto-rp-discovery** can be configured; the two mechanisms cannot be enabled together. **bsr-candidate** for IPv6 and **auto-rp-discovery** for IPv4 can be enabled together.

Default bsr-candidate shutdown

Platforms All

6.115 buffer-allocation

buffer-allocation

Syntax **buffer-allocation min** *percentage* **max** *percentage*
no buffer-allocation

Context **[Tree]** (config>card>fp>egress>wred-queue-control buffer-allocation)

Full Context configure card fp egress wred-queue-control buffer-allocation

Description The buffer-allocation command defines the amount of buffers that will be set aside for WRED queue buffer pools. Note that the **min** *percentage* and max *percentage* parameters must be set to the same value. The forwarding plane protects against cross application buffer starvation by implementing a hierarchy of buffer pools. At the top of the hierarchy are mega-pools. Mega-pools are used to manage buffers at a system application level. Two mega-pools are currently used by the system. The first (default) mega-pool services all non-WRED type queues and when WRED queues are not enabled will contain all available forwarding plane queue buffers. When WRED queuing is enabled, the second mega-pool (the WRED mega-pool) is given buffers from the default mega-pool based on the buffer-allocation command.

The mega-pools provide buffers to the second tier buffer pools. The default mega-pool services all default pools. As the name implies, the WRED mega-pool services all the WRED buffer pools created for the WRED queues. The WRED mega-pool allows each WRED queue pool to be configured to an appropriate size while allowing the sum of the WRED queue pool sizes to oversubscribe the total amount set aside for WRED queue buffering without affecting the queues using the default pools.

No buffers are allocated to the WRED mega-pool until the wred-queue-control shutdown command is set to no shutdown. When the shutdown command is executed, all buffers allocated to the WRED mega-pool are returned to the default mega-pool and all WRED queues are returned to their default buffer pool.

The **no** form of this command immediately restores the default min and max percentage values for sizing the WRED mega-pool.

Default buffer-allocation min 25.00 max 25.00

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **min** *percentage* — Specifies that the required keyword defines the minimum percentage of total egress forwarding plane queue buffers that will be applied to the WRED mega-pool. The value given for *percentage* must be less than or equal to the value given for the **max** *percentage*. Percentages are defined with an accuracy of hundredths of a percent in the nn.nn format (15.65 = 15.65%).

Values 0.00 to 99.99

Default 25.00

max *percentage* — Specifies that the required keyword defines the maximum percentage of total egress forwarding plane queue buffers that may be applied to the WRED mega-pool. The value given for *percentage* must be equal to or greater than the value given for the **min** *percentage*. Percentages are defined with an accuracy of hundredths of a percent in the nn.nn format (15.65 = 15.65%).

Values 0.01 to 99.99

Default 25.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.116 buffer-pool

buffer-pool

Syntax **buffer-pool** *value*

Context **[Tree]** (config>port>sonet-sdh>path>atm>custom-buffer-mode buffer-pool)

Full Context configure port sonet-sdh path atm custom-buffer-mode buffer-pool

Description This command configures the ATM port buffer pool percentage.

Parameters *value* — Specifies the percentage of the buffers configured on this interface over the maximum allowed.

Values 1 to 100

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

6.117 buffer-type

buffer-type

Syntax **buffer-type** *buffer-type*

Context **[Tree]** (config>app-assure>group>evt-log buffer-type)

Full Context configure application-assurance group event-log buffer-type

Description This command specifies the type of buffer to be used in the event log.

Default buffer-type linear

Parameters *buffer-type* — Specifies the type of event type.

Values **linear** — Specifies a linear buffer which once full will stop recording events until it is cleared.

circular — Specifies a circular buffer whereby older entries will be overwritten by newer entries.

syslog—Specifies that events are stored offline on a syslog host.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

6.118 buffering

buffering

Syntax [**no**] **buffering**

Context **[Tree]** (config>call-trace buffering)

Full Context configure call-trace buffering

Description This command specifies whether messages should be buffered for sessions where the trace key is not yet known, for example, a username for a PPP session. When the key indicates a match for a traced session, the router sends the buffered messages immediately. If the key does not match a trace, the router discards the buffered messages. By default, the router does not buffer any message and thus initial messages may not be traced.

The **no** form of this command reverts to the default value.

Default no buffering

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

buffering

Syntax [**no**] **buffering**

Context **[Tree]** (config>aaa>radius-srv-plcy buffering)

Full Context configure aaa radius-server-policy buffering

Description Commands in this context configure RADIUS message buffering.

The **no** form of this command disables RADIUS message buffering.

6.119 build-packet

build-packet

Syntax **build-packet**

Context **[Tree]** (config>test-oam build-packet)
[Tree] (debug>oam build-packet)

Full Context configure test-oam build-packet
debug oam build-packet

Description Commands in this context configure packet header templates or the OAM test packet to be used when running an **oam find-egress** test.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

6.120 buildout

buildout

Syntax **buildout** {**long** | **short**}

Context **[Tree]** (config>port>tdm buildout)

Full Context configure port tdm buildout

Description This command specifies line buildout (cable length) for physical DS-1/DS-3 ports.

Default buildout short

Parameters **long** — Sets the line buildout for length runs up to 450 feet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

short — Sets the line buildout for length runs up to 225 feet.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

6.121 bundle

bundle

Syntax **bundle** *bundle-name* [**create**]
no bundle *bundle-name*

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy bundle)

Full Context configure mcast-management multicast-info-policy bundle

Description This command creates or edits channel bundles within a multicast information policy. Bundles are used for two main purposes. First, bundles are used by the multicast CAC function to group multicast channels into a common bandwidth context. The CAC function limits the ability for downstream nodes to join multicast channels based on the egress interfaces ability to handle the multicast traffic. Bundling allows multicast channels with common preference or application to be managed into a certain percentage of the available bandwidth.

The second function of bundles is to provide a simple provisioning mechanism. Each bundle within a multicast information policy has a set of default channel parameters. If each channel provisioned in to the bundle can use the default parameters for the bundle, the provisioning and configuration storage requirements are minimized.

Up to 31 explicit bundles may be defined within a multicast information policy (32 including the default bundle).

Once a bundle is created, the default channel parameters should be configured and the individual channel ranges should be defined. Within each channel range, override parameters may be defined that override the default channel parameters. Further overrides are supported within the channel range based on explicit source overrides.

A bundle can be deleted at any time (except for the default bundle). When a bundle is deleted, all configuration information within the bundle is removed including multicast channel ranges. Any multicast records using the bundle should be reevaluated. Multicast CAC and ECMP managers should also be updated.

Default Bundle

Each multicast information policy contains a bundle named **default**. The default bundle cannot be deleted. Any multicast channel that fails to match a channel range within an explicit bundle is automatically associated with the default bundle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes a bundle from the multicast information policy. The default bundle cannot be removed from the policy.

Default bundle “default”

Parameters *bundle-name* — Specifies bundle expressed as an ASCII string with up to 16 characters and must follow normal naming conventions. If bundle-name already exists, the system enters the bundle context for editing purposes. If bundle-name does not exist, the system creates the defined bundle in the policy and enter the bundle context for editing purposes.

create — The create keyword is required if creating a new multicast information policy bundle when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the bundle name already exists.

Platforms All

bundle

Syntax **bundle** [**detail**]
no bundle

Context **[Tree]** (debug>router>gmpls>packet bundle)

Full Context debug router gmpls packet bundle

Description This command enables debugging for GMPLS Bundle packets.

The **no** form of the command disables debugging for GMPLS Bundle packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

bundle

Syntax **bundle** [**detail**]
no bundle

Context **[Tree]** (debug>router>rsvp>packet bundle)

Full Context debug router rsvp packet bundle

Description This command debugs bundle events.

The **no** form of the command disables the debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **detail** — Displays detailed information about bundle events.

Platforms All

bundle

Syntax **bundle** *bundle-name* [**create**]
no bundle *bundle-name*

Context **[Tree]** (config>router>mcac>policy bundle)

Full Context configure router mcac policy bundle

Description This command creates the context that enables the grouping of MCAC group addresses into bundles.

When a number of multicast groups or BTV channels are grouped into a single bundle, then policing, if a join for a particular MC-group (BTV channel), can depend on whether:

1. There is enough physical bandwidth on the egress interface.
2. The given channel is a mandatory or optional channel.
   - If optional, is there sufficient bandwidth according to the policy settings for the relevant interface.
   - If optional, is there sufficient bandwidth within the bundle.

The **no** form of this command removes the named bundle from the configuration.

Parameters *bundle-name* — Specifies the multicast bundle name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be no enclosed within double quotes.

create — Mandatory keyword when creating a bundle instance. The create keyword requirement can be enabled or disabled in the **environment**>**create** context.

Platforms All

6.122 burst-limit

burst-limit

Syntax **burst-limit** {**default** | *size* [**bytes** | **kilobytes**]}
no burst-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>sub-if>grp-if>sap>egress>queue-override>queue burst-limit)

Full Context configure service vprn subscriber-interface group-interface sap egress queue-override queue burst-limit

Description The queue **burst-limit** command defines an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The **no** form of this command restores the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies. When specified within a queue-override queue context, any current burst limit override for the queue is removed and the queue's burst limit is controlled by its defining policy.

Default no burst-limit

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and, by default, is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** qualifier must be added following size.

Values 0 to 13671 kilobytes
0 to 14000000 bytes

Default No default for *size*; use the **default** keyword to specify default burst limit.

bytes — Specifies that the value given for *size* must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for *size* must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is **kilobytes**.

burst-limit

Syntax **burst-limit** {**default** | *size* [**bytes** | **kilobytes**]}
no burst-limit

Context [Tree] (config>port>ethernet>access>egr>qgrp>qover>q burst-limit)

Full Context configure port ethernet access egress queue-group queue-overrides queue burst-limit

Description The queue **burst-limit** command overrides the shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The **no** form of this command removes the current burst limit override for the queue. The queue's burst limit is controlled by its defining template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no burst-limit

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and, by default, is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** qualifier must be added following size.

Values 1 to 13671 kilobytes
1 to 14000000 bytes

Default No default for *size*; use the **default** keyword to specify default burst limit.

bytes — Specifies that the value given for *size* must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for *size* must be interpreted as the burst limit in kilobytes. If neither **bytes** nor **kilobytes** is specified, the default qualifier is **kilobytes**.

Platforms All

burst-limit

Syntax **burst-limit** *size* [**bytes** | **kilobytes**]
no burst-limit

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue burst-limit)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue burst-limit)
[Tree] (config>service>epipe>sap>egress>queue-override>queue burst-limit)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue burst-limit)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue burst-limit)

Full Context configure service apipe sap egress queue-override queue burst-limit
configure service cpipe sap egress queue-override queue burst-limit
configure service epipe sap egress queue-override queue burst-limit
configure service fpipe sap egress queue-override queue burst-limit
configure service ipipe sap egress queue-override queue burst-limit

Description The queue **burst-limit** command defines an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The **no** form of this command restores the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies. When specified within a queue-override queue context, any current burst limit override for the queue is removed and the queue's burst limit is controlled by its defining policy.

Default no burst-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and, by default, is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** qualifier must be added following size.

Values 1 to 13671 kilobytes
14000000 bytes

Default No default for *size*; use the **default** keyword to specify default burst limit.

bytes — Specifies that the value given for *size* must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for *size* must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is **kilobytes**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress queue-override queue burst-limit
- configure service fpipe sap egress queue-override queue burst-limit

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue burst-limit

All

- configure service epipe sap egress queue-override queue burst-limit
- configure service ipipe sap egress queue-override queue burst-limit

burst-limit

Syntax **burst-limit** {**default** | *size* [**bytes** | **kilobytes**]}
no burst-limit

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue burst-limit)

Full Context configure service vpls sap egress queue-override queue burst-limit

Description The queue **burst-limit** command defines an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate. The **no** form of this command restores the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies. When specified within a queue-override queue context, any current burst limit override for the queue is removed and the queue's burst limit is controlled by its defining policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no burst-limit

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and by default is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** qualifier must be added following size.

Values 1 to 13671 kilobytes
1 to 14000000 bytes

Default No default for *size*; use the **default** keyword to specify default burst limit.

bytes — Specifies that the value given for size must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for size must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is **kilobytes**.

Platforms All

burst-limit

Syntax **burst-limit** {**default** | *size* [**bytes** | **kilobytes**]}
no burst-limit

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress>queue-override>queue burst-limit)

Full Context configure service ies subscriber-interface group-interface sap egress queue-override queue burst-limit

Description The queue **burst-limit** command defines an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The **no** form of this command restores the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies. When specified within a queue-override queue context, any current burst limit override for the queue is removed and the queue's burst limit is controlled by its defining policy.

Default no burst-limit

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and, by default, is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** qualifier must be added following size.

Values 0 to 13671 kilobytes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

0 to or 14000000 bytes

Default No default for *size*; use the **default** keyword to specify default burst limit.

bytes — Specifies that the value given for *size* must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for *size* must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is **kilobytes**.

burst-limit

Syntax **burst-limit** *size* [**bytes** | **kilobytes**]
no burst-limit

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override burst-limit)

Full Context configure service vprn interface sap egress queue-override burst-limit

Description The queue **burst-limit** command defines an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The **no** form of this command restores the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies. When specified within a queue-override queue context, any current burst limit override for the queue is removed and the queue's burst limit is controlled by its defining policy.

Default no burst-limit

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and, by default, is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** qualifier must be added following size.

Values 1 to 14000000

bytes — Specifies that the value given for *size* must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for *size* must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is **kilobytes**.

burst-limit

Syntax **burst-limit** *size* [**bytes** | **kilobytes**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no burst-limit

Context [Tree] (config>qos>sap-ingress>queue burst-limit)

Full Context configure qos sap-ingress queue burst-limit

Description The **queue burst-limit** command is used to define an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The **burst-limit** command is supported under the sap-ingress and sap-egress QoS policy queues. The command is also supported under the ingress and egress queue-group-templates queues.

The **no** form of this command is used to restore the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies or queue group templates. When specified within a **queue-override queue** context, any current burst limit override for the queue will be removed and the queue's burst limit will be controlled by its defining policy or template.

Default no burst-limit

Parameters *size* — Specifies an explicit burst limit size. The value is expressed as an integer and, by default, is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the byte qualifier must be added following size.

Values 1 to 13,671 kbytes or 14,000,000 bytes

Default No default for size; use the default keyword to specify default burst limit.

bytes — Specifies that the value given for size must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for size must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is kilobytes.

Platforms All

burst-limit

Syntax **burst-limit** {**default** | *size* [**bytes** | **kilobytes**]}
no burst-limit

Context [Tree] (config>qos>sap-egress>queue burst-limit)

Full Context configure qos sap-egress queue burst-limit

Description The **queue burst-limit** command defines an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **burst-limit** command is supported under the **sap-ingress** and **sap-egress** QoS policy queues. The command is also supported under the ingress and egress **queue-group-templates** queues.

The **no** form of this command restores the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies or queue group templates. When specified within a **queue-override queue** context, any current burst limit override for the queue is removed and the queue's burst limit is controlled by its defining policy or template.

Default no burst-limit

Parameters **default** — Reverts the queue's burst limit to the system default value.

size — Specifies an explicit burst limit size. The value is expressed as an integer and by default is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the **bytes** keyword must be added following *size*.

Values 1 to 13671 kilobytes
0 to 14,000,000 bytes

Default No default for *size*; use the **default** keyword to specify default burst limit.

bytes — Specifies that the value given for size must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for size must be interpreted as the burst limit in kilobytes. If neither bytes nor kilobytes is specified, the default qualifier is **kilobytes**.

Platforms All

burst-limit

Syntax **burst-limit** {*size* [**bytes** | **kilobytes**] | **default**}
no burst-limit

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue burst-limit)
[Tree] (config>qos>qgrps>ing>qgrp>queue burst-limit)

Full Context configure qos queue-group-templates egress queue-group queue burst-limit
configure qos queue-group-templates ingress queue-group queue burst-limit

Description The queue burst-limit command is used to define an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue's shaping rate.

The burst-limit command is supported under the sap-ingress and sap-egress QoS policy queues. The command is also supported under the ingress and egress queue-group-templates queues.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command is used to restore the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies or queue group templates. When specified within a queue-override queue context, any current burst limit override for the queue will be removed and the queue's burst limit will be controlled by its defining policy or template.

Parameters *size* — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and by default is interpreted as the burst limit in kilobytes. If the value is intended to be interpreted in bytes, the byte qualifier must be added following size.

Values 1 to 14,000 (14,000 or 14,000,000 depending on bytes or kilobytes)

bytes — Specifies that the value given for size must be interpreted as the burst limit in bytes.

kilobytes — Specifies that the value given for size must be interpreted as the burst limit in kilobytes.

Platforms All

6.123 bw-activity

bw-activity

Syntax **bw-activity** {**use-admin-bw** | **dynamic** [**falling-delay** *seconds*]} [**black-hole-rate** *kbps*]
no bw-activity

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle bw-activity)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel bw-activity)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>source-override bw-activity)

Full Context configure mcast-management multicast-info-policy bundle bw-activity
configure mcast-management multicast-info-policy bundle channel bw-activity
configure mcast-management multicast-info-policy bundle source-override bw-activity

Description This command defines how the multicast ingress path manager determines the amount of bandwidth required by a multicast channel. The default setting is dynamic which causes the bandwidth manager to use the bandwidth policies dynamic rate table entries to determine the current rate. The alternative setting is **use-admin-bw** which causes the bandwidth manager to use the configured admin-bw associated with the channel. The **use-admin-bw** setting also requires an active and inactive threshold to be defined which allows the bandwidth manager to determine when the channel is actively using ingress path bandwidth and when the channel is idle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **use-admin-bw** setting requires that the channel be configured with an admin-bw value that is not equal to 0 in the same context as the **bw-activity** command using the setting. Once a context has the **use-admin-bw** command configured, the context's admin-bw value cannot be set to 0 and the no admin-bw command fails.

This command also supports an optional **black-hole-rate** *kbps* command that defines at which current rate a channel should be placed in the black-hole state. This is intended to provide a protection mechanism against multicast channels that exceed a reasonable rate and cause outages in other channels.

The **no** form of this command restores the default bandwidth activity monitoring setting (dynamic or null depending on the context).

Parameters **use-admin-bw | dynamic** — The **use-admin-bw** and **dynamic** keywords are mutually exclusive and one must be specified when executing the **bw-activity** command. The **use-admin-bw** keyword indicates the channels current ingress bandwidth should be derived from the **admin-bw** setting. The **admin-bw** setting must not currently be set to 0 for the **use-admin-bw** setting to succeed. The **dynamic** keyword indicates that the multicast ingress path manager should use the dynamic rate table (as defined in the bandwidth-policy) to derive the channels current ingress rate.

falling-delay *seconds* — Specifies the value the bandwidth manager uses the falling-delay threshold to hold on to the previous highest bandwidth until the delay time has expired while operating in dynamic bandwidth mode. This allows the bandwidth manager to ignore momentary drops in channel bandwidth.

Values 10 to 3600

Default 30

Bundle default:	dynamic
Channel default:	Null (undefined)
Source-override default:	Null (undefined)

black-hole-rate *kbps* — Specifies a rate at which a channel is placed in the black-hole state. This parameter is expressed, in kb/s, as an integer and represents multiples of 1,000 bits per second.

Values 1 to 40000000

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

6.124 bypass-resignal-timer

bypass-resignal-timer

Syntax **bypass-resignal-timer** *minutes*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no bypass-resignal-timer

Context [Tree] (config>router>mpls bypass-resignal-timer)

Full Context configure router mpls bypass-resignal-timer

Description This command triggers the periodic global re-optimization of all dynamic bypass LSP paths associated with RSVP P2P LSP. The operation is performed at each expiry of the user configurable bypass LSP resignal timer.

When this command is enabled, MPLS requests CSPF for the best path for each dynamic bypass LSP originated on this node. The constraints, hop-limit, SRLG and admin-group constraints, of the first associated LSP primary path that originally triggered the signaling of the bypass LSP must be satisfied. To do this, MPLS saves this initial Path State Block (PSB) of that LSP primary path, even if the latter is torn down.

CSPF first updates the SRLG membership of the current bypass LSP path and checks if the path violates the SRLG constraint of the initial PSB. It then attempts a new path computation for the bypass LSP using the initial PSB constraints. If CSPF returns no path or returns a new path with a cost that is lower than the current path, MPLS does not signal the new bypass path. If CSPF returns a new path with a cost that is lower than the current one, MPLS signals it. Also, if the new bypass path is SRLG strict disjoint with the primary path of the original PSB while the current path is SRLG loose disjoint, the manual bypass path is resignaled regardless of cost comparison.

Once the new path is successfully signaled, MPLS evaluates each PSB of each PLR (that is, each unique avoid-node or avoid-link constraint) associated with the current bypass LSP path to check if the corresponding LSP primary path constraints are still satisfied by the new bypass LSP path. If so, the PSB association is moved to the new bypass LSP.

Each PSB for which the constraints are not satisfied remains associated with the PLR on the current bypass LSP and is checked at the next timer or manual bypass re-optimization. Additionally, if SRLG FRR loose disjointness is configured using the **configure router mpls srlg-frr** command and the current bypass LSP is SRLG disjoint with a primary path while the new bypass LSP is not SRLG disjoint, the PSB association is not moved. When CSPF does not return a new bypass path or it returns a less optimal one, the PSBs remain associated with the current bypass path. However, it is possible that CSPF found the current bypass LSP path no longer satisfies the SRLG constraint of one or more PLRs after the update of the current path SRLG information. In that case, MPLS detaches from current bypass path the PSB associations of these PLRs. These orphaned PSBs are re-evaluated by the FRR background task which checks unprotected PSBs on a regular basis and following the same above procedure.

If a specific PLR associated with a bypass LSP is active, the corresponding PSBs remain associated with the current PLR until the Global Revertive Make-Before-Break (MBB) tears down all corresponding primary paths, which also causes the current PLR to be removed.

Note: While it is in the preceding state, the older PLR does not get any new PSB association until the specific PLR with an active bypass LSP is removed. When the last PLR is removed, the older bypass LSP is torn down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This feature is not supported with inter-area dynamic bypass LSP and bypass LSP protecting S2L paths of a P2MP LSP.

The **no** form of this command disables the periodic global re-optimization of dynamic bypass LSP paths.

Default no bypass-resignal timer.

Parameters *minutes* — Specifies the time, in minutes, MPLS waits before attempting to resignal dynamic bypass LSP paths originated on the system.

Values 1 to 10080

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7 c Commands

7.1 c-mcast-signaling

c-mcast-signaling

Syntax **c-mcast-signaling** {**bgp** | **pim**}
no c-mcast-signaling

Context **[Tree]** (config>service>vprn>mvpn c-mcast-signaling)

Full Context configure service vprn mvpn c-mcast-signaling

Description This command specifies BGP or PIM, for PE-to-PE signaling of CE multicast states. When this command is set to PIM and neighbor discovery by BGP is disabled, PIM peering will be enabled on the inclusive tree.

Changes may only be made to this command when the mvpn node is shutdown.

The **no** form of this command reverts it back to the default.

Default c-mcast-signaling bgp

Parameters **bgp** — Specifies to use BGP for PE-to-PE signaling of CE multicast states. Auto-discovery must be enabled.

pim — Specifies to use PIM for PE-to-PE signaling of CE multicast states.

Platforms All

7.2 ca-name

ca-name

Syntax **ca-name** *ca-name*
no ca-name

Context **[Tree]** (config>port>ethernet>dot1x>macsec>sub-port ca-name)

Full Context configure port ethernet dot1x macsec sub-port ca-name

Description This command configures the Connectivity Association (CA) linked to this MACsec sub-port. The specified CA provides the MACsec parameter to be used or negotiated with other peers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the CA from the MACsec sub-port.

Parameters *ca-name* — Specifies the appropriate ca to be used under this MACsec sub-port, up to 32 characters.

Platforms All

7.3 ca-profile

ca-profile

Syntax [**no**] **ca-profile** *name*

Context **[Tree]** (config>ipsec>cert-profile>entry>send-chain ca-profile)

Full Context configure ipsec cert-profile entry send-chain ca-profile

Description This command specifies a CA certificate in the specified **ca-profile** to be sent to the peer.

Multiple configurations (up to seven) of this command are allowed in the same entry.

Parameters *name* — Specifies the profile name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ca-profile

Syntax **ca-profile** *name* [**create**]
no ca-profile *name*

Context **[Tree]** (config>system>security>pki ca-profile)

Full Context configure system security pki ca-profile

Description This command creates a new **ca-profile** or enters the configuration context of an existing **ca-profile**. Up to 128 ca-profiles can be created in the system. A **shutdown** of the **ca-profile** will not affect the current up and running **ipsec-tunnel** or **ipsec-**gw that is associated with the **ca-profile**. However, authentication afterwards will fail with a **shutdown ca-profile**.

Executing a **no shutdown** command in this context causes the system to reload the configured cert-file and crl-file.

A **ca-profile** can be applied under the **ipsec-tunnel** or **ipsec-gw** configuration.

The **no** form of this command removes the name parameter from the configuration. A ca-profile cannot be removed until all the associated entities (ipsec-tunnel/gw) have been removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the name of the **ca-profile** up to 32 characters.

create — Keyword used to create a new **ca-profile**. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

ca-profile

Syntax [**no**] **ca-profile** *profile-name*

Context **[Tree]** (debug>certificate>auto-crl-update ca-profile)
[Tree] (debug>certificate>cmpv2 ca-profile)
[Tree] (debug>certificate>ocsp ca-profile)

Full Context debug certificate auto-crl-update ca-profile
debug certificate cmpv2 ca-profile
debug certificate ocsp ca-profile

Description This command debugs output of the specified CA profile.

- Protection method of each message is logged.
- All HTTP messages are logged. Format allows offline analysis using Wireshark.
- In the event of failed transactions, saved certificates are not deleted from file system for further debug and analysis.
- The system allows CMPv2 debugging for multiple ca-profile at the same time.

Parameters *profile-name* — Specifies the name of the CA profile, up to 32 characters.

Platforms All

ca-profile

Syntax [**no**] **ca-profile** *name*

Context **[Tree]** (config>system>security>tls>cert-profile>entry>send-chain ca-profile)

Full Context configure system security tls cert-profile entry send-chain ca-profile

Description This command enables a certificate authority (CA) certificate in the specified CA profile to be sent to the peer. Up to seven configurations of this command are permitted in the same entry.

The **no** form of the command disables the transmission of a CA certificate from the specified CA profile.

Parameters *name* — Specifies the name of the certificate authority profile, up to 32 characters in length.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.4 cacert

cacert

Syntax **cacert est-profile** *name* **output** *output-cert-filename* [**force**]

Context **[Tree]** (admin>certificate>est cacert)

Full Context admin certificate est cacert

Description This command downloads a Certificate Authority (CA) certificate from an EST server specified by the EST profile. The downloaded certificate is imported and saved with the filename specified by the *output-cert-filename*.

Parameters *name* — Specifies the EST profile name, up to 32 characters

output-cert-filename — Specifies the filename of the resulting CA certificate, up to 200 characters

force — Overwrites the existing file with same filename

Platforms All

7.5 cache

cache

Syntax **cache** [**create**]
no cache

Context **[Tree]** (config>python>py-policy cache)

Full Context configure python python-policy cache

Description Commands in this context configure the limits of the caching API inside the Python scripts.

The **no** form of this command removes the configured cache parameters from the configuration.

Parameters **create** — This keyword is required when first creating the Python policy. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cache

Syntax **cache**

Context **[Tree]** (config>router>radius-proxy>server cache)
[Tree] (config>service>vprn>radius-proxy>server cache)

Full Context configure router radius-proxy server cache
configure service vprn radius-proxy server cache

Description Commands in this context configure the cache under radius-proxy server. The cache contains per-subscriber authentication information learned from RADIUS authentication messages, and is used to authorize subsequent DHCP requests.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.6 cache-reset

cache-reset

Syntax [**no**] **cache-reset**

Context **[Tree]** (debug>router>rpki-session>packet cache-reset)

Full Context debug router rpki-session packet cache-reset

Description This command enables debugging for cache reset RPKI packets.

The **no** form of this command disables debugging for cache reset RPKI packets.

Platforms All

7.7 cache-response

cache-response

Syntax [**no**] **cache-response**

Context **[Tree]** (debug>router>rpki-session>packet cache-response)

Full Context debug router rpki-session packet cache-response

Description This command enables debugging for cache response RPKI packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables debugging for cache response RPKI packets.

Platforms All

7.8 cache-size

cache-size

Syntax **cache-size** *num-entries*
no cache-size

Context **[Tree]** (config>cflowd cache-size)

Full Context configure cflowd cache-size

Description This command specifies the maximum number of active flows to maintain in the flow cache table.

The **no** form of this command resets the number of active entries back to the default value.

Default cache-size 65536

Parameters *num-entries* — Specifies the maximum number of entries maintained in the cflowd cache. The number depends on the CPM version.

Values

For the 7450 ESS and 7750 SR (cfm-xp, SF/CPM3):	1000 to 250000
For the 7450 ESS and 7750 SR (CPM4 or CPM5):	1000 to 1000000
For the 7950 XRS:	1000 to 1500000

Default

For the 7450 ESS and 7750 SR:	65536 (64K)
For the 7950 XRS:	500000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.9 cak

cak

Syntax **cak** *hex-string* [**hash** | **hash2** | **custom**]
no cak

Context **[Tree]** (config>macsec>conn-assoc>static-cak>pre-shared-key cak)

Full Context configure macsec connectivity-association static-cak pre-shared-key cak

Description Specifies the connectivity association key (CAK) for a pre-shared key. Two values are derived from CAK.

- Key Encryption Key (KEK), this is used to encrypt the MKA and SAK (symmetric key used for data path PDUs) to be distributed between all members.
- Integrity Check Value (ICK), this is used to authenticate the MKA and SAK PDUs to be distributed between all members.

The **no** form of this command removes the value.

Parameters *hex-string* — Specifies the value of the CAK.

Values up to 64 hexadecimal characters, 32 hexadecimal characters for 128-bit key and 64 hexadecimal characters for 256-bit key

hash — Keyword, specifying the hash scheme.

hash2 — Keyword, specifying the hash scheme.

custom — Specifies the custom encryption for management interface.

Platforms All

7.10 calculate-counts

calculate-counts

Syntax [**no**] **calculate-counts**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query calculate-counts)

Full Context configure subscriber-mgmt wlan-gw tunnel-query calculate-counts

Description This command specifies whether or not to count the number of tunnels matching the specified criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: Do not enable this command if the expected number of tunnels is large.

Default no calculate-counts

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.11 call-trace

call-trace

Syntax **call-trace**

Context **[Tree]** (config call-trace)

Full Context configure call-trace

Description Commands in this context configure parameters related to the call trace debugging tool.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

call-trace

Syntax **call-trace**

Context **[Tree]** (debug call-trace)

Full Context debug call-trace

Description Commands in this context set up various call trace debug sessions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.12 called-station-id

called-station-id

Syntax [**no**] **called-station-id**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>auth-policy>include-radius-attribute called-station-id)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute called-station-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute called-station-id
configure subscriber-mgmt authentication-policy include-radius-attribute called-station-id

Description This command includes called station ID attributes.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

called-station-id

Syntax [**no**] **called-station-id**

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx>include-avp called-station-id)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp called-station-id)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp called-station-id
configure subscriber-mgmt diameter-application-policy nasreq include-avp called-station-id

Description This command includes called station ID attributes.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

called-station-id

Syntax **called-station-id** [*called-station-id*]
no called-station-id

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gy>include-avp called-station-id)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp called-station-id

Description This command configures the value of the called station ID AVP.

The **no** form of this command returns the command to the default setting.

Parameters *called-station-id* — Specifies the called station ID, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

called-station-id

Syntax [**no**] **called-station-id**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>rad-acct-plcy>include called-station-id)
[Tree] (config>ipsec>rad-auth-plcy>include called-station-id)

Full Context configure ipsec radius-accounting-policy include-radius-attribute called-station-id
configure ipsec radius-authentication-policy include-radius-attribute called-station-id

Description This command includes called station ID attributes.

The **no** form of this command excludes called station ID attributes.

Default no called-station-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

called-station-id

Syntax [**no**] **called-station-id**

Context [Tree] (config>aaa>isa-radius-plcy>acct-include-attributes called-station-id)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes called-station-id)

Full Context configure aaa isa-radius-policy acct-include-attributes called-station-id
configure aaa isa-radius-policy auth-include-attributes called-station-id

Description This command includes called station id attributes.

The **no** form of the command excludes called station id attributes.

Default no called-station-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.13 calling-number-format

calling-number-format

Syntax **calling-number-format** *ascii-spec*
no calling-number-format

Context [Tree] (config>router>l2tp calling-number-format)
[Tree] (config>service>vprn>l2tp calling-number-format)

Full Context configure router l2tp calling-number-format
configure service vprn l2tp calling-number-format

Description This command what string to put in the Calling Number AVP, for L2TP control messages related to a session in this L2TP protocol instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default calling-number-format "%S %s"

Parameters *ascii-spec* — Specifies the L2TP calling number AVP.

Values

ascii-spec	char-specification ascii-spec		
	char-specification	ascii-char | char-origin	
	ascii-char	a printable ASCII character	
	char-origin	%origin	
	origin	S | c | r | s | l	
		S	system name, the value of TIMETRA-CHASSIS-MIB::tmnxChassisName
		c	Agent Circuit Id
		r	Agent Remote Id
		s	SAP ID, formatted as a character string
		l	Logical Line ID

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.14 calling-station-id

calling-station-id

Syntax [**no**] **calling-station-id**

Context **[Tree]** (config>aaa>l2tp-acct-plcy>include-radius-attribute calling-station-id)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute calling-station-id

Description This command enables the inclusion of the **calling-station-id** attribute in RADIUS authentication requests and RADIUS accounting messages.

Default no calling-station-id

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

calling-station-id

Syntax [**no**] **calling-station-id**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>rad-acct-plcy>include calling-station-id)
[Tree] (config>ipsec>rad-auth-plcy>include calling-station-id)

Full Context configure ipsec radius-accounting-policy include-radius-attribute calling-station-id
configure ipsec radius-authentication-policy include-radius-attribute calling-station-id

Description This command enables the inclusion of the **calling-station-id** attribute in RADIUS authentication requests and RADIUS accounting messages.

Default no calling-station-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

calling-station-id

Syntax **calling-station-id**
calling-station-id {**llid | mac** | **remote-id** | **sap-id** | **sap-string**}
no calling-station-id

Context [Tree] (config>service>ies>if>sap calling-station-id)
[Tree] (config>service>ies>sub-if>grp-if>sap calling-station-id)
[Tree] (config>service>vpls>sap calling-station-id)
[Tree] (config>service>vprn>if>sap calling-station-id)
[Tree] (config>service>vprn>sub-if>grp-if>sap calling-station-id)
[Tree] (config>subscr-mgmt>auth-plcy>include-radius-attribute calling-station-id)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute calling-station-id)

Full Context configure service ies interface sap calling-station-id
configure service ies subscriber-interface group-interface sap calling-station-id
configure service vpls sap calling-station-id
configure service vprn interface sap calling-station-id
configure service vprn subscriber-interface group-interface sap calling-station-id
configure subscriber-mgmt radius-accounting-policy include-radius-attribute calling-station-id
configure subscriber-mgmt authentication-policy include-radius-attribute calling-station-id

Description This command enables the inclusion of the **calling-station-id** attribute in RADIUS authentication requests and RADIUS accounting messages.

The **no** form of this command reverts to the default.

Default calling-station-id sap-string

Parameters **llid** — Specifies that the logical link identifier (LLID) is mapping from a physical to logical identification of a subscriber line and supplied by a RADIUS llid-server.

mac — Specifies that the MAC address is sent.

remote-id — Specifies that the remote ID is sent.

sap-id — Specifies that the SAP ID is sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap-string — Specifies that the value is the inserted value set at the SAP level. If no **calling-station-id** value is set at the SAP level, the **calling-station-id** attribute will not be sent.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

calling-station-id

Syntax **calling-station-id** [**type** {**llid** | **mac** | **remote-id** | **sap-id** | **sap-string**}]
no calling-station-id

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp calling-station-id)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp calling-station-id)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp calling-station-id
configure subscriber-mgmt diameter-application-policy nasreq include-avp calling-station-id

Description This command includes the calling-station-id AVP in the specified format.

The **no** form of this command reverts to the default.

Parameters **type** — Specifies the format of the Calling-Station-ID AVP.

Values **llid** — The logical link identifier (LLID) is the mapping from a physical to logical identification of a subscriber line and supplied by a RADIUS llid-serv

mac — Specifies that the MAC address is sent.

remote-id — Specifies that the remote ID is sent

sap-id — Specifies that the sap-id is sent

sap-string — Specifies that the value is the inserted value set at the SAP level. If no **calling-station-id** value is set at the SAP level, the **calling-station-id** attribute will not be sent.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

calling-station-id

Syntax [**no**] **calling-station-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes calling-station-id)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes calling-station-id)

Full Context configure aaa isa-radius-policy acct-include-attributes calling-station-id
configure aaa isa-radius-policy auth-include-attributes calling-station-id

Description This command enables the inclusion of the calling-station-id attribute in RADIUS authentication requests and RADIUS accounting messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no calling-station-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.15 cancel-commit

cancel-commit

Syntax [**no**] **cancel-commit**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization cancel-commit)

Full Context configure system security profile netconf base-op-authorization cancel-commit

Description This command enables the NETCONF cancel-commit operation.

The **no** form of this command disables the operation.

Default no cancel-commit

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

7.16 candidate

candidate

Syntax **candidate**

Context **[Tree]** (candidate)

Full Context candidate

Description Commands in this context edit candidate configurations.

Commands in the **candidate** CLI branch, except **candidate edit**, are available only when in edit-cfg mode.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

candidate

Syntax [**no**] **candidate**

Context **[Tree]** (config>system>netconf>capabilities candidate)

Full Context configure system netconf capabilities candidate

Description This command enables support of the candidate datastore in the SR OS NETCONF server. If the candidate is disabled then requests that reference the candidate datastore return an error, and when a NETCONF client establishes a new session the candidate capability is not advertised in the SR OS <hello>. This command also controls support of the <commit> and <discard-changes> operations.

When **management-interface configuration-mode** is set to **classic**, then the candidate capability is disabled, even if **candidate** is configured.

The **no** form of the command disables support of the candidate datastore in the SR OS NETCONF server.

Default candidate

Platforms All

7.17 cannot-change-password

cannot-change-password

Syntax [**no**] **cannot-change-password**

Context **[Tree]** (config>system>security>user>console cannot-change-password)

Full Context configure system security user console cannot-change-password

Description This command allows a user the privilege to change their password for both FTP and console login.

To disable a user's privilege to change their password, use the **cannot-change-password** form of this command.

Note: The **cannot-change-password** flag is not replicated when a user copy is performed. A new-password-at-login flag is created instead.

Default no cannot-change-password

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

7.18 capacity-cost

capacity-cost

Syntax **capacity-cost** *cost*
no capacity-cost

Context [Tree] (config>app-assure>group>policy>app-profile capacity-cost)

Full Context configure application-assurance group policy app-profile capacity-cost

Description This command configures an application profile capacity cost. Capacity-Cost based load balancing allows a cost to be assigned to diverted SAPs (with the app-profile) and this is then used for load-balancing SAPs between ISAs as well as for a threshold that notifies the operator if/when capacity planning has been exceeded.

Default capacity-cost 1

Parameters *cost* — Specifies the profile capacity cost.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.19 captive-redirect

captive-redirect

Syntax **captive-redirect**

Context [Tree] (config>app-assure>group>http-redirect captive-redirect)

Full Context configure application-assurance group http-redirect captive-redirect

Description This command configures the captive redirect capability for an HTTP redirect policy. HTTP redirect policies using captive redirect can be used in conjunction with a session filter policy and will terminate TCP flows in the ISA-AA card before reaching the Internet to redirect subscribers to the predefined redirect URL. Non-HTTP TCP flows are TCP reset. Captive redirect uses the provisioned VLAN id to send the HTTP response to subscribers; therefore this VLAN id must be properly assigned in the same VPN as the subscriber. The operator can select the URL arguments to include in the redirect URL using either a specific template id or by configuring the redirect URL using one of the supported macro substitution keywords.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.20 capture

capture

Syntax **capture** [{**start** | **stop**}]

Context **[Tree]** (debug>pcap capture)

Full Context debug pcap capture

Description This command starts and stops the packet capture process for the specified *session-name*.

Parameters **start** — Starts the packet capture process and also start or restarts the FTP or TFTP session. If the FTP or TFTP server is unreachable, the command prompt rejects further input until the retires are timed out after 24 seconds (after four attempts of about six seconds each). If the same file name is unchanged in the **config**>**mirror**>**mirror-dest**>**pcap** context between captures, this command overwrites the file content.

stop — Stops the packet capture process and also stops the FTP or TFTP session. If the FTP or TFTP server is unreachable, the command prompt rejects further input until the retires are timed out after 24 seconds (after four attempts of about six seconds each).

Platforms All

7.21 capture-sap

capture-sap

Syntax **capture-sap** *sap-id* [**encap-val** *qtag*[.*qtag*]] [**mode** *mode*]
no capture-sap *sap-id*

Context **[Tree]** (debug>dynsvc>data-triggers capture-sap)

Full Context debug dynamic-services data-triggers capture-sap

Description This command enables or disables the generation of dynamic services data trigger debug events, such as:

- data trigger received

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- authentication
- data trigger SAP created
- dynamic service SAP created
- dropped data trigger with drop reason such as data trigger exists or lockout active.

Multiple capture SAPs can be specified simultaneously.

Optionally, a single **encap-val** per **capture-sap** can be specified to limit the output of the debug events to the data trigger events with the specified encapsulation.

Optionally, the debug output can be restricted to dropped data trigger events only.

Parameters *sap-id* — Specifies the dynamic services data trigger capture SAP for which debug events should be logged.

encap-val *qtag[.qtag]* — Optionally restrict the debug output to data trigger events with the specified encapsulation.

Values 1 to 4094

mode — Optionally restrict the debug output to specific events.

Values all—log all data trigger events
dropped-only—log only dropped data trigger events

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.22 card

card

Syntax [**no**] **card** *slot-number*

Context **[Tree]** (config card)

Full Context configure card

Description This mandatory command enables access to the chassis card IOM, MDA, XCM and XMA CLI contexts.

The **no** form of this command removes the card from the configuration. All associated ports, services, and MDAs must be shutdown.

Default no card

Parameters *slot-number* — Specifies the slot number of the card in the chassis. The maximum slot number is platform dependent. Refer to the hardware installation guides.

Values 1 to 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

7.23 card-type

card-type

Syntax **card-type** *card-type* [**level** *card-level*]
no card-type

Context **[Tree]** (config>card card-type)

Full Context configure card card-type

Description This mandatory command adds an IOM/XCM to the device configuration for the slot. The card type can be preprovisioned, meaning that the card does not need to be installed in the chassis.

A card must be provisioned before an MDA, connector, or port can be configured.

A card can only be provisioned in a slot that is vacant, meaning no other card can be provisioned (configured) for that particular slot. To reconfigure a slot position, use the **no** form of this command to remove the current information.

A card can only be provisioned in a slot if the card type is allowed in the slot. An error message is generated if an attempt is made to provision a card type that is not allowed.

If a card is inserted that does not match the configured card type for the slot, then a log event and facility alarm is raised. The alarm is cleared when the correct card type is installed or the configuration is modified.

A log event and facility alarm are is raised if an administratively enabled card is removed from the chassis. The alarm is cleared when the correct card type is installed or the configuration is modified. A log event is issued when a card is removed that is administratively disabled.

Because IMMs do not have the capability to install separate MDAs, the configuration of the MDA is automatic. This configuration only includes the default parameters such as default buffer policies. Commands to manage the MDA such as **shutdown** and so on, remain in the MDA configuration context.

Some card hardware can support two different firmware loads. One load includes the base Ethernet functionality, including 10G WAN mode, but does not include 1588 port-based timestamping. The second load includes the base Ethernet functionality and 1588 port-based timestamping, but does not include 10G WAN mode. These are identified as two card types that are the same, except for a “-ptp” suffix to indicate the second loadset; for example, *imm40-10gb-sfp* and *imm40-10gb-sfp-ptp*. A hard reset of the card occurs when switching between the two provisioned types.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An appropriate alarm is raised if a partial or complete card failure is detected. The alarm is cleared when the error condition ceases.

New generations of cards include variants controlled by hardware and software licensing. For these cards, the license level must be provisioned in addition to the card type. A card can not become operational unless the provisioned license level matches the license level of the card installed into the slot. The set of license levels varies by card type.

The provisioned level controls aspects related to connector provisioning and the consumption of hardware egress queues and egress policers. Changes to the provisioned license level may be blocked if configuration exists that would not be permitted with the new target license level.

If the license level is not specified, the level is set to the highest license level for that card.

The **no** form of this command removes the card from the configuration.

Default no card-type

Parameters *card-type* — Specifies the type of card to be configured and installed in that slot. Values for this attribute vary by platform and release. The release notes include a listing of all supported card-types and their CLI strings. In addition, the command can be queried to check which card-types are relevant for the active platform type. Some examples include iom4-e-b and imm-2pac-fp3.

card-level — Specifies the license level of the card, up to 32 characters. Possible values vary by card type.

Platforms All

7.24 carrier-carrier-vpn

carrier-carrier-vpn

Syntax [**no**] **carrier-carrier-vpn**

Context **[Tree]** (config>service>vprn carrier-carrier-vpn)

Full Context configure service vprn carrier-carrier-vpn

Description This command configures a VPRN service to support a Carrier Supporting Carrier model. It should be configured on a network provider's CSC-PE device.

This command cannot be applied to a VPRN unless it has no SAP or spoke-SDP interfaces. Once this command has been entered one or more MPLS-capable CSC interfaces can be created in the VPRN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the Carrier Supporting Carrier capability from a VPRN.

Default no carrier-carrier-vpn

Platforms All

7.25 category

category

Syntax **category** *category-name* [**create**]
no category *category-name*

Context **[Tree]** (config>subscr-mgmt>cat-map category)

Full Context configure subscriber-mgmt category-map category

Description Commands in this context configure RADIUS credit control, Diameter credit control (Gy), Diameter Gx Usage Monitoring, or Idle-Timeout.

Up to sixteen categories can be configured per category map. The internal category for Gx session level Usage Monitoring is included in this limit. The instantiation of the internal category is controlled with the **gx-session-level-usage** command.

Parameters *category-name* — Specifies the category name, up to 32 characters.

create — Keyword used to create a category instance. The **create** keyword can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

category

Syntax **category** *category-name* [**create**]
no category *category-name*

Context **[Tree]** (config>subscr-mgmt>sla-prof>cat-map category)

Full Context configure subscriber-mgmt sla-profile category-map category

Description This command defines the category in the category map to be used for the idle timeout monitoring of subscriber hosts.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *category-name* — Specifies the name, up to 32 characters, of the category where the queues and policers are defined for idle timeout monitoring of subscriber hosts.

create — Keyword used to create a category instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

category

Syntax **category** *category* **block**
no category *category*

Context **[Tree]** (config>app-assure>group>url-filter>web-service>profile category)

Full Context configure application-assurance group url-filter web-service profile category

Description This command configures the category that will be blocked in the category profile.

The **no** form of this command removes the category blocking configuration.

Parameters *category* — Specifies the URL category name for the configured web service, up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.26 category-map

category-map

Syntax **category-map** *category-map-name* [**create**]
no category-map *category-map-name*

Context **[Tree]** (config>subscr-mgmt category-map)

Full Context configure subscriber-mgmt category-map

Description This command specifies the category map name.

The **no** form of this command reverts to the default.

Parameters *category-map-name* — Specifies the category map name, up to 32 characters.

create — Keyword used to create a category map instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

category-map

Syntax **category-map** *category-map-name*
no category-map

Context **[Tree]** (config>subscr-mgmt>sla-prof category-map)

Full Context configure subscriber-mgmt sla-profile category-map

Description This command references the category-map to be used for the idle-timeout monitoring of subscriber hosts associated with this sla-profile. The **category-map** must already exist in the **config**>**subscr-mgmt** context.

The **no** form of this command reverts to the default.

Parameters *category-map-name* — Specifies the name of the category map, up to 32 characters, where the activity-threshold and the category is defined for idle-timeout monitoring of subscriber hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.27 category-map-name

category-map-name

Syntax **category-map-name** *category-map-name* [**create**]
no category-map-name *category-map-name*

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings category-map-name)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings category-map-name)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings category-map-name
configure subscriber-mgmt local-user-db ppp host identification-strings category-map-name

Description This command specifies the category map name.

The **no** form of this command removes the category map name from the configuration.

Parameters *category-map-name* — Specifies an existing category map name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.28 cbs

cbs

Syntax **cbs** *percent-of-resv-cbs*
no cbs

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2-paths>primary-paths>queue-parameters cbs)
[Tree] (config>mcast-mgmt>bw-plcy>t2-paths>secondary-paths>queue-parameters cbs)

Full Context configure mcast-management bandwidth-policy t2-paths primary-paths queue-parameters cbs
configure mcast-management bandwidth-policy t2-paths secondary-paths queue-parameters cbs

Description This command overrides the default Committed Buffer Size (CBS) for each individual path's queue. The queues CBS threshold is used when requesting buffers from the systems ingress buffer pool to indicate whether the requested buffer should be removed from the reserved portion of the buffer pool or the shared portion. When the queue's fill depth is below or equal to the CBS threshold, the requested buffer comes from the reserved portion. Once the queues depth exceeds the CBS threshold, buffers come from the shared portion.

The **cbs** *percent-of-resv-cbs* parameter is defined as a percentage of the reserved portion of the pool. The system allows the sum of all CBS values to equal more than 100% allowing for oversubscription of the reserved portion of the pool. If the reserved portion is oversubscribed and the queues are currently using more reserved space than provisioned in the pool, the pool automatically starts using the shared portion of the pool for within-CBS buffer allocation. The shared early detection slopes can assume more buffers that exist within the shared portion that may cause the early detection function to fail.

For the primary-path and secondary-path queues, the percentage is applied to a single queue for each path.

The **no** form of this command restores the path queues default CBS value.

Parameters *percent-of-resv-cbs* — Specifies the percent of buffers reserved from the total buffer pool space, expressed as a decimal integer. If 10 MB is the total buffers in the buffer pool, a value of 10 would reserve 1MB (10%) of buffer space for the forwarding class queue. The value 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can be applied for scheduling purposes).

Values 0 to 100

Default

Primary:	5
Secondary:	30

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue cbs)
[Tree] (config>subscr-mgmt>sla-prof>ingress>qos>queue cbs)

Full Context configure subscriber-mgmt sla-profile egress qos queue cbs
configure subscriber-mgmt sla-profile ingress qos queue cbs

Description This command can be used to override specific attributes of the specified queue's CBS parameters. It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queues' CBS settings into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets.

The **no** form of this command returns the CBS size to the size as configured in the QoS policy.

Default no cbs

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values 0 to 1048576, **default**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

cbs

Syntax **cbs** *size* [**bytes** | **kilobytes**]
no cbs

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>policer cbs)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>policer cbs)

Full Context configure subscriber-mgmt sla-profile egress qos policer cbs
configure subscriber-mgmt sla-profile ingress qos policer cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to configure the policer's CIR leaky bucket's exceed threshold. The CIR bucket's exceed threshold represents the committed burst tolerance allowed by the policer. If the policer's forwarding rate is equal to or less than the policer's defined CIR, the CIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the forwarding rate increases beyond the profiling rate, the amount of data allowed to be in-profile above the rate is capped by the threshold.

The policer's **cbs** size defined in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command returns the policer to its default CBS size.

Parameters *size* — Specifies the size parameter and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456

bytes — Specifies the size parameter the size parameter in bytes. When **bytes** is defined, the value given for size is interpreted as the queue's MBS value given in bytes.

kilobytes — Specifies the size parameter in kilobytes. When **kilobytes** is defined, the value is interpreted as the queue's MBS value given in kilobytes.

Default kilobyte

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue cbs)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue cbs)
[Tree] (config>service>vpls>sap>egress>queue-override>queue cbs)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue cbs)

Full Context configure service ies interface sap egress queue-override queue cbs
configure service ies interface sap ingress queue-override queue cbs
configure service vpls sap egress queue-override queue cbs
configure service vpls sap ingress queue-override queue cbs

Description This command overrides specific attributes of the specified queue's CBS parameters.

It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue's CBS settings into the defined reserved total.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets.

If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The **no** form of this command returns the CBS size to the default value.

Parameters *size-in-kbytes* — Specifies the size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10 kbytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values 0 to 1048576, default

Platforms All

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue cbs)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue cbs)

Full Context configure service vprn interface sap egress queue-override queue cbs
configure service vprn interface sap ingress queue-override queue cbs

Description This command can be used to override specific attributes of the specified queue's CBS parameters.

It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue's CBS setting into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets.

If the CBS value is larger than the MBS value, an error occurs, preventing the CBS change.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the CBS to the default value.

Default no cbs

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the queue. For a value of 10 kbytes, enter the number 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimum reserved size can be applied for scheduling purposes).

Values 0 to 131072 or default

Platforms All

cbs

Syntax **cbs** *burst-size*
no cbs

Context **[Tree]** (config>subscr-mgmt>isa-policer cbs)

Full Context configure subscriber-mgmt isa-policer cbs

Description This command specifies the committed burst-size value of this policer. This can only be set on dual-bucket-bandwidth policers.

The **no** form of this command reverts to its default.

Default cbs 0

Parameters *burst-size* — Specifies the committed burst-size in kbytes.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

cbs

Syntax **cbs** {*size* [**bytes** | **kilobytes**] | **default**}
no cbs

Context **[Tree]** (config>card>fp>ingress>access>qgrp>policer-over>plcr cbs)
[Tree] (config>card>fp>ingress>network>qgrp>policer-over>plcr cbs)

Full Context configure card fp ingress access queue-group policer-override policer cbs
configure card fp ingress network queue-group policer-override policer cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the policer's CIR leaky bucket's exceed threshold. The CIR bucket's exceed threshold represents the committed burst tolerance allowed by the policer. If the policer's forwarding rate is equal to or less than the policer's defined CIR, the CIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the forwarding rate increases beyond the profiling rate, the amount of data allowed to be in-profile above the rate is capped by the threshold.

The policer's **cbs** size defined in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command returns the policer to its default CBS size.

Parameters *size* — Specifies that the *size* parameter is required when specifying **cbs** and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **bytes** and **kilobytes** keywords are mutually exclusive and are used to explicitly define whether *size* represents bytes or kilobytes.

Values 0 to 2683435456

bytes — When **bytes** is defined, the value given for size is interpreted as the queue's CBS value given in bytes.

kilobytes — When **kilobytes** is defined, the value is interpreted as the queue's CBS value given in kilobytes.

Default **kilobyte**

default — Specifying the keyword **default** sets the CBS to its default value.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover>q cbs)
[Tree] (config>port>ethernet>access>ing>qgrp>qover>q cbs)
[Tree] (config>port>ethernet>network>egr>qover>q cbs)

Full Context configure port ethernet access egress queue-group queue-overrides queue cbs
configure port ethernet access ingress queue-group queue-overrides queue cbs
configure port ethernet network egress queue-overrides queue cbs

Description This command defines the default committed buffer size for the template queue. Overall, the CBS command follows the same behavior and provisioning characteristics as the CBS command in the queue-group or network QoS policy. The exception is the addition of the cbs-value qualifier keywords bytes or kilobytes.

The **no** form of this command restores the default CBS size to the template queue.

Default cbs default

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10 kbytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values 0 to 1048576 or default

Platforms All

cbs

Syntax **cbs** *size* [**bytes** | **kilobytes**]
no cbs

Context **[Tree]** (config>service>apipe>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>apipe>sap>ingress>policer-over>plcr cbs)
[Tree] (config>service>cpipe>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>cpipe>sap>ingress>policer-over>plcr cbs)
[Tree] (config>service>epipe>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>epipe>sap>ingress>policer-over>plcr cbs)
[Tree] (config>service>fpipe>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>fpipe>sap>ingress>policer-over>plcr cbs)
[Tree] (config>service>ipipe>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>ipipe>sap>ingress>policer-over>plcr cbs)

Full Context configure service apipe sap egress policer-override policer cbs
configure service apipe sap ingress policer-override policer cbs
configure service cpipe sap egress policer-override policer cbs
configure service cpipe sap ingress policer-override policer cbs
configure service epipe sap egress policer-override policer cbs
configure service epipe sap ingress policer-override policer cbs
configure service fpipe sap egress policer-override policer cbs
configure service fpipe sap ingress policer-override policer cbs
configure service ipipe sap egress policer-override policer cbs
configure service ipipe sap ingress policer-override policer cbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured CBS parameter for the specified *policer-id*.

The **no** form of this command returns the CBS size to the default value.

Default no cbs

Parameters *size* — The size parameter is required when specifying cbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bytes — When bytes is defined, the value given for *size* is interpreted as the policer's MBS value in bytes.

kilobytes — When kilobytes is defined, the value given for *size* is interpreted as the policer's MBS value in kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress policer-override policer cbs
- configure service fpipe sap egress policer-override policer cbs
- configure service fpipe sap ingress policer-override policer cbs
- configure service cpipe sap egress policer-override policer cbs

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap ingress policer-override policer cbs
- configure service ipipe sap egress policer-override policer cbs
- configure service epipe sap ingress policer-override policer cbs
- configure service epipe sap egress policer-override policer cbs

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-override policer cbs
- configure service apipe sap egress policer-override policer cbs

cbs

Syntax **cbs** {*size-in-kbytes* | **default**}
no cbs

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue cbs)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue cbs)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue cbs)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue cbs)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue cbs)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue cbs)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue cbs)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue cbs)
[Tree] (config>service>epipe>sap>egress>queue-override>queue cbs)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue cbs)

Full Context configure service apipe sap egress queue-override queue cbs
configure service apipe sap ingress queue-override queue cbs
configure service cpipe sap egress queue-override queue cbs
configure service cpipe sap ingress queue-override queue cbs
configure service epipe sap egress queue-override queue cbs
configure service epipe sap ingress queue-override queue cbs
configure service fpipe sap egress queue-override queue cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service fpipe sap ingress queue-override queue cbs
configure service ipipe sap egress queue-override queue cbs
configure service ipipe sap ingress queue-override queue cbs

Description This command can be used to override specific attributes of the specified queue's CBS parameters.

It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a specific access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue's CBS setting into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly to drop packets.

The **no** form of this command returns the CBS size to the default value.

Default no cbs

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is wanted, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values 0 to 131072, default

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress queue-override queue cbs
- configure service fpipe sap ingress queue-override queue cbs
- configure service cpipe sap egress queue-override queue cbs
- configure service cpipe sap ingress queue-override queue cbs

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue cbs
- configure service apipe sap ingress queue-override queue cbs

All

- configure service epipe sap egress queue-override queue cbs
- configure service epipe sap ingress queue-override queue cbs
- configure service ipipe sap egress queue-override queue cbs
- configure service ipipe sap ingress queue-override queue cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cbs

Syntax **cbs** *size* [{**bytes** | **kilobytes**}]
no cbs

Context **[Tree]** (config>service>vpls>sap>egress>policer-override>plcr cbs)
[Tree] (config>service>vpls>sap>ingress>policer-override>plcr cbs)

Full Context configure service vpls sap egress policer-override policer cbs
configure service vpls sap ingress policer-override policer cbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured CBS parameter for the specified policer-id.

The **no** form of this command returns the CBS size to the default value.

Default no cbs

Parameters *size* — This parameter is required when specifying CBS override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

cbs

Syntax **cbs** *size* [{**bytes** | **kilobytes**}]
no cbs

Context **[Tree]** (config>service>ies>if>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>ies>if>sap>ingress>policer-over>plcr cbs)

Full Context configure service ies interface sap egress policer-override policer cbs
configure service ies interface sap ingress policer-override policer cbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured CBS parameter for the specified policer-id.

The **no** form of this command returns the CBS size to the default value.

Default no cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — This parameter is required when specifying CBS override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

cbs

Syntax **cbs** *size* [{**bytes** | **kilobytes**}]
no cbs

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-over>plcr cbs)
[Tree] (config>service>vprn>if>sap>ingress>policer-over>plcr cbs)

Full Context configure service vprn interface sap egress policer-override policer cbs
configure service vprn interface sap ingress policer-override policer cbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured CBS parameter for the specified policer-id.

The **no** form of this command returns the CBS size to the default value.

Default no cbs

Parameters *size* — This parameter is required when specifying CBS override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

cbs

Syntax **cbs** *congested-cbs*
no cbs

Context **[Tree]** (config>app-assure>group>policer>congestion-override cbs)
[Tree] (config>app-assure>group>policer>congestion-override-stage2 cbs)

Full Context configure application-assurance group policer congestion-override cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group policer congestion-override-stage2 cbs

Description This command configures the committed burst size for a policer. It is recommended that CBS is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. CBS is configurable for dual-bucket bandwidth policers only.

The **no** form of this command removes the congested CBS value from the configuration

Parameters *congested-cbs* — Specifies the committed burst size, in kbytes, when the access-network-level, which the subscriber belongs to, is in a congested state.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cbs

Syntax **cbs** *committed-burst-size*
no cbs

Context **[Tree]** (config>app-assure>group>policer cbs)
[Tree] (config>app-assure>group>tod-override cbs)

Full Context configure application-assurance group policer cbs
configure application-assurance group tod-override cbs

Description This command configures the committed burst size for a policer. It is recommended that CBS is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. CBS is configurable for dual-bucket bandwidth policers only.

The **no** form of this command removes the committed burst size from the configuration.

Parameters *committed-burst-size* — Specifies an integer value defining size, in kbytes, for the CBS of the policer.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cbs

Syntax **cbs** *size* [**bytes** | **kilobytes**]
no cbs

Context **[Tree]** (config>qos>sap-ingress>dyn-policer cbs)
[Tree] (config>qos>sap-egress>dyn-policer cbs)
[Tree] (config>qos>sap-ingress>policer cbs)
[Tree] (config>qos>sap-egress>policer cbs)

Full Context configure qos sap-egress dynamic-policer cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos sap-egress policer cbs
configure qos sap-ingress dynamic-policer cbs
configure qos sap-ingress policer cbs

Description This command configures the policer's CIR leaky bucket's exceed threshold. The CIR bucket's exceed threshold represents the committed burst tolerance allowed by the policer. If the policer's forwarding rate is equal to or less than the policer's defined CIR, the CIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the forwarding rate increases beyond the profiling rate, the amount of data allowed to be in-profile above the rate is capped by the threshold.

The policer's **cbs** size defined in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command returns the policer to its default CBS size.

By default, the CBS is 16 Mbytes when CIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured CBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max CIR capped to 3968 kbytes, with a minimum of 256 bytes.

Parameters *size* **[bytes | kilobytes]** — Specifies an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure qos sap-ingress dynamic-policer cbs
- configure qos sap-egress dynamic-policer cbs

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-egress policer cbs
- configure qos sap-ingress policer cbs

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context **[Tree]** (config>qos>sap-egress>queue cbs)
[Tree] (config>qos>sap-ingress>queue cbs)

Full Context configure qos sap-egress queue cbs
configure qos sap-ingress queue cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command provides a mechanism to override the default reserved buffers for the queue. It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potentially large number of service queues and the economy of statistical multiplexing the individual queue's CBS settings into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high- and low-priority RED slopes on the pool, causing them to miscalculate when to start randomly dropping packets.

If the CBS value is larger than the MBS value, the CBS is capped to the value of the MBS or the minimum CBS value. If the MBS and CBS values are configured to be equal (or nearly equal), this will result in the CBS being slightly higher than the value configured.

The **no** form of this command returns the CBS size to the default value.

Default cbs default

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10 kbytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes) The CBS maximum value used is constrained by the pool size in which the queue exists.

Values 0 to 1048576 or default

Minimum configurable non-zero value: 6 kbytes on an FP2, 7680 bytes on an FP3, and 16 kbytes on an FP4

Minimum non-zero default value: maximum of 10 ms of CIR, or 6 kbytes on an FP2, 7680 bytes on an FP3, and 16 kbytes on an FP4

Platforms All

cbs

Syntax **cbs** *percent*
no cbs

Context **[Tree]** (config>qos>network-queue>queue cbs)

Full Context configure qos network-queue queue cbs

Description The Committed Burst Size (**cbs**) command specifies the relative number of reserved buffers for a specific ingress network FP forwarding class queue or egress network port forwarding class queue. The value is entered as a percentage.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The CBS for a queue is used to determine whether it has exhausted its reserved buffers while enqueuing packets. When the queue has exceeded the number of buffers considered in reserve for this queue, it must contend with other queues for the available shared buffer space within the buffer pool. Access to this shared pool space is controlled through Random Early Detection (RED) slope application.

Two RED slopes are maintained in each buffer pool. A high-priority slope is used by in-profile packets. A low-priority slope is used by out-of-profile packets. At egress, there are two additional RED slopes maintained in each buffer pool: the highplus slope is used by inplus-profile packets, and the exceed slope is used by exceed-profile packets. All network control and management packets are considered in-profile. Assured packets are handled by their in-profile and out-of-profile markings. All best-effort packets are considered out-of-profile. Premium queues should be configured such that the CBS percent is sufficient to prevent shared buffering of packets. This is generally taken care of by the CIR scheduling of premium queues and the overall small amount of traffic on the class. Premium queues in a properly designed system will drain before all others, limiting their buffer utilization.

The RED slopes will detect congestion conditions and work to discard packets and slow down random TCP session flows through the queue. The RED slope definitions can be defined, modified, or disabled through the slope policy assigned to the FP for the network ingress buffer pool or assigned to the network port for network egress buffer pools.

The resultant CBS size can be larger than the MBS. This will result in a portion of the CBS for the queue to be unused and should be avoided.

The **no** form of this command returns the CBS size for the queue to the default for the forwarding class.

Default The cbs forwarding class defaults are listed in the Table 35.

Table 35 **CBS Forwarding Class Defaults**

Forwarding Class	Forwarding Class Label	Default CBS
Network-Control	nc	3
High-1	h1	3
Expedited	ef	1
High-2	h2	1
Low-1	l1	3
Assured	af	1
Low-2	l2	3
Best-Effort	be	1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Special Cases

Forwarding Class Queue on Egress Network Port or Channel — For network egress, each forwarding class is supported by an egress queue on a per network port basis. These forwarding class-based queues are automatically created when a port or channel is placed in the network mode. The configuration parameters for each queue come from the applied egress network-queue policy on the network port or channel. Forwarding class queue on egress channel applies only to the 7450 ESS and 7750 SR.

The **cbs** value is used to calculate the queue's CBS size based on the total amount of buffer space allocated for the buffer pool on the egress network port or channel. This buffer pool size will dynamically fluctuate based on the port or channel's egress pool size setting.

The total reserved buffers based on the total percentages can exceed 100 percent. This might not be desirable and should be avoided as a rule of thumb. If the total percentage equals or exceeds 100 percent of the buffer pool size, no buffers will be available in the shared portion of the pool. Any queue exceeding its CBS size will experience a hard drop on all packets until it drains below this threshold.

Forwarding Class Queue on Ingress FP — For network ingress, each forwarding class is supported by an ingress queue per FP. These forwarding class queues are automatically created when a single port or channel is placed in the network mode on the FP and are removed when all network ports or channels are removed from the FP (defined as access). The configuration parameters for each queue come from the applied ingress policy under the network context of the FP.

The **cbs** value is used to calculate the queue's CBS size based on the total amount of buffer space allocated for the network ingress buffer pool on the FP. This buffer pool will dynamically fluctuate based on the sum of all ingress pool sizes for all network ports and channels on the FP.

The total reserved buffers based on the total percentages can exceed 100 percent. This might not be desirable and should be avoided as a rule of thumb. If the total percentage equals or exceeds 100 percent of the buffer pool size, no buffers will be available in the shared portion of the pool. Any queue exceeding its CBS size will experience a hard drop on all packets until it drains below this threshold.

Parameters *percent* — The percent of buffers reserved from the total buffer pool space, expressed as a decimal integer. If 10 Mbytes is the total buffer space in the buffer pool, a value of 10 would reserve 1 Mbyte (10%) of buffer space for the forwarding class queue. The value 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can be applied for scheduling purposes).

Values 0 to 100

Platforms All

cbs

Syntax **cbs** {*size-in-kbytes* | **default**}
no cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>qgrps>egr>qgrp>policer cbs)
[Tree] (config>qos>qgrps>ing>qgrp>policer cbs)

Full Context configure qos queue-group-templates egress queue-group policer cbs
configure qos queue-group-templates ingress queue-group policer cbs

Description The **cbs** command is used to define the default committed buffer size for the template queue or the CBS for the template policer. Overall, the cbs command follows the same behavior and provisioning characteristics as the cbs command in the SAP ingress and egress QoS policy.

The **no** form of this command restores the default CBS size to the template policer.

Default default

Parameters *size-in-kbytes* — For the queues, the size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10 kbytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes). For policers, the size parameter is an integer expression of the number of kilobytes for the policer CBS.

Values 0 to 2683435456, **default**

Minimum default value: 16 Mbytes when CIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured CBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max CIR capped to 3968 kbytes, with a minimum of 256 bytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

cbs

Syntax **cbs** {*size-in-kbytes* | **default**}
no cbs

Context [Tree] (config>qos>qgrps>egr>qgrp>queue cbs)
[Tree] (config>qos>qgrps>ing>qgrp>queue cbs)

Full Context configure qos queue-group-templates egress queue-group queue cbs
configure qos queue-group-templates ingress queue-group queue cbs

Description The **cbs** command is used to define the default committed buffer size for the template queue or the CBS for the template policer. Overall, the cbs command follows the same behavior and provisioning characteristics as the cbs command in the SAP ingress and egress QoS policy.

The **no** form of this command restores the default CBS size to the template policer.

Default default

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size-in-kbytes* — For the queues, the size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10 kbytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes). For policers, the size parameter is an integer expression of the number of kilobytes for the policer CBS.

Values 0 to 1048576 or **default**

Minimum configurable non-zero value: 6 kbytes on an FP2, 7680 bytes on an FP3, and 16 kbytes on an FP4

Minimum non-zero default value: maximum of 10 ms of CIR or 6 kbytes on an FP2, 7680 bytes on an FP3, and 16 kbytes on an FP4

Platforms All

cbs

Syntax **cbs** *percent*
no cbs

Context **[Tree]** (config>qos>shared-queue>queue cbs)

Full Context configure qos shared-queue queue cbs

Description The Committed Burst Size (**cbs)** command specifies the relative amount of reserved buffers for a specific ingress shared queue. The value is entered as a percentage.

The CBS for a queue is used to determine whether it has exhausted its reserved buffers while enqueuing packets. When the queue has exceeded the amount of buffers considered in reserve for this queue, it must contend with other queues for the available shared buffer space within the buffer pool.

The resultant CBS size can be larger than the MBS. This will result in a portion of the CBS for the queue being unused and should be avoided.

Default The queue CBS defaults are listed in Table 36.

Table 36 **Queue CBS Default Values**

Queue	Default CBS
1	1
2	3
3	10
4	3
5	10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 36 **Queue CBS Default Values**

Queue	Default CBS
6	10
7	3
8	3
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

Parameters *percent* — The percent of buffers reserved from the total buffer pool space, expressed as a decimal integer. The value 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can be applied for scheduling purposes).

Values 0 to 100

Platforms All

cbs

Syntax **cbs** *cbs*
no cbs

Context **[Tree]** (config>system>cpm-queue>queue cbs)

Full Context configure system cpm-queue queue cbs

Description This command specifies the amount of buffer that can be drawn from the reserved buffer portion of the queue's buffer pool.

Parameters *cbs* — Specifies the committed burst size in kbytes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.29 cc-error

cc-error

Syntax [**no**] **cc-error**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms cc-error)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms cc-error)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms cc-error)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms cc-error
configure mcast-management multicast-info-policy bundle channel video analyzer alarms cc-error
configure mcast-management multicast-info-policy bundle video analyzer alarms cc-error

Description This command configures the analyzer to check the continuity counter. The continuity counter should be incremented per PID; otherwise, it is considered a continuity counter error.

Default no cc-error

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

7.30 ccm-enable

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep ccm-enable)

Full Context configure eth-tunnel path eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>lag>eth-cfm>mep ccm-enable)
[Tree] (config>port>ethernet>eth-cfm>mep ccm-enable)

Full Context configure lag eth-cfm mep ccm-enable
configure port ethernet eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>service>epipe>spoke-sdp>eth-cfm>mep ccm-enable)
[Tree] (config>service>epipe>sap>eth-cfm>mep ccm-enable)

Full Context configure service epipe sap eth-cfm mep ccm-enable
configure service epipe spoke-sdp eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>service>vpls>eth-cfm>mep ccm-enable)
[Tree] (config>service>vpls>sap>eth-cfm>mep ccm-enable)
[Tree] (config>service>vpls>mesh-sdp>mep ccm-enable)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep ccm-enable)

Full Context configure service vpls eth-cfm mep ccm-enable
configure service vpls mesh-sdp mep ccm-enable
configure service vpls sap eth-cfm mep ccm-enable
configure service vpls spoke-sdp eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep ccm-enable)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep ccm-enable)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep ccm-enable)

Full Context configure service ies interface sap eth-cfm mep ccm-enable
configure service ies interface spoke-sdp eth-cfm mep ccm-enable
configure service ies subscriber-interface group-interface sap eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep ccm-enable

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep ccm-enable
- configure service ies interface sap eth-cfm mep ccm-enable

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep ccm-enable)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep ccm-enable)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm ccm-enable)

Full Context configure service vprn interface sap eth-cfm mep ccm-enable
configure service vprn interface spoke-sdp eth-cfm mep ccm-enable
configure service vprn subscriber-interface group-interface sap eth-cfm ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>router>if>eth-cfm>mep ccm-enable)

Full Context configure router interface eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-enable

Syntax [**no**] **ccm-enable**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep ccm-enable)

Full Context configure eth-ring path eth-cfm mep ccm-enable

Description This command enables the generation of CCM messages.

The **no** form of the command disables the generation of CCM messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.31 ccm-hold-time

ccm-hold-time

Syntax **ccm-hold-time** {**down** *down-timeout*] [**up** *up-timeout*}
no ccm-hold-time

Context **[Tree]** (config>eth-tunnel ccm-hold-time)

Full Context configure eth-tunnel ccm-hold-time

Description This command allows a sub second CCM enabled MEP to delay a transition to a failed state if a configured remote CCM peer has timed out. The MEP will remain in the UP state for 3.5 times CCM interval + down-delay.

The **no** form of this command removes the additional delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **down** *down-timeout* — Specifies the time, in centiseconds, used for the hold-timer for associated Continuity Check (CC) Session down event dampening. This guards against reporting excessive member operational state transitions.

This is implemented by not advertising subsequent transitions of the CC state to the Ethernet Tunnel Group until the configured timer has expired.

Values 0 to 1000

Default 0

up *up-timeout* — Specifies the time, in deciseconds, used for the hold-timer for associated Continuity Check (CC) Session up event dampening. This guards against reporting excessive member operational state transitions.

This is implemented by not advertising subsequent transitions of the CC state to the Ethernet Tunnel Group until the configured timer has expired.

Values 0 to 5000

Default 20

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-hold-time

Syntax **ccm-hold-time down** *timer*
no ccm-hold-time

Context **[Tree]** (config>eth-cfm>domain>assoc ccm-hold-time)

Full Context configure eth-cfm domain association ccm-hold-time

Description This command allows a sub second CCM enabled MEP to delay a transition to a failed state if a configured remote CCM peer has timed out. The MEP remains in the UP state for 3.5 times CCM interval + down-delay.

The **no** form of this command removes the additional delay.

Default no ccm-hold-time

Parameters **down** *timer* — Specifies the amount of time to delay, in centiseconds.

Values 0 to 1000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-hold-time

Syntax **ccm-hold-time** [**down** *down-timeout*] [**up** *up-timeout*]
no ccm-hold-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>eth-ring ccm-hold-time)

Full Context configure eth-ring ccm-hold-time

Description This command configures eth-ring dampening timers. See the **down** and **up** commands for more information.

The **no** form of the command sets the up and down timers to the default values.

Parameters *down-timeout* — Specifies the down timeout, in centiseconds.

Values 0 to 5000

up-timeout — Specifies the hold-time for reporting the recovery, in deciseconds.

Values 0 to 5000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.32 ccm-interval

ccm-interval

Syntax **ccm-interval** *interval*
no ccm-interval

Context [Tree] (config>eth-cfm>domain>assoc ccm-interval)

Full Context configure eth-cfm domain association ccm-interval

Description This command configures the CCM transmission interval for all MEPs in the association.

The **no** form of this command reverts to the default value.

Default no ccm-interval

Parameters *interval* — Specifies the interval between CCM transmissions to be used by all MEPs in the MA.

Values 10 milliseconds, 100 milliseconds, 1 second, 10 seconds, 60 seconds, 600 seconds

Default 10 (seconds)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.33 ccm-ltm-priority

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep ccm-ltm-priority)

Full Context configure eth-tunnel path eth-cfm mep ccm-ltm-priority

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of this command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>lag>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>port>ethernet>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>router>if>eth-cfm>mep ccm-ltm-priority)

Full Context configure lag eth-cfm mep ccm-ltm-priority
configure port ethernet eth-cfm mep ccm-ltm-priority
configure router interface eth-cfm mep ccm-ltm-priority

Description This command specifies the priority of the CCM and LTM messages transmitted by the MEP. Since CCM does not apply to the Router Facility MEP only the LTM priority is of value under that context.

The **no** form of this command reverts to the default values.

Default no ccm-ltm-priority

Parameters *priority* — Specifies the priority value.

Values 0 to 7

Default 7, highest priority for CCMs and LTMs transmitted by the MEP

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>service>epipe>spoke-sdp>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>epipe>sap>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>ipipe>sap>eth-cfm>mep ccm-ltm-priority)

Full Context configure service epipe sap eth-cfm mep ccm-ltm-priority
configure service epipe spoke-sdp eth-cfm mep ccm-ltm-priority
configure service ipipe sap eth-cfm mep ccm-ltm-priority

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of this command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>service>vpls>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>vpls>sap>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>vpls>mesh-sdp>mep ccm-ltm-priority)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep ccm-ltm-priority)

Full Context configure service vpls eth-cfm mep ccm-ltm-priority
configure service vpls mesh-sdp mep ccm-ltm-priority
configure service vpls sap eth-cfm mep ccm-ltm-priority
configure service vpls spoke-sdp eth-cfm mep ccm-ltm-priority

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of this command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *priority* — Specifies the priority of CCM and LTM messages

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep ccm-ltm-priority)

Full Context configure service ies interface sap eth-cfm mep ccm-ltm-priority
configure service ies interface spoke-sdp eth-cfm mep ccm-ltm-priority
configure service ies subscriber-interface group-interface sap eth-cfm mep ccm-ltm-priority

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of this command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep ccm-ltm-priority

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep ccm-ltm-priority
- configure service ies interface spoke-sdp eth-cfm mep ccm-ltm-priority

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep ccm-ltm-priority)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm ccm-ltm-priority)

Full Context configure service vprn interface sap eth-cfm mep ccm-ltm-priority
configure service vprn interface spoke-sdp eth-cfm mep ccm-ltm-priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap eth-cfm ccm-ltm-priority

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of this command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep ccm-ltm-priority)

Full Context configure eth-ring path eth-cfm mep ccm-ltm-priority

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of the command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.34 ccm-padding-size

ccm-padding-size

Syntax **ccm-padding-size** *ccm-padding*
no ccm-padding-size

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep ccm-padding-size)
[Tree] (config>lag>eth-cfm>mep ccm-padding-size)

Full Context configure eth-tunnel path eth-cfm mep ccm-padding-size
configure lag eth-cfm mep ccm-padding-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command inserts additional padding in the CCM packets.

The **no** form of this command reverts to the default.

Parameters *ccm-padding* — Specifies the additional padding in the CCM packets, in octets.

Values 3 to 1500

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ccm-padding-size

Syntax **ccm-padding-size** *ccm-padding*
no ccm-padding-size *ccm-padding*

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>ipipe>sap>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>vpls>sap>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep ccm-padding-size)
[Tree] (config>port>ethernet>eth-cfm>mep ccm-padding-size)
[Tree] (config>lag>eth-cfm>mep ccm-padding-size)
[Tree] (config>router>if>eth-cfm>mep ccm-padding-size)

Full Context configure lag eth-cfm mep ccm-padding-size
configure port ethernet eth-cfm mep ccm-padding-size
configure router interface eth-cfm mep ccm-padding-size
configure service epipe sap eth-cfm mep ccm-padding-size
configure service epipe spoke-sdp eth-cfm mep ccm-padding-size
configure service ipipe sap eth-cfm mep ccm-padding-size
configure service vpls mesh-sdp eth-cfm mep ccm-padding-size
configure service vpls sap eth-cfm mep ccm-padding-size
configure service vpls spoke-sdp eth-cfm mep ccm-padding-size

Description Set the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

Default no ccm-padding-size

Parameters *ccm-padding* — Specifies the byte size of the Optional Data TLV.

Values 3 to 1500

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ccm-padding-size

Syntax **ccm-padding-size** *ccm-padding*
no ccm-padding-size

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep ccm-padding-size)

Full Context configure service ies interface sap eth-cfm mep ccm-padding-size
configure service ies interface spoke-sdp eth-cfm mep ccm-padding-size
configure service ies subscriber-interface group-interface sap eth-cfm mep ccm-padding-size

Description Set the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

Default ccm-padding-size

Parameters *ccm-padding* — Specifies the byte size of the Optional Data TLV.

Values 3 to 1500

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep ccm-padding-size

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep ccm-padding-size
- configure service ies interface sap eth-cfm mep ccm-padding-size

ccm-padding-size

Syntax **ccm-padding-size** *ccm-padding*
no ccm-padding-size

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep ccm-padding-size)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep ccm-padding-size)

Full Context configure service vprn interface sap eth-cfm mep ccm-padding-size
configure service vprn interface spoke-sdp eth-cfm mep ccm-padding-size
configure service vprn subscriber-interface group-interface sap eth-cfm mep ccm-padding-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer 2 encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

Parameters *ccm-padding* — Specifies the byte size of the Optional Data TLV.

Values 3 to 1500

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep ccm-padding-size

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm mep ccm-padding-size
- configure service vprn interface sap eth-cfm mep ccm-padding-size

ccm-padding-size

Syntax **ccm-padding-size** *ccm-padding*
no ccm-padding-size

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep ccm-padding-size)

Full Context configure eth-ring path eth-cfm mep ccm-padding-size

Description This command inserts additional padding in the CCM packets.

The **no** form of the command reverts to the default.

Parameters **ccm-padding** — Specifies the additional padding in the CCM packets.

Values 3 to 1500 octets

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.35 ccm-tlv-ignore

ccm-tlv-ignore

Syntax **ccm-tlv-ignore** [**interface-status**] [**port-status**]
no ccm-tlv-ignore

Context **[Tree]** (config>port>ethernet>eth-cfm>mep ccm-tlv-ignore)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>lag>eth-cfm>mep ccm-tlv-ignore)
[Tree] (config>router>if>eth-cfm>mep ccm-tlv-ignore)

Full Context configure lag eth-cfm mep ccm-tlv-ignore
configure port ethernet eth-cfm mep ccm-tlv-ignore
configure router interface eth-cfm mep ccm-tlv-ignore

Description This command allows the receiving MEP to ignore the specified TLVs in CCM PDU. Ignored TLVs will be reported as absent and will have no impact on the MEP state machine.

The **no** form of this command means the receiving MEP will process all recognized TLVs in the CCM PDU.

Default no ccm-tlv-ignore

Parameters **interface-status** — Ignores the interface status TLV on reception.

port-status — Ignores the port status TLV on reception.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.36 ccrt-replay

ccrt-replay

Syntax **ccrt-replay**

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx ccrt-replay)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy ccrt-replay)

Full Context configure subscriber-mgmt diameter-application-policy gx ccrt-replay
configure subscriber-mgmt diameter-application-policy gy ccrt-replay

Description Commands in this context configure CCR-T replay. CCR-T replay is enabled with a **no shutdown** of this context. If a communication failure between client and server occurs, CCR-T replay enables the retransmission of CCR-T messages for a Gx or Gy session at a configured intervals until a valid response (CCA-t) is received or until the configured **max-lifetime** period expires, whichever comes first.

In Gx, replaying CCR-T messages ensures that the Gx session is cleared on the PCRF side in cases where the peering session to the PCRF was not available at the time that the initial and the first retransmitted CCR-T was sent.

In Gy, replaying CCR-T messages ensures that the final credit control usage reporting is not lost for billing by the OCS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The subscriber host or session that triggered the Gx or Gy session that is in CCR-T replay mode is deleted from the system at the time that the initial CCR-T is sent. All resources associated with the subscriber host or session, such as queues, DHCP lease states, and PPPoE session states are released. The orphaned Gx and Gy sessions in replay mode are left in the system.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.37 cd

cd

Syntax **cd** [*file-url*]

Context **[Tree]** (file cd)

Full Context file cd

Description This command displays or changes the current working directory in the local file system.

Parameters *file-url* — Specifies the file URL.

Values

local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length 99 chars max each
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 199 characters
remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

If no *file-url* is entered, the current working directory is displayed.

.. — signifies the parent directory. This can be used in place of an actual directory name in a *directory-url*.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

directory-url — Specifies the destination directory.

Platforms All

7.38 ce-address

ce-address

Syntax **ce-address** *ip-address*
no ce-address

Context **[Tree]** (config>service>ipipe>sap ce-address)
[Tree] (config>service>ipipe>spoke-sdp ce-address)

Full Context configure service ipipe sap ce-address
configure service ipipe spoke-sdp ce-address

Description This command specifies the IP address of the CE device associated with an Ipipe SAP or spoke SDP. In the case of a SAP, it is the address of the CE device directly attached to the SAP. For a spoke SDP, it is the address of the CE device reachable through that spoke SDP (for example, attached to the SAP on the remote node). The address must be a host address (no subnet addresses are accepted) as there must be only one CE device attached to an Ipipe SAP. The CE address specified at one end of an Ipipe will be used in processing ARP messages at the other endpoint, as the router acts as a proxy for ARP messages.

On a 7450 ESS, this command specifies the IP address of the CE device associated with an Ipipe SAP. In the case of a SAP, it is the address of the CE device directly attached to the SAP. The address must be a host address (no subnet addresses are accepted) as there must be only one CE device attached to an Ipipe SAP. The CE address specified at one end of an Ipipe will be used in processing ARP messages at the other endpoint, as the router acts as a proxy for ARP messages.

Parameters *ip-address* — Specifies the IP address of the CE device associated with an Ipipe SAP.

Platforms All

7.39 ce-address-discovery

ce-address-discovery

Syntax **ce-address-discovery** [**keep**]
ce-address-discovery ipv6 [**keep**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ce-address-discovery

Context [Tree] (config>service>ipipe ce-address-discovery)

Full Context configure service ipipe ce-address-discovery

Description This command specifies whether the service will automatically discover the CE IP addresses.

When enabled, the addresses will be automatically discovered on SAPs that support address discovery, and on the spoke SDPs. When enabled, addresses configuration on the Ipipe SAP and spoke SDPs will not be allowed.

If disabled, CE IP addresses must be manually configured for the SAPs to become operationally up.

Default no ce-address-discovery

Parameters **ipv6** — The **ipv6** keyword enables IPv6 CE address discovery support on the Ipipe so that both IPv4 and IPv6 address discovery are supported. If the **ipv6** keyword is not included, then only IPv4 address discovery is supported and IPv6 packets are dropped.

keep — The keep keyword is only applicable to eth-legacy-fault-notification. This option maintains the CE address discovered even when the SAP on which the address was learned fails. The ARP entry will not be maintained if the SAP is administratively shutdown, the **clear service id** *svc-id* {**arp** | **neighbor**} is used to remove the ARP entry or the node reboots.

Platforms All

7.40 cell-concatenation

cell-concatenation

Syntax **cell-concatenation**

Context [Tree] (config>service>apipe>spoke-sdp cell-concatenation)

Full Context configure service apipe spoke-sdp cell-concatenation

Description Commands in this context provide access to the various options that control the termination of ATM cell concatenation into an MPLS frame. Several options can be configured simultaneously. The concatenation process for a specified MPLS packet ends when the first concatenation termination condition is met. The concatenation parameters apply only to ATM N:1 cell mode VLL.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.41 cell-format

cell-format

Syntax **cell-format** {**uni** | **nni**}

Context **[Tree]** (config>port>sonet-sdh>path>atm cell-format)
[Tree] (config>port>tdm>ds1>channel-group>atm cell-format)
[Tree] (config>port>tdm>ds3>atm cell-format)
[Tree] (config>port>tdm>e1>channel-group>atm cell-format)
[Tree] (config>port>tdm>e3>atm cell-format)
[Tree] (config>port>ml-bundle>ima>atm cell-format)

Full Context configure port multilink-bundle ima atm cell-format
configure port sonet-sdh path atm cell-format
configure port tdm ds1 channel-group atm cell-format
configure port tdm ds3 atm cell-format
configure port tdm e1 channel-group atm cell-format
configure port tdm e3 atm cell-format

Description This command configures the ATM cell format.

Parameters **uni** — Specifies the user-to-network interface (UNI) cell format.

nni — Specifies the network-to-network interface (NNI) cell format.

Platforms 7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle ima atm cell-format

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group atm cell-format
- configure port tdm e3 atm cell-format
- configure port tdm ds3 atm cell-format
- configure port tdm e1 channel-group atm cell-format

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure port sonet-sdh path atm cell-format

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.42 cem

cem

Syntax **cem**

Context **[Tree]** (config>service>cpipe>sap cem)
[Tree] (config>service>epipe>sap cem)

Full Context configure service cpipe sap cem
configure service epipe sap cem

Description Commands in this context specify circuit emulation (CEM) properties.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap cem

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service epipe sap cem

cem

Syntax **cem**

Context **[Tree]** (config>mirror>mirror-dest>sap cem)

Full Context configure mirror mirror-dest sap cem

Description Commands in this context specify circuit emulation (CEM) mirroring properties.

Ingress and egress options cannot be supported at the same time on a CEM encap-type SAP. The options must be configured in either the ingress **or** egress contexts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.43 cert

cert

Syntax **cert** *cert-filename*
no cert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>cert-profile>entry cert)

Full Context configure ipsec cert-profile entry cert

Description This command specifies the file name of an imported certificate for the cert-profile entry.

The **no** form of this command removes the cert-file-name from the entry configuration.

Default no cert

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cert

Syntax **cert**

Context [Tree] (config>ipsec>trans-mode-prof>dyn cert)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>dyn cert)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn cert)
[Tree] (config>service>ies>if>sap>ipsec-gw cert)
[Tree] (config>service>vprn>if>sap>ipsec-gw cert)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn cert)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying cert
configure router interface ipsec ipsec-tunnel dynamic-keying cert
configure service ies interface ipsec ipsec-tunnel dynamic-keying cert
configure service ies interface sap ipsec-gw cert
configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert
configure service vprn interface sap ipsec-gw cert

Description Commands in this context configure certificate parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec ipsec-transport-mode-profile dynamic-keying cert
- configure service vprn interface sap ipsec-gw cert
- configure service ies interface sap ipsec-gw cert

VSR

- configure service ies interface ipsec ipsec-tunnel dynamic-keying cert
- configure router interface ipsec ipsec-tunnel dynamic-keying cert
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert

cert

Syntax **cert** *cert-filename*
no cert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>security>tls>cert-profile>entry cert)

Full Context configure system security tls cert-profile entry cert

Description This command specifies the file name of an imported certificate for the **cert-profile** entry.

The **no** form of the command removes the certificate.

Default no cert

Parameters *cert-filename* — Specifies the file name of the TLS certificate, up to 95 characters in length.

Platforms All

7.44 cert-file

cert-file

Syntax **cert-file** *filename*
no cert-file

Context [Tree] (config>system>security>pki>ca-profile cert-file)

Full Context configure system security pki ca-profile cert-file

Description This command specifies the filename of a file in cf3:\system-pki\cert as the CA's certificate of the ca-profile.

Notes:

- The system will perform following checks against configured cert-file when a **no shutdown** command is issued:
  - Configured cert-file must be a DER formatted X.509v3 certificate file.
  - All non-optional fields defined in section 4.1 of RFC5280 must exist and conform to the RFC 5280 defined format.
  - Check the version field to see if its value is 0x2.
  - Check The Validity field to see that if the certificate is still in validity period.
  - X509 basic constraints extension must exists, and CA Boolean must be True.
  - If Key Usage extension exists, then at least keyCertSign and cRLSign should be asserted.
  - If the certificate is not a self-signing certificate, then system will try to look for issuer's CA's certificate to verify if this certificate is signed by issuer's CA; but if there is no such CA-profile configured, then system will just proceed with a warning message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If the certificate is not a self-signing certificate, then system will try to look for issuer's CA's CRL to verify that it has not been revoked; but if there is no such CA-profile configured or there is no such CRL, then system will just proceed with a warning message.

If any of above checks fails, then the **no shutdown** command will fail.

- Changing or removing of **cert-file** is only allowed when the **ca-profile** is in a **shutdown** state.

The **no** form of this command removes the filename from the configuration.

Parameters *filename* — Specifies a local CF card file URL.

Platforms All

7.45 cert-profile

cert-profile

Syntax **cert-profile** *profile-name* [**create**]
no cert-profile *profile-name*

Context **[Tree]** (config>ipsec cert-profile)

Full Context configure ipsec cert-profile

Description This command creates a new cert-profile or enters the configuration context of an existing cert-profile.

The **no** form of this command removes the profile name from the cert-profile configuration.

Parameters *profile-name* — Specifies the name of the certification profile up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cert-profile

Syntax **cert-profile** *name*
no cert-profile

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>dyn>cert cert-profile)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn>cert cert-profile)
[Tree] (config>service>ies>if>sap>ipsec-gw>cert cert-profile)
[Tree] (config>service>vprn>if>sap>ipsec-gw>cert cert-profile)
[Tree] (config>service>vprn>if>sap>ipsec-tun>dyn>cert cert-profile)
[Tree] (config>router>if>ipsec>ipsec-tun>dyn>cert cert-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>ipsec>trans-mode-prof>dyn>cert cert-profile)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying cert cert-profile
configure router interface ipsec ipsec-tunnel dynamic-keying cert cert-profile
configure service ies interface ipsec ipsec-tunnel dynamic-keying cert cert-profile
configure service ies interface sap ipsec-gw cert cert-profile
configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert cert-profile
configure service vprn interface sap ipsec-gw cert cert-profile
configure service vprn interface sap ipsec-tunnel dynamic-keying cert cert-profile

Description This command specifies the name of certificate profile to be used for authentication.

The **no** form of this command removes the name from the configuration.

Parameters *name* — Specifies the profile name, up to 32 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec ipsec-transport-mode-profile dynamic-keying cert cert-profile
- configure service vprn interface sap ipsec-tunnel dynamic-keying cert cert-profile
- configure service vprn interface sap ipsec-gw cert cert-profile
- configure service ies interface sap ipsec-gw cert cert-profile

VSR

- configure service ies interface ipsec ipsec-tunnel dynamic-keying cert cert-profile
- configure router interface ipsec ipsec-tunnel dynamic-keying cert cert-profile
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert cert-profile

cert-profile

Syntax **cert-profile** *profile-name* [**create**]
no cert-profile *profile-name*

Context [Tree] (config>system>security>tls cert-profile)

Full Context configure system security tls cert-profile

Description This command configures TLS certificate profile information. The certificate profile contains the certificates that are sent to the TLS peer (server or client) to authenticate itself. It is mandatory for the TLS server to send this information. The TLS client may optionally send this information upon request from the TLS server.

The **no** form of the command deletes the specified TLS certificate profile.

Parameters *profile-name* — Specifies the name of the TLS certificate profile, up to 32 characters in length.

create — Keyword used to create the TLS certificate profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

cert-profile

Syntax **cert-profile** *name*
no cert-profile

Context **[Tree]** (config>system>security>tls>client-tls-profile cert-profile)

Full Context configure system security tls client-tls-profile cert-profile

Description This command assigns a TLS certificate profile to be used by the TLS client profile. This certificate is sent to the server for authentication of the client and public key.

The **no** form of the command removes the TLS certificate profile assignment.

Parameters *name* — Specifies the name of the TLS certificate profile, up to 32 characters in length.

Platforms All

cert-profile

Syntax **cert-profile** *name*
no cert-profile

Context **[Tree]** (config>system>security>tls>server-tls-profile cert-profile)

Full Context configure system security tls server-tls-profile cert-profile

Description This command assigns a TLS certificate profile to be used by the TLS server profile. This certificate is sent to the client for authentication of the server and public key.

The **no** form of the command removes the TLS certificate profile assignment.

Parameters *name* — Specifies the name of the TLS certificate profile, up to 32 characters in length.

Platforms All

7.46 cert-request

cert-request

Syntax **cert-request ca** *ca-profile-name* **current-key** *key-filename* **current-cert** *cert-filename* [**hash-alg** *hash-algorithm*] **newkey** *key-filename* **subject-dn** *subject-dn* [**domain-name** *domain-names*] [**ip-addr** *ip-address* | *ipv6-address*] **save-as** *save-path-of-result-cert*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (admin>certificate>cmpv2 cert-request)

Full Context admin certificate cmpv2 cert-request

Description This command requests an additional certificate after the system has obtained the initial certificate from the CA.

The request is authenticated by a signature signed by the current-key, along with the current-cert. The hash algorithm used for signature is depends on the key type:

- DSA key: SHA1
- RSA key: MD5/SHA1/SHA224 | SHA256 | SHA384 | SHA512, by default is SHA1

In some cases, the CA may not return a certificate immediately, due to reasons such as **request processing need manual intervention**. In such cases, the **admin certificate cmpv2 poll** command can be used to poll the status of the request.

Parameters **ca** *ca-profile-name* — Specifies a ca-profile name which includes CMP server information up to 32 characters.

current-key *key-filename* — Specifies corresponding certificate issued by the CA up to 95 characters.

current-cert *cert-filename* — Specifies the file name of an imported certificate that is attached to the certificate request up to 95 characters.

newkey *key-filename* — Specifies the file name of the imported key up to 95 characters.

hash-alg *hash-algorithm* — Specifies the hash algorithm for RSA key.

Values md5,sha1,sha224,sha256,sha384,sha512

subject-dn *dn* — Specifies the subject of the requesting certificate up to 256 characters.

Values attr1=val1,attr2=val2where: attrN={C | ST | O | OU | CN}

save-as *save-path-of-result-cert* — Specifies the save full path name of saving the result certificate, up to 200 characters.

domain-name *domain-names* — Specifies FQDNs for SubjectAltName of the requesting certificate, separated by commas, up to 512 characters.

ip-addr *ip-address* **|** *ipv6-address* — Specifies an IPv4 or IPv6 address for SubjectAltName of the requesting certificate.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.47 cert-sync

cert-sync

Syntax [**no**] **cert-sync**

Context **[Tree]** (admin>redundancy cert-sync)
[Tree] (config>redundancy cert-sync)

Full Context admin redundancy cert-sync
configure redundancy cert-sync

Description This command automatically synchronizes the certificate/CRL/key when importing or generating (for the key). If a new CF card is inserted into slot3 into the backup CPM, the system will sync the whole system-pki directory from the active CPM.

Default enabled

Platforms All

7.48 certificate

certificate

Syntax **certificate** *certificate-file*
no certificate

Context **[Tree]** (config>app-assure>group>certificate-profile certificate)

Full Context configure application-assurance group certificate-profile certificate

Description This command indicated the file name of the certificate to be added to the profile.

The **no** form of this command removes the certificate from the profile.

Default no certificate

Parameters *certificate-file* — Specifies the name of the certificate file, up to 95 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

certificate

Syntax **certificate**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (admin certificate)

Full Context admin certificate

Description Commands in this context configure X.509 certificate related operational parameters. For information about CMPv6 admin certificate commands, see the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter and Extended Services Appliance Guide.*

Platforms All

certificate

Syntax certificate

Context **[Tree]** (debug certificate)

Full Context debug certificate

Description Commands in this context debug certificates.

Platforms All

certificate

Syntax **certificate** *filename*

Context **[Tree]** (debug>ipsec certificate)

Full Context debug ipsec certificate

Description This command enables debug for certificate chain computation in cert-profile.

Parameters *filename* — Displays the filename of imported certificate, up to 95 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.49 certificate-display-format

certificate-display-format

Syntax **certificate-display-format** {**ascii** | **utf8**}

Context **[Tree]** (config>system>security>pki certificate-display-format)

Full Context configure system security pki certificate-display-format

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the display format used for the Certificates and Certificate Revocation Lists.

Default certificate-display-format ascii

Parameters **ascii** — Specifies the ASCII format to use for the Certificates and Certificate Revocation Lists.

utf8 — Specifies the UTF8 format to use for the Certificates and Certificate Revocation Lists.

Platforms All

7.50 certificate-expiration-warning

certificate-expiration-warning

Syntax **certificate-expiration-warning** *hours* [**repeat** *repeat-hours*]
no certificate-expiration-warning

Context **[Tree]** (config>system>security>pki certificate-expiration-warning)

Full Context configure system security pki certificate-expiration-warning

Description With this command configured, the system issues two types of warnings related to certificate expiration:

- **BeforeExp —** A warning message issued before certificate expire
- **AfterExp —** A warning message issued when certificate expire

This command specifies when system will issue **BeforeExp** message before a certificate expires. For example, with c**ertificate-expiration-warning 5**, the system will issue a **BeforeExp** message 5 hours before a certificate expires. An optional **repeat** <*repeat-hour*> parameter will enable the system to repeat the **BeforeExp** message every hour until the certificate expires.

If the user only wants **AfterExp**, then **certificate-expiration-warning 0** can be used to achieve this.

BeforeExp and **AfterExp** warnings can be cleared in following cases:

- The certificate is reloaded by the **admin certificate reload** command. In this case, if the reloaded file is not expired, then **AfterExp** is cleared. And, if the reloaded file is outside of configured warning window, then the **BeforeExp** is also cleared.
- When the **ca-profile/ipsec-gw/ipsec-tunnel/cert-profile** is shutdown, then **BeforeExp** and **AfterExp** of corresponding certificates are cleared.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- When **no certificate-expiration-warning** command is configured, then all existing **BeforeExp** and **AfterExp** are cleared.
- Users may change the configuration of the **certificate-expiration-warning** so that certain certificates are no longer in the warning window. **BeforeExp** of corresponding certificates are cleared.
- If the system time changes so that the new time causes the certificates to no longer be in the warning window, then **BeforeExp** is cleared. If the new time causes an expired certificate to come non-expired, then **AfterExp** is cleared.

Default no certificate-expiration-warning

Parameters *hours* — Specifies the amount of time before a certificate expires when system issues BeforeExp.

Values 0 to 8760

repeat-hours — Specifies the time the system will repeat BeforeExp every repeat-hour.

Values 0 to 8760

Platforms All

7.51 certificate-profile

certificate-profile

Syntax **certificate-profile** *cert-prof-name* [**create**]
no certificate-profile *cert-prof-name*

Context **[Tree]** (config>app-assure>group certificate-profile)

Full Context configure application-assurance group certificate-profile

Description This command creates a certificate profile to be used for certificate-based encryption in HTTP header enrichment.

The **no** form of this command removes the certificate profile.

Parameters *cert-profile-name* — Specifies the name of the profile, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.52 cflash-cap-alarm

cflash-cap-alarm

Syntax **cflash-cap-alarm** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-alarm *cflash-id*

Context **[Tree]** (config>system>thresholds cflash-cap-alarm)

Full Context configure system thresholds cflash-cap-alarm

Description This command enables capacity monitoring of the compact flash specified in this command. The severity level is alarm. Both a rising and falling threshold can be specified.

The **no** form of this command removes the configured compact flash threshold alarm.

Parameters *cflash-id* — Specifies the name of the cflash device to be monitored.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

rising-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold value represents units of 512 bytes.

Values -2147483648 to 2147483647

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value represents units of 512 bytes.

Values -2147483648 to 2147483647

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

seconds — Specifies the polling period, in seconds, over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

alarm-type — Specifies the alarm that may be sent when this alarm is first created

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Configuration example

```
cflash-cap-alarm cf1-A: rising-threshold 50000000 falling-threshold 49999900
interval 120 rmon-event-type both start-alarm rising
```

Platforms All

7.53 cflash-cap-alarm-pct

cflash-cap-alarm-pct

Syntax **cflash-cap-alarm-pct** *cflash-id* **rising-threshold** *percentage* [**falling-threshold**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percentage] **interval** *seconds* [**rmon-event-type** *event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-alarm-pct *cflash-id*

Context **[Tree]** (config>system>thresholds cflash-cap-alarm-pct)

Full Context configure system thresholds cflash-cap-alarm-pct

Description This command enables capacity monitoring of the compact flash specified in this command. The usage is monitored as a percentage of the capacity of the compact flash. The severity level is alarm. Both a rising and falling threshold can be specified.

The **no** form of this command removes the configured compact flash threshold alarm.

Parameters *cflash-id* — Specifies the name of the cflash device to be monitored.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

rising-threshold *percentage* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

Default 0

falling-threshold *percentage* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

Default 0

seconds — Specifies the polling period, in seconds, over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

alarm-type — Specifies the alarm that may be sent when this alarm is first created.

If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Configuration example

```
cflash-cap-alarm-pct cf1-A: rising-threshold 70 falling-
threshold 60 interval 120 rmon-event-type both start-alarm rising
```

Platforms All

7.54 cflash-cap-warn

cflash-cap-warn

Syntax **cflash-cap-warn** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-warn *cflash-id*

Context **[Tree]** (config>system>thresholds cflash-cap-warn)

Full Context configure system thresholds cflash-cap-warn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables capacity monitoring of the compact flash specified in this command.

The severity level is warning. Both a rising and falling threshold can be specified. The **no** form of this command removes the configured compact flash threshold warning.

Parameters *cflash-id* — Specifies that the cflash-id specifies the name of the cflash device to be monitored.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

rising-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold value represents units of 512 bytes.

Values -2147483648 to 2147483647

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value represents units of 512 bytes.

Values -2147483648 to 2147483647

Default 0

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and a SR OS logger event are generated.

none — No action is taken.

Default both

alarm-type — Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Configuration example

```
cflash-cap-warn cf1-B: rising-threshold 2000000 falling-threshold 1999900
interval 240 rmon-event-type trap start-alarm either
```

Platforms All

7.55 cflash-cap-warn-pct

cflash-cap-warn-pct

Syntax **cflash-cap-warn-pct** *cflash-id* **rising-threshold** *percentage* [**falling-threshold** *percentage*] **interval** *seconds* [**rmon-event-type** *event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-warn-pct *cflash-id*

Context **[Tree]** (config>system>thresholds cflash-cap-warn-pct)

Full Context configure system thresholds cflash-cap-warn-pct

Description This command enables capacity monitoring of the compact flash specified in this command. The usage is monitored as a percentage of the capacity of the compact flash.

The severity level is warning. Both a rising and falling threshold can be specified. The **no** form of this command removes the configured compact flash threshold warning.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *cflash-id* — Specifies that the cflash-id specifies the name of the cflash device to be monitored.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

rising-threshold *percentage* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated **startup-alarm** is equal to **rising** or **either**.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal to the **falling-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

Default 0

falling-threshold *percentage* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated **startup-alarm** is equal to **falling** or **either**.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal to the **rising-threshold** value.

The threshold value is the percentage of used space versus capacity for the specified compact flash.

Values 0 to 100

Default 0

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations, which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

both —Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

alarm-type — Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and **startup-alarm** is equal to **rising** or **either**, a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and **startup-alarm** is equal to **falling** or **either**, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Configuration example

```
cflash-cap-warn-pct cf1-B: rising-threshold 70 falling-threshold 60
interval 240 rmon-event-type trap start-alarm either
```

Platforms All

7.56 cflowd

cflowd

Syntax [**no**] **cflowd**

Context **[Tree]** (config>service>epipe>sap cflowd)

Full Context configure service epipe sap cflowd

Description This command enables cflowd to collect traffic flow samples through a service interface (SAP) for analysis. When cflowd is enabled on an Ethernet service SAP, the Ethernet traffic can be sampled and processed by the system's cflowd engine and exported to IPFIX collectors with the l2-ip template enabled.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the SAP level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

For L2 services, only ingress sampling is supported.

Default no cflowd

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

cflowd

Syntax [**no**] **cflowd**

Context **[Tree]** (config>service>vpls>sap cflowd)

Full Context configure service vpls sap cflowd

Description This command enables cflowd to collect traffic flow samples through a service interface (SAP) for analysis. When cflowd is enabled on an Ethernet service SAP, the Ethernet traffic can be sampled and processed by the system's cflowd engine and exported to IPFIX collectors with the l2-ip template enabled.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the SAP level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

For Layer 2 services, only ingress sampling is supported.

Default no cflowd

Platforms All

cflowd

Syntax **cflowd**

Context **[Tree]** (config>app-assure>group cflowd)

Full Context configure application-assurance group cflowd

Description Commands in this context configure cflowd parameters for the application assurance group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cflowd

Syntax [**no**] **cflowd**

Context **[Tree]** (config cflowd)

Full Context configure cflowd

Description This command creates the context to configure cflowd.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes all configuration under cflowd including the deletion of all configured collectors. This can only be executed if cflowd is in a shutdown state.

Default no cflowd

Platforms All

7.57 cflowd-parameters

cflowd-parameters

Syntax **cflowd-parameters**

Context **[Tree]** (config>service>ies>if cflowd-parameters)
[Tree] (config>service>ies>sub-if>grp-if cflowd-parameters)
[Tree] (config>service>vprn>sub-if>grp-if cflowd-parameters)

Full Context configure service ies interface cflowd-parameters
configure service ies subscriber-interface group-interface cflowd-parameters
configure service vprn subscriber-interface group-interface cflowd-parameters

Description This command creates the configuration context to configure cflowd parameters for the associated IP interfaces.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When Cflowd is enabled at the interface level, all packets forwarded by the interface are subjected to analysis according to the **cflowd** configuration.

At a minimum, the **sampling** command must be configured within this context in order to enable cflowd sampling, otherwise traffic sampling will not occur.

Default no cflowd-parameters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface cflowd-parameters
- configure service vprn subscriber-interface group-interface cflowd-parameters

All

- configure service ies interface cflowd-parameters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cflowd-parameters

Syntax **cflowd-parameters**

Context **[Tree]** (config>service>vprn>if cflowd-parameters)
[Tree] (config>service>vprn>nw-if cflowd-parameters)

Full Context configure service vprn interface cflowd-parameters
configure service vprn network-interface cflowd-parameters

Description This command creates the configuration context to configure cflowd parameters for the associated IP interfaces.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement.

At a minimum, the **sampling** command must be configured within this context in order to enable cflowd sampling, otherwise traffic sampling will not occur.

Default no cflowd-parameters

Platforms All

cflowd-parameters

Syntax **cflowd-parameters**

Context **[Tree]** (config>router>if cflowd-parameters)

Full Context configure router interface cflowd-parameters

Description This command creates the configuration context to configure cflowd parameters for the associated IP interfaces.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement.

At a minimum, the **sampling** command must be configured within this context in order to enable cflowd sampling, otherwise traffic sampling will not occur.

Default no cflowd-parameters

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.58 cfm-mac-advertisement

cfm-mac-advertisement

Syntax [**no**] **cfm-mac-advertisement**

Context **[Tree]** (config>service>vpls>bgp-evpn cfm-mac-advertisement)

Full Context configure service vpls bgp-evpn cfm-mac-advertisement

Description This command enables the advertisement and withdrawal, as appropriate, of the IEEE MAC address associated with the MP (MEP and MIP) created on a SAP, Spoke or Mesh, in an EVPN service.

The up-date occurs each time an MP is added or deleted, or an IEEE MAC address is changed for an MP on a SAP, Spoke or Mesh within the service. The size of the update depends on the number of MPs in the service affected by the modification.

Only enable this functionality, as required, for services that require a resident MAC address to properly forward unicast traffic and that do not perform layer two MAC learning as part of the data plane.

Local MP IEEE MAC addresses are not stored in the local FDB and, as such, cannot be advertised through a control plane to a peer without this command.

The **no** version of the command disables the functionality and withdraws all previously advertised MP IEEE MAC addresses.

Platforms All

7.59 cfm-opcode

cfm-opcode

Syntax **cfm-opcode** {**lt** | **gt** | **eq**} *opcode*
cfm-opcode range *start end*
no cfm-opcode

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match cfm-opcode)

Full Context configure system security management-access-filter mac-filter entry match cfm-opcode

Description This command specifies the type of opcode checking to be performed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the cfm-opcode match condition is configured then a check must be made to see if the Ethertype is either IEEE802.1ag or Y1731. If the Ethertype does not match then the packet is not CFM and no match to the cfm-opcode is attempted.

The CFM (ieee802.1ag or Y1731) opcode can be assigned as a range with a start and an end number or with a (less than lt, greater than gt, or equal to eq) operator.

If no range with a start and an end or operator (lt, gt, eq) followed by an opcode with the value between 0 and 255 is defined then the command is invalid.

Table 37 lists the opcode values.

Table 37 **Opcode Values**

CFM PDU or Organization	Acronym	Configurable Numeric Value (Range)
Reserved for IEEE 802.1 0		0
Continuity Check Message	CCM	1
Loopback Reply	LBR	2
Loopback Message	LBM	3
Linktrace Reply	LTR	4
Linktrace Message	LTM	5
Reserved for IEEE 802.1		6 – 31
Reserved for ITU		32
	AIS	33
Reserved for ITU		34
	LCK	35
Reserved for ITU		36
	TST	37
Reserved for ITU		38
	APS	39
Reserved for ITU		40
	MCC	41
	LMR	42
	LMM	43
Reserved for ITU		44

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 37 **Opcode Values**

CFM PDU or Organization	Acronym	Configurable Numeric Value (Range)
	1DM	45
	DMR	46
	DMM	47
Reserved for ITU		48 – 63
Reserved for IEEE 802.1 0		64 - 255

Defined by ITU-T Y.1731 32 - 63

Defined by IEEE 802.1.64 - 255

Default no cfm-opcode

Parameters *opcode* — Specifies the opcode checking to be performed.

start — specifies the start number.

Values 0 to 255

end — Specifies the end number.

Values 0 to 255

lt | gt | eq — Specifies comparison operators.

Platforms All

7.60 cfm-vlan-tag

cfm-vlan-tag

Syntax **cfm-vlan-tag** *qtag1*[.*qtag2*]
no cfm-vlan-tag

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep cfm-vlan-tag)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep cfm-vlan-tag)
[Tree] (config>service>vpls>eth-cfm>mep cfm-vlan-tag)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep cfm-vlan-tag)
[Tree] (config>service>vpls>sap>eth-cfm>mep cfm-vlan-tag)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep cfm-vlan-tag)

Full Context configure service epipe sap eth-cfm mep cfm-vlan-tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe spoke-sdp eth-cfm mep cfm-vlan-tag
configure service vpls eth-cfm mep cfm-vlan-tag
configure service vpls mesh-sdp eth-cfm mep cfm-vlan-tag
configure service vpls sap eth-cfm mep cfm-vlan-tag
configure service vpls spoke-sdp eth-cfm mep cfm-vlan-tag

Description This command configures VLAN tags to apply to locally-generated CFM PDUs for egress processing.

The **no** form of the command removes the qtags from the configuration.

Parameters *qtag1* — Specifies the outer VLAN ID.

Values 1 to 4094

qtag2 — Specifies the inner VLAN ID and can only be specified if qtag1 is configured.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.61 chain-to-system-filter

chain-to-system-filter

Syntax [**no**] **chain-to-system-filter**

Context **[Tree]** (config>filter>ip-filter chain-to-system-filter)
[Tree] (config>filter>ipv6-filter chain-to-system-filter)

Full Context configure filter ip-filter chain-to-system-filter
configure filter ipv6-filter chain-to-system-filter

Description This command chains this filter to a currently active system filter. When the filter is chained to the system filter, the system filter rules are executed first, and the filter rules are only evaluated if no match on the system filter was found.

The **no** form of the command detaches this filter from the system filter.

Operational note:

If no system filter is currently active, the command has no effect.

Default no chain-to-system-filter

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.62 challenge

challenge

Syntax **challenge** {**always**}
no challenge

Context **[Tree]** (config>router>l2tp challenge)
[Tree] (config>service>vprn>l2tp challenge)

Full Context configure router l2tp challenge
configure service vprn l2tp challenge

Description This command configures the use of challenge-response authentication.

The **no** form of this command reverts to the default **never** value.

Default no challenge

Parameters **always** — Specifies that the challenge-response authentication is always used.

Default no challenge

Values always

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

challenge

Syntax **challenge** *always*
no challenge

Context **[Tree]** (config>service>vprn>l2tp>group challenge)

Full Context configure service vprn l2tp group challenge

Description This command configures the use of challenge-response authentication.

The **no** form of this command reverts to the default **never** value.

Default no challenge

Parameters *always* — Specifies when challenge-response is to be used for the authentication of the tunnels in this L2TP group.

Values always

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

challenge

Syntax **challenge** {**always** | **never**}
no challenge

Context **[Tree]** (config>service>vprn>l2tp>group>tunnel challenge)

Full Context configure service vprn l2tp group tunnel challenge

Description This command configures the use of challenge-response authentication.

The **no** form of this command removes the parameter from the configuration and indicates that the value on group level will be taken.

Default no challenge

Parameters **always** — Specifies that challenge-response authentication should always be used for the tunnel.

never — Specifies that challenge-response authentication should never be used for the tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.63 change-reporting-action

change-reporting-action

Syntax **change-reporting-action** *reporting-action*
no change-reporting-action

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile change-reporting-action)

Full Context configure subscriber-mgmt gtp peer-profile change-reporting-action

Description This command specifies the value of the change reporting action IE sends to the peer in applicable messages. The peer needs to indicate support first using the appropriate flag in the indication IE.

This is overridden by AAA, if AAA explicitly request notification changes for either ECGI, TAI or both. If AAA does not request any notification changes or only the generic location change, the configured value is used.

The **no** form of this command indicates that the IE is not sent, unless specified by AAA.

Default no change-reporting-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *reporting-action* — Specifies the reporting action value as per TS 29.274.

Values 0 to 255, cgi-sai, rai, tai, ecgi, cgi-sai-rai, tai-ecgi

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.64 channel

channel

Syntax **channel** *ip-address* [*ip-address*] [**create**]
no channel *ip-address* [*ip-address*]

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle channel)

Full Context configure mcast-management multicast-info-policy bundle channel

Description This command defines explicit channels or channel ranges that are associated with the containing bundle. A channel or channel range is defined by their destination IP addresses. A channel may be defined using either IPv4 or IPv6 addresses. If a channel range is being defined, both the start and ending addresses must be the same type.

A specific channel may only be defined within a single channel or channel range within the multicast information policy. A defined channel range cannot overlap with an existing channel range.

If a channel range is to be shortened, extended, split or moved to another bundle, it must first be removed from its existing bundle.

Each specified channel range creates a containing context for any override parameters for the channel range. By default, no override parameters exist.

The **no** form of this command removes the specified multicast channel from the containing bundle.

Parameters *ip-address* — Specifies the starting and ending destination IP addresses for a channel range. If only the start channel *ip-address* parameter is given, the channel ranges comprises of a single multicast channel.

If both the starting and ending address are specified, all addresses within the range including the specified address are part of the channel range.

IPv4 or IPv6 addresses may be defined. All specified addresses must be valid multicast destination addresses. The starting IP address must be numerically lower than the ending IP address.

Values Any valid IP multicast destination address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — This keyword is required if creating a new multicast channel range when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified channel range already exists.

Platforms All

channel

Syntax **channel** *mcast-address* **source** *ip-address* [**channel-name** *channel-name*]
no channel *mcast-address* **source** *ip-address*

Context **[Tree]** (config>service>ies>video-interface channel)
[Tree] (config>service>vprn>video-interface channel)

Full Context configure service ies video-interface channel
configure service vprn video-interface channel

Description This command configures channel parameters for ad insertion.

Parameters *mcast-address* — Specifies the multicast address.

source *ip-address* — Specifies the source IP address.

channel-name *channel-name* — Specifies the channel name up to 32 characters in length.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

channel

Syntax **channel** *start-address end-address* **bw** *bandwidth* [**class** *class*] [**type** *type*] [**source** *prefixl prefix-length*]
no channel *start-address end-address* [**source** *prefixlprefix-length*]

Context **[Tree]** (config>router>mcac>policy>bundle channel)

Full Context configure router mcac policy bundle channel

Description This command creates a multicast channel within the bundle where it is configured. A join for a particular multicast channel can be accepted if:

1. Mandatory channels:

   A sufficient bandwidth exists on the interface according to the policy settings for the interface. There is always sufficient BW available on the bundle level because mandatory channels get BW pre-reserved.
2. Optional channels:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A sufficient BW exists on both interface and bundle level.

A channel definition can be either IPv4 (*start-address, end-address, source-address* are IPv4 addresses) or IPv6. A single bundle can have either IPv4 or IPv6 or IPv6 and IPv4 channel definitions. A single policy can mix any of those bundles.

Overlapping channels are not allowed. Two channels overlap if they contain same groups and the same source address prefix (or both do not specify source address prefix). Two channels with same groups and different source prefixes (including one of the channels having no source configured or one of the channels having more specific prefix than the other) do not overlap and are treated as separate channels.

When joining a group from multiple sources, MCAC accounts for that only once when no source address is specified or a prefix for channel covers both sources. Channel BW should be adjusted accordingly or source-aware channel definition should be used if that is not desired.

If a bundle is removed, the channels associated are also removed and every multicast group that was previously policed (because it was in the bundle that contained the policy) becomes free of constraints.

When a new bundle is added to a MCAC policy, the bundle's established groups on a given interfaces are accounted by the policy. Even if this action results in exceeding the bundle's constrain, no active multicast groups are removed. When a leave message is received for an existing optional channel, then the multicast stream is pruned and subsequent new joins may be denied in accordance with the policy. It is possible that momentarily there may be insufficient bandwidth, even for mandatory channels, in this bundle.

Parameters *start-address* — Specifies the beginning multicast IP address that identifies a multicast stream (BTV channel). Both addresses have to be either IPv4 or IPv6.

Values This must be a valid IPv4 or IPv6 multicast group address

end-address — Specifies the ending multicast IP address that identifies a multicast stream (BTV channel). Both addresses have to be either IPv4 or IPv6.

Values This must be a valid IPv4 or IPv6 multicast group address

prefix/prefix-length — Specifies the source of the multicast IP stream. This must be a valid IPv4 or IPv6 multicast source address prefix.

Values address-prefix/prefix-length

address-prefix is valid IPv4/IPv6 multicast source IP address prefix (local scope excluded)

prefix-length [0 to 32] for IPv4 [0 to 128] for IPv6

bandwidth — Specifies the bandwidth required by this channel in kb/s. If this bandwidth is configured for a mandatory channel then this bandwidth is reserved by subtracting the amount from the total available bandwidth for all potential egress interfaces and the bundle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If this bandwidth is configured as an optional channel then this bandwidth must be available for both the bundle and the egress interface requesting the channel to be added. Once the channel has been added the available bandwidth for the bundle and the interface must be reduced by the configured bandwidth of channel.

Values 10 to 10000000 kb/s

class — Provides deeper classification of channels used in the algorithm when LAG ports change state.

Values high, low

Default low

type — Specifies the channel to be either mandatory or optional.

mandatory — When the **mandatory** keyword is specified, then the bandwidth is reserved by subtracting it from the total available for all the potential egress interfaces and the bundle.

optional — When the **optional** keyword is specified then the bandwidth must be available on both the bundle and the egress interface that requests the channel to be added. Once the channel has been added the available bandwidth for the bundle and the interface must be reduced by the configured bandwidth of channel.

Values mandatory, optional

Default optional

Platforms All

7.65 channel-group

channel-group

Syntax [**no**] **channel-group** *channel-group-id*

Context **[Tree]** (config>port>tdm>ds1 channel-group)
[Tree] (config>port>tdm>e1 channel-group)

Full Context configure port tdm ds1 channel-group
configure port tdm e1 channel-group

Description This command creates DS0 channel groups in a channelized DS1 or E1 circuit. Channel groups cannot be further subdivided.

The **no** form of this command deletes the specified DS1 or E1 channel.

Parameters *channel-group-id* — Identifies the channel-group ID number.

Values DS1: 1 to 24 E1: 1 to 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

7.66 channelized

channelized

Syntax **channelized** {**ds1** | **e1**}
no channelized

Context **[Tree]** (config>port>tdm>ds3 channelized)

Full Context configure port tdm ds3 channelized

Description This command specifies that the associated DS-3 is a channelized DS-3 with DS-1/E-1 sub-channels. Depending on the MDA type, the DS-3 parameters must be disabled if clear channel is the default (for example, on m12-ds3 MDAs). Clear channel is a channel that uses out-of-band signaling, not in-band signaling, so the channel's entire bit rate is available. Channelization must be explicitly specified. The no form specifies the associated DS-3 is a clear channel circuit and cannot contain sub-channel DS-1s/E-1s. The sub-channels must be deleted first before the **no** command is executed.

Default no channelized.

Parameters **ds1** — Specifies that the channel is DS-1.

e1 — Specifies that the channel is E-1.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

7.67 chap-challenge-length

chap-challenge-length

Syntax **chap-challenge-length min** *length* **max** *length*
no chap-challenge-length

Context **[Tree]** (config>router>l2tp>group>ppp chap-challenge-length)
[Tree] (config>router>l2tp>group>tunnel>ppp chap-challenge-length)
[Tree] (config>service>vprn>l2tp>group>tunnel chap-challenge-length)

Full Context configure router l2tp group ppp chap-challenge-length
configure router l2tp group tunnel ppp chap-challenge-length
configure service vprn l2tp group tunnel chap-challenge-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum and minimum PPP CHAP challenge length.

The **no** form of this command reverts to the default value.

Default chap-challenge-length min 32 max 64

Parameters **min** *length* — Specifies the minimum PPP CHAP challenge length.

Values 8 to 64

Default 32

max *length* — Specifies the maximum PPP CHAP challenge length.

Values 8 to 64

Default 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

chap-challenge-length

Syntax **chap-challenge-length min** *length* **max** *length*
no chap-challenge-length

Context **[Tree]** (config>service>vprn>l2tp>group>ppp chap-challenge-length)

Full Context configure service vprn l2tp group ppp chap-challenge-length

Description This command configures the maximum and minimum PPP CHAP challenge length.

The **no** form of this command reverts to the default value.

Default chap-challenge-length min 32 max 64

Parameters **min** *length* — Specifies the minimum PPP CHAP challenge length.

Values 8 to 64

max *length* — Specifies the maximum PPP CHAP challenge length.

Values 8 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.68 characteristic

characteristic

Syntax **characteristic** *characteristic-name* **value** *value-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no characteristic *characteristic-name*

Context [Tree] (config>app-assure>group>policy-override>policy characteristic)

Full Context configure application-assurance group policy-override policy characteristic

Description This command configure an override characteristic and value.

Parameters *characteristic-name* — Specifies the characteristic name, up to 32 characters.

value-name — Specifies the override characteristic value for the application profile characteristic used by the Application assurance subscriber.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

characteristic

Syntax **characteristic** *characteristic-name* **value** *value-name*
no characteristic *characteristic-name*

Context [Tree] (config>app-assure>group>policy>app-profile characteristic)

Full Context configure application-assurance group policy app-profile characteristic

Description This command assigns one of the existing values of an existing application service option characteristic to the application profile.

The **no** form of this command removes the characteristic from the application profile.

Parameters *characteristic-name* — Specifies the name of an existing ASO characteristic.

value-name — Specifies the name for the application profile characteristic up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

characteristic

Syntax **characteristic** *characteristic-name*

Context [Tree] (config>app-assure>group>aqp>entry>action characteristic)

Full Context configure application-assurance group app-qos-policy entry action characteristic

Description This command enables the system to use the value of the characteristic name specified in the app-qos-policy url-filter action for the configurable ICAP x-header name provisioned in the url-filter policy. The ICAP server can then use this value to decide which url-filter policy to apply instead of applying a filter policy based on the subscriber name.

Parameters *characteristic-name* — Specifies the name of the characteristic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

characteristic

Syntax **characteristic** *characteristic-name* **{eq | neq}** *value-name*
no characteristic *characteristic-name*

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match characteristic)

Full Context configure application-assurance group policy app-qos-policy entry match characteristic

Description This command adds an existing characteristic and its value to the match criteria used by this AQP entry.

The **no** form of this command removes the characteristic from match criteria for this AQP entry.

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

characteristic-name — Specifies the name of the existing ASO characteristic, up to 32 characters in length.

value-name — Specifies the name of an existing value for the characteristic, up to 32 characters in length.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

characteristic

Syntax **characteristic** *characteristic-name* [**create**]
no characteristic *characteristic-name*

Context **[Tree]** (config>app-assure>group>policy>aso characteristic)

Full Context configure application-assurance group policy app-service-options characteristic

Description This command creates the characteristic of the application service options.

The **no** form of this command deletes characteristic option. To delete a characteristic, it must not be referenced by other components of application assurance.

Parameters *characteristic-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic.

create — Mandatory keyword used to create when creating a characteristic. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.69 charging-characteristics

charging-characteristics

Syntax **charging-characteristics**

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile charging-characteristics)

Full Context configure subscriber-mgmt gtp peer-profile charging-characteristics

Description Commands in this context configure charging characteristics.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.70 charging-group

charging-group

Syntax **charging-group** *charging-group-name*
no charging-group

Context **[Tree]** (config>app-assure>group>policy>app-group charging-group)
[Tree] (config>app-assure>group>policy>application charging-group)

Full Context configure application-assurance group policy app-group charging-group
configure application-assurance group policy application charging-group

Description This command associates an application or app-group to an application assurance charging group.

The **no** form of this command deletes the charging group association.

Default no charging-group

Parameters *charging-group-name* — Specifies a string of up to 32 characters uniquely identifying an existing charging group in the system.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

charging-group

Syntax **charging-group** {**eq** | **neq**} *charging-group-name*
no charging-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>policy>aqp>entry>match charging-group)

Full Context configure application-assurance group policy app-qos-policy entry match charging-group

Description This command adds charging-group to match criteria used by this AQP entry.

The **no** form of this command removes the charging-group from match criteria for this AQP entry.

Default no charging-group

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

charging-group-name — Specifies the name of the existing application group entry. The application-group name is configured in the **config>app-assure>group>policy>aqp>entry>match** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

charging-group

Syntax **charging-group** *charging-group-name* [**create**]
no charging-group *charging-group-name*

Context [Tree] (config>app-assure>group>policy charging-group)

Full Context configure application-assurance group policy charging-group

Description This command creates a charging group for an application assurance policy.

The **no** form of this command deletes the charging group from the configuration. All associations must be removed to delete a group.

Default no charging-group

Parameters *charging-group-name* — Specifies a string of up to 32 characters uniquely identifying an existing charging group in the system.

create — Mandatory keyword used when creating an charging group. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

charging-group

Syntax **charging-group** *charging-group-name* **export-using** *export-method* [*export-method*...(up to 2 max)]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

charging-group *charging-group-name* **no-export**
no charging-group *charging-group-name*

Context [Tree] (config>app-assure>group>statistics>aa-sub charging-group)

Full Context configure application-assurance group statistics aa-sub charging-group

Description This command configures aa-sub accounting statistics for export of charging groups of a given AA ISA group/partition.

The **no** form of this command removes the parameters from the configuration.

Parameters *charging-group-name* — Specifies the name of the charging group. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

export-using *export-method* — Specifies that the method of stats export to be used.

Values accounting-policy, radius-accounting-policy

no-export — Allows the operator to enable the referred to a charging group to be selected (via Diameter) for Gx-usage monitoring. Gx usage monitoring is enabled automatically (and this command is not shown) if the **export-using** parameter is selected for the respective charging group.

Usage monitoring must be enabled at the group:partition level (**config>app-assure>group>statistics>aa-sub>usage-monitoring**) as well in order to allow any application/application group/charging group usage monitoring.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.71 charging-rule-base-name

charging-rule-base-name

Syntax **charging-rule-base-name category-map-name**
charging-rule-base-name *string*
no charging-rule-base-name

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gy>avp charging-rule-base-name)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp charging-rule-base-name

Description This command includes the Charging-Rule-Base-Name AVP with the specified value in all Diameter DCCA CCR messages.

The **no** form of this command removes the Charging-Rule-Base-Name AVP from the Diameter DCCA CCR messages.

Default charging-rule-base-name category-map-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **category-map-name** — This keyword specifies the name of the category-map in use.

string — Specifies a string of up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.72 chassis-level

chassis-level

Syntax **chassis-level**

Context **[Tree]** (config>mcast-management chassis-level)

Full Context configure mcast-management chassis-level

Description Commands in this context configure multicast plane bandwidth parameters. The chassis-level CLI node contains the multicast plane replication limit for each switch fabric multicast plane.

The chassis-level node always exists and contains the configuration command to define the total replication rates for primary and secondary associated ingress paths for each switch fabric multicast plane.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

7.73 chassis-mode

chassis-mode

Syntax **chassis-mode** *chassis-mode* [**force**]

Context **[Tree]** (config>system chassis-mode)

Full Context configure system chassis-mode

Description This command is retained for historic reasons, and was used to control the set of features and scaling available based on the variants of IOMs present in the node. As of release 15.0, the set of supported IOMs no longer requires this differentiation using this command. The command still exists but the mode is fixed at **chassis mode d**.

Default chassis-mode d

Parameters *chassis-mode* — Specifies the chassis modes:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

d: This mode corresponds to scaling and feature set associated with iom3-xp.

force — Forces an upgrade from a lesser scaling and feature set to a greater one.

Platforms 7450 ESS, 7750 SR-7/12

7.74 check-id-kp-cmcra-only

check-id-kp-cmcra-only

Syntax [**no**] **check-id-kp-cmcra-only**

Context **[Tree]** (config>system>security>pki>est-profile check-id-kp-cmcra-only)

Full Context configure system security pki est-profile check-id-kp-cmcra-only

Description This command enables checking id-kp-cmcRA in the EST certificate. When enabled, instead of the subject or subject alternative name, only the id-kp-cmcRA existence in extended key usage extension of EST server certificate is checked. The id-kp-cmcRA identifies a Registration Authority.

The **no** form of this command reverts to the default value.

Default no check-id-kp-cmcra-only

Platforms All

7.75 check-zero

check-zero

Syntax **check-zero** {**enable** | **disable**}
no check-zero

Context **[Tree]** (config>service>vprn>rip check-zero)
[Tree] (config>service>vprn>rip>group check-zero)
[Tree] (config>service>vprn>rip>group>neighbor check-zero)
[Tree] (config>service>vprn>ripng check-zero)
[Tree] (config>service>vprn>ripng>group check-zero)
[Tree] (config>service>vprn>ripng>group>neighbor check-zero)

Full Context configure service vprn rip check-zero
configure service vprn rip group check-zero

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn rip group neighbor check-zero
configure service vprn ripng check-zero
configure service vprn ripng group check-zero
configure service vprn ripng group neighbor check-zero

Description This command enables checking for zero values in fields specified to be zero by the RIPv1 and RIPv2 specifications.

The **no** form of this command disables this check and allows the receipt of RIP messages even if the mandatory zero fields are non-zero.

Default no check-zero

Parameters **enable** — Enables checking of the mandatory zero fields in the RIPv1 and RIPv2 specifications and rejecting noncompliant RIP messages.

disable — Disables the checking and allows the receipt of RIP messages even if the mandatory zero fields are non-zero.

Platforms All

check-zero

Syntax **check-zero** {**enable** | **disable**}
no check-zero

Context **[Tree]** (config>router>rip check-zero)
[Tree] (config>router>rip>group check-zero)
[Tree] (config>router>rip>group>neighbor check-zero)
[Tree] (config>router>ripng check-zero)
[Tree] (config>router>ripng>group check-zero)
[Tree] (config>router>ripng>group>neighbor check-zero)

Full Context configure router rip check-zero
configure router rip group check-zero
configure router rip group neighbor check-zero
configure router ripng check-zero
configure router ripng group check-zero
configure router ripng group neighbor check-zero

Description This command enables checking for zero values in fields specified to be zero by the RIPv1 and RIPv2 specifications.

The **check-zero enable** command enables checking of the mandatory zero fields in the RIPv1 and RIPv2 specifications and rejecting non-compliant RIP messages.

The **check-zero disable** command disables this check and allows the receipt of RIP messages even if the mandatory zero fields are non-zero.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This configuration parameter can be set at three levels: global level (applies to all groups and neighbor interfaces), group level (applies to all neighbor interfaces in the group) or neighbor level (only applies to the specified neighbor interface). The most specific value is used. In particular if no value is set (**no check-zero**), the setting from the less specific level is inherited by the lower level.

The **no** form of the command removes the **check-zero** command from the configuration.

Special Cases **RIP Global —** By default, check-zero is disabled at the global RIP instance level.

Parameters **enable** — Specifies to reject RIP messages which do not have zero in the RIPv1 and RIPv2 mandatory fields.

disable — Specifies allows receipt of RIP messages which do not have the mandatory zero fields reset.

Platforms All

7.76 checksum

checksum

Syntax **checksum** {**md5** | **sha256**} *file-url*

Context **[Tree]** (file checksum)

Full Context file checksum

Description This command computes and displays a checksum for a file.

Parameters **md5** — Specifies the use of the MD5 algorithm to produce the file checksum.

sha256 — Specifies the use of the SHA-256 algorithm to produce the file checksum.

file-url — Specifies the location of the file.

Values

local-url	[*cflash-id*/][*file-path*] up to 200 characters, including cflash-id directory length 99 chars max each
remote-url	[{ftp:// | tftp:// | http:// | https://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 199 characters
remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	x:x:x:x:x:x:d.d.d.d[*-interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

7.77 child-control

child-control

Syntax **child-control**

Context **[Tree]** (config>qos>adv-config-policy child-control)

Full Context configure qos adv-config-policy child-control

Description This command contains parameters that are intended to allow more precise control of the method that hierarchical virtual scheduling employs to emulate the effect of a scheduling context upon a member child queue or policer.

This command edits the parameters that control the child requested bandwidth and parental bandwidth distribution for all policers and queues associated with the policy.

Platforms All

7.78 chli-event

chli-event

Syntax **chli-event** {**forward** | **backward** | **aggregate**} **threshold** *raise-threshold* [**clear** *clear-threshold*]
no chli-event {**forward** | **backward** | **aggregate**}

Context **[Tree]** (config>oam-pm>session>ethernet>slm>loss-events chli-event)
[Tree] (config>oam-pm>session>ethernet>lmm>loss-events chli-event)
[Tree] (config>oam-pm>session>ip>twamp-light>loss-events chli-event)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure oam-pm session ethernet lmm loss-events chli-event
configure oam-pm session ethernet slm loss-events chli-event
configure oam-pm session ip twamp-light loss-events chli-event

Description This command sets the consecutive high loss interval (CHLI) threshold to be monitored and the associated thresholds using the counter of the specified direction. The aggregate is a function of summing forward and backward. This value is only used as a threshold mechanism and is not part of the stored statistics. If the optional **clear** *clear-threshold* parameter is not specified, the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and regardless of any previous window. Each unique event can only be raised once within measurement interval. If the optional **clear** *clear-threshold* parameter is specified, the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is carried forward to following measurement intervals. If a threshold crossing event is raised another is raised until a measurement interval completes and the clear threshold has not been exceeded. A clear event is raised under that condition.

The **no** form of this command removes the event threshold for frame loss ratio. The direction must be included with the **no** command.

Default no chli-event forward

no chli-event backward

no chli-event aggregate

Parameters **forward** — Specifies the threshold is applied to the forward direction count.

backward — Specifies the threshold is applied to the backward direction count.

aggregate — Specifies the threshold is applied to the aggregate count (sum of forward and backward).

raise-threshold — Specifies the numerical value compared to the CHLI counter that is the rising threshold that determines when the event is to be generated, when the percentage of loss value is reached.

Values 1 to 864000

clear-threshold — Specifies an optional numerical value compared to the CHLI counter used for stateful behavior that allows the operator to configure a value lower than the rising percentage to indicate when the clear event should be generated.

Values 0 to 863999
A value of zero means that the CHLI counter must be 0.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events chli-event

All

- configure oam-pm session ethernet lmm loss-events chli-event
- configure oam-pm session ethernet slm loss-events chli-event

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.79 cipher

cipher

Syntax **cipher** *index* **name** *cipher-name*
no cipher *index*

Context **[Tree]** (config>system>security>ssh>client-cipher-list cipher)
[Tree] (config>system>security>ssh>server-cipher-list cipher)

Full Context configure system security ssh client-cipher-list cipher
configure system security ssh server-cipher-list cipher

Description This command enables the configuration of a cipher. Client-ciphers are used when the SR OS is acting as an SSH client. Server-ciphers are used when the SR OS is acting as an SSH server.

The **no** form of this command removes the index and cipher name from the configuration.

Default no cipher *index*

Parameters *index* — Specifies the index of the cipher in the list.

Values 1 to 255

cipher-name — Specifies the algorithm used when performing encryption or decryption.

Values For SSHv1:
Client ciphers: des, 3des, blowfish
Server ciphers: 3des, blowfish
Table 38 lists the default ciphers used for SSHv1:

Table 38 **SSHv1 Default Ciphers**

Cipher index value	Cipher name
200	3des
205	blowfish
210	des

Note: blowfish and des are not permitted in FIPS-140-2 mode.

Values For SSHv2:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Client ciphers: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc, aes128-ctr, aes192-ctr, aes256-ctr

Server ciphers: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc, aes128-ctr, aes192-ctr, aes256-ctr

Table 39 lists the default ciphers used for SSHv2:

Table 39 **SSHv2 Default Ciphers**

Cipher index value	Cipher name
190	aes256-ctr
192	aes192-ctr
194	aes128-ctr
200	aes128-cbc
205	3des-cbc
210	blowfish-cbc
215	cast128-cbc
220	arcfour
225	aes192-cbc
230	aes256-cbc
235	rijndael-cbc

Note: blowfish-cbc, cast128-cbc, arcfour, and rijndael-cbc are not permitted in FIPS-140-2 mode.

Platforms All

cipher

Syntax **cipher** *index* **name** *cipher-suite-code*
no cipher *index*

Context **[Tree]** (config>system>security>tls>client-cipher-list cipher)
[Tree] (config>system>security>tls>server-cipher-list cipher)

Full Context configure system security tls client-cipher-list cipher

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security tls server-cipher-list cipher

Description This command configures the cipher suite to be negotiated by the server and client.

Parameters *index* — Specifies the index number. The index number provides the location of the cipher in the negotiation list, with the lower index numbers being higher in the negotiation list and the higher index numbers being at the bottom of the list.

Values 1 to 255

cipher-suite-code — Specifies the cipher suite code.

Values
tls-rsa-with-null-md5
tls-rsa-with-null-sha
tls-rsa-with-null-sha256
tls-rsa-with-3des-ede-cbc-sha
tls-rsa-with-aes128-cbc-sha
tls-rsa-with-aes256-cbc-sha
tls-rsa-with-aes128-cbc-sha256
tls-rsa-with-aes256-cbc-sha256
tls-rsa-with-aes128-gcm-sha256
tls-rsa-with-aes256-gcm-sha384

Platforms All

7.80 cipher-list

cipher-list

Syntax **cipher-list** *name*
no cipher-list

Context **[Tree]** (config>system>security>tls>client-tls-profile cipher-list)

Full Context configure system security tls client-tls-profile cipher-list

Description This command assigns the cipher list to be used by the TLS client profile for negotiation in the client Hello message.

Parameters *name* — Specifies the name of the cipher list.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cipher-list

Syntax **cipher-list** *name*
no cipher-list

Context **[Tree]** (config>system>security>tls>server-tls-profile cipher-list)

Full Context configure system security tls server-tls-profile cipher-list

Description This command assigns a cipher list to be used by the TLS server profile. This cipher list is used to find matching ciphers with the cipher list that is received from the client.

The **no** form of the command removes the cipher list.

Parameters *name* — Specifies the name of the cipher list, up to 32 characters in length.

Platforms All

7.81 cipher-suite

cipher-suite

Syntax **cipher-suite** *cipher-suite*
no cipher-suite

Context **[Tree]** (config>macsec>connectivity-association cipher-suite)

Full Context configure macsec connectivity-association cipher-suite

Description This command configures encryption of data path PDUs. When all parties in the Connectivity Association (CA) have the SAK, they use the above algorithm in conjunction with the SAK to encrypt the data path PDUs.

The XPN 64 bit (extended packet number) can be used for higher rate ports such as 10 GigE to minimize the window rollover and renegotiation of the SAK.

The **no** form of this command disables encryption of data path PDUs.

Default cipher-suite gcm-aes-128

Parameters *cypher-suite* — Specifies the algorithm.

Values gcm-aes-128 — algorithm is used for control plain encryption
gcm-aes-256 — algorithm is used for control plain encryption
gcm-aes-xpn-128 — algorithm with extended packet number is used for control plain encryption

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gcm-aes-xpn-256 — algorithm with extended packet number is used for control plain encryption

Platforms All

7.82 cir

cir

Syntax **cir** *congested-cir*
no cir

Context **[Tree]** (config>app-assure>group>policer>congestion-override cir)

Full Context configure application-assurance group policer congestion-override cir

Description This command provides a mechanism to configure the CIR for the congestion override policer. It is recommended that the CIR is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. The CIR is configurable for dual-bucket bandwidth policers only.

The **no** form of this command resets the CIR value to its default.

Default cir 0

Parameters *congested-cir* — Specifies an integer value defining size, in kilobytes, for the CIR of the policer.

Values 0 to 100000000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

cir

Syntax **cir** *cir-rate*
no cir

Context **[Tree]** (config>app-assure>group>policer>congestion-override-stage2 cir)

Full Context configure application-assurance group policer congestion-override-stage2 cir

Description This command provides a mechanism to configure the CIR for the congestion override policer. It is recommended that the CIR is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. The CIR is configurable for dual-bucket bandwidth policers only.

The **no** form of this command resets the CIR value to its default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default cir 0

Parameters *cir-rate* — Specifies an integer value defining size, in kilobytes, for the CIR of the policer.

Values 0 to 100000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.83 cir-non-profiling

cir-non-profiling

Syntax [**no**] **cir-non-profiling**

Context **[Tree]** (config>qos>sap-ingress>queue cir-non-profiling)

Full Context configure qos sap-ingress queue cir-non-profiling

Description This command prevents the modification of the profile of a packet depending on the queue rate compared to its configured CIR. The CIR continues to be used to affect the scheduling priority of a queue. The **cir-non-profiling** command and the **queue police** command are mutually exclusive.

The **cir-non-profiling** command is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

The **cir-non-profiling** command should not be configured under a SAP ingress QoS policy queue associated with a LAG which spans FP4-based and FP2- or FP3-based hardware as the resulting operation could be different depending on which hardware type the traffic ingresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

cir-non-profiling

Syntax [**no**] **cir-non-profiling**

Context **[Tree]** (config>qos>queue-group-templates>ingress>queue-group>queue cir-non-profiling)

Full Context configure qos queue-group-templates ingress queue-group queue cir-non-profiling

Description This command prevents the modification of the profile of a packet-dependent queue rate compared to its configured CIR. The CIR continues to be used to affect the scheduling priority of a queue. The **cir-non-profiling** and the **queue police** commands are mutually exclusive.

cir-non-profiling is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-non-profiling should not be configured under an ingress queue group template queue associated with a LAG which spans FP4-based and FP2/FP3-based hardware as the resulting operation could be different depending on which hardware type the traffic ingresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

7.84 circuit-id

circuit-id

Syntax **circuit-id string** *ascii-string*
circuit-id hex *hex-string*
no circuit-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident circuit-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-ident circuit-id)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification circuit-id
configure subscriber-mgmt local-user-db ppp host host-identification circuit-id

Description This command specifies the circuit ID to match for a host lookup. When the LUDB is accessed using a DHCPv4 server, the circuit ID is matched against DHCP Option 82.

Note: This command is only used when **circuit-id** is configured as one of the **match-list** parameters.

The **no** form of this command removes the circuit ID from the configuration.

Parameters *ascii-string* — Specifies the circuit ID from the Option 82, up to 127 characters.

hex-string — Specifies the circuit ID in hexadecimal format from the Option 82.

Values 0x0 to 0xFFFFFFFF (maximum 254 hex nibbles)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

circuit-id

Syntax **circuit-id sap-id**
circuit-id string *ASCII string*
no circuit-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>ali circuit-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt local-user-db ppp host access-loop-information circuit-id

Description This command specifies a circuit-id for PPPoE hosts. A circuit ID received in PPPoE tags has precedence over the LUDB specified circuit ID.

The **no** form of this command reverts to the default.

Parameters **sap-id** — Specifies to use the SAP ID of the PPPoE session as the circuit ID.

ASCII string — Specifies the circuit ID as a string, up to 63 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

circuit-id

Syntax **circuit-id**
circuit-id {**ascii-tuple** | **if-index** | **sap-id** | **vlan-ascii-tuple**}
circuit-id hex [*hex-string*]
no circuit-id

Context **[Tree]** (config>service>ies>if>dhcp>option circuit-id)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option circuit-id)
[Tree] (config>service>vpls>sap>dhcp>option circuit-id)
[Tree] (config>service>vprn>if>dhcp>option circuit-id)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option circuit-id)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option circuit-id)

Full Context configure service ies interface dhcp option circuit-id
configure service ies subscriber-interface group-interface dhcp option circuit-id
configure service vpls sap dhcp option circuit-id
configure service vprn interface dhcp option circuit-id
configure service vprn subscriber-interface group-interface dhcp option circuit-id
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option circuit-id

Description When enabled, the router sends an ASCII-encoded tuple in the **circuit-id** sub-option of the DHCP packet. This ASCII-tuple consists of the access-node-identifier, service-id, and SAP-ID, separated by "|". If no keyword is configured, then the circuit-id sub-option will not be part of the information option (Option 82). When the command is configured without any parameters, it equals to circuit-id ascii-tuple.

To send a tuple in the circuit ID, the **action replace** command must be configured in the same context.

If disabled, the **circuit-id** sub-option of the DHCP packet is left empty.

The **no** form of this command specifies to leave the circuit-id option of the packet empty.

Default circuit-id ascii-tuple

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **ascii-tuple** — Specifies that the ASCII-encoded concatenated tuple consisting of the access-node-identifier, service-id, and interface-name is used.

ifindex — Specifies that the interface index is used. The If Index of a router interface can be displayed using the command **show>router>if>detail**.

sap-id — Specifies that the SAP identifier is used.

vlan-ascii-tuple — Specifies that the format will include VLAN-id and dot1p bits in addition to what is included in ascii-tuple already. The format is supported on dot1q and qinq ports only. Thus, when the Option 82 bits are stripped, dot1p bits are copied to the Ethernet header of an outgoing packet.

hex-string — Specifies the hex value of this option.

Values 0x0 to 0xFFFFFFFF...(up to 64 hex nibbles)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option circuit-id
- configure service vprn subscriber-interface group-interface dhcp option circuit-id
- configure service ies subscriber-interface group-interface dhcp option circuit-id

All

- configure service vprn interface dhcp option circuit-id
- configure service ies interface dhcp option circuit-id
- configure service vpls sap dhcp option circuit-id

circuit-id

Syntax [**no**] **circuit-id**

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute circuit-id)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute circuit-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute circuit-id
configure subscriber-mgmt authentication-policy include-radius-attribute circuit-id

Description This command enables the generation of the Broad Band Forum Agent-Circuit-Id Vendor Specific AVP in Diameter NASREQ AAR messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

circuit-id

Syntax [**no**] **circuit-id**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>avp circuit-id)

Full Context configure subscriber-mgmt diameter-application-policy nasreq include-avp circuit-id

Description This command includes the Broad Band Forum Agent-Circuit-Id Vendor Specific AVP in Diameter NASREQ AAR messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

circuit-id

Syntax [**no**] **circuit-id** *circuit-id*

Context [Tree] (debug>service>id>ppp circuit-id)

Full Context debug service id ppp circuit-id

Description This command enable PPP debug for the specified circuit-id.

Multiple circuit-id filters can be specified in the same debug command.

The **no** form of this command disables debugging.

Parameters *circuit-id* — Specifies the circuit-id in PADI.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

circuit-id

Syntax [**no**] **circuit-id**

Context [Tree] (config>aaa>isa-radius-plcy>acct-include-attributes circuit-id)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes circuit-id)

Full Context configure aaa isa-radius-policy acct-include-attributes circuit-id
configure aaa isa-radius-policy auth-include-attributes circuit-id

Description This command enables the generation of the Broad Band Forum Agent-Circuit-Id Vendor Specific AVP in Diameter NASREQ AAR messages.

Default no circuit-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

circuit-id

Syntax **circuit-id** {**ascii-tuple** | **ifindex** | **if-name** | **port-id** | **vlan-ascii-tuple** | **none**}
no circuit-id

Context **[Tree]** (config>router>if>dhcp>option circuit-id)

Full Context configure router interface dhcp option circuit-id

Description When enabled, the router sends the interface index (If Index) in the **circuit-id** suboption of the DHCP packet. The If Index of a router interface can be displayed using the command **show>router>if>detail**. This option specifies data that must be unique to the router that is relaying the circuit.

If disabled, the **circuit-id** suboption of the DHCP packet will be left empty.

The **no** form of this command returns the system to the default.

Default circuit-id ascii-tuple

Parameters **ascii-tuple** — Specifies that the ASCII-encoded concatenated tuple will be used which consists of the access-node-identifier, service-id, and interface-name, separated by "| ".

ifindex — Specifies that the interface index will be used. The If Index of a router interface can be displayed using the command **show>router>if>detail**.

if-name — Specifies the interface name.

port-id — Specifies the port ID.

vlan-ascii-tuple — Specifies that the format will include VLAN-id and dot1p bits in addition to what is included in ascii-tuple already. The format is supported on dot1q and qinq ports only. Therefore, when the Option 82 bits are stripped, dot1p bits will be copied to the Ethernet header of an outgoing packet.

none — Specifies that no circuit should be used.

Platforms All

7.85 circuit-id-from-auth

circuit-id-from-auth

Syntax [**no**] **circuit-id-from-auth**

Context **[Tree]** (config>subscr-mgmt>ipoe-plcy circuit-id-from-auth)

Full Context configure subscriber-mgmt ipoe-session-policy circuit-id-from-auth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command takes the circuit ID value from the authentication server to identify the session.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.86 cisco-hdlc

cisco-hdlc

Syntax **cisco-hdlc**

Context **[Tree]** (config>port>sonet-sdh>path cisco-hdlc)
[Tree] (config>port>tdm>ds1>channel-group cisco-hdlc)
[Tree] (config>port>tdm>ds3 cisco-hdlc)
[Tree] (config>port>tdm>e1>channel-group cisco-hdlc)
[Tree] (config>port>tdm>e3 cisco-hdlc)

Full Context configure port sonet-sdh path cisco-hdlc
configure port tdm ds1 channel-group cisco-hdlc
configure port tdm ds3 cisco-hdlc
configure port tdm e1 channel-group cisco-hdlc
configure port tdm e3 cisco-hdlc

Description Commands in this context configure Cisco HDLC parameters. Cisco HDLC is an encapsulation protocol that governs information transfer. It specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

Cisco HDLC monitors line status on a serial interface by exchanging keepalive request messages with peer network devices. It also allows routers to discover IP addresses of neighbors by exchanging Serial Link Address Resolution Protocol (SLARP) address-request and address-response messages with peer network.

Only IES SAPs (including SAPs in VPRN service) can provision a Cisco-HDLC-capable configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path cisco-hdlc

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group cisco-hdlc
- configure port tdm e3 cisco-hdlc
- configure port tdm ds3 cisco-hdlc
- configure port tdm e1 channel-group cisco-hdlc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cisco-hdlc

Syntax **cisco-hdlc** [*port-id*]
no cisco-hdlc

Context **[Tree]** (debug cisco-hdlc)

Full Context debug cisco-hdlc

Description This command configures debugging for Cisco-HDLC encapsulation.

Parameters *port-id* — Specifies the physical port ID.

Values slot/mda/port[.channel]

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.87 cisco-nas-port

cisco-nas-port

Syntax **cisco-nas-port** [**ethernet** *binary-spec-eth*] [**atm** *binary-spec-atm*]
no cisco-nas-port

Context **[Tree]** (config>router>l2tp cisco-nas-port)
[Tree] (config>service>vprn>l2tp cisco-nas-port)

Full Context configure router l2tp cisco-nas-port
configure service vprn l2tp cisco-nas-port

Description This command configures the L2TP Cisco NAS port AVP.

The **no** form of this command removes the specified L2TP Cisco NAS port AVP.

Default no cisco-nas-port

Parameters *binary-spec-eth* — Specifies the string to put in the Cisco-NAS-Port AVP for L2TP control messages related to a PPPoE session in this L2TP protocol instance.

binary-spec-atm — Specifies the string to put in the Cisco-NAS-Port AVP, for L2TP control messages related to a PPPoA (PPP over ATM) session in this L2TP protocol instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cisco-nas-port

Syntax **cisco-nas-port** [**ethernet** *binary-spec*] [**atm** *binary-spec*]
no cisco-nas-port

Context **[Tree]** (config>service>vprn>l2tp cisco-nas-port)

Full Context configure service vprn l2tp cisco-nas-port

Description This command enables the AVP Cisco-nas-port to include the slot/mda/port along with the pseudowire port ID. If the pseudowire is terminated on a LAG, the slot/mda/port cannot be populated and only the pseudowire ID is included.

The **no** form of this command enables the AVP Cisco-nas-port.

Default no cisco-nas-port

Parameters *binary-spec* — Specifies the NAS port attribute.

Values		
binary-spec	<bit-specification> <binary-spec>	
bit-specification	0 | 1 | <bit-origin>	
bit-origin	*<number-of-bits><origin>	
number-of-bits	1 to 32	
origin	s | m | p | o | i | v | c	
	s	slot number
	m	MDA number
	p	port number, lag-id, pw-id or pxc-id
	o	outer VLAN ID
	i	inner VLAN ID
	v	ATM VPI
	c	ATM VCI or PXC subport (subport a = 0, subport b = 1)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.88 ckn

ckn

Syntax **ckn** *hex-string*
no ckn

Context **[Tree]** (config>macsec>conn-assoc>static-cak>pre-shared-key ckn)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure macsec connectivity-association static-cak pre-shared-key ckn

Description Specifies the connectivity association key name (CKN) for a pre-shared key.

CKN is appended to the MKA for identification of the appropriate CAK by the peer.

The **no** form of this command reverts to the default value.

Parameters *hex-string* — Specifies the value of the CKN.

Values 32 octets char (64 hex)

Platforms All

7.89 class

class

Syntax [**no**] **class** *class-number*

Context **[Tree]** (config>port>ethernet>egress>hs-sec-shaper class)

Full Context configure port ethernet egress hs-secondary-shaper class

Description This command specifies the HS secondary shaper class.

The **no** form of this command reverts the rate for this class to the default value.

Parameters *class-number* — Specifies the HS secondary shaper class identifier.

Values 1 to 6

Platforms 7750 SR-7/12/12e

class

Syntax [**no**] **class**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes class)

Full Context configure aaa isa-radius-policy acct-include-attributes class

Description This command enables the generation of the class RADIUS attribute.

Default no class

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

class

Syntax **class** *class-id*

Context **[Tree]** (config>qos>mlppp-profile-egress class)
[Tree] (config>qos>mlppp-profile-ingress class)

Full Context configure qos mlppp-profile-egress class
configure qos mlppp-profile-ingress class

Description This command provides the MLPPP class context for the user to configure the ingress or egress MLPPP bundle QoS parameters for this profile.

Parameters *class-id* — Specifies a class for this policy.

Values 0 to 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

class

Syntax **class** *class-id*

Context **[Tree]** (config>qos>mc-fr-profile-egress class)
[Tree] (config>qos>mc-fr-profile-ingress class)

Full Context configure qos mc-fr-profile-egress class
configure qos mc-fr-profile-ingress class

Description This command provides the Frame Relay scheduling class context for the user to configure the ingress or egress QoS parameters of an MLFR bundle or an FRF.12 UNI/NNI link for this profile.

Parameters *class-id* — Specifies the Frame Relay scheduling class number.

Values 0 to 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.90 class-forwarding

class-forwarding

Syntax [**no**] **class-forwarding**

Context **[Tree]** (config>service>vprn class-forwarding)

Full Context configure service vprn class-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the CBF for VPRN-v4/v6 prefixes resolved to RSVP-TE LSPs.

The **no** form of this command disables the CBF for VPRN-v4/v6 prefixes resolved to RSVP-TE LSPs.

Default no class-forwarding

Platforms All

class-forwarding

Syntax **class-forwarding cbf-mode** {**lsr** | **ler** | **lsr-and-ler**}
no class-forwarding

Context **[Tree]** (config>router>ldp class-forwarding)

Full Context configure router ldp class-forwarding

Description This command enables class-based forwarding for packets that belong to one of the eight forwarding classes (be, l2, af, l1, h2, ef, h1, and nc). For the LER role, class-based forwarding is performed in conjunction with ECMP. At LER, this function applies to packets whose prefixes resolve to an LDP FEC. This LDP FEC resolves to a set of IGP shortcuts (RSVP-TE LSPs). At LSR, this function applies to labeled LDP packets whose FEC resolves to an IGP shortcut. Refer to “Class-based Forwarding of LDP Prefix Packets over IGP Shortcuts” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for detailed information on this capability.

The **no** form of this command disables class-based forwarding.

Default no class-forwarding

Parameters **cbf-mode lsr** — Enables class-forwarding at LSR and disables any previously enabled mode.

cbf-mode ler — Enables class-forwarding at LER and disables any previously enabled mode.

cbf-mode lsr-and-ler — Enables class-forwarding at both LSR and LER, and disables any previously enabled mode.

Platforms All

class-forwarding

Syntax [**no**] **class-forwarding**

Context **[Tree]** (config>router>mpls>lsp>config>router>mpls>lsp-template class-forwarding)

Full Context configure router mpls lsp config router mpls lsp-template class-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure class based forwarding parameters for a given LSP or LSP-template.

A change in the Class-Based Forwarding configuration may result in a change of forwarding behavior.

The **no** form removes any Class-Based Forwarding configuration associated to that LSP or LSP-template.

Default no class-forwarding

class-forwarding

Syntax [**no**] **class-forwarding**

Context **[Tree]** (config>router class-forwarding)

Full Context configure router class-forwarding

Description This command enables class-based forwarding (CBF) over IGP shortcuts. When the **class-forwarding** command is enabled, the following types of packets are forwarded based on their forwarding class:

- packets of BGP prefixes
- CPM originated packets for the families (IPv4 only, IPv6 only, or both IPv4 and IPv6) which have been enabled over IGP shortcuts using the **igp-shortcut** CLI context in one or more IGP instances

The SR OS CBF implementation supports spraying of packets over a maximum of four forwarding sets of ECMP LSPs. The user must define a class-forwarding policy object in MPLS to configure the mapping of FCs to the forwarding sets. Then, the user assigns the CBF policy name and set ID to each MPLS LSP that is used in IGP shortcuts.

When a BGP IPv4 or IPv6 prefix is resolved, the FC of the packet is used to look up the forwarding set ID. Then, a modulo operation is performed on the tunnel next-hops of this set ID only, to spray packets of this FC. The data path concurrently implements CBF and ECMP within the tunnels of each set ID.

CPM-originated packets on the router, including control plane and OAM packets, are forwarded over a single LSP from the set of LSPs that the packet's FC is mapped to, as per the CBF configuration.

Note: Weighted ECMP, at the transport tunnel level of BGP prefixes over IGP shortcuts and the CBF feature on a per BGP next-hop basis are mutually exclusive.

Default no class-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

class-forwarding

Syntax **class-forwarding** [**default-lsp** *lsp-name*]
no class-forwarding

Context **[Tree]** (config>service>sdp class-forwarding)

Full Context configure service sdp class-forwarding

Description This command enables the forwarding of a service packet over the SDP based on the class of service of the packet. Specifically, the packet is forwarded on the RSVP LSP or static LSP whose forwarding class matches that of the packet. The user maps the system forwarding classes to LSPs using the **config>service>sdp>class-forwarding>fc** command. If there is no LSP that matches the packet's forwarding class, the default LSP is used. If the packet is a VPLS multicast/broadcast packet and the user did not explicitly specify the LSP to use under the **config>service>sdp>class-forwarding>multicast-lsp** context, then the default LSP is used.

VLL service packets are forwarded based on their forwarding class only if shared queuing is enabled on the ingress SAP. Shared queuing must be enabled on the VLL ingress SAP if class-forwarding is enabled on the SDP the service is bound to. Otherwise, the VLL packets will be forwarded to the LSP which is the result of hashing the VLL service ID. Since there are eight entries in the ECMP table for an SDP, one LSP ID for each forwarding class, the resulting load balancing of VLL service ID is weighted by the number of times an LSP appears on that table. For instance, if there are eight LSPs, the result of the hashing will be similar to when class based forwarding is disabled on the SDP. If there are fewer LSPs, then the LSPs which were mapped to more than one forwarding class, including the default LSP, will have proportionally more VLL services forwarding to them.

Class-based forwarding is not supported on a spoke SDP used for termination on an IES or VPRN service. All packets are forwarded over the default LSP.

The **no** form of the command deletes the configuration and the SDP reverts back to forwarding service packets based on the hash algorithm used for LAG and ECMP.

Default no class-forwarding

Parameters **default-lsp** *lsp-name* — Specifies the default LSP for the SDP. This LSP name must exist and must have been associated with this SDP using the *lsp-name* configured in the **config>service>sdp>lsp** context. The default LSP is used to forward packets when there is no available LSP which matches the packet's forwarding class. This could be because the LSP associated with the packet's forwarding class is down, or that the user did not configure a mapping of the packet's forwarding class to an LSP using the **config>service>sdp>class-forwarding>fc** command. The default LSP is also used to forward VPLS service multicast/broadcast packets in the absence of a user configuration indicating an explicit association to one of the SDP LSPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: When the default LSP is down, the SDP is also brought down. The user will not be able to enter the class-forwarding node if the default LSP was not previously specified. In other words, the class-forwarding for this SDP will remain shutdown.

Platforms All

class-forwarding

Syntax [**no**] **class-forwarding**

Context **[Tree]** (config>router>ospf>segm-rtng class-forwarding)
[Tree] (config>router>isis>segm-rtng class-forwarding)

Full Context configure router isis segment-routing class-forwarding
configure router ospf segment-routing class-forwarding

Description This command enables Class Based Forwarding with ECMP for SR-ISIS or SR-OSPF resolved to RSVP-TE LSPs as IGP shortcuts. For CBF+ECMP to be effective, a class forwarding policy must be defined. In addition, FC to set associations and RSVP-TE LSPs to set associations must be defined.

The **no** form of this command disables Class Based Forwarding with ECMP for SR-ISIS or SR-OSPF resolved to RSVP-TE LSPs as IGP shortcuts.

Default no class-forwarding

Platforms All

7.91 class-forwarding-policy

class-forwarding-policy

Syntax **class-forwarding-policy** *policy-name*
no class-forwarding-policy *policy-name*

Context **[Tree]** (config>router>mpls class-forwarding-policy)

Full Context configure router mpls class-forwarding-policy

Description This command configures the class-based forwarding (CBF) policy used in the CBF feature of an LDP FEC or a BGP prefix over IGP shortcuts.

Parameters *policy-name* — Specifies the name of the class forwarding policy, up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

7.92 class-pool

class-pool

Syntax [**no**] **class-pool** *alt-class-pool-id*

Context **[Tree]** (config>qos>hs-port-pool-policy>alt-port-class-pools class-pool)

Full Context configure qos hs-port-pool-policy alt-port-class-pools class-pool

Description Commands in this context configure a class pool's parent mid-pool, dynamic port bandwidth weight, explicit percentage of mid-pool size, or a slope policy. Six alternate port-class pools always exist (one for each of the six scheduling classes) and do not need to be created.

The **no** form of the command restores the default **parent-mid-pool** association to **mid-pool none**, restores the default allocation **port-bw-weight 1** setting (**explicit-percent** disabled), and restores the default slope policy to the specified class-pool.

Parameters *alt-class-pool-id* — Specifies the class pool ID.

Values 1 to 6

Platforms 7750 SR-7/12/12e

class-pool

Syntax [**no**] **class-pool** *std-class-pool-id*

Context **[Tree]** (config>qos>hs-port-pool-policy>std-port-class-pools class-pool)

Full Context configure qos hs-port-pool-policy std-port-class-pools class-pool

Description Commands in this context configure class pool's parent mid-pool, dynamic port bandwidth weight, explicit percentage of mid-pool size, or a slope policy. Six alternate port-class pools always exist (one for each of the six scheduling classes) and do not need to be created.

The **no** form of the command restores the default **parent-mid-pool association** to **mid-pool 1**, restores the default allocation **port-bw-weight 1** setting (**explicit-percent** disabled), and restore the default slope policy to the specified class-pool.

Parameters *std-class-pool-id* — Specifies the class pool ID.

Values 1 to 6

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.93 class-type

class-type

Syntax **class-type** *ct-number*
no class-type

Context **[Tree]** (config>router>mpls>lsp class-type)
[Tree] (config>router>mpls>lsp>primary class-type)
[Tree] (config>router>mpls>lsp>secondary class-type)
[Tree] (config>router>mpls>lsp-template class-type)

Full Context configure router mpls lsp class-type
configure router mpls lsp primary class-type
configure router mpls lsp secondary class-type
configure router mpls lsp-template class-type

Description This command configures the Diff-Serv Class Type (CT) for an LSP, the LSP primary path, or the LSP secondary path. The path level configuration overrides the LSP level configuration. However, only one CT per LSP path will be allowed as per RFC 4124.

The signaled CT of a dynamic bypass is always be CT0 regardless of the CT of the primary LSP path. The setup and hold priorities must be set to default values, that is, 7 and 0 respectively. This assumes that the operator configured a couple of TE classes, one which combines CT0 and a priority of 7 and the other which combines CT0 and a priority of 0. If not, the bypass LSP will not be signaled and will go into the down state.

The operator cannot configure the CT, setup priority, and hold priority of a manual bypass. They are always signaled with CT0 and the default setup and holding priorities.

The signaled CT and setup priority of a detour LSP must match those of the primary LSP path it is associated with.

If the operator changes the CT of an LSP or of an LSP path, or changes the setup and holding priorities of an LSP path, the path will be torn down and retried.

An LSP which does not have the CT explicitly configured will behave like a CT0 LSP when Diff-Serv is enabled.

If the operator configured a combination of a CT and a setup priority and/or a combination of a CT and a holding priority for an LSP path that are not supported by the user-defined TE classes, the LSP path will be kept in a down state and an error code will be displayed in the show command output for the LSP path.

The **no** form of this command reverts to the default value.

Default class-type 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ct-number* — Specifies the Diff-Serv Class Type number.

Values 0 to 7

Platforms All

7.94 class-type-bw

class-type-bw

Syntax **class-type-bw ct0** *%-link-bandwidth* **ct1***%-link-bandwidth* **ct2***%-link-bandwidth* **ct3***%-link-bandwidth* **ct4***%-link-bandwidth* **ct5***%-link-bandwidth* **ct6***%-link-bandwidth* **ct7***%-link-bandwidth*

no class-type-bw

Context [Tree] (config>router>rsvp>diffserv-te class-type-bw)
[Tree] (config>router>rsvp>interface class-type-bw)

Full Context configure router rsvp diffserv-te class-type-bw
configure router rsvp interface class-type-bw

Description This command configures the percentage of RSVP interface bandwidth each CT shares, for example, the Bandwidth Constraint (BC).

The absolute value of the CT share of the interface bandwidth is derived as the percentage of the bandwidth advertised by IGP in the Maximum Reservable Link Bandwidth TE parameter, for example, the link bandwidth multiplied by the RSVP interface **subscription** *percentage* parameter.

Note: This configuration also exists at RSVP interface level and the interface specific configured value overrides the global configured value. The BC value can be changed at any time.

The RSVP interface **subscription** *percentage* parameter is configured in the **config>router>rsvp>interface** context.

The operator can specify the Bandwidth Constraint (BC) for a CT which is not used in any of the TE class definition but that does not get used by any LSP originating or transiting this node.

When Diff-Serv is disabled on the node, this model degenerates into a single default CT internally with eight preemption priorities and a non-configurable BC equal to the Maximum Reservable Link Bandwidth. This would behave exactly like CT0 with eight preemption priorities and BC= Maximum Reservable Link Bandwidth if Diff-Serv was enabled.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **ct0** (**ct1**/**ct2**/ —**ct7**) %*link-bandwidth* — The Diff-Serv Class Type number. One or more system forwarding classes can be mapped to a CT.

Values 0 to 100 %

Default 0

Platforms All

7.95 class-weight

class-weight

Syntax **class-weight** *weight*
no class-weight

Context **[Tree]** (config>service>epipe>sap>egress>queue-override>hs-wrr-group class-weight)
[Tree] (config>service>ipipe>sap>egress>queue-override>hs-wrr-group class-weight)

Full Context configure service epipe sap egress queue-override hs-wrr-group class-weight
configure service ipipe sap egress queue-override hs-wrr-group class-weight

Description This command overrides the class weight of this WRR group at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

class-weight

Syntax **class-weight** *weight*
no class-weight

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>hs-wrr-group class-weight)

Full Context configure service vpls sap egress queue-override hs-wrr-group class-weight

Description This command overrides the class weight of this WRR group at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

class-weight

Syntax **class-weight** *weight*
no class-weight

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>hs-wrr-group class-weight)

Full Context configure service ies interface sap egress queue-override hs-wrr-group class-weight

Description This command overrides the class weight of this WRR group at its parent primary shaper relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

class-weight

Syntax **class-weight** *weight*
no class-weight

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>hs-wrr-group class-weight)

Full Context configure service vprn interface sap egress queue-override hs-wrr-group class-weight

Description This command overrides the class weight of this WRR group at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.96 classes

classes

Syntax **classes** *limit*
no classes

Context **[Tree]** (config>card>fp>ingress>policy-accounting classes)

Full Context configure card fp ingress policy-accounting classes

Description This command configures the maximum number of source and destination classes that can be instantiated for accounting purposes on the interfaces of a specific card or FP.

The **no** form of this command specifies that no resources are reserved for source or destination classes.

Parameters *limit* — Specifies the number of accounting classes.

Values 1000 to 128000

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

7.97 classic-cli

classic-cli

Syntax **classic-cli**

Context **[Tree]** (config>system>management-interface>cli classic-cli)

Full Context configure system management-interface cli classic-cli

Description Commands in this context configure parameters related to classic CLI capabilities.

Platforms All

classic-cli

Syntax **classic-cli**

Context **[Tree]** (config>system>security>management-interface classic-cli)

Full Context configure system security management-interface classic-cli

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure hash-control for the classic CLI interface.

Platforms All

7.98 classic-lsn-max-subscriber-limit

classic-lsn-max-subscriber-limit

Syntax **classic-lsn-max-subscriber-limit** *max*
no classic-lsn-max-subscriber-limit

Context **[Tree]** (config>service>vprn>nat>inside>deterministic classic-lsn-max-subscriber-limit)
[Tree] (config>router>nat>inside>deterministic classic-lsn-max-subscriber-limit)

Full Context configure router nat inside deterministic classic-lsn-max-subscriber-limit
configure service vprn nat inside deterministic classic-lsn-max-subscriber-limit

Description This command affects ingress hashing of the subscribers for deterministic NAT. It will also affect hashing of the subscribers for non-deterministic NAT if the both types of NAT are configured simultaneously. The hashing will ensure that traffic load is distributed over multiple MS-ISAs in the system. For deterministic LSN44, (32 – n) bits of the source IP address will be considered for hashing, where 2^n= classic-lsn-max-subscriber-limit.

The scope of this command is the inside routing instance. This command must match the largest subscriber limit of all pools that are referenced by nat-policies configured within the corresponding inside routing instance.

This parameter must be configured before any prefix is configured and can be modified only if there are no prefixes configured under the deterministic NAT CLI hierarchy.

If non-deterministic NAT is not used simultaneously with deterministic NAT within a routing context, then hashing for non-deterministic NAT will be performed based on the subscriber.

Default no classic-lsn-max-subscriber-limit

Parameters *max* — The power of 2 (2^n) number that must match the largest subscriber limit number in a deterministic pool referenced from this inside routing instance. The range for this command is the same as the subscriber-limit command under the pool hierarchy.

classic-lsn-max-subscriber-limit

Syntax **classic-lsn-max-subscriber-limit** *max*
no classic-lsn-max-subscriber-limit

Context **[Tree]** (config>router>nat>inside classic-lsn-max-subscriber-limit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>nat>inside classic-lsn-max-subscriber-limit)

Full Context
configure router nat inside classic-lsn-max-subscriber-limit
configure service vprn nat inside classic-lsn-max-subscriber-limit

Description
This command sets the granularity of traffic distribution in the upstream direction across the MS-ISA within the scope of an inside routing context. Traffic distribution mechanism is based on the source IPv4 addresses/prefixes. More granular distribution is based on the IPv4 address, while distribution based on the IPv4 prefix (determined by prefix length) will be less granular. The granularity will further decrease with shorter prefix length.

For example, a prefix length of 32 will distribute individual /32 IPv4 addresses over multiple MS-ISAs in an ISA group. This will ensure better traffic load balancing at the expense of forwarding table utilization on the outside (public side) where each /32 is installed in the forwarding table. On the contrary, shorter prefixes will ensure better utilization of the forwarding table on the outside, at the expense of coarser spread of IP addresses over multiple MS-ISAs.

This command affects all flavors of LSN44 within the inside routing contexts, although its primary use is intended for deterministic NAT and dnat-only.

The length of the prefix that is used for distribution purposes is (32-n), where 2^n= classic-lsn-max-subscriber-limit. For example, if traffic distribution is based on the IPv4 address (prefix length = 32), then n must be 0. From here, it follows that classic-lsn-max-subscriber-limit must be set to 1:

Prefix length = 32 -> 32-n = 32 -> n=0 -> 2^0= 1 = *classic-lsn-max-subscriber-limit*
classic-lsn-max-subscriber-limit = 1

The implicit method given by this command uses power of 2 calculations to provide prefix length for traffic distribution purposes. This roundabout approach to determine the prefix-length has roots in deterministic NAT where this command was originally introduced.

Even though deterministic NAT and dnat-only have very little in common, the method (and CLI syntax) for calculating the prefix length using the classic-lsn-max-subscriber-limit parameter for traffic distribution purposes is shared between the two. In dnat-only, this parameter is important from an operational perspective since it affects traffic load balancing over MS-ISA and the size of the routing table.

This command must be configured before any prefix is configured and can be modified only if there are no prefixes configured under the deterministic NAT.

Parameters
max — The power of 2 (2^n) value which in deterministic NAT must match the largest subscriber-limit value in any deterministic pool referenced from this inside routing instance.

In **dnat-only**, this value can be set to any value from the allowed range.

In both cases, this value will determine the prefix-length (17-32) that will directly influence load distribution between the MS-ISAs and the size of the routing table.

Values 1,2,4,8 to 32768

Platforms
7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.99 classic-lsn-sub

classic-lsn-sub

Syntax [**no**] **classic-lsn-sub router** *router-instance* **ip** *ip-address*

Context **[Tree]** (config>li>li-source>nat classic-lsn-sub)

Full Context configure li li-source nat classic-lsn-sub

Description This command configures a classic LSN subscriber sources.

The **no** form of this command removes the parameter from the configuration.

Parameters *router-instance* — Specifies the router instance the pool belongs to, either by router name or service ID.

Values *router-name*: “Base” | “management”

Default Base

ip-address — Specifies the IP address in a.b.c.d format.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.100 classification-overrides

classification-overrides

Syntax **classification-overrides**

Context **[Tree]** (config>app-assure>group>url-filter>web-service classification-overrides)

Full Context configure application-assurance group url-filter web-service classification-overrides

Description Commands in this context create a classification override and allows the operator to manually set the category of a hostname.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.101 classifier

classifier

Syntax **classifier** *classifier* **category-set-id** *category-set*
no classifier

Context **[Tree]** (config>app-assure>group>url-filter>web-service classifier)

Full Context configure application-assurance group url-filter web-service classifier

Description This command selects the web service to use from the supported web services.

The **no** form of this command removes the selected web service.

Default no classifier

Parameters *classifier* — Specifies the web service to use.

Values web-service-1 | web-service-2

category-set — Specifies the category ID set to use for URL categorization. A category-set ID defines the list of categories that the web service uses to perform URL categorization.

Values 1 to 2

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.102 clear

clear

Syntax **clear**

Context **[Tree]** (admin clear)

Full Context admin clear

Description Commands in this context clear statistics.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.103 clear-alarm-msg

clear-alarm-msg

Syntax **clear-alarm-msg** *message-string*
no clear-alarm-msg

Context **[Tree]** (config>system>alarm-contact-input clear-alarm-msg)

Full Context configure system alarm-contact-input clear-alarm-msg

Description This command configures a message string to send with SNMP trap and log event messages that are generated when the system clears an alarm. The system generates the default message “Alarm Input Cleared” if no message is configured. The **clear-alarm-msg** string is included in the log event when the pin changes to the normal state.

The **no** form of this command reverts to the default message “Alarm Input Cleared”.

Default no clear-alarm-msg

Parameters *message-string* — Specifies a printable character string, up to 160 characters.

Platforms 7750 SR-a

7.104 clear-df-bit

clear-df-bit

Syntax [**no**] **clear-df-bit**

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel clear-df-bit)
[Tree] (config>service>ies>if>sap>ip-tunnel clear-df-bit)
[Tree] (config>service>vprn>if>ipsec>ip-tunnel clear-df-bit)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel clear-df-bit)
[Tree] (config>router>if>ipsec>ipsec-tunnel clear-df-bit)

Full Context configure router interface ipsec ipsec-tunnel clear-df-bit
configure service ies interface ipsec ipsec-tunnel clear-df-bit
configure service ies interface sap ip-tunnel clear-df-bit
configure service vprn interface ipsec ip-tunnel clear-df-bit
configure service vprn interface sap ipsec-tunnel clear-df-bit

Description This command instructs the MS-ISA to reset the DF bit to 0 in all payload IP packets associated with the GRE or IPsec tunnel, before any potential fragmentation resulting from the **ip-mtu** command (this requires a modification of the header checksum).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the DF bit reset.

Default no clear-df-bit

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ip-tunnel clear-df-bit
- configure service vprn interface sap ipsec-tunnel clear-df-bit

VSR

- configure router interface ipsec ipsec-tunnel clear-df-bit
- configure service ies interface ipsec ipsec-tunnel clear-df-bit

clear-df-bit

Syntax [**no**] **clear-df-bit**

Context **[Tree]** (config>service>vprn>if clear-df-bit)

Full Context configure service vprn interface clear-df-bit

Description This command specifies whether to clear the Do not Fragment (DF) bit in the outgoing packets in this tunnel.

clear-df-bit

Syntax [**no**] **clear-df-bit**

Context **[Tree]** (config>ipsec>tnl-temp clear-df-bit)

Full Context configure ipsec tunnel-template clear-df-bit

Description This command enables clearing of the Do-not-Fragment bit.

Default no clear-df-bit

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.105 clear-ocsp-cache

clear-ocsp-cache

Syntax **clear-ocsp-cache** [*entry-id*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (admin>certificate clear-ocsp-cache)

Full Context admin certificate clear-ocsp-cache

Description This command clears the current OCSP response cache. If optional issuer and serial-number are not specified, then all current cached results are cleared.

Parameters *entry-id* — Specifies the local cache entry identifier of the certificate to clear.

Values 1 to 2000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.106 clear-request

clear-request

Syntax **clear-request ca** *ca-profile-name*

Context [Tree] (admin>certificate>cmpv2 clear-request)

Full Context admin certificate cmpv2 clear-request

Description This command clears current pending CMPv2 requests toward the specified CA. If there are no pending requests, it will clear the saved result of prior request.

Parameters **ca** *ca-profile-name* — Specifies a ca-profile name up to 32 characters.

Platforms All

7.107 clear-tag-mode

clear-tag-mode

Syntax **clear-tag-mode** *clear-tag-mode*
no clear-tag-mode

Context [Tree] (config>macsec>connectivity-association clear-tag-mode)

Full Context configure macsec connectivity-association clear-tag-mode

Description This command puts 802.1Q tags in clear text before the SecTAG. There are two modes: **single-tag** and **dual-tag**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 40 explains the encrypted dot1q and QinQ packet format when clear-tag-mode single-tag or dual-tag is configured.

The **no** form of this command puts all dot1q tags encrypted after the SecTAG.

Table 40 **Encrypted Dot1q and QinQ Packet Format**

Unencrypted format	Clear-tag-mode	Pre-encryption (Tx)	Pre-decryption (Rx)
Single tag (dot1q)	single-tag	DA, SA, TPID, VID, Etype	DA, SA, TPID, VID, SecTag
Single tag (dot1q)	dual-tag	DA, SA, TPID, VID, Etype	DA, SA, TPID, VID, SecTag
Double tag (q-in-q)	single-tag	DA, SA, TPID1, VID1, IPID2, VID2, Etype	DA, SA, TPID1, VID1, SecTag
Double tag (QinQ)	dual-tag	DA, SA, TPID1, VID1, IPID2, VID2, Etype	DA, SA, TPID1, VID1, IPID2, VID2, SecTag

Default no clear-tag-mode

Parameters *clear-tag-mode* — Specifies the clear tag mode.

Values single-tag, dual-tag

Platforms All

7.108 cli

cli

Syntax [**no**] **cli**

Context **[Tree]** (debug>dynsvc>scripts>event cli)
[Tree] (debug>dynsvc>scripts>inst>event cli)
[Tree] (debug>dynsvc>scripts>script>event cli)

Full Context debug dynamic-services scripts event cli
debug dynamic-services scripts instance event cli
debug dynamic-services scripts script event cli

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables/disables the generation of a specific dynamic data service script debugging event output: cli.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

cli

Syntax [**no**] **cli**

Context **[Tree]** (debug>vsd>scripts>event cli)
[Tree] (debug>vsd>scripts>instance cli)

Full Context debug vsd scripts event cli
debug vsd scripts instance cli

Description This command enables/disables the generation of a specific script debugging event output: **cli**.

Platforms All

cli

Syntax **cli**

Context **[Tree]** (config>system>management-interface cli)

Full Context configure system management-interface cli

Description Commands in this context configure CLI capabilities.

Platforms All

cli

Syntax **cli** {**warning** | **info**}

Context **[Tree]**
(config>system>management-interface>cli>md-cli>environment>message-severity-level cli)

Full Context configure system management-interface cli md-cli environment message-severity-level cli

Description This command specifies the threshold for CLI messages.

Default cli info

Parameters **warning** — Specifies that WARNING messages are displayed but INFO messages are suppressed.

info — Specifies that INFO messages and WARNING messages are displayed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

7.109 cli-engine

cli-engine

Syntax **cli-engine** {**classic-cli** | **md-cli**} [{**classic-cli** | **md-cli**}]
no cli-engine

Context **[Tree]** (config>system>management-interface>cli cli-engine)

Full Context configure system management-interface cli cli-engine

Description This command configures the system-wide CLI engine. One or both engines can be configured.

In order for the changes to the **cli-engine** parameter to take effect, log out of the CLI session and start a new session.

Parameters **classic-cli** — Specifies the classic CLI.

md-cli — Specifies the MD-CLI.

Platforms All

7.110 cli-script

cli-script

Syntax **cli-script**

Context **[Tree]** (config>system>security cli-script)

Full Context configure system security cli-script

Description Commands in this context configure the security parameters in the system.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.111 cli-session-group

cli-session-group

Syntax **cli-session-group** *session-group-name* [**create**]
no cli-session-group *session-group-name*

Context **[Tree]** (config>system>security cli-session-group)

Full Context configure system security cli-session-group

Description This command is used to configure a session group that can be used to limit the number of CLI sessions available to members of the group.

Parameters *session-group-name* — Specifies a particular session group.

Platforms All

7.112 cli-user

cli-user

Syntax **cli-user** *name*
no cli-user

Context **[Tree]** (config>service>dynsvc>policy cli-user)

Full Context configure service dynamic-services dynamic-services-policy cli-user

Description This command specifies the CLI user to be used to execute the dynamic data services CLI scripts. With the specified user's profile, it is possible to further restrict the internal list of allowed commands to be executed via dynamic data service CLI scripts.

The **no** form of this command sets the CLI user to an internal user with all configuration rights.

Parameters *name* — Specifies the CLI user name that must exist in the >config>system>security CLI context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

cli-user

Syntax **cli-user** *user-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no cli-user

Context [Tree] (config>system>security>cli-script>authorization>cron cli-user)
[Tree] (config>system>security>cli-script>authorization>event-handler cli-user)
[Tree] (config>system>security>cli-script>authorization>vsd cli-user)

Full Context configure system security cli-script authorization cron cli-user
configure system security cli-script authorization event-handler cli-user
configure system security cli-script authorization vsd cli-user

Description This command configures the user context under which various types of CLI scripts should execute in order to authorize the script commands. TACACS+ and RADIUS users and authorization are not permitted for **cli-script** authorization.

The **vsd cli-user** command configures the CLI user for the configuration coming from VSD (fully dynamic VSD integration model). The user profile determines what set of CLI commands can be executed by the VSD. This set of commands is a sub-set of the commands allowed by the system for the VSD. You can use the **tools dump service vsd-services command-list** to check the allowed commands.

The **no** form of this command configures scripts to execute with no restrictions and without performing authorization.

Default no cli-user

Parameters *user-name* — The name of a user in the local node database. TACACS+ or RADIUS users can not be used. The user configuration should reference a valid local profile for authorization.

Platforms All

7.113 client

client

Syntax **client** *client-index* [**create**]
no client *client-index*

Context [Tree] (config>ipsec>client-db client)

Full Context configure ipsec client-db client

Description This command creates a new IPsec client entry in the client-db or enters the configuration context of an existing client entry.

There may be multiple client entries defined in the same client-db. If there are multiple entries that match the new tunnel request, then the system will select the entry that has smallest client-index.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters **client-index** — Specifies the ID of the client entry.

Values 1 to 8000

create — Keyword used to create the security policy instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

client

Syntax **client all**
client *ip-address*
no client

Context **[Tree]** (debug>system>grpc client)

Full Context debug system grpc client

Description This command enables debug output for all clients for a particular client.

The **no** form of this command deactivates debugging for all clients.

Parameters **all** — Specifies that debugging will occur for all clients.

ip-address — Specifies the IPv4 or IPv6 address of the client.

Platforms All

client

Syntax **client**

Context **[Tree]** (config>system>security>ssh>key-re-exchange client)

Full Context configure system security ssh key-re-exchange client

Description Commands in this context enable the key re-exchange for SR OS as an SSH client.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.114 client-application

client-application

Syntax **client-application** [**ppp-v4**] [**ipoe-v4**]
no client-application

Context **[Tree]** (config>service>ies>sub-if>grp-if>local-address-assignment client-application)
[Tree] (config>service>ies>sub-if>local-address-assignment client-application)
[Tree] (config>service>vprn>sub-if>grp-if>local-address-assignment client-application)
[Tree] (config>service>vprn>sub-if>local-address-assignment client-application)

Full Context configure service ies subscriber-interface group-interface local-address-assignment client-application
configure service ies subscriber-interface local-address-assignment client-application
configure service vprn subscriber-interface group-interface local-address-assignment client-application
configure service vprn subscriber-interface local-address-assignment client-application

Description This command enables local DHCP Server pool management for PPPoXv4 clients.

A pool of IP addresses can be shared between IPoE clients that rely on DHCP protocol (lease renewal process) and PPPoX clients where address allocation is not dependent on DHCP messaging but instead an IP address allocation within the pool is tied to the PPPoX session.

The **no** form of this command disables Local Address Assignment for any protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

client-application

Syntax **client-application** [**ppp-slaac**] [**ipoe-wan**] [**ipoe-slaac**]
no client-application

Context **[Tree]** (config>service>vprn>sub-if>grp-if>lcl-addr-assign>ipv6 client-application)

Full Context configure service vprn subscriber-interface group-interface local-address-assignment ipv6 client-application

Description This command defines the client application that uses the local address server to perform address assignment. This feature is relies on RADIUS or local-user-database to return a pool name. The pool name is matched again the pools defined in the local-dhcp6-server configuration. The name of the local-dhcp6-server must also be provisioned.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **ppp-slaac** — Indicates using the local DHCPv6 prefix pool to assign SLAAC prefixes for hosts. The pool name where the prefixes are used for SLAAC prefix assignment are obtained from RADIUS or local-user-database during the authentication process. The RADIUS attribute Alc-slaac-ipv6-pool is used to indicate the SLAAC pool name for PPPoE hosts.

ipoe-wan — Indicates using the local DHCPv6 pool for IA_NA address assignment and a static pre-defined prefixes for IA_PD. Both the IA_NA pool name and the IA_PD static framed-prefix are either obtained from RADIUS or LUDB during authentication. With RADIUS, it must return both IA_NA Framed-IPv6-Pool and IA_PD Delegated-IPv6-Prefix after a successful authentication. With LUDB, it must have ipv6-wan-address-pool and ipv6-delegated-prefix populated. This feature is specific to this use case and is not required for other combinations of DHCPv6 assignments such as IA_NA and IA_PD address assignment through RADIUS or LUDB.

ipoe-slaac — Indicates using the local DHCPv6 prefix pool to assign SLAAC prefixes for hosts. The pool name where the prefixes are used for SLAAC prefix assignment are obtained from RADIUS or local-user-database during the authentication process. The RADIUS attribute Alc-slaac-ipv6-pool is used to indicate the SLAAC pool name for PPPoE hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.115 client-applications

client-applications

Syntax **client-applications** [**dhcp**] [**ppp**]
no client-applications

Context **[Tree]** (config>service>vprn>sub-if>dhcp client-applications)
[Tree] (config>service>ies>sub-if>dhcp client-applications)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp client-applications)
[Tree] (config>service>ies>sub-if>grp-if>dhcp client-applications)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy client-applications)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay client-applications)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy client-applications)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay client-applications)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>proxy client-applications)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay client-applications)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>proxy client-applications)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>relay client-applications)

Full Context configure service ies subscriber-interface dhcp client-applications
configure service ies subscriber-interface group-interface dhcp client-applications
configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server client-applications

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface ipv6 dhcp6 relay client-applications
configure service ies subscriber-interface ipv6 dhcp6 proxy-server client-applications
configure service ies subscriber-interface ipv6 dhcp6 relay client-applications
configure service vprn subscriber-interface dhcp client-applications
configure service vprn subscriber-interface group-interface dhcp client-applications
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server client-applications
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay client-applications
configure service vprn subscriber-interface ipv6 dhcp6 proxy-server client-applications
configure service vprn subscriber-interface ipv6 dhcp6 relay client-applications

Description This command enables DHCP relay and proxy-server for the configured client types.

The **no** form of this command reverts to the default.

Default dhcp

Parameters **dhcp** — Enables IPoE clients to use the DHCP relay or proxy-server.

ppp — Enables PPPoE clients to use the DHCP relay or proxy-server that PPPoE attempts to request an IP address for a PPPoE client from the DHCP server assigned to PPPoE node.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.116 client-cert-subject-key-id

client-cert-subject-key-id

Syntax [**no**] **client-cert-subject-key-id**

Context **[Tree]** (config>ipsec>rad-auth-plcy>include client-cert-subject-key-id)

Full Context configure ipsec radius-authentication-policy include-radius-attribute client-cert-subject-key-id

Description This command enables the inclusion of the Subject Key Identifier of the peer's certificate in the RADIUS Access-Request packet as VSA: Alc-Subject-Key-Identifier. Refer to the *7750 SR and VSR RADIUS Attributes Reference Guide* for more information.

Default no client-cert-subject-key-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.117 client-cipher-list

client-cipher-list

Syntax **client-cipher-list protocol-version** *version*

Context **[Tree]** (config>system>security>ssh client-cipher-list)

Full Context configure system security ssh client-cipher-list

Description This command enables the configuration of a list of allowed ciphers by the SSH client.

Parameters *version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1 2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2

Platforms All

client-cipher-list

Syntax **client-cipher-list** *name* [**create**]
no client-cipher-list *name*

Context **[Tree]** (config>system>security>tls client-cipher-list)

Full Context configure system security tls client-cipher-list

Description This command creates a cipher list that the client sends to the server in the client Hello message. It is a list of ciphers that are supported and preferred by the SR OS to be used in the TLS session. The server matches this list against the server cipher list. The most preferred cipher found in both lists is chosen.

Parameters *name* — Specifies the name of the client cipher list, up to 32 characters in length.

create — Keyword used to create the client cipher list.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.118 client-db

client-db

Syntax **client-db** *db-name* [**create**]
no client-db *db-name*

Context **[Tree]** (config>ipsec client-db)

Full Context configure ipsec client-db

Description This command creates a new IPsec client-db or enters the configuration context of an existing client-db.

An IPsec client-db can be used for IKEv2 dynamic LAN-to-LAN tunnel authentication and authorization. When a new tunnel request is received, the system will match the request to the client entries configured in client-db and use credentials returned by the matched client entry for authentication. If authentication succeeds, the system could also use the IPsec configuration parameters (such as **private-service-id**) returned by the matched entry to set up the tunnel.

The configured client-db is referenced under the ipsec-gw configuration context using the **client-db** command.

The **no** form of this command removes the *db-name* from the configuration.

Parameters *db-name* — Specifies the name of this IPsec client up to 32 characters.

create — Keyword used to create the security policy instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

client-db

Syntax **client-db** *name*
client-db *name* **fallback**
client-db *name* **no-fallback**
no client-db

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw client-db)
[Tree] (config>service>vprn>if>sap>ipsec-gw client-db)

Full Context configure service ies interface sap ipsec-gw client-db
configure service vprn interface sap ipsec-gw client-db

Description This command enables the use of an IPsec client database. The system uses the specified client database to authenticate IKEv2 dynamic LAN-to-LAN tunnel.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no client-db

Parameters *name* — Specifies the name of the client database.

fallback — Specifies whether or not this IPsec gateway falls back to the default authentication policy when the IPsec tunnel authentication request fails to match any clients in the IPsec database.

no-fallback — Specifies that if the client database lookup fails to return a matched result, the system will fail the tunnel setup.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

client-db

Syntax [**no**] **no client-db** *db-name*

Context **[Tree]** (debug>ipsec client-db)

Full Context debug ipsec client-db

Description This command enables debugging for the specified IPsec client-db.

Parameters *db-name* — Specifies the IPsec client database name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.119 client-down-delay

client-down-delay

Syntax **client-down-delay** *client-down-delay*
no client-down-delay

Context **[Tree]** (config>system>satellite>eth-sat client-down-delay)

Full Context configure system satellite eth-sat client-down-delay

Description This command sets the delay between the last available uplink becoming unavailable and the disabling of associated Ethernet satellite client ports.

The **no** form of this command disables the delay and reverts to the current behavior.

Default no client-down-delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *client-down-delay* — Sets the number of seconds to wait between the last available uplink becoming unavailable and the disabling of associated ethernet satellite client ports.

Values 0 to 1800

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.120 client-id

client-id

Syntax **client-id** {**mac-pppoe-session-id**}
no client-id

Context **[Tree]** (config>service>ies>sub-if>grp-if>pppoe>dhcp-client client-id)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe>dhcp-client client-id)

Full Context configure service ies subscriber-interface group-interface pppoe dhcp-client client-id
configure service vprn subscriber-interface group-interface pppoe dhcp-client client-id

Description This command inserts a DHCP client identifier option 61 in DHCP client messages for PPPoE sessions that obtain IPv4 addresses from a third party DHCP server. By default, a DHCP client identifier option 61 is not included.

The **no** form of this command reverts to the default.

Default no client-id

Parameters **mac-pppoe-session-id** — Specifies that the DHCP client identifier option 61 contains a type value with type set to zero (1 octet) and value set to the PPPoE client MAC address (6 octets) and the PPPoE session ID (2 octets). For example:

Opt 61 (hex) = 00 00 10 94 A0 45 E5 00 01

where:

00 = type

00 10 94 A0 45 E5 = PPPoE client MAC address

00 01 = PPPoE session ID

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.121 client-identification

client-identification

Syntax **client-identification**

Context **[Tree]** (config>ipsec>client-db>client client-identification)

Full Context configure ipsec client-db client client-identification

Description Commands in this context configure client ID information of this IPsec client.

If there are multiple match input are configured in the match-list of the client-db, then all corresponding match criteria must be configured for the client-entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.122 client-ip

client-ip

Syntax **client-ip** {**eq** | **neq**} *ip-address*
no client-ip

Context **[Tree]** (debug>app-assure>group>traffic-capture>match client-ip)

Full Context debug application-assurance group traffic-capture match client-ip

Description This command configures debugging of a client IP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.123 client-kex-list

client-kex-list

Syntax **client-kex-list**

Context **[Tree]** (config>system>security>ssh client-kex-list)

Full Context configure system security ssh client-kex-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure SSH KEX algorithms for SR OS as a client.

An empty list is the default list that the SSH KEX advertises. The default list contains the following:

diffie-hellman-group16-sha512

diffie-hellman-group14-sha256

diffie-hellman-group14-sha1

diffie-hellman-group1-sha1

Platforms All

7.124 client-mac

client-mac

Syntax **client-mac** {**odd** | **even**}
no client-mac

Context **[Tree]** (config>service>ies>sub-if>grp-if>dhcp>osel client-mac)
[Tree] (config>service>vprn>sub-if>dhcp>osel client-mac)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>osel client-mac)

Full Context configure service ies subscriber-interface group-interface dhcp offer-selection client-mac
configure service vprn subscriber-interface dhcp offer-selection client-mac
configure service vprn subscriber-interface group-interface dhcp offer-selection client-mac

Description Commands in this context configure a delay for the Discover message from the designated client MAC addresses.

The **no** form of this command removes the client MAC configuration.

Parameters **odd** — Specifies to use the odd client MAC address.

even — Specifies to use the even client MAC address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

client-mac

Syntax **client-mac** {**odd** | **even**}
no client-mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection client-mac)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>advertise-selection client-mac)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection client-mac)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection client-mac

Description Commands in this context configure a solicit delay or preference option value in function of the source MAC address of the solicit message.

The **no** form of this command removes the client MAC configuration.

Parameters **odd** — Specifies to use the odd client MAC address.

even — Specifies to use the even client MAC address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.125 client-mac-address

client-mac-address

Syntax [**no**] **client-mac-address**

Context [Tree] (config>service>ies>if>dhcp>option>vendor client-mac-address)
[Tree] (config>service>ies>sub-if>dhcp>option client-mac-address)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option>vendor client-mac-address)
[Tree] (config>service>vprn>if>dhcp>option>vendor client-mac-address)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option>vendor client-mac-address)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option>vendor client-mac-address)
[Tree] (config>service>vpls>sap>dhcp>option>vendor client-mac-address)

Full Context configure service ies interface dhcp option vendor-specific-option client-mac-address
configure service ies subscriber-interface dhcp option client-mac-address
configure service ies subscriber-interface group-interface dhcp option vendor-specific-option client-mac-address
configure service vpls sap dhcp option vendor-specific-option client-mac-address
configure service vprn interface dhcp option vendor-specific-option client-mac-address
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option client-mac-address
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option client-mac-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the sending of the MAC address in the Nokia vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command disables the sending of the MAC address in the Nokia vendor-specific sub-option of the DHCP relay packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option client-mac-address
- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option client-mac-address
- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option client-mac-address

All

- configure service ies interface dhcp option vendor-specific-option client-mac-address
- configure service vpls sap dhcp option vendor-specific-option client-mac-address
- configure service vprn interface dhcp option vendor-specific-option client-mac-address

client-mac-address

Syntax [**no**] **client-mac-address**

Context **[Tree]** (config>router>if>dhcp>option client-mac-address)

Full Context configure router interface dhcp option client-mac-address

Description This command enables the sending of the MAC address in the Nokia vendor specific suboption of the DHCP relay packet.

The **no** form of this command disables the sending of the MAC address in the Nokia vendor specific suboption of the DHCP relay packet.

Default no client-mac-address

7.126 client-mac-list

client-mac-list

Syntax **client-mac-list**

Context **[Tree]** (config>system>security>ssh client-mac-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security ssh client-mac-list

Description Commands in this context configure SSH MAC algorithms for SR OS as a client.

Platforms All

7.127 client-meg-level

client-meg-level

Syntax **client-meg-level** [[*level* [*level*]]
no client-meg-level

Context **[Tree]** (config>port>ethernet>eth-cfm>mep>ais-enable client-meg-level)
[Tree] (config>lag>eth-cfm>mep>ais-enable client-meg-level)

Full Context configure lag eth-cfm mep ais-enable client-meg-level
configure port ethernet eth-cfm mep ais-enable client-meg-level

Description This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level. Only the lowest client MEG level will be used for facility MEPs.

The **no** form of this command reverts to the default values.

Parameters *level* — Specifies the client MEG level.

Values 1 to 7

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

client-meg-level

Syntax **client-meg-level** [[*level* [*level* ...]]
no client-meg-level

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep client-meg-level)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>ais-enable client-meg-level)

Full Context configure service epipe sap eth-cfm mep client-meg-level
configure service epipe spoke-sdp eth-cfm ais-enable client-meg-level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the client maintenance entity group (MEG) level or levels to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level.

Parameters *level* — Specifies the client MEG level.

Values 1 to 7

Default 1

client-meg-level

Syntax **client-meg-level** [[*level* [*level* ...]]
no client-meg-level

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable client-meg-level)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable client-meg-level)

Full Context configure service vpls mesh-sdp eth-cfm mep ais-enable client-meg-level
configure service vpls spoke-sdp eth-cfm mep ais-enable client-meg-level

Description This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level.

Parameters *level* — Specifies the client MEG level

Values 1 to 7

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.128 client-name

client-name

Syntax **client-name** *name*
no client-name

Context **[Tree]** (config>ipsec>client-db>client client-name)

Full Context configure ipsec client-db client client-name

Description This command specifies the name of the client entry. The client name can be used in CLI navigation or in show commands.

Default no client-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the name of the client.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.129 client-port

client-port

Syntax **client-port** {**eq** | **neq**} *port-num*
no client-port

Context **[Tree]** (debug>app-assure>group>traffic-capture>match client-port)

Full Context debug application-assurance group traffic-capture match client-port

Description This command configures debugging of a client port.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.130 client-tls-profile

client-tls-profile

Syntax **client-tls-profile** *name*
no client-tls-profile

Context **[Tree]** (config>system>security>pki>est-profile client-tls-profile)

Full Context configure system security pki est-profile client-tls-profile

Description This command configures the TLS client profile to be assigned to applications for encryption. The profile creates the TLS connection to the EST server.

The **no** form of this command removes the name from the configuration.

Default no client-tls-profile

Parameters *name* — Specifies the name of the client TLS profile, up to 32 characters

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

client-tls-profile

Syntax **client-tls-profile** *name* [**create**]
no client-tls-profile *name*

Context **[Tree]** (config>system>security>tls client-tls-profile)

Full Context configure system security tls client-tls-profile

Description This command configures the TLS client profile to be assigned to applications for encryption.

Parameters *name* — Specifies the name of the client TLS profile, up to 32 characters in length.

create — Keyword used to create the client TLS profile.

Platforms All

client-tls-profile

Syntax **client-tls-profile** *name*
no client-tls-profile

Context **[Tree]** (config>system>management-interface>remote-management client-tls-profile)

Full Context configure system management-interface remote-management client-tls-profile

Description This command configures the TLS client profile used for encryption by all remote managers. This command and **allow-unsecure-connection** are mutually exclusive.

If this command is also configured for a specific manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command causes the profile configuration not to be used.

Parameters *name* — Specifies the name of the client TLS profile, up to 32 characters.

Platforms All

client-tls-profile

Syntax **client-tls-profile** *name*
no client-tls-profile

Context **[Tree]** (config>system>management-interface>remote-management>manager client-tls-profile)

Full Context configure system management-interface remote-management manager client-tls-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the TLS client profile used for encryption by this remote manager. This command and **allow-unsecure-connection** are mutually exclusive.

This command takes precedence over the same command configured in the global context (**config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command causes the profile configuration to be inherited from the global context (**config**>**system**>**management-interface**>**remote-management**).

Parameters *name* — Specifies the name of the client TLS profile, up to 32 characters.

Platforms All

7.131 clli-code

clli-code

Syntax **clli-code** *clli-code*
no clli-code

Context **[Tree]** (config>system clli-code)

Full Context configure system clli-code

Description This command creates a Common Language Location Identifier (CLLI) code string for the SR-series router. A CLLI code is an 11-character standardized geographic identifier that uniquely identifies geographic locations and certain functional categories of equipment unique to the telecommunications industry.

No CLLI validity checks other than truncating or padding the string to eleven characters are performed.

Only one CLLI code can be configured, if multiple CLLI codes are configured the last one entered overwrites the previous entry.

The **no** form of the command removes the CLLI code.

Default no clli-code

Parameters *clli-code* — Specifies the 11 character string CLLI code. Any printable, seven bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. If more than 11 characters are entered, the string is truncated. If less than 11 characters are entered the string is padded with spaces.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.132 clock-mode

clock-mode

Syntax **clock-mode adaptive**
clock-mode differential [**timestamp-freq** {19440 | 77760 | 103680}]

Context **[Tree]** (config>card>mda clock-mode)

Full Context configure card mda clock-mode

Description This command defines the clocking mode on the specified MDA. This command is only supported on CES MDAs.

Default clock-mode adaptive

Parameters **adaptive** — Specifies that MDA is in the adaptive clock mode. This MDA can use adaptive clock recovery methods.

differential — Specifies that MDA is in the differential clock mode. This MDA can use differential clock recovery methods.

timestamp-freq — Sets the differential timestamp frequency to be 103.68 MHz (default), 77,76 MHZ or 19.44 MHz. The frequency value is entered in kHz, thus valid values are 103680, 77760 and 19440. If this parameter is omitted, the default timestamp frequency of 103.68 MHz is used.

Values 19440, 77760, 103680

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

7.133 clock-offset

clock-offset

Syntax **clock-offset** *seconds*
no clock-offset

Context **[Tree]** (config>oam-pm>session>meas-interval clock-offset)

Full Context configure oam-pm session meas-interval clock-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows measurement intervals with a boundary-type of clock aligned to be offset from the default time of day clock. The configured offset must be smaller than the size of the measurement interval. As an example, an offset of 120 (seconds) shifts the start times of the measurement intervals by two minutes from their default alignments with respect to the time of day clock.

The **no** form of this command sets the offset to 0.

Default clock-offset 0

Parameters *seconds* — Specifies the number of seconds to offset a clock-alignment measurement interval from its default.

Values 0 to 86399

Default 0

Platforms All

7.134 clock-source

clock-source

Syntax **clock-source** {**loop-timed** | **node-timed**}

Context **[Tree]** (config>port>sonet-sdh clock-source)

Full Context configure port sonet-sdh clock-source

Description This command configures the clock to be used for transmission of data out towards the line. The options are to use the locally recovered clock from the line's receive data stream or the node central reference.

When changing the clock source for a port on an OC-48 MDA, a brief transmit interruption can occur on all ports of that MDA. Note that all SONET/SDH MDAs support loop timing.

The **node-timed** parameter in this command is supported by TDM satellite.

Parameters **loop-timed** — The link recovers the clock from the received data stream.

node-timed — The link uses the internal clock when transmitting data.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

clock-source

Syntax **clock-source** {**loop-timed** | **node-timed** | **adaptive** | **differential**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>port>tdm>ds1 clock-source)
[Tree] (config>port>tdm>ds3 clock-source)
[Tree] (config>port>tdm>e1 clock-source)
[Tree] (config>port>tdm>e3 clock-source)

Full Context
configure port tdm ds1 clock-source
configure port tdm ds3 clock-source
configure port tdm e1 clock-source
configure port tdm e3 clock-source

Description
This command configures the clock to be used for transmission of data out towards the line. The options are to use the locally recovered clock from the line's receive data stream, the node central reference, or an adaptively recovered clock using the received packets.

The following tables show MDAs that support loop timing at DS3/E3 and DS1/E1 channelization options.

TDM DS3/E3	LoopTimed	Default
Channelized OC-12	No	node-timed
Channelized OC-3	No	node-timed
Channelized DS3/E3	No	node-timed
Channelized ASAP OC-12	Yes	node-timed
Channelized ASAP OC-3	Yes	node-timed
Channelized ASAP DS3/E3	Yes	node-timed
CES OC-3	Yes	node-timed

TDM DS1/E1	LoopTimed	Default
Channelized OC-12	Yes	loop-timed
Channelized OC-3	Yes	loop-timed
Channelized DS3/E3	Yes	loop-timed
Channelized ASAP OC-12	Yes	loop-timed
Channelized ASAP OC-3	Yes	loop-timed
Channelized ASAP DS3/E3	Yes	loop-timed
CES OC-3	Yes	loop-timed

Parameters
loop-timed — The link recovers the clock from the received data stream.

node-timed — The link uses the internal clock when transmitting data.

adaptive — The clock is adaptively recovered from the rate at which data is received and not from the physical layer. Adaptive timing is only supported on ds1 and e1 channels.

differential — The clock is recovered from differential RTP timestamp header. Differential timing is only supported on ds1 and e1 channels.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

7.135 clock-type

clock-type

Syntax **clock-type boundary**
clock-type ordinary {**master** | **slave**}

Context **[Tree]** (config>system>ptp clock-type)

Full Context configure system ptp clock-type

Description This command configures the type of clock. The clock type can only be changed when PTP is shutdown.

The clock type cannot be changed to ordinary master if the PTP reference is no shutdown. In addition, the clock type cannot be changed to ordinary master if there are peers configured. The clock type is restricted based on the profile. See the **profile** command description for the details of the restrictions.

When enabling a PTP with clock-type boundary, at least one reference into the central frequency clock must be enabled using the **configure system sync-if-timing [bits |ref1 |ref2 | ptp| synce]** command.

Default clock-type ordinary slave

Parameters **boundary** — Specifies that the system is a boundary clock, which may be anywhere in the master-slave clock hierarchy. It can obtain timing from a master clock, and provide timing to multiple slave clocks concurrently.

ordinary master — Specifies that the system is a grandmaster clock in the master-slave hierarchy. The system provides timing to multiple slave clocks in the network.

ordinary slave — Specifies that the system is always a slave clock in the master-slave hierarchy. The system derives its timing from one or more master clocks in the network.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.136 close-session

close-session

Syntax [**no**] **close-session**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization close-session)

Full Context configure system security profile netconf base-op-authorization close-session

Description This command enables the NETCONF close-session operation.

The **no** form of this command disables the operation.

Default no close-session

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

7.137 clp-change

clp-change

Syntax [**no**] **clp-change**

Context **[Tree]** (config>service>apipe>spoke-sdp>cell-concat clp-change)

Full Context configure service apipe spoke-sdp cell-concatenation clp-change

Description This command enables the configuration of CLP change to be an indication to complete the cell concatenation operation.

The **no** form of this command resets the configuration to ignore the CLP change as an indication to complete the cell concatenation.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.138 clp-tagging

clp-tagging

Syntax [**no**] **clp-tagging**

Context **[Tree]** (config>qos>atm-td-profile clp-tagging)

Full Context configure qos atm-td-profile clp-tagging

Description This command controls the setting of the CLP bit in the ATM cell header for egress traffic on an IES or VPRN SAP.

When enabled, traffic queued on expedited queues has the CLP bit set to zero, while traffic on non-expedited queues has the CLP bit set to one.

The **no** form of this command sets the CLP bit set to zero.

Default no clp-tagging

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

7.139 cluster

cluster

Syntax **cluster** *cluster-id*
no cluster

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy cluster)

Full Context configure subscriber-mgmt bgp-peering-policy cluster

Description This command configures the cluster ID for a route reflector server.

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be non-clients.

When a route reflector receives a route, first it must select the best path from all the paths received. If the route was received from a non-client peer, then the route reflector sends the route to all clients in the cluster. If the route came from a client peer, the route reflector sends the route to all non-client peers and to all client peers except the originator.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For redundancy, a cluster can have multiple route reflectors.

Confederations can also be used to remove the full IBGP mesh requirement within an AS.

The **no** form of this command deletes the cluster ID and effectively disables the Route Reflection for the given group.

Parameters *cluster-id* — Specifies the route reflector cluster ID is expressed in dot decimal notation.

Values Any 32 bit number in dot decimal notation. (0.0.0.1 to 255.255.255.255)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

cluster

Syntax **cluster** *cluster-id*
no cluster

Context **[Tree]** (config>service>vprn>bgp cluster)
[Tree] (config>service>vprn>bgp>group cluster)
[Tree] (config>service>vprn>bgp>group>neighbor cluster)

Full Context configure service vprn bgp cluster
configure service vprn bgp group cluster
configure service vprn bgp group neighbor cluster

Description This command configures the cluster ID for a route reflector server.

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be non-clients.

When a route reflector receives a route, first it must select the best path from all the paths received. If the route was received from a non-client peer, then the route reflector sends the route to all clients in the cluster. If the route came from a client peer, the route reflector sends the route to all non-client peers and to all client peers except the originator.

For redundancy, a cluster can have multiple route reflectors.

Confederations can also be used to remove the full IBGP mesh requirement within an AS.

The **no** form of this command deletes the cluster ID and effectively disables the Route Reflection for the given group.

Default no cluster — No cluster ID is defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *cluster-id* — The route reflector cluster ID is expressed in dot decimal notation.

Values Any 32 bit number in dot decimal notation. (0.0.0.1 to 255.255.255.255)

Platforms All

cluster

Syntax **cluster** *cluster-id* **orr-location** *location-id* [**allow-local-fallback**]]

Context **[Tree]** (config>router>bgp cluster)

Full Context configure router bgp cluster

Description This command configures the cluster ID for a route reflector server ID and implicitly configures the associated BGP sessions as route reflector clients of the BGP instance. If an ORR location ID is specified with the cluster ID, the clients in that cluster receive routes optimal for that specific location; refer to *draft-ietf-idr-bgp-optimal-route-reflection* for more information.

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be non-clients.

When a route reflector receives best path from a non-client peer, it sends the route to all clients. When the route reflector receives a best path from a client peer it sends the route to all non-client and all client peers except the originator.

With optimal route reflection, the best path advertised to a client takes location ID into account, which means that if the tie-break for best path (or Add-Paths) comes down to next-hop IGP cost, the IGP costs will be calculated relative to the specified location. In the SR OS implementation, the IGP costs from arbitrary ORR locations are calculated using OSPF/OSPFv3, IS-IS, or BGP-LS information in the TE DB.

Default no cluster

Parameters *ip-address* — Specifies the route reflector cluster ID is expressed in dot decimal notation.

Values Any 32 bit number in dot decimal notation. (0.0.0.1 to 255.255.255.255)

orr-location *location-id* — Specifies the optimal route reflection location index for this set of route reflector clients.

Values 1 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

allow-local-fallback — Controls the behavior when there are no BGP routes to advertise to the RR clients that are reachable from the perspective of their ORR location. If this option is configured, the RR is allowed (in this circumstance only), to advertise the best reachable BGP path from its own topology location. If this option is not configured and this situation applies, then no route is advertised to the clients.

Platforms All

cluster

Syntax **cluster** *cluster-id* **orr-location** *location-id* [**allow-local-fallback**]]
cluster *cluster-id*
no cluster

Context **[Tree]** (config>router>bgp>group cluster)
[Tree] (config>router>bgp>group>neighbor cluster)

Full Context configure router bgp group cluster
configure router bgp group neighbor cluster

Description This command configures the cluster ID for a route reflector server ID and implicitly configures the associated BGP sessions as route reflector clients of the BGP instance. If an ORR location ID is specified with the cluster ID, the clients in that cluster receive routes optimal for that specific location; see *draft-ietf-idr-bgp-optimal-route-reflection* for more information.

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be non-clients.

When a route reflector receives best path from a non-client peer, it sends the route to all clients. When the route reflector receives a best path from a client peer it sends the route to all non-client and all client peers except the originator.

With optimal route reflection, the best path advertised to a client takes location ID into account, which means that if the tie-break for best path (or Add-Paths) comes down to next-hop IGP cost, the IGP costs will be calculated relative to the specified location. In the SR OS implementation, the IGP costs from arbitrary ORR locations are calculated using OSPF/OSPFv3, IS-IS, or BGP-LS information in the TE DB.

The **no** form of this command deletes the cluster ID and effectively disables route reflection for the group.

Default no cluster

Parameters *ip-address* — Specifies the route reflector cluster ID is expressed in dot decimal notation.

Values Any 32 bit number in dot decimal notation. (0.0.0.1 to 255.255.255.255)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

orr-location *location-id* — Specifies the optimal route reflection location index for this set of route reflector clients.

Values 1 to 255

allow-local-fallback — Controls the behavior when there are no BGP routes to advertise to the RR clients that are reachable from the perspective of their ORR location. If this option is configured, the RR is allowed (in this circumstance only), to advertise the best reachable BGP path from its own topology location. If this option is not configured and this situation applies, then no route is advertised to the clients.

Platforms All

7.140 cluster-id

cluster-id

Syntax **cluster-id** *ip-address/mask* [*ip-address/mask*]
cluster-id none
no cluster-id

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from cluster-id)

Full Context configure router policy-options policy-statement entry from cluster-id

Description This command enables BGP routes to be matched based on the IP addresses encoded in the CLUSTER_LIST attribute.

The first i*p-address/mask pair* is matched against the most recently added cluster ID. Each subsequent *ip-address/mask* pair is tested against the next most recent cluster ID.

For example, to match all routes reflected by the RR with cluster ID 1.1.1.1 and then any other RR before reaching the router where the policy is applied, use the command **cluster-id 0.0.0.0/0 1.1.1.1/32**.

Note: The command matches routes with two or more cluster IDs; the third and older cluster IDs are not evaluated and are automatically considered matching.

The **cluster-id none** form of this command only matches BGP routes without any CLUSTER_LIST attribute.

A non-BGP route does not match a policy entry if it contains the **cluster-id** command.

Default no cluster-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the 32-bit cluster ID in dotted decimal notation.

Values a.b.c.d

mask — Specifies a bit mask to apply to the *ip-address* parameter.

Values 0 to 32 (0 is only allowed if the *ip-address* is 0.0.0.0)

none — Specifies that only BGP routes without a CLUSTER_LIST attribute should be matched.

Platforms All

7.141 cmpv2

cmpv2

Syntax **cmpv2**

Context **[Tree]** (admin>certificate cmpv2)

Full Context admin certificate cmpv2

Description Commands in this context configure CMPv2 operations.

Platforms All

cmpv2

Syntax **cmpv2**

Context **[Tree]** (config>system>security>pki>ca-profile cmpv2)

Full Context configure system security pki ca-profile cmpv2

Description Commands in this context configure CMPv2 parameters.

Platforms All

cmpv2

Syntax [**no**] **cmpv2**

Context **[Tree]** (debug>certificate cmpv2)

Full Context debug certificate cmpv2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging of CMPv2 operations.

Platforms All

7.142 cn

cn

Syntax [**no**] **cn** *index* **type** *type* **value** *common-name-value*

Context **[Tree]** (config>system>security>pki>common-name-list cn)

Full Context configure system security pki common-name-list cn

Description This command creates a CN list entry in text or regexp format.

The **no** form of this command removes the specified entry.

Parameters *index* — Specifies the index number of the entry.

type — Specifies the type of the entry.

Values ip-address, domain-name

common-name-value — Specifies the IP address or domain name value, up to 255 characters maximum.

7.143 coa

coa

Syntax **coa** [**port** *udp-port*]
no coa

Context **[Tree]** (config>aaa>isa-radius-plcy>servers>server coa)

Full Context configure aaa isa-radius-policy servers server coa

Description This command configures Change of Authorization (CoA) messages.

Default no coa

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *udp-port* — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.144 coa-script-policy

coa-script-policy

Syntax **coa-script-policy** *policy-name*
no coa-script-policy

Context **[Tree]** (config>subscr-mgmt>auth-plcy coa-script-policy)

Full Context configure subscriber-mgmt authentication-policy coa-script-policy

Description This command configures the RADIUS script policy used to change the RADIUS attributes of the Change-of-Authorization messages.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the Python script policy to modify the Change-of-Authorization messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

coa-script-policy

Syntax **coa-script-policy** *policy-name*
no coa-script-policy

Context **[Tree]** (config>router>radius-server>server coa-script-policy)
[Tree] (config>service>vprn>radius-server>server coa-script-policy)

Full Context configure router radius-server server coa-script-policy
configure service vprn radius-server server coa-script-policy

Description This command specifies the RADIUS script policy to modify the Change-of-Authorization messages sent from this RADIUS server.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the name of radius-script-policy up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.145 code-type

code-type

Syntax **code-type** [**sonet** | **sdh**]
[**no**] **code-type**

Context **[Tree]** (config>port>ethernet>ssm code-type)

Full Context configure port ethernet ssm code-type

Description This command configures the encoding of synchronization status messages. For example, whether to use an SDH or SONET set of values. Configuring the network-type is only applicable to SyncE ports. It is not configurable on SONET/SDH ports. For the network-type, sdh refers to ITU-T G.781 Option I, while sonet refers to G.781 Option II (equivalent to Telcordia GR-253-CORE).

Default code-type sdh

Parameters **sdh** — Specifies the values used on a G.781 Option 1 compliant network.

sonet — Specifies the values used on a G.781 Option 2 compliant network.

Platforms All

7.146 coherent

coherent

Syntax **coherent**

Context **[Tree]** (config>port>dwdm coherent)

Full Context configure port dwdm coherent

Description This command configures the coherent optical module parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.147 cold-start-wait

cold-start-wait

Syntax **cold-start-wait** *seconds*
no cold-start-wait

Context **[Tree]** (config>log>app-route-notifications cold-start-wait)

Full Context configure log app-route-notifications cold-start-wait

Description The time delay that must pass before notifying specific CPM applications that a route is available after a cold reboot.

Default no cold-start-wait

Parameters *seconds* — Time delay in seconds.

Values 1 to 300

Platforms All

7.148 collect-aa-acct-stats

collect-aa-acct-stats

Syntax [**no**] **collect-aa-acct-stats**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm collect-aa-acct-stats)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm collect-aa-acct-stats)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt collect-aa-acct-stats
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt collect-aa-acct-stats

Description This command enables Application Assurance account statistics collection.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.149 collect-lmm-fc-stats

collect-lmm-fc-stats

Syntax **collect-lmm-fc-stats**

Context [Tree] (config>service>epipe>sap>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>ipipe>sap>eth-cfm collect-lmm-fc-stats)

Full Context configure service epipe sap eth-cfm collect-lmm-fc-stats
configure service epipe spoke-sdp eth-cfm collect-lmm-fc-stats
configure service ipipe sap eth-cfm collect-lmm-fc-stats

Description Commands in this context configure per-forwarding class (FC) LMM information collection.

This command is mutually exclusive with the **collect-lmm-stats** command when there is entity resource contention.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

collect-lmm-fc-stats

Syntax **collect-lmm-fc-stats**

Context [Tree] (config>service>vpls>mesh-sdp>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>vpls>sap>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm collect-lmm-fc-stats)

Full Context configure service vpls mesh-sdp eth-cfm collect-lmm-fc-stats
configure service vpls sap eth-cfm collect-lmm-fc-stats
configure service vpls spoke-sdp eth-cfm collect-lmm-fc-stats

Description Commands in this context configure per-forwarding class (FC) LMM information collection.

This command is mutually exclusive with the **collect-lmm-stats** command when there is entity resource contention.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

collect-lmm-fc-stats

Syntax **collect-lmm-fc-stats**

Context [Tree] (config>service>ies>if>sap>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm collect-lmm-fc-stats)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm collect-lmm-fc-stats)

Full Context configure service ies interface sap eth-cfm collect-lmm-fc-stats
configure service ies interface spoke-sdp eth-cfm collect-lmm-fc-stats
configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats

Description Commands in this context configure per-forwarding class (FC) LMM information collection.

This command is mutually exclusive with the **collect-lmm-stats** command when there is entity resource contention.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm collect-lmm-fc-stats
- configure service ies interface spoke-sdp eth-cfm collect-lmm-fc-stats

collect-lmm-fc-stats

Syntax **collect-lmm-fc-stats**

Context [Tree] (config>service>vprn>if>sap>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm collect-lmm-fc-stats)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm collect-lmm-fc-stats)

Full Context configure service vprn interface sap eth-cfm collect-lmm-fc-stats
configure service vprn interface spoke-sdp eth-cfm collect-lmm-fc-stats
configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats

Description Commands in this context configure per-forwarding class (FC) LMM information collection.

This command is mutually exclusive with the **collect-lmm-stats** command when there is entity resource contention.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm collect-lmm-fc-stats
- configure service vprn interface spoke-sdp eth-cfm collect-lmm-fc-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

collect-lmm-fc-stats

Syntax **collect-lmm-fc-stats**

Context **[Tree]** (config>router>if>eth-cfm>mep collect-lmm-fc-stats)

Full Context configure router interface eth-cfm mep collect-lmm-fc-stats

Description This command enables the collection of per-forwarding class LMM statistics.

The **collect-lmm-fc-stats** and **collect-lmm-stats** commands are mutually exclusive when there is entity resource contention.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.150 collect-lmm-stats

collect-lmm-stats

Syntax [**no**] **collect-lmm-stats**

Context **[Tree]** (config>lag>eth-cfm>mep collect-lmm-stats)
[Tree] (config>port>ethernet>eth-cfm>mep collect-lmm-stats)
[Tree] (config>router>if>eth-cfm>mep collect-lmm-stats)

Full Context configure lag eth-cfm mep collect-lmm-stats
configure port ethernet eth-cfm mep collect-lmm-stats
configure router interface eth-cfm mep collect-lmm-stats

Description This command enables the collection of statistics on the facility MEPs. This command is an object under the Facility MEP. This is at a different level of the hierarchy than collection of lmm statistics for service SAPs and MPLS SDP Bindings. The show mep command can be used to determine is the Facility MEP is collecting stats.

The **no** form of this command disables and deletes the counters for this SAP, Binding or facility.

Default no collect-lmm-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

collect-lmm-stats

Syntax [**no**] **collect-lmm-stats**

Context **[Tree]** (config>service>epipe>sap>eth-cfm collect-lmm-stats)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>epipe>spoke-sdp>eth-cfm collect-lmm-stats)
[Tree] (config>service>vpls>sap>eth-cfm collect-lmm-stats)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm collect-lmm-stats)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm collect-lmm-stats)
[Tree] (config>service>ipipe>sap>eth-cfm collect-lmm-stats)

Full Context
configure service epipe sap eth-cfm collect-lmm-stats
configure service epipe spoke-sdp eth-cfm collect-lmm-stats
configure service ipipe sap eth-cfm collect-lmm-stats
configure service vpls mesh-sdp eth-cfm collect-lmm-stats
configure service vpls sap eth-cfm collect-lmm-stats
configure service vpls spoke-sdp eth-cfm collect-lmm-stats

Description
This command enables the collection of statistics on the SAP or MPLS SDP binding on which the ETH- LMM test is configured. The collection of LMM statistics must be enabled if a MEP is launching or responding to ETH-LMM packets. If LMM statistics collection is not enabled, the counters in the LMM and LMR PDU do not represent accurate measurements and all measurements should be ignored. The **show sap-using eth-cfm collect-lmm-stats** command and the **show sdp-using eth-cfm collect-lmm-stats command** can be used to display entities that are collecting stats.

The **no** form of this command disables and deletes the counters for this SAP or MPLS SDP binding.

Default
no collect-lmm-stats

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

collect-lmm-stats

Syntax
[**no**] **collect-lmm-stats**

Context
[Tree] (config>service>ies>if>sap>eth-cfm collect-lmm-stats)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm collect-lmm-stats)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm collect-lmm-stats)

Full Context
configure service ies interface sap eth-cfm collect-lmm-stats
configure service ies interface spoke-sdp eth-cfm collect-lmm-stats
configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats

Description
This command enables the collection of statistics on the SAP or MPLS SDP binding on which the ETH- LMM test is configured. The collection of LMM statistics must be enabled if a MEP is launching or responding to ETH-LMM packets. If LMM statistics collection is not enabled, the counters in the LMM and LMR PDU do not represent accurate measurements and all measurements should be ignored. The **show sap-using eth-cfm collect-lmm-stats** command and the **show sdp-using eth-cfm collect-lmm-stats command** can be used to display which entities are collecting stats.

The **no** form of this command disables and deletes the counters for this SAP or MPLS SDP binding.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no collect-lmm-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm collect-lmm-stats
- configure service ies interface sap eth-cfm collect-lmm-stats

collect-lmm-stats

Syntax **collect-lmm-stats**
no collect-lmm-stats

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm collect-lmm-stats)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm collect-lmm-stats)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm collect-lmm-stats)

Full Context configure service vprn interface sap eth-cfm collect-lmm-stats
configure service vprn interface spoke-sdp eth-cfm collect-lmm-stats
configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-stats

Description This command enables the collection of statistics on the SAP or MPLS SDP binding on which the ETH- LMM test is configured. The collection of LMM statistics must be enabled if a MEP is launching or responding to ETH-LMM packets. If LMM statistics collection is not enabled, the counters in the LMM and LMR PDU do not represent accurate measurements and all measurements should be ignored. The **show>service>sap-using>eth-cfm>collect-lmm-stats** command and the **show>service>sdp-using>eth-cfm>collect-lmm-stats** command can be used to display which entities are collecting stats.

The **no** form of this command disables and deletes the counters for this SAP or MPLS SDP binding.

Default no collect-lmm-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-stats

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm collect-lmm-stats
- configure service vprn interface sap eth-cfm collect-lmm-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.151 collect-stats

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>subscr-mgmt>sub-prof collect-stats)

Full Context configure subscriber-mgmt sub-profile collect-stats

Description When enabled, the agent collects non-RADIUS accounting statistics.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default collect-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap collect-stats)
[Tree] (config>service>vprn>sub-if>grp-if>sap collect-stats)

Full Context configure service ies subscriber-interface group-interface sap collect-stats
configure service vprn subscriber-interface group-interface sap collect-stats

Description When enabled, the agent collects non-RADIUS accounting statistics on a subscriber profile.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM cards. However, the CPU does not obtain the results and write them to the billing file. If a subsequent **col**lect-stats command is issued then the counters written to the billing file include all the traffic.

Default collect-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>service>ies>if>sap collect-stats)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>sap collect-stats)
[Tree] (config>service>vpls>spoke-sdp collect-stats)
[Tree] (config>service>vpls>mesh-sdp collect-stats)

Full Context configure service ies interface sap collect-stats
configure service vpls mesh-sdp collect-stats
configure service vpls sap collect-stats
configure service vpls spoke-sdp collect-stats

Description This command enables accounting and statistical data collection for either the SAP or SDP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM cards. However, the CPU does not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default collect-stats

Platforms All

collect-stats

Syntax [**no**] **collect-stats**

Context [Tree] (config>card>fp>ingress>access>queue-group collect-stats)
[Tree] (config>card>fp>ingress>network>queue-group collect-stats)

Full Context configure card fp ingress access queue-group collect-stats
configure card fp ingress network queue-group collect-stats

Description This command enables the collection of accounting and statistical data for the queue group on the forwarding plane. When applying accounting policies, the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated, however, the CPU does not obtain the results and write them to the billing file. If the **collect-stats** command is issued again (enabled), then the counters written to the billing file will include the traffic collected while the **no collect-stats** command was in effect.

Default no collect-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

collect-stats

Syntax [**no**] **collect-stats**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context

[Tree] (config>port>ethernet>access>egr>qgrp collect-stats)
[Tree] (config>port>ethernet>access>ing>qgrp collect-stats)
[Tree] (config>port>ethernet>network>egr>qgrp collect-stats)
[Tree] (config>port>ethernet>network collect-stats)
[Tree] (config>port>ethernet collect-stats)
[Tree] (config>port>sonet-sdh>path>network collect-stats)
[Tree] (config>port>tdm>ds1>channel-group>network collect-stats)
[Tree] (config>port>tdm>ds3>network collect-stats)
[Tree] (config>port>tdm>e1>channel-group>network collect-stats)
[Tree] (config>port>tdm>e3>network collect-stats)

Full Context

configure port ethernet access egress queue-group collect-stats
configure port ethernet access ingress queue-group collect-stats
configure port ethernet collect-stats
configure port ethernet network collect-stats
configure port ethernet network egress queue-group collect-stats
configure port sonet-sdh path network collect-stats
configure port tdm ds1 channel-group network collect-stats
configure port tdm ds3 network collect-stats
configure port tdm e1 channel-group network collect-stats
configure port tdm e3 network collect-stats

Description

This command enables the collection of accounting and statistical data for the network interface. When applying accounting policies, the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated by the XCM/IOM cards, however, the CPU does not obtain the results and write them to the billing file. If the **collect-stats** command is issued again (enabled), then the counters written to the billing file will include the traffic collected while the **no collect-stats** command was in effect.

Default

no collect-stats

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path network collect-stats

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group network collect-stats
- configure port tdm e3 network collect-stats
- configure port tdm ds3 network collect-stats
- configure port tdm ds1 channel-group network collect-stats

All

- configure port ethernet network collect-stats
- configure port ethernet access ingress queue-group collect-stats
- configure port ethernet network egress queue-group collect-stats
- configure port ethernet access egress queue-group collect-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port ethernet collect-stats

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>service>apipe>sap collect-stats)
[Tree] (config>service>cpipe>sap collect-stats)
[Tree] (config>service>epipe>sap collect-stats)
[Tree] (config>service>epipe>spoke-sdp collect-stats)
[Tree] (config>service>fpipe>sap collect-stats)
[Tree] (config>service>ipipe>sap collect-stats)

Full Context configure service apipe sap collect-stats
configure service cpipe sap collect-stats
configure service epipe sap collect-stats
configure service epipe spoke-sdp collect-stats
configure service fpipe sap collect-stats
configure service ipipe sap collect-stats

Description This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default no collect-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap collect-stats
- configure service cpipe sap collect-stats

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap collect-stats

All

- configure service epipe spoke-sdp collect-stats
- configure service ipipe sap collect-stats
- configure service epipe sap collect-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>service>ies>if>spoke-sdp collect-stats)

Full Context configure service ies interface spoke-sdp collect-stats

Description This command enables statistics collection.

Platforms All

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>service>vprn>if>sap collect-stats)
[Tree] (config>service>vprn>if>spoke-sdp collect-stats)

Full Context configure service vprn interface sap collect-stats
configure service vprn interface spoke-sdp collect-stats

Description This command enables accounting and statistical data collection for either an interface SAP or interface SAP spoke SDP, or network port. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default no collect-stats

Platforms All

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>router>ldp>egr-stats collect-stats)

Full Context configure router ldp egr-stats collect-stats

Description This command enables accounting and statistical data collection. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **no collect-stats** command is issued the statistics are still accumulated by the forwarding engine. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default collect-stats

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>router>mpls>ingr-stats>lsp collect-stats)
[Tree] (config>router>mpls>ingr-stats>p2mp-template-lsp collect-stats)
[Tree] (config>router>mpls>ingr-stats>p2p-template-lsp collect-stats)
[Tree] (config>router>mpls>lsp>egr-stats collect-stats)
[Tree] (config>router>mpls>lsp>ingr-stats collect-stats)
[Tree] (config>router>mpls>lsp-template>egr-stats collect-stats)

Full Context configure router mpls ingress-statistics lsp collect-stats
configure router mpls ingress-statistics p2mp-template-lsp collect-stats
configure router mpls ingress-statistics p2p-template-lsp collect-stats
configure router mpls lsp egress-statistics collect-stats
configure router mpls lsp ingress-statistics collect-stats
configure router mpls lsp-template egress-statistics collect-stats

Description This command enables accounting and statistical data collection. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

The **config>router>mpls>ingr-stats>p2mp-template-lsp>collect-stats** command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

When the **no collect-stats** command is issued, the statistics are still accumulated by the forwarding engine. However, the CPU does not write the results to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic collected while the **no collect-stats** command was in effect.

Default collect-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router mpls lsp ingress-statistics collect-stats

All

- configure router mpls ingress-statistics p2mp-template-lsp collect-stats
- configure router mpls ingress-statistics p2p-template-lsp collect-stats
- configure router mpls ingress-statistics lsp collect-stats
- configure router mpls lsp-template egress-statistics collect-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router mpls lsp egress-statistics collect-stats

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>app-assure>group>statistics>aa-admit-deny collect-stats)
[Tree] (config>app-assure>group>statistics>aa-partition collect-stats)
[Tree] (config>app-assure>group>statistics>aa-sub collect-stats)
[Tree] (config>app-assure>group>statistics>aa-sub-study collect-stats)
[Tree] (config>app-assure>group>statistics>app-grp collect-stats)
[Tree] (config>app-assure>group>statistics>application collect-stats)
[Tree] (config>app-assure>group>statistics>protocol collect-stats)
[Tree] (config>isa>aa-grp>statistics collect-stats)

Full Context configure application-assurance group statistics aa-admit-deny collect-stats
configure application-assurance group statistics aa-partition collect-stats
configure application-assurance group statistics aa-sub collect-stats
configure application-assurance group statistics aa-sub-study collect-stats
configure application-assurance group statistics app-group collect-stats
configure application-assurance group statistics application collect-stats
configure application-assurance group statistics protocol collect-stats
configure isa aa-group statistics collect-stats

Description This command enables statistic collection within the applicable context.

Default no collect-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

collect-stats

Syntax [**no**] **collect-stats**

Context **[Tree]** (config>service>pw-template collect-stats)
[Tree] (config>service>sdp collect-stats)

Full Context configure service pw-template collect-stats
configure service sdp collect-stats

Description This command enables accounting and statistical data collection for either the SDP. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM or XCM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no collect-stats

Platforms All

7.152 collection-interval

collection-interval

Syntax **collection-interval** *minutes*
no collection-interval

Context **[Tree]** (config>log>acct-policy collection-interval)

Full Context configure log accounting-policy collection-interval

Description This command configures the accounting collection interval.

Parameters *minutes* — Specifies the interval between collections, in minutes.

Values 1 to 120 A range of 1 to 4 is only allowed when the record type is set to SAA.

Platforms All

7.153 collector

collector

Syntax **collector** *ip-address*[**:***port*] [**create**]
no collector *ip-address*[**:***port*]

Context **[Tree]** (config>app-assure>group>cflowd collector)

Full Context configure application-assurance group cflowd collector

Description This command defines a flow data collector for cflowd data. The IP address of the flow collector must be specified. The UDP port number is an optional parameter. If it is not set, the default of 2055 is used.

Parameters *ip-address* — Specifies the IP address of the flow data collector in dotted decimal notation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port — Specifies the UDP port of flow data collector.

Values 1 to 65535

Default 2055

create — Keyword used to create the flow data collector.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

collector

Syntax **collector router** *router-instance* **ip** *ip-address* [**create**]
no collector router *router-instance* **ip** *ip-address*

Context **[Tree]** (config>service>ipfix>export-policy collector)

Full Context configure service ipfix ipfix-export-policy collector

Description This command defines an external collector node that will collect IPFIX records sent by 7750 SR node. The IPFIX records will be streamed to the collector node using UDP transport. Traffic is originated from a random ephemeral UDP port to the destination port 4739. Up to two collector nodes can be defined for redundancy purposes.

UDP streams are stateless due to the significant volume of transactions. However they do contain 32bit sequence numbers such that packet loss can be identified.

Multiple IPFIX records are sent in a single UDP packet. UDP packet transmission is triggered when the packet size containing IPFIX records exceeds the configured MTU value or the internal timer which is set to 250ms, whichever occurs first.

Parameters **router** *router-instance* — Router instance from which the collector node is reachable.

Values
<router-name> | <service-id>
router-name: "Base"
service-id: 1 to 2147483647

ip ip-address — IPv4 address of the external collector node to which IPFIX records will be sent.

create — Keyword used to create the collector instance.

Platforms All

collector

Syntax **collector router** *router-name* **ip** *ip-address* [**create**]
collector service-name *service-name* **ip** *ip-address* [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no collector router *router-name* **ip** *ip-address*
no collector service-name *service-name* **ip** *ip-address*

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy collector)

Full Context configure service nat syslog syslog-export-policy collector

Description This command defines an external collector node that collects syslog records. The syslog records are streamed to the collector node using UDP transport. Traffic is originated from a random ephemeral UDP port to the destination port 514. Up to two collector nodes can be defined for redundancy purposes.

Stateless UDP streams are used as transport due to the significant volume of transactions. However, they do contain 32-bit sequence numbers so packet loss can be identified. The sequence numbers are generated per BB-ISA per collector, and within each stream they are monotonically increased by 1. Overlapping sequence numbers between BB-ISAs can be differentiated by the MDA ID field carried in the syslog message.

Multiple syslog records are sent in a single UDP packet. UDP packet transmission is triggered when the packet size containing syslog records exceeds the configured MTU value or the configurable timer, whichever occurs first.

The **no** form of the command removes the parameters from the configuration.

Parameters *router-name* — Specifies the router instances from which the collector node is reachable.

ip-address — Specifies the IPv4 address of the external collector node to which the syslog records are sent.

service-name — Specifies the service name from which the collector node is reachable.

create — Keyword used to create the collector instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

collector

Syntax **collector** *ip-address*[:*port*] [**version** *version*]
no collector *ip-address*[:*port*]

Context **[Tree]** (config>cflowd collector)

Full Context configure cflowd collector

Description This command defines a flow data collector for cflowd data. The IP address and version of the flow collector must be specified. The UDP port number is an optional parameter. If it is not set, the default of 2055 is used for all collector versions. To connect to an IPFIX (version 10) collector using the IPFIX default port, specify port 4739 when defining the collector. A maximum of eight collectors can be configured.

The **no** form of this command removes the flow collector definition from the config and stops the export of data to the collector. The collector needs to be shut down to be deleted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the address of a remote cflowd collector host to receive the exported cflowd data.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x-[interface]

port — Specifies the UDP port number on the remote cflowd collector host to receive the exported cflowd data.

Values 1 to 65535

Default 2055

version — Specifies the version of the flow data collector.

Values 5, 8, 9, 10

Default 5

Platforms All

collector

Syntax **collector** *collector-id* [**create**]
no collector *collector-id*

Context **[Tree]** (config>app-assure>group>cflowd>direct-export collector)

Full Context configure application-assurance group cflowd direct-export collector

Description This command configures the Cflowd direct export collector.

The system uses the collectors when the Cflowd admin state shuts down and then re-enabled (**no shutdown** state). The system re-assigns the collectors to the groups or AA-ISAs or when a Cflowd collector ID is created. The collector IDs are used when a new group is added later.

When a collector ID is removed, the groups (AA-ISAs) that are assigned to this collector are removed and assigned to another available collector. The affected ISAs reset their collector statistics as they change to the new collector.

In addition, a Cflowd collector assignment to a group or AA-ISA is done only in the following conditions:

- the admin state is in a **no shutdown** state for the AA group or the AA group Cflowd
- a collector is available under the AA group with at least one address in a **no shutdown** admin state

If an AA group or AA-ISA is assigned a collector, shutting down, or the group unassigns the group from the cflowd collector.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the collector ID from the configuration.

Parameters *collector-id* — Specifies the Cflowd direct export collector ID.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.154 color

color

Syntax **color** *color*
no color

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy color)

Full Context configure router segment-routing sr-policies static-policy color

Description This command associates a color value with a statically defined segment routing policy. This is a mandatory parameter and configuration command to enable the segment routing policy; if the color parameter value is not configured, the execution of the **no shutdown** command on the static segment routing policy fails.

The **no** form of this command removes the color association.

Default no color

Parameters *color* — Specifies the color ID.

Values 0 to 4294967295

Platforms All

color

Syntax **color** *color-id*
no color

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from color)

Full Context configure router policy-options policy-statement entry from color

Description This command configures an SR Policy color ID as a route policy match criterion.

This match criterion is only used in import policies.

The **no** form of this command removes the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *color-id* — Specifies the SR policy color ID.

Values 0 to 4294967295

Platforms All

7.155 combined-max-sessions

combined-max-sessions

Syntax **combined-max-sessions** *number-of-sessions*
no combined-max-sessions

Context **[Tree]** (config>system>security>cli-session-group combined-max-sessions)
[Tree] (config>system>security>profile combined-max-sessions)

Full Context configure system security cli-session-group combined-max-sessions
configure system security profile combined-max-sessions

Description This command is used to limit the number of combined SSH/TELNET based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.

The **no** form of this command disables the command and the profile/group limit is not applied to the number of combined sessions.

Default no combined-max-sessions

Parameters *number-of-sessions* — Specifies the maximum number of allowed combined SSH/TELNET based CLI sessions.

Values 0 to 50

Platforms All

7.156 command-accounting-during-load

command-accounting-during-load

Syntax [**no**] **command-accounting-during-load**

Context **[Tree]** (config>system>security>management-interface>md-cli command-accounting-during-load)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security management-interface md-cli command-accounting-during-load

Description This command controls command accounting performed on the contents of a file loaded using the MD-CLI **load** or **rollback** command.

When enabled, all commands in the loaded file are logged, which may decrease the system response time with large files.

When disabled, command accounting is not performed during a load or rollback operation, which may increase the system response time by reducing the number of command accounting messages, especially when remote AAA servers are used.

The **load** or **rollback** command itself is always logged.

The **no** form of this command disables command accounting during a load or rollback operation.

Default command-accounting-during-load

Platforms All

7.157 command-completion

command-completion

Syntax **command-completion**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment command-completion)

Full Context configure system management-interface cli md-cli environment command-completion

Description This command configures keystrokes to trigger command completion.

Platforms All

7.158 commit

commit

Syntax **commit**

Context **[Tree]** (config>app-assure>group>policy commit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group policy commit

Description This command commits changes made during the current editing session. None of the policy changes done will take effect until commit command is issued. If the changes can be successfully committed, no errors detected during the commit during cross-reference verification against exiting application assurance configuration, the editing session will also be closed.

The newly committed policy takes effect immediately for all new flows, existing flows will transition onto the new policy shortly after the commit.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

commit

Syntax **commit**

Context **[Tree]** (config>router>bfd commit)

Full Context configure router bfd commit

Description This command saves the changes made to a BFD template during an active session and makes the changes active.

Platforms All

commit

Syntax **commit**

Context **[Tree]** (config>router>route-next-hop-policy commit)

Full Context configure router route-next-hop-policy commit

Description This command saves the changes made to route next-hop templates during an active session.

Default commit

Platforms All

commit

Syntax **commit** [**confirmed** *timeout*] [**comment** *comment*]
commit no-checkpoint [**confirmed** *timeout*]

Context **[Tree]** (candidate commit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context candidate commit

Description This command applies the changes in the candidate configuration to the active running configuration. The candidate changes will take operational effect.

If a commit operation is successful then all of the candidate changes will take operational effect and the candidate is cleared. If there is an error in the processing of the commit, or a 'commit confirmed' is not confirmed and an auto-revert occurs, then the router will return to a configuration state with none of the candidate changes applied. The operator can then continue editing the candidate and try a commit later.

By default, the SR OS will automatically create a new rollback checkpoint after a commit operation. The rollback checkpoint will contain the new configuration changes made by the commit. An optional **no-checkpoint** keyword can be used to avoid the auto-creation of a rollback checkpoint after a commit.

A commit operation is blocked if a rollback revert is currently being processed.

Parameters **confirmed** — specifies that the commit operation (if successful) should be automatically reverted (undone) at the end of the timeout period unless the operator issues the confirm command before the timeout period expires. A rollback checkpoint is created after the commit operation (if successful) and will remain available whether the commit is auto-reverted or not. The contents of the candidate will remain visible (candidate view) and changes to the candidate are blocked until the timeout is completed or the **candidate confirm** command is executed. If the timeout expires and an auto-revert occurs, then the original candidate config will be available in edit-cfg mode.

Standard line-by-line non-transactional configuration commands (including via SNMP) are not blocked during the countdown period and any changes made to the configuration during the countdown period will be rolled back if the timeout expires. The confirmed option is useful when changes are being made that could impact management reachability to the router.

A rollback revert is blocked during the countdown period until the commit has been confirmed.

timeout — Specifies the auto-revert timeout period, in minutes.

Values 1 to 168

no-checkpoint — Specifies to avoid the automatic creation of a rollback checkpoint for a successful commit.

comment *comment* — Adds a comment up to 255 characters to the automatic rollback checkpoint.

commit

Syntax **commit**

Context **[Tree]** (config>system>sync-if-timing commit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system sync-if-timing commit

Description This command saves changes made to the system synchronous interface timing configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

commit

Syntax **commit**

Context **[Tree]** (config>router>policy-options commit)

Full Context configure router policy-options commit

Description This command is required to save changes made to a route policy.

Platforms All

commit

Syntax [**no**] **commit**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization commit)

Full Context configure system security profile netconf base-op-authorization commit

Description This command enables the NETCONF commit operation.

The **no** form of this command disables the operation.

Default no commit

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.159 common-name-list

common-name-list

Syntax **common-name-list** *name* [**create**]

Context **[Tree]** (config>system>security>pki common-name-list)

Full Context configure system security pki common-name-list

Description This command configures a list of common names (CNs) that will be used to authenticate X.509.3 certificates. If the CN field of the X.509.3 certificate matches any of the CNs in the list, then the certificate can be used.

Parameters *name* — Specifies the name of the CN list, up to 32 characters maximum.

Platforms All

7.160 community

community

Syntax **community** *community-name* [**hash** | **hash2** | **custom**] [**access-permissions**] [**version** *SNMP-version*] [**src-access-list** *list-name*]
no community *community-name* [**hash** | **hash2** | **custom**]

Context **[Tree]** (config>service>vprn>snmp community)

Full Context configure service vprn snmp community

Description This command sets the SNMP community name(s) to be used with the associated VPRN instance. These VPRN community names are used to associate SNMP v1/v2c requests with a particular vprn context and to return a reply that contains VPRN-specific data or limit SNMP access to data in a specific VPRN instance.

VPRN snmp communities configured with an access permission of 'r' are automatically associated with the default access group "snmp-vprn-ro" and the "vprn-view" view (read only). VPRN snmp communities configured with an access permission of 'rw' are automatically associated with the default access group "snmp-vprn" and the "vprn-view" view (read/write).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The community in an SNMP v1/v2 request determines the SNMP context (i.e., the vprn# for accessing SNMP tables) and not the VPRN of the incoming interface on which the request was received. When an SNMP request arrives on VPRN 5 interface “ringo” with a destination IP address equal to the “ringo” interface, but the community in the SNMP request is the community configured against VPRN 101, then the SNMP request will be processed using the VPRN 101 context. (the response will contain information about VPRN 101). It is recommended to avoid using a simple series of vprn snmp-community values that are similar to each other (for example, avoid my-vprncomm-1, my-vprn-comm-2, etc).

The **no** form of this command removes the SNMP community name from the given VPRN context.

Parameters *community-name* — Specifies the SNMP v1/v2c community name. This is a secret/ confidential key used to access SNMP and specify a context (base vs vprn1 vs vprn2).

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

version *SNMP-version* — Specifies the SNMP version.

Values v1, v2c, both

access-permissions — Specifies the access rights to MIB objects.

Values **r** — Grants only read access to MIB objects. Creates an association of the community-name with the **snmp-vprn-ro** access group.**rw** — Grants read and write access to MIB objects. Creates an association of the community-name with the **snmp-vprn** access group.

list-name — Configures the **community** to reference a specific **src-access-list** (created under **configure system security snmp**), which will be used to validate the source IP address of all received SNMP requests that use this **community**. Multiple **community** (vprn or base router) and **usm-community** instances can reference the same **src-access-list**.

Platforms All

community

Syntax **community** *comm-id* [*comm-id*]
no community [*comm-id* [*comm-id*]]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>static-route-entry community)

Full Context configure service vprn static-route-entry community

Description This command associates a list of up to 12 BGP communities (any mix of standard, extended, and large communities) with the static route. These communities can be matched in route policies and are automatically added to BGP routes that are created from the static route.

The communities specified at this level of the static route causes communities configured under the next-hop, black-hole, and indirect contexts of the static route to be ignored.

The **no** form of this command removes the association.

Default no community

Parameters *comm-id* — Specifies a BGP community value, up to 72 characters.

Values [*as-num:comm-val* | *well-known-comm* | *ext-comm* | *large-comm*]

where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **null** | **no-export** | **no-export-subconfed** | **no-advertise** | **llgr-stale** | **no-llgr** | **blackhole**
- *ext-comm* — the extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - color:co-bits:*color-value*

  where:
  - *target* — route target
  - *origin* — route origin
  - *ip-address* — a.b.c.d
  - *ext-comm-val* — 0 to 4294967295
  - *ext-asnum* — 0 to 4294967295
  - *val-in-mbps* — 0 to 16777215
  - *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
  - *value1* — 0000 to FFFF
  - *value2* — 0 to FFFFFFFFFFFF
  - *co-bits* — 00, 01, 10 or 11
  - *color-value* — 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *large-comm — asn-or-ex:val-or-ex:val-or-ex*

Platforms All

community

Syntax **community** *comm-id*
no community [*comm-id*]

Context **[Tree]** (config>service>vprn>static-route-entry>black-hole community)
[Tree] (config>service>vprn>static-route-entry>indirect community)
[Tree] (config>service>vprn>static-route-entry>next-hop community)

Full Context configure service vprn static-route-entry black-hole community
configure service vprn static-route-entry indirect community
configure service vprn static-route-entry next-hop community

Description This command associates one BGP community (standard, extended or large) with a next-hop of the static route. This community can be matched in route policies and automatically added to BGP routes that are created from the static route.

Any community specified in one of these contexts is overridden by any communities specified at the prefix level of the static route entry.

The **no** form of this command removes the association.

Default no community

Parameters *comm-id* — Specifies a BGP community value, up to 72 characters.

Values [*as-num:comm-val* | *well-known-comm* | *ext-comm* | *large-comm*]
where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **null** | **no-export** | **no-export-subconfed** | **no-advertise** | **llgr-stale** | **no-llgr** | **blackhole**
- *ext-comm* — the extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - color:co-bits:*color-value*

where:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *target* — route target
- *origin* — route origin
- *ip-address* — a.b.c.d
- *ext-comm-val* — 0 to 4294967295
- *ext-asnum* — 0 to 4294967295
- *val-in-mbps* — 0 to 16777215
- *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
- *value1* — 0000 to FFFF
- *value2* — 0 to FFFFFFFFFFFF
- *co-bits* — 00, 01, 10 or 11
- *color-value* — 0 to 4294967295

• *large-comm — asn-or-ex:val-or-ex:val-or-ex*

Platforms All

community

Syntax **community** *comm-id*
no community [*comm-id*]

Context **[Tree]** (config>service>vprn>static-route-entry>ip-sec-tunnel community)

Full Context configure service vprn static-route-entry ip-sec-tunnel community

Description This configuration option associates a BGP community with the static route. The community can be matched in route policies and is automatically added to BGP routes exported from the static route.

The **no** form of this command removes the community association.

Default no community

Parameters *comm-id* — Specifies community IDs, up to 72 characters.

Values [*2 byte asnumber:comm-val* | *well-known-comm*]
where:

- *2 byte as-number* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **no-export** | **no-export-subconfed** | **no-advertise**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

community

Syntax **community** *community-name*
no community

Context **[Tree]** (config>router>ldp>session-params>peer community)
[Tree] (config>router>ldp>targeted-session>peer-template community)

Full Context configure router ldp session-parameters peer community
configure router ldp targeted-session peer-template community

Description This command configures a community name associated with a targeted session to a specified peer. The community is a local configuration for a targeted session. FECs received over a session of a given community are taken to belong to that community, and are redistributed over sessions of the same community.

The SR OS router uses the following rules for community:

- If both the session parameters for a specified peer and targeted peer template that is applied to session have the default configuration then no community applies.
- If the session parameters for a peer have the default configuration, but targeted session peer template has an explicit configuration for community, then the targeted peer template configuration will be used.
- If the session parameters have an explicit configuration for community, and the targeted session peer template has the default configuration, then the session parameter configuration applies.
- If both session parameters and targeted peer template have an explicit configuration for community, then the session parameter configuration is used.

The **no** form of this command removes the community from the session to the peer. FEC subsequently received over the session are treated as having no community.

Default no community

Parameters *community-name* — Specifies the string defining the LDP community assigned to the session. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string.

Platforms All

community

Syntax **community** *comm-id*
no community [*comm-id*]

Context **[Tree]** (config>router>static-route-entry>black-hole community)
[Tree] (config>router>static-route-entry>indirect community)
[Tree] (config>router>static-route-entry>next-hop community)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router static-route-entry black-hole community
configure router static-route-entry indirect community
configure router static-route-entry next-hop community

Description This command associates one BGP community (standard, extended or large) with a next-hop of the static route. This community can be matched in route policies and automatically added to BGP routes that are created from the static route.

Any community specified in one of these contexts is overridden by any communities specified at the prefix level of the static route entry.

The **no** form of this command removes the association.

Default no community

Parameters *comm-id* — Specifies a BGP community value, up to 72 characters.

Values [*as-num:comm-val* | *well-known-comm* | *ext-comm* | *large-comm*]

where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **null** | **no-export** | **no-export-subconfed** | **no-advertise** | **llgr-stale** | **no-llgr** | **blackhole**
- *ext-comm* — the extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - color:co-bits:*color-value*

  where:
  - *target* — route target
  - *origin* — route origin
  - *ip-address* — a.b.c.d
  - *ext-comm-val* — 0 to 4294967295
  - *ext-asnum* — 0 to 4294967295
  - *val-in-mbps* — 0 to 16777215
  - *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
  - *value1* — 0000 to FFFF
  - *value2* — 0 to FFFFFFFFFFFF
  - *co-bits* — 00, 01, 10 or 11
  - *color-value* — 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *large-comm — asn-or-ex:val-or-ex:val-or-ex*

Platforms All

community

Syntax **community** *comm-id* [*comm-id*]
no community [*comm-id* [*comm-id*]]

Context **[Tree]** (config>router>static-route-entry community)

Full Context configure router static-route-entry community

Description This command associates a list of up to 12 BGP communities (any mix of standard, extended, and large communities) with the static route. These communities can be matched in route policies and are automatically added to BGP routes that are created from the static route.

The communities specified at this level of the static route causes communities configured under the next-hop, black-hole and indirect contexts of the static route to be ignored.

The **no** form of this command removes the association.

Default no community

Parameters *comm-id* — Specifies a BGP community value, up to 72 characters.

Values [*as-num:comm-val* | *well-known-comm* | *ext-comm* | *large-comm*]
where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *well-known-comm* — **null** | **no-export** | **no-export-subconfed** | **no-advertise** | **llgr-stale** | **no-llgr** | **blackhole**
- *ext-comm* — the extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - color:co-bits:*color-value*

  where:
  - *target* — route target
  - *origin* — route origin
  - *ip-address* — a.b.c.d
  - *ext-comm-val* — 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *ext-asnum* — 0 to 4294967295
- *val-in-mbps* — 0 to 16777215
- *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
- *value1* — 0000 to FFFF
- *value2* — 0 to FFFFFFFFFFFF
- *co-bits* — 00, 01, 10 or 11
- *color-value* — 0 to 4294967295

• *large-comm — asn-or-ex:val-or-ex:val-or-ex*

Platforms All

community

Syntax **community** *community-string* [**hash** | **hash2** | **custom**] *access-permissions* [**version** *SNMP-version*] [**src-access-list** *list-name*]
no community *community-string* [**hash** | **hash2** | **custom**]

Context **[Tree]** (config>system>security>snmp community)

Full Context configure system security snmp community

Description This command creates SNMP community strings for SNMPv1 and SNMPv2c access. This command is used in combination with the predefined access groups and views. To create custom access groups and views and associate them with SNMPv1 or SNMPv2c access use the **usm-community** command.

When configured, community implies a security model for SNMPv1 and SNMPv2c only.

For SNMPv3 security, the **access group** command must be configured.

The **no** form of the command removes the specified community string.

Parameters *community-string* — Configures the SNMPv1 and/or SNMPv2c community string.

Values community-string — Specifies the community string. Allowed values are any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

hash-key — Up to 33 characters

hash2-key — Up to 96 characters

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

access-permissions — Configures the access permissions for objects in the MIB.

r — Grants only read access to objects in the MIB, except security objects, using the internal "snmp-ro" access group and the "no-security" snmp view.

rw — Grants read and write access to all objects in the MIB, using the internal "snmp-rw" access group and the "no-security" snmp view.

rwa — Grants read and write access to all objects in the MIB, including security, using the internal snmp-rwa access group and the iso snmp view.

mgmt — Assigns a unique SNMP community string for SNMP access via the management router instance. This community uses the internal snmp-mgmt access group and the mgmt snmp view.

vpls-mgmt — Assigns a unique SNMP community string for SNMP access via the vpls-management router instance. This community uses the internal snmp-vpls-mgmt access group and mgmt-view snmp view.

version {**v1** | **v2c** | **both**} — Configures the scope of the community string to be for SNMPv1, SNMPv2c, or both SNMPv1 and SNMPv2c access.

Default both

list-name — Configures the **community** to reference a specific **src-access-list**, which will be used to validate the source IP address of all received SNMP requests that use this community. Multiple community, usm-community, or VPRN SNMP community instances can reference the same src-access-list.

Platforms All

community

Syntax [**no**] **community** *name*

Context **[Tree]** (config>router>policy-options community)

Full Context configure router policy-options community

Description This command creates a route policy community list or expression to use in route policy entries. A community list is an unordered set of community values (members). In general a route matches a community list if it has any of the member values. A community expression is a set of community values that are arranged in a logical expression using operators such as AND, OR, and NOT. A route matches a community expression if it satisfies the logic of the expression.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For additional information, see the **expression** and **members** commands in the **config**>**router**>**policy-options**>**community** context.

The **no** form of this command deletes the community list or the provided community ID.

Default no community

Parameters *name* — Specifies the community list name. Allowed values are any string up to 64 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

Platforms All

community

Syntax **community add** *name* [*name*]
community remove *name* [*name*]
community replace *name* [*name*]
no community

Context **[Tree]** (config>router>policy-options>policy-statement>default-action community)
[Tree] (config>router>policy-options>policy-statement>entry>action community)

Full Context configure router policy-options policy-statement default-action community
configure router policy-options policy-statement entry action community

Description This command adds or removes a BGP community list to or from routes matching the route policy statement entry.

If no community list is specified, the community path attribute is not changed.

The community list changes the community path attribute according to the **add** and **remove** keywords.

The **no** form of this command disables the action to edit the community path attribute for the route policy entry.

Default no community

Parameters *name* — Specifies up to 28 names.

add — The specified community list is added to any existing list of communities.

remove — The specified community list is removed from the existing list of communities.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

replace — The specified community list replaces any existing community attribute. name — The community list name. Allowed values are any string up to 64 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end"," @variable@end", or "start@variable@".

Platforms All

community

Syntax **community** *comm-name*
community expression *expression*
no community

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from community)

Full Context configure router policy-options policy-statement entry from community

Description This command adds or removes a BGP community list to or from routes matching the route policy statement entry.

If no community list is specified, the community path attribute is not changed.

The community list changes the community path attribute according to the **add** and **remove** keywords.

The **no** form of this command disables the action to edit the community path attribute for the route policy entry.

Default no community

Parameters *comm-name* — Specifies up to 28 names.

expression — Applies parameters to routes matching the entry.

Values expression is one of the following up to 900 characters:
<expression> {AND| OR} <expression>
[NOT] (<expression>)
[NOT] "["<comm-name>"]

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.161 community-count

community-count

Syntax **community-count** *count* [**equal** | **or-higher** | **or-lower**] [**standard** | **extended** | **large**]
no community-count

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from community-count)

Full Context configure router policy-options policy-statement entry from community-count

Description This command matches BGP routes based on community length (that is, the number of community members in the COMMUNITY, EXTENDED_COMMUNITY, or LARGE_COMMUNITY the attributes).

If no comparison qualifiers are present (**equal**, **or-higher**, **or-lower**), then **equal** is the implied default.

Without the optional **standard**, **extended**, or **large** keyword, the community length applies to the total number of communities, of all types. If some keywords are present, then only the types specified are counted against the limit.

A non-BGP route does not match a policy entry if it contains the **community-count** command.

Default no community-count

Parameters *count* — Specifies the number of community members.

Values 0 to 1024, or a parameter, up to 32 characters, name delimited by a starting and ending at-sign (@) character

equal — Specifies that matched routes should have the same number of AS path elements as the value specified.

or-higher — Specifies that matched routes should have the same or a greater number of community members as the value specified.

or-lower — Specifies that matched routes should have the same or a lower number of community members as the value specified.

standard — Specifies that only communities in the COMMUNITY attribute should be counted.

extended — Specifies that only communities in the EXTENDED_COMMUNITY attribute should be counted.

large — Specifies that only communities in the LARGE_COMMUNITY attribute should be counted.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.162 compare

compare

Syntax **compare** *checkpoint1* **to** *checkpoint2*

Context **[Tree]** (admin compare)

Full Context admin compare

Description This command displays the differences between rollback checkpoints and the active operational configuration, with source1 as the base/first file to which source2 is compared.

A compare operation does not check authorization of each line of output. Permission to execute the compare operation from the admin branch of CLI (authorization for the **admin rollback compare** or **admin compare** command itself) should only be given to users who are allowed to view the entire configuration, similar to permissions for **admin display-config**.

Default The defaults for source1 and source2 are context aware and differ based on the branch in which the command is executed. In general, the default for source1 matches the context from which the command is issued.

- In the admin node: No defaults. source1 and source2 must be specified.
- In the admin>rollback node:
  source1 default = active-cfg, source2 default = latest-rb
  compare: equivalent to “compare active-cfg to latest-rb”
  compare to source2: equivalent to “compare active-cfg to source2”
- In a config>*xx* node:
  compare to source2: equivalent to “compare active-cfg to source2”

Parameters *checkpoint1, checkpoint2* — Specifies comparison information.

Values **active-cfg** — The current operational configuration that is active in the node.

latest-rb — The most recent rollback checkpoint (the checkpoint file at the configured rollback-location with “*.rb” as the suffix).

rescue — The rescue configuration (at the configured rescue-location).

checkpoint-id — An ID indicating a specific rollback checkpoint. A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback-location) with “*.rb.1” as the suffix, 2 for file “*.rb.2”, and so on.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

compare

Syntax **compare** [**to** *checkpoint2*]
compare *checkpoint1* **to** *checkpoint2*

Context **[Tree]** (admin>rollback compare)

Full Context admin rollback compare

Description This command displays the differences between rollback checkpoints and the active operational configuration, with source1 as the base/first file to which source2 is compared.

A compare operation does not check authorization of each line of output. Permission to execute the compare operation from the admin branch of CLI (authorization for the **admin rollback compare** or **admin compare** command itself) should only be given to users who are allowed to view the entire configuration, similar to permissions for **admin display-config**.

Default The defaults for source1 and source2 are context aware and differ based on the branch in which the command is executed. In general, the default for source1 matches the context from which the command is issued.

- In the admin node: No defaults. source1 and source2 must be specified.
- In the admin>rollback node:
  source1 default = active-cfg, source2 default = latest-rb
  compare: equivalent to “compare active-cfg to latest-rb”
  compare to source2: equivalent to “compare active-cfg to source2”
- In a config>*xx* node:
  compare to source2: equivalent to “compare active-cfg to source2”

Parameters *checkpoint1, checkpoint2* — Specifies comparison information.

Values **active-cfg** — The current operational configuration that is active in the node.

latest-rb — The most recent rollback checkpoint (the checkpoint file at the configured rollback-location with “*.rb” as the suffix).

rescue — The rescue configuration (at the configured rescue-location).

checkpoint-id — An ID indicating a specific rollback checkpoint. A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback-location) with “*.rb.1” as the suffix, 2 for file “*.rb.2”, and so on.

Platforms All

compare

Syntax **compare** [**to** *checkpoint2*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

compare *checkpoint1* **to** *checkpoint2*

Context **[Tree]** (global compare)

Full Context global compare

Description This command can be used in any branch under configure, but not with configure itself. The command syntax, parameter names, and default values are context aware and will differ based on the branch in which the command is executed.

This command displays the differences between rollback checkpoints and the active operational configuration, with source1 as the base/first file to which source2 is compared. This command displays the comparison for the configuration context where it is entered and all branches below that context level.

A compare operation does not check authorization of each line of output. Permission to execute the compare operation from the admin branch of CLI (authorization for the **admin rollback compare** or **admin compare** command itself) should only be given to users who are allowed to view the entire configuration, similar to permissions for **admin display-config**.

Parameters *checkpoint1, checkpoint2* — Specifies comparison information.

Values **active-cfg** — The current operational configuration that is active in the node.

latest-rb — The most recent rollback checkpoint (the checkpoint file at the configured rollback-location with "*.rb" as the suffix).

rescue — The rescue configuration (at the configured rescue-location).

checkpoint-id — An ID indicating a specific rollback checkpoint. A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback-location) with "*.rb.1" as the suffix, 2 for file "*.rb.2", and so on.

7.163 compare-origin-validation-state

compare-origin-validation-state

Syntax [**no**] **compare-origin-validation-state**

Context **[Tree]** (config>service>vprn>bgp>best-path-selection compare-origin-validation-state)

Full Context configure service vprn bgp best-path-selection compare-origin-validation-state

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the comparison of origin validation states during the BGP decision process. When this command is configured, a new step is inserted in the BGP decision process after the removal of invalid routes and before the comparison of Local Preference. This step compares the origin validation state so a BGP route with a “Valid” state is preferred over a BGP route with a “Not-Found” state. A BGP route with a “Not-Found” state is preferred over a BGP route with an “Invalid” state assuming that these routes are considered “usable”.

This comparison only applies to BGP routes learned from VPRN BGP peers. It does not apply to any comparison involving BGP-VPN routes that have been imported into the VPRN.

The **no** form of this command causes the new step to be skipped during the BGP decision process.

Default no compare-origin-validation-state

Platforms All

compare-origin-validation-state

Syntax [**no**] **compare-origin-validation-state**

Context **[Tree]** (config>router>bgp>best-path-selection compare-origin-validation-state)

Full Context configure router bgp best-path-selection compare-origin-validation-state

Description When this command is configured, a new step is inserted in the BGP decision process after removal of invalid routes and before the comparison of Local Preference. The new step compares the RPKI origin validation state so that a BGP route with a ‘Valid’ state is preferred over a BGP route with a ‘Not-Found’ state, and a BGP route with a ‘Not-Found’ state is preferred over a BGP route with an ‘Invalid’ state assuming that these routes are considered ‘usable’.

The new step is skipped when **no compare-origin-validation-state** is configured.

Default no compare-origin-validation-state

Platforms All

7.164 compatibility

compatibility

Syntax **compatibility** *mode*

Context **[Tree]** (config>port>dwdm>coherent compatibility)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port dwdm coherent compatibility

Description This command configures the optical mode and rate of operation.

Parameters *mode* — Specifies the optical mode.

Values
- **long-haul** - The port operates in the native long-haul mode.
- **long-haul-non-diff** - The port operates in the native long-haul mode using non-differential encoding.
- **metro** - The port operates in the native metro regional mode.
- **access** - The port operates in the native access mode (80km reach).
- **interop** - The port operates in the third party interop mode.
- **interop2**-The port operates in the third party interop mode with alternate differential encoding.
- **interop3**-The port operates in the CFP2-DCO Rev A0 Staircase FEC interop mode.

Default long-haul

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.165 compatible-rfc1583

compatible-rfc1583

Syntax [**no**] **compatible-rfc1583**

Context **[Tree]** (config>service>vprn>ospf compatible-rfc1583)

Full Context configure service vprn ospf compatible-rfc1583

Description This command enables OSPF summary and external route calculations in compliance with RFC 1583 and earlier RFCs.

RFC 1583 and earlier RFCs use a different method to calculate summary and external route costs. To avoid routing loops, all routers in an OSPF domain should perform the same calculation method.

Although it would be favorable to require all routers to run a more current compliance level, this command allows the router to use obsolete methods of calculation.

This command is not supported in OSPF3.

The **no** form of this command enables the post-RFC1583 method of summary and external route calculation.

Default compatible-rfc1583 — RFC 1583 compliance is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

compatible-rfc1583

Syntax [**no**] **compatible-rfc1583**

Context **[Tree]** (config>router>ospf compatible-rfc1583)

Full Context configure router ospf compatible-rfc1583

Description This command enables OSPF summary and external route calculations in compliance with RFC1583 and earlier RFCs.

RFC1583 and earlier RFCs use a different method to calculate summary and external route costs. To avoid routing loops, all routers in an OSPF domain should perform the same calculation method.

Although it would be favorable to require all routers to run a more current compliance level, this command allows the router to use obsolete methods of calculation.

The **no** form of this command enables the post-RFC1583 method of summary and external route calculation.

Default compatible-rfc1583

Platforms All

7.166 compatible-version

compatible-version

Syntax **compatible-version** *version*
no compatible-version

Context **[Tree]** (config>eth-ring compatible-version)

Full Context configure eth-ring compatible-version

Description This command configures eth-ring compatibility version for the G.8032 state machine and messages. The default is version 2 and all router switches use this version. If there is a need to interwork with third party devices that only support version 1 this can be set to version 1.

The **no** form of this command set the compatibility version to 2.

Default compatible-version 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *version* — Specifies the version of the G.8032 state machine.

Values 1, 2

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.167 complexity-rules

complexity-rules

Syntax **complexity-rules**

Context **[Tree]** (config>system>security>password complexity-rules)

Full Context configure system security password complexity-rules

Description This command defines a list of rules for configurable password options.

Note: This command applies to local users.

Platforms All

7.168 comprehensive

comprehensive

Syntax **comprehensive**

Context **[Tree]** (config>app-assure>group>cflowd comprehensive)

Full Context configure application-assurance group cflowd comprehensive

Description Commands in this context configure cflowd comprehensive statistics output parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.169 compress

compress

Syntax **compress** {**acfc** [**pfc**] | **pfc** [**acfc**]}
no compress

Context **[Tree]** (config>port>tdm>ds1>channel-group>ppp compress)
[Tree] (config>port>tdm>e1>channel-group>ppp compress)

Full Context configure port tdm ds1 channel-group ppp compress
configure port tdm e1 channel-group ppp compress

Description This command enables and disables Protocol Field Compression (PFC) per RFC 1661, *The Point-to-Point Protocol (PPP),* Section 6.5 and Address and Control Field Compression (ACFC) as per Section 6.6.

This command is only supported on DS-1 and E-1 channel groups on ASAP MDAs.

The **no** form of this command disables the header compression.

Default no compress

Parameters **acfc** — Specifies address and control field compression.

pfc — Specifies protocol field compression.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

7.170 conditional-expression

conditional-expression

Syntax **conditional-expression**

Context **[Tree]** (config>router>policy-options>policy-statement>entry conditional-expression)

Full Context configure router policy-options policy-statement entry conditional-expression

Description This command creates the context to configure a route existence expression.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.171 confederation

confederation

Syntax **confederation** *confed-as-num* [**members** *as-number* [*as-number*]]
no confederation *confed-as-num* **members** *as-number* [*as-number*]
no confederation

Context **[Tree]** (config>service>vprn confederation)

Full Context configure service vprn confederation

Description This command configures the VPRN BGP instance to participate in a BGP confederation. BGP confederations can be used to reduce the number of IBGP sessions required within an AS.

When a VPRN BGP instance is part of a confederation, it can form confederation-EBGP sessions with CE router peers in a different sub-autonomous systems of the same confederation as well as regular EBGP sessions with CE router peers outside the confederation. A VPRN BGP instance that is part of a confederation cannot import or export its routes to the base router instance (as VPN-IP routes).

The **no** form of this command deletes the specified member AS from the confederation. When members are not specified in the no statement, the entire list is removed and confederations is disabled. When the last member of the list is removed, confederations is disabled.

Default no confederation

Parameters *confed-as-num* — The confederation AS number defined as a decimal value.

Values 1 to 4294967295

members *as-number* — The AS number(s) that are members of the confederation, each expressed as a decimal integer. Configure up to 15 members per confed-as-num.

Values 1 to 4294967295

Platforms All

confederation

Syntax **confederation** *confed-as-num* [**members** *as-number* [*as-number*]]
no confederation *confed-as-num* **members** *as-number* [*as-number*]
no confederation

Context **[Tree]** (config>router confederation)

Full Context configure router confederation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates confederation autonomous systems within an AS.

This technique is used to reduce the number of IBGP sessions required within an AS. Route reflection is another technique that is commonly deployed to reduce the number of IBGP sessions.

The **no** form of this command deletes the specified member AS from the confederation.

When no members are specified in the **no** statement, the entire list is removed and **confederation** is disabled.

When the last member of the list is removed, **confederation** is disabled.

Default no confederation - no confederations are defined.

Parameters *confed-as-num* — Specifies the confederation AS number expressed as a decimal integer.

Values 1 to 65535

as-number — Specifies the AS number of members that are part of the confederation, expressed as a decimal integer. Up to 15 members per *confed-as-num* can be configured.

Values 1 to 65535

Platforms All

7.172 confidence

confidence

Syntax **confidence eq** *equal-value*
confidence gte *greater-than-or-equal-value*
confidence lt *less-than-value*

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match>flow-attribute confidence)

Full Context configure application-assurance group policy app-qos-policy entry match flow-attribute confidence

Description This command configures the confidence level of the flow attribute for use as match criteria.

Parameters **eq** *equal-value* — Specifies that a successful match occurs when the flow attribute confidence level is equal to the specified value.

Values 0 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gte *greater-than-or-equal-value* — Specifies that a successful match occurs when the flow attribute confidence level is greater than or equal to the specified value.

Values 0 to 100

lt *less-than-value* — Specifies that a successful match occurs when the flow attribute confidence level is less than the specified value.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.173 config-backup

config-backup

Syntax **config-backup** *count*
no config-backup

Context **[Tree]** (config>system config-backup)

Full Context configure system config-backup

Description This command configures the maximum number of backup versions maintained for configuration files and BOF.

For example, assume the **config-backup** *count* is set to 5 and the configuration file is called *xyz.cfg.* When a **save** command is executed, the file *xyz.cfg* is saved with a 1 extension. Each subsequent **config-backup** command increments the numeric extension until the maximum count is reached.

xyz.cfg xyz.cfg.1 xyz.cfg.2 xyz.cfg.3 xyz.cfg.4 xyz.cfg.5 xyz.ndx

Each persistent index file is updated at the same time as the associated configuration file. When the index file is updated, then the save is performed to *xyz.cfg* and the index file is created as *xyz.ndx*. Synchronization between the active and standby CPM is performed for all configurations and their associated persistent index files.

The **no** form of the command returns the configuration to the default value.

Default config-backup 5

Parameters *count* — Specifies the maximum number of backup revisions.

Values 1 to 200

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.174 configuration-mode

configuration-mode

Syntax **configuration-mode** {**classic** | **mixed** | **model-driven**}

Context **[Tree]** (config>system>management-interface configuration-mode)

Full Context configure system management-interface configuration-mode

Description This command controls which management interfaces are used for editing and changing the configuration of the router.

Default configuration-mode classic

Parameters **classic** — Enables editing of router configuration via classic CLI and SNMP management interfaces, but not using model-driven interfaces.

model-driven — Enables editing of router configuration via model-driven management interfaces (NETCONF with 'Nokia' YANG models, MD-CLI or gRPC), but not using classic interfaces.

mixed — Enables editing of router configuration using a mix of classic and/or model-driven management interfaces (with some restrictions and limitations).

Platforms All

7.175 configure

configure

Syntax **configure**

Context **[Tree]** (configure configure)

Full Context configure

Description Commands in this context edit the system configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.176 confirm

confirm

Syntax **confirm**

Context **[Tree]** (candidate confirm)

Full Context candidate confirm

Description This command is used to stop an automatic reversion to the previous configuration after the **candidate commit confirmed** command was used. If the **confirm** command is not executed before the commit confirmed timeout period expires then the previous commit changes will be undone and the previous candidate configuration will be available for editing and a subsequent commit.

During the countdown the contents of the candidate will remain visible (candidate view) and changes to the candidate are blocked until the timeout is completed or the candidate confirm command is executed. Executing the **confirm** command clears the contents of the candidate and allows editing of the candidate.

7.177 cong-priority-threshold

cong-priority-threshold

Syntax **cong-priority-threshold** *preference-level*
no cong-priority-threshold

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle cong-priority-threshold)

Full Context configure mcast-management multicast-info-policy bundle cong-priority-threshold

Description This command defines the preference level threshold where records change from low congestion priority to high congestion priority. Congestion priority is used by the ingress multicast path queues to map packets entering the queue to either the low drop-tail or the MBS drop-tail threshold. If congestion occurs on the queue, the queue depth increases. As the queue depth increases beyond the low drop-tail, packets with low priority congestion priority are discarded. This leaves room in the queue for packets with high congestion priority until the queue reaches the MBS threshold.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default congestion priority threshold is 4. This means that multicast channels with a preference level of 0 to 3 are treated as having low congestion priority and channels with preference level of 4 to 7 are treated as having a high congestion priority. The **cong-priority-threshold** command can be used to change the default threshold. Any multicast channel with a preference equal to or higher than the configured threshold is treated with high congestion priority.

The **cong-priority-threshold** value is also used by the multicast CAC manager to derive the class of a channel matched by the multicast information policy. Channels with a preference less than the configured threshold are treated as low class and channels with a preference equal to or greater than the threshold is treated as high class.

Changing the **cong-priority-threshold** value causes all channels congestion priority to be reevaluated. Both the ingress multicast path managers and multicast CAC managers must be updated.

The **no** form of this command restores the default congestion priority preference threshold value.

Default cong-priority-threshold 4

Parameters *preference-level* — Specifies the **cong-priority-threshold** where records change from low congestion priority to high congestion priority.

Values 0 to 7

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

7.178 congestion-override

congestion-override

Syntax **congestion-override**

Context **[Tree]** (config>app-assure>group>policer congestion-override)

Full Context configure application-assurance group policer congestion-override

Description Commands in this context configure per subscriber congestion bandwidth policer override rates.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.179 congestion-override-stage2

congestion-override-stage2

Syntax **congestion-override-stage2**

Context **[Tree]** (config>app-assure>group>policer congestion-override-stage2)

Full Context configure application-assurance group policer congestion-override-stage2

Description Commands in this context configure per-subscriber stage 2 congestion bandwidth policer override rates.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.180 congestion-threshold

congestion-threshold

Syntax **congestion-threshold** *percent*
no congestion-threshold

Context **[Tree]** (config>qos>hw-agg-shap-sched-plcy congestion-threshold)

Full Context configure qos hw-agg-shaper-scheduler-policy congestion-threshold

Description This command configures the congestion threshold for the hardware aggregate shaper scheduler policy, which, if exceeded, triggers the hardware aggregate scheduler algorithm.

Default congestion-threshold 90

Parameters *percent* — Specifies the congestion threshold as a percentage of the scheduler rate.

Values 0 to 100

Platforms 7750 SR-1, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.181 connect-retry

connect-retry

Syntax **connect-retry** *seconds*
no connect-retry

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy connect-retry)

Full Context configure subscriber-mgmt bgp-peering-policy connect-retry

Description This command configures the BGP connect retry timer value in seconds.

When this timer expires, BGP tries to reconnect to the configured peer.

The **no** form of this command used at the global level reverts to the default value.

Default connect-retry 120

Parameters *seconds* — The BGP Connect Retry timer value in seconds, expressed as a decimal integer.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

connect-retry

Syntax **connect-retry** *seconds*
no connect-retry

Context **[Tree]** (config>service>vprn>bgp connect-retry)
[Tree] (config>service>vprn>bgp>group connect-retry)
[Tree] (config>service>vprn>bgp>group>neighbor connect-retry)

Full Context configure service vprn bgp connect-retry
configure service vprn bgp group connect-retry
configure service vprn bgp group neighbor connect-retry

Description This command configures the BGP connect retry timer value in seconds.

When this timer expires, BGP tries to reconnect to the configured peer. This configuration parameter can be set at three levels: global level (applies to all peers), peer-group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default 120 seconds

Parameters *seconds* — Specifies the BGP connect retry timer value in seconds, expressed as a decimal integer.

Values 1 to 65535

Platforms All

connect-retry

Syntax **connect-retry** *seconds*
no connect-retry

Context **[Tree]** (config>router>origin-validation>rpki-session connect-retry)

Full Context configure router origin-validation rpki-session connect-retry

Description This command configures the time in seconds to wait between one TCP connection attempt that fails and the next attempt. The default (with **no connect-retry**) is 120 seconds.

Default no connect-retry

Parameters *seconds* — Specifies time in seconds.

Values 1 to 65535

Platforms All

connect-retry

Syntax **connect-retry** *seconds*
no connect-retry

Context **[Tree]** (config>router>bgp connect-retry)
[Tree] (config>router>bgp>group connect-retry)
[Tree] (config>router>bgp>group>neighbor connect-retry)

Full Context configure router bgp connect-retry
configure router bgp group connect-retry
configure router bgp group neighbor connect-retry

Description This command configures the BGP connect retry timer value in seconds.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this timer expires, BGP tries to reconnect to the configured peer. This configuration parameter can be set at three levels: global level (applies to all peers), peer-group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default connect-retry 120

Parameters *seconds* — The BGP Connect Retry timer value in seconds expressed as a decimal integer.

Values 1 to 65535

Platforms All

connect-retry

Syntax **connect-retry** *seconds*
no connect-retry

Context **[Tree]** (config>bmp>station>connection connect-retry)

Full Context configure bmp station connection connect-retry

Description This command configures the BMP connect retry timer value. When this timer expires, BMP tries to reconnect to the configured monitoring station. This timer is applicable when the connection to the monitoring station is not yet established.

The **no** form of this command reverts to the default value.

Default connect-retry 120

Parameters *seconds* — Specifies the BMP connect retry timer in seconds.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.182 connection

connection

Syntax **connection** *connection-id* [**create**]
no connection *connection-id*

Context **[Tree]** (config>service>vprn>sub-if>grp-if>bonding-parameters connection)
[Tree] (config>service>ies>sub-if>grp-if>bonding-parameters connection)

Full Context configure service ies subscriber-interface group-interface bonding-parameters connection
configure service vprn subscriber-interface group-interface bonding-parameters connection

Description This command configures a node where per-connection parameters can be defined. The ID is used as a connection identifier for bonding whenever differentiation between connections is required.

The **no** form of this command removes the connection configuration from this bonding context, which can only be done when bonding is administratively disabled.

Parameters *connection-id* — Specifies the connection ID to be assigned to connections matching the node's parameters.

Values 1,2

connection

Syntax **connection** *connection-id*
connection use-incoming

Context **[Tree]** (config>service>vprn>sub-if>grp-if>bonding-parameters>mcast connection)
[Tree] (config>service>ies>sub-if>grp-if>bonding-parameters>mcast connection)

Full Context configure service ies subscriber-interface group-interface bonding-parameters mcast connection
configure service vprn subscriber-interface group-interface bonding-parameters mcast connection

Description This command configures the connection that should be used for sending out multicast traffic in a bonding context. Traffic can either be forced to use one *connection-id* or follow the connection where the setup message (IGMP/MLD) was received first (**use-incoming**).

The **no** form of this command removes the connection configuration from this bonding context, which can only be done when bonding is administratively disabled.

Default connection use-incoming

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *connection-id* — Specifies the connection ID.

Values 1, 2

connection

Syntax **connection**

Context **[Tree]** (config>bmp>station connection)

Full Context configure bmp station connection

Description Commands in this context configure connection parameters for the BMP monitoring station.

Platforms All

7.183 connection-profile

connection-profile

Syntax **connection-profile** *conn-prof-id* [**create**]
no connection-profile *conn-prof-id*

Context **[Tree]** (config connection-profile)

Full Context configure connection-profile

Description This command creates a profile for the user to configure the list of discrete VPI/VCI values to be assigned to an ATM SAP of an Apipe VLL of **vc-type atm-cell.**

A connection profile can only be applied to a SAP which is part of an Apipe VLL service of **vc-type atm-cell**. The ATM SAP can be on a regular port or APS port.

A maximum of 8000 connection profiles can be created on the system.

The **no** form of this command deletes the profile from the configuration.

Parameters *conn-prof-id* — Specifies the profile number.

Values 1 to 8000

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.184 connection-profile-vlan

connection-profile-vlan

Syntax **connection-profile-vlan** *conn-prof-id* [**create**]
no connection-profile-vlan *conn-prof-id*

Context **[Tree]** (config connection-profile-vlan)

Full Context configure connection-profile-vlan

Description Commands in this context configure the VLAN ranges that will be associated with a service SAP.

Each connection-profile-vlan must be explicitly configured.

Parameters *conn-prof-id* — Specifies the connection-profile identifier. This value will be configured in the service along with the SAP when the user associates a VLAN bundle to a single SAP. For example, a SAP defined in a dot1q port 1/1/1 that matches all the VLANs defined in the connection-profile-vlan 1 will be created as '**sap 1/1/1:cp-1 create**'.

Values 1 to 8000

Platforms All

7.185 connection-timeout

connection-timeout

Syntax **connection-timeout** *seconds*
no connection-timeout

Context **[Tree]** (config>system>management-interface>remote-management connection-timeout)

Full Context configure system management-interface remote-management connection-timeout

Description This command configures the amount of time that all remote managers cannot be reached before they are considered to be down.

If this command is also configured for a specific manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command reverts to the default.

Default connection-timeout 60

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the connection timeout in seconds.

Values 1 to 3600

Platforms All

connection-timeout

Syntax **connection-timeout** *seconds*
no connection-timeout

Context **[Tree]** (config>system>management-interface>remote-management>manager connection-timeout)

Full Context configure system management-interface remote-management manager connection-timeout

Description This command configures the amount of time that this remote manager cannot be reached before it is considered to be down.

This command takes precedence over the same command configured in the global context (**config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command reverts to the default.

Default connection-timeout 60

Parameters *seconds* — Specifies the connection timeout in seconds.

Values 1 to 3600

Platforms All

7.186 connection-timer

connection-timer

Syntax **connection-timer** *seconds*
no connection-timer

Context **[Tree]** (config>aaa>diam>node connection-timer)
[Tree] (config>aaa>diam>node>peer connection-timer)

Full Context configure aaa diameter node connection-timer
configure aaa diameter node peer connection-timer

Description This command configures the Diameter node connection timer that defines the time the systems waits before attempting to reconnect to a peer after the connection was lost.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Default connection-timer 30

Parameters *seconds* — Specifies the Diameter node connection timer.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

connection-timer

Syntax [**no**] **connection-timer** *connection-time*

Context **[Tree]** (config>aaa>diam-peer-plcy connection-timer)
[Tree] (config>aaa>diam-peer-plcy>peer connection-timer)

Full Context configure aaa diameter-peer-policy connection-timer
configure aaa diameter-peer-policy peer connection-timer

Description This command defines the frequency of attempts to open a TCP connection to each peer within a given Diameter client node. Once a TCP connection fails to be established (due to timeouts of TCP SYN packets) or an existing TCP connection fails, the next attempt to open the connection will be tried upon the expiry of the connection-timer. There is no limit on the number of attempts.

The **no** form of this command reverts to the default.

Default connection-timer 30

Parameters *connection-time* — Specifies the amount of time, in seconds, for the diameter peer policy connection.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.187 connectivity-association

connectivity-association

Syntax **connectivity-association** *ca-name* [**create**]
no connectivity-association *ca-name*

Context **[Tree]** (config>macsec connectivity-association)

Full Context configure macsec connectivity-association

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a connectivity association. MACsec connectivity associations are applied to a port dot1x configuration to enable MACsec on that port.

The **no** form of this command removes the connectivity association.

Parameters *ca-name* — The name of the connectivity association, a string up to 32 characters long.

create — Mandatory while creating an entry.

Platforms All

7.188 connectivity-verification

connectivity-verification

Syntax **connectivity-verification** [**count** *nr-of-attempts*] [**timeout** *timeout-seconds*] [**retry-time** *retry-seconds*]
no connectivity-verification

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile connectivity-verification)

Full Context configure subscriber-mgmt vrgw brg brg-profile connectivity-verification

Description This command configures the BRG connectivity verification. The system uses ICMP Echo request messages for connectivity verification.

When the last host associated with a BRG is removed, a ping mechanism is used to verify if the BRG is still active. This command specifies the parameters used in this mechanism.

The **no** form of this command disables the BRG ping mechanism and removes the BRG without verification. Any configured hold time still applies.

Default connectivity-verification count 3 timeout 30 retry-time 900

Parameters *nr-of-attempts* — Specifies the number of connectivity verification attempts this system makes before a BRG is considered down.

Values 1 to 5

timeout-seconds — Specifies the time, in seconds, after which an unanswered ping is considered failed.

Values 5 to 60

retry-seconds — Specifies the time, in seconds, that the system waits while it considers a BRG down before it starts a new connectivity verification cycle. If a ping succeeds, the mechanism will be retried after this time.

Values 300 to 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.189 connectivity-verify

connectivity-verify

Syntax **connectivity-verify**

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring connectivity-verify)
[Tree] (config>redundancy>mc>peer>mc>l3-ring connectivity-verify)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring connectivity-verify
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify

Description Commands in this context configure a node connectivity check.

Platforms All

7.190 connector

connector

Syntax **connector**

Context **[Tree]** (config>port connector)

Full Context configure port connector

Description Commands in this context configure connector parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.191 consider-system-ip-in-gep

consider-system-ip-in-gep

Syntax [**no**] **consider-system-ip-in-gep**

Context **[Tree]** (config>router>ldp consider-system-ip-in-gep)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ldp consider-system-ip-in-gep

Description When this command is enabled, the system interprets the presence or absence of the system IP and its associated action in the applied Global Export Policies in the same way as for other interfaces' IP addresses. In that case:

- if the system IP is not present, its FEC will not be exported or it will be withdrawn if it has been exported
- if the system IP is present with "accept", its FEC will be exported
- if the system IP is present with "deny", its FEC will not be exported or it will be withdrawn if it had been exported

Enabling or disabling this command leads to the applied Global Export Policies being reevaluated.

The **no** form of this command causes the system to not interpret the presence or absence of the system IP in applied Global Export Policies, and the FEC for the system IP is exported (default behavior).

Default no consider-system-ip-in-gep

Platforms All

7.192 console

console

Syntax **console**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment console)

Full Context configure system management-interface cli md-cli environment console

Description Commands in this context configure console parameters.

Platforms All

console

Syntax **console**

Context **[Tree]** (config>system>security>user console)
[Tree] (config>system>security>user-template console)

Full Context configure system security user console
configure system security user-template console

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates the context to configure user profile membership for the console (either Telnet or CPM serial port user).

Platforms All

7.193 console-speed

console-speed

Syntax **console-speed** *baud-rate*
no console-speed

Context **[Tree]** (bof console-speed)

Full Context bof console-speed

Description This command configures the console port baud rate.

When this command is issued while editing the BOF file used for the most recent boot, both the BOF file and the active configuration are changed immediately.

The **no** form of this command reverts to the default value.

Default console-speed 115200

Parameters *baud-rate* — Specifies the console port baud rate, expressed as a decimal integer.

Values 9600, 19200, 38400, 57600, 115200

Platforms All

7.194 contact

contact

Syntax **contact** *contact-information*
no contact *contact-information*

Context **[Tree]** (config>service>cust contact)

Full Context configure service customer contact

Description This command configures contact information for a customer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Include any customer-related contact information such as a technician's name or account contract name.

The **no** form of this command removes the contact information from the customer ID.

Default no contact

Parameters *contact-information* — Specifies customer contact information entered as an ASCII character string up to 80 characters in length. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.

Platforms All

contact

Syntax **contact** *contact-name*
no contact

Context **[Tree]** (config>system contact)

Full Context configure system contact

Description This command creates a text string that identifies the contact name for the device.

Only one contact can be configured, if multiple contacts are configured the last one entered will overwrite the previous entry.

The **no** form of the command reverts to default.

Default no contact

Parameters *contact-name* — Specifies the contact name character string. The string can be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

7.195 context

context

Syntax [**no**] **context**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment>prompt context)

Full Context configure system management-interface cli md-cli environment prompt context

Description This command displays the current command context in the prompt.

The **no** form of this command suppresses the current command context in the prompt.

Default context

Platforms All

7.196 continuous

continuous

Syntax [**no**] **continuous**

Context **[Tree]** (config>saa>test continuous)

Full Context configure saa test continuous

Description This command specifies whether the SAA test is continuous. Once a test is configured as continuous, it cannot be started or stopped with the **oam saa** *test-name* {**start** | **stop**} command.

This option is not applicable to all SAA test types. Support is included for the following types:

- **cpe-ping**
- **dns**
- **eth-cfm-loopback**
- **eth-cfm-two-way-delay**
- **eth-cfm-two-way-slm**
- **icmp-ping** (not applicable to **rapid** type)
- **lsp-ping**
- **mac-ping**
- **sdp-ping**
- **vccv-ping**
- **vprn-ping**

The **no** form of this command disables the continuous execution of the test.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.197 control

control

Syntax **control**

Context **[Tree]** (config>subscr-mgmt>sla-profile control)

Full Context configure subscriber-mgmt sla-profile control

Description This command specifies whether this SLA profile can be used by a session that is set up by a specific control plane.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

control

Syntax **control**

Context **[Tree]** (config>subscr-mgmt>sub-profile control)

Full Context configure subscriber-mgmt sub-profile control

Description Commands in this context configure the subscriber profile to be used by a session that is set up by a specific control plane.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.198 control-channel

control-channel

Syntax [**no**] **control-channel** *lmp-cc-id*

Context **[Tree]** (config>router>lmp>peer control-channel)

Full Context configure router lmp peer control-channel

Description Commands in this context configure an IP control channel for use by GMPLS UNI control plane (RSVP and LMP).

Default no control-channel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *lmp-cc-id* — An unsigned integer identifier for the control channel.

Values 1 to 4294967295

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.199 control-channel-router

control-channel-router

Syntax **control-channel-router** *router-name*
no control-channel-router

Context **[Tree]** (config>router>lmp>peer control-channel-router)

Full Context configure router lmp peer control-channel-router

Description This command configures a control channel router instance on the CPM to use as the endpoint of the GMPLS IP control channel (IPCC). If a control channel router that is not "Base" is configured, then the **gmpls-loopback-address** command must be configured to refer to the GMPLS loopback IP interface configured within the control channel router.

The **config**>**router**>**gmpls**>**peer** *peer-node-id* command must specify a peer that is reachable via a control channel router instance configured for LMP.

The **no** form of the command removes the IPCC from the control channel router instance.

Default no control-channel-router

Parameters *router-name* — Specifies the 64-byte ASCII name of a virtual router interface.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.200 control-channel-status

control-channel-status

Syntax [**no**] **control-channel-status**

Context **[Tree]** (config>service>apipe>spoke-sdp control-channel-status)
[Tree] (config>service>cpipe>spoke-sdp control-channel-status)
[Tree] (config>service>epipe>spoke-sdp control-channel-status)
[Tree] (config>service>vpls>spoke-sdp control-channel-status)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service apipe spoke-sdp control-channel-status
configure service cpipe spoke-sdp control-channel-status
configure service epipe spoke-sdp control-channel-status
configure service vpls spoke-sdp control-channel-status

Description This command enables the configuration of static pseudowire status signaling on a spoke SDP for which signaling for its SDP is set to OFF.

A control-channel-status **no shutdown** is allowed only if all of the following are true:

- SDP signaling is off.
- The control-word is enabled (the control-word is disabled by default)
- The service type is Epipe, Apipe, VPLS, Cpipe, or IES/VPRN
- Mate SDP signaling is off (in vc-switched services)
- The pw-path-id is configured for this spoke SDP.

The **no** form of this command removes control channel status signaling from a spoke SDP. It can only be removed if control channel status is shut down.

Default no control-channel-status

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp control-channel-status

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp control-channel-status

All

- configure service epipe spoke-sdp control-channel-status
- configure service vpls spoke-sdp control-channel-status

control-channel-status

Syntax **control-channel-status**

Context **[Tree]** (config>service>ies>if>spoke-sdp control-channel-status)

Full Context configure service ies interface spoke-sdp control-channel-status

Description This command enables the configuration of static pseudowire status signaling on a spoke-SDP for which signaling for its SDP is set to OFF.

A control-channel-status no shutdown is allowed only if all of the following are true:

- SDP signaling is off.
- The control-word is enabled (the control-word is disabled by default)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The service type is Epipe, Apipe, VPLS, Cpipe, or IES/VPRN
- Mate SDP signaling is off (in vc-switched services)
- The pw-path-id is configured for this spoke-SDP.

The **no** form of this command removes control channel status signaling from a spoke-SDP. It can only be removed if control channel status is shut down.

Default no control-channel-status

Platforms All

control-channel-status

Syntax **control-channel-status**

Context **[Tree]** (config>service>vprn>if>spoke-sdp control-channel-status)
[Tree] (config>service>vprn>red-if>spoke-sdp control-channel-status)

Full Context configure service vprn interface spoke-sdp control-channel-status
configure service vprn redundant-interface spoke-sdp control-channel-status

Description This command enables the configuration of static pseudowire status signaling on a spoke SDP for which signaling for its SDP is set to OFF.

A control-channel-status no shutdown is allowed only if all of the following are true:

- SDP signaling is off.
- The control-word is enabled (the control-word is disabled by default)
- The service type is Epipe, Apipe, VPLS, Cpipe, or IES/VPRN
- Mate SDP signaling is off (in vc-switched services)
- The pw-path-id is configured for this spoke SDP.

The **no** form of this command removes control channel status signaling from a spoke SDP. It can only be removed if control channel status is shut down.

Default no control-channel-status

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp control-channel-status

All

- configure service vprn interface spoke-sdp control-channel-status

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

control-channel-status

Syntax **control-channel-status**

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp control-channel-status)
[Tree] (config>mirror>mirror-dest>spoke-sdp control-channel-status)

Full Context configure mirror mirror-dest remote-source spoke-sdp control-channel-status
configure mirror mirror-dest spoke-sdp control-channel-status

Description Commands in this context configure static pseudowire status signaling on a spoke SDP for which signaling for its SDP is set to OFF. For more information about control channel status configuration for the spoke SDP, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide: VLL, VPLS, PBB, and EVPN Services Guide*.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.201 control-mep

control-mep

Syntax [**no**] **control-mep**

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep control-mep)

Full Context configure eth-tunnel path eth-cfm mep control-mep

Description This command enables the Ethernet tunnel control on the MEP. The use of control-mep command is mandatory for an Ethernet tunnel. MEP detection of failure using CCM may be enabled or disabled independently of the control mep.

The **no** form of this command disables Ethernet ring control.

Default no control-mep

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

control-mep

Syntax [**no**] **control-mep**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep control-mep)

Full Context configure eth-ring path eth-cfm mep control-mep

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the Ethernet ring control on the MEP. The use of control-mep command is mandatory for a ring. MEP detection of failure using CCM may be enabled or disabled independently of the control mep.

The **no** form of this command disables Ethernet ring control.

Default no control-mep

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.202 control-tag

control-tag

Syntax **control-tag** *qtag*[*.qtag*]
no control-tag

Context **[Tree]** (config>eth-tunnel>path control-tag)

Full Context configure eth-tunnel path control-tag

Description This command specifies the VLAN-ID to be used for Ethernet CFM and G.8031 control plane exchanges. If the operator wants to replace an existing control-tag, the parent path needs to be in shutdown state, then deleted and recreated before a new control-tag can be specified.

The **no** form of this command is used just to indicate that a control-tag is not configured. The procedure described above, based on 'no path' command must be used to un-configure/ change the control-tag assigned to the path.

Default no control-tag

Parameters *qtag[.qtag]* — Specifies the value of the VLAN ID to be used for the control tag.

Values 0 to 4094, untagged option is not supported, *

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.203 control-word

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls control-word)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>bgp-evpn>mpls control-word)

Full Context configure service epipe bgp-evpn mpls control-word
configure service vpls bgp-evpn mpls control-word

Description This command enables the transmission and reception of the **control-word**. As defined in RFC7432, the use of the control-word helps avoid frame disordering.

It is enabled or disabled for all EVPN-MPLS destinations at the same time.

Default no control-word

Platforms All

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>service>sdp>binding>pw-port control-word)

Full Context configure service sdp binding pw-port control-word

Description This command enables the setting of the control word bit in the label message. Control words are used to distinguish a PW payload (Ethernet) from an IP payload (identified by the first nibble past the bottom MPLS label, either 4 or 6) carried over an MPLS network.

Based on the payload type, the transit MPLS node can make an appropriate load balancing decision. Load balancing can rely on the MPLS labels, or rely on additional fields that are available only in IP header (source and destination IP addresses and ports).

The presence of a control word indicates that the header following the last MPLS label in the frame is not an IP header.

The **no** form of this command disables setting the control word bit in the label message.

Default no control-word

Platforms All

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>service>apipe>spoke-sdp control-word)
[Tree] (config>service>cpipe>spoke-sdp control-word)
[Tree] (config>service>epipe>spoke-sdp control-word)
[Tree] (config>service>fpipe>spoke-sdp control-word)
[Tree] (config>service>ipipe>spoke-sdp control-word)

Full Context configure service apipe spoke-sdp control-word

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service cpipe spoke-sdp control-word
configure service epipe spoke-sdp control-word
configure service fpipe spoke-sdp control-word
configure service ipipe spoke-sdp control-word

Description The control word command provides the option to add a control word as part of the packet encapsulation for pseudowire types for which the control word is optional. These are Ethernet pseudowires (Epipe). For the 7750 SR only, ATM N:1 cell mode pseudowires (apipe vc-types atm-vcc and atm-vpc) and VT pseudowire (apipe vc-type atm-cell).

The configuration for the two directions of the pseudowire must match because the control word negotiation procedures described in Section 6.2 of RFC 4447 are not supported. The C-bit in the pseudowire FEC sent in the label mapping message is set to 1 when the control word is enabled. Otherwise, it is set to 0.

The service will only come up if the same C-bit value is signaled in both directions. If a spoke-sdp is configured to use the control word but the node receives a label mapping message with a C-bit clear, the node releases the label with the an “Illegal C-bit” status code as per Section 6.1 of RFC 4447. As soon as the user also enabled the control the remote peer, the remote peer will withdraw its original label and will send a label mapping with the C-bit set to 1 and the VLL service will be up in both nodes. The control word must be enabled to allow MPLS-TP OAM to be used on a static spoke-sdp in a Apipe, Epipe and Cpipe service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp control-word

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp control-word

All

- configure service epipe spoke-sdp control-word
- configure service ipipe spoke-sdp control-word

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>service>vpls>spoke-sdp control-word)

Full Context configure service vpls spoke-sdp control-word

Description The control word command provides the option to add a control word as part of the packet encapsulation for pseudowire types for which the control word is optional. These are Ethernet pseudowires (Epipe). For the 7750 SR only, ATM N:1 cell mode pseudowires (apipe vc-types atm-vcc and atm-vpc) and VT pseudowire (apipe vc-type atm-cell).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configuration for the two directions of the pseudowire must match because the control word negotiation procedures described in Section 6.2 of RFC 4447 are not supported. The C-bit in the pseudowire FEC sent in the label mapping message is set to 1 when the control word is enabled. Otherwise, it is set to 0.

The service will only come up if the same C-bit value is signaled in both directions. If a spoke-sdp is configured to use the control word but the node receives a label mapping message with a C-bit clear, the node releases the label with the an “Illegal C-bit” status code as per Section 6.1 of RFC 4447. As soon as the user also enabled the control the remote peer, the remote peer will withdraw its original label and will send a label mapping with the C-bit set to 1 and the VLL service will be up in both nodes. The control word must be enabled to allow MPLS-TP OAM to be used on a static spoke-sdp in a Apipe, Epipe and Cpipe service.

Platforms All

control-word

Syntax [**no**] **control word**

Context **[Tree]** (config>service>vpls>mesh-sdp control-word)
[Tree] (config>service>vpls>spoke-sdp control-word)

Full Context configure service vpls mesh-sdp control-word
configure service vpls spoke-sdp control-word

Description This command enables the use of the control word on pseudowire packets in VPLS and enables the use of the control word individually on each mesh SDP or spoke-SDP. By default, the control word is disabled. When the control word is enabled, all VPLS packets, including the BPDU frames, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match. The **no** form of this command reverts the mesh SDP or spoke-SDP to the default behavior of not using the control word. The control word must be enabled to use MPLS-TP OAM on a static spoke-sdp terminating in a VPLS.

Default no control word

Platforms All

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>service>ies>if>spoke-sdp control-word)

Full Context configure service ies interface spoke-sdp control-word

Description This command enables the PW control word on spoke-SDPs terminated on an IES or VPRN interface. The control word must be enabled to allow MPLS-TP OAM on the spoke-sdp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

It is only valid for MPLS-TP spoke-SDPs when used with IES and VPRN services.

Default no control-word

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>service>vprn>if>spoke-sdp control-word)
[Tree] (config>service>vprn>red-if>spoke-sdp control-word)

Full Context configure service vprn interface spoke-sdp control-word
configure service vprn redundant-interface spoke-sdp control-word

Description This command enables the PW control word on spoke SDPs terminated on an IES or VPRN interface. The control word must be enabled to allow MPLS-TP OAM on the spoke SDP

It is only valid for MPLS-TP spoke SDPs when used with IES and VPRN services.

The no form of this command disables the control work on spoke SDPs.

Default no control-word

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn redundant-interface spoke-sdp control-word

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp control-word

control-word

Syntax [**no**] **control-word**

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp control-word)
[Tree] (config>mirror>mirror-dest>spoke-sdp control-word)

Full Context configure mirror mirror-dest remote-source spoke-sdp control-word
configure mirror mirror-dest spoke-sdp control-word

Description This command enables the PW control word on spoke SDPs that are part of a mirror-destination.

The control word must be enabled to allow MPLS-TP OAM on a spoke SDP.

It is only valid for spoke SDPs that are part of a mirror service of type **ether**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the control word.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure mirror mirror-dest remote-source spoke-sdp control-word

All

- configure mirror mirror-dest spoke-sdp control-word

control-word

Syntax **control-word**

Context **[Tree]** (config>test-oam>build-packet>header control-word)

Full Context configure test-oam build-packet header control-word

Description This command creates a control-word header for inclusion in a build packet instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.204 controlword

controlword

Syntax [**no**] **controlword**

Context **[Tree]** (config>service>pw-template controlword)

Full Context configure service pw-template controlword

Description This command enables the use of the control word on pseudowire packets in VPLS and VPWS and enables the use of the control word individually on each mesh-sdp or spoke-sdp. By default, the control word is disabled. When the control word is enabled, all VPLS/VPWS packets, including the BPDU frames, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match.

The **no** form of the command reverts the mesh SDP or spoke-sdp to the default behavior of not using the control word.

Default no controlword

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.205 convergence

convergence

Syntax **convergence**

Context **[Tree]** (config>service>vprn>bgp convergence)

Full Context configure service vprn bgp convergence

Description Commands in this context configure route convergence delay.

Platforms All

convergence

Syntax **convergence**

Context **[Tree]** (config>router>bgp convergence)

Full Context configure router bgp convergence

Description Commands in this context configure route convergence delay.

Platforms All

7.206 convert-file

convert-file

Syntax **convert-file** *filename* **to** *output-file-name* **format** {**secure** | **legacy**} [**force**]

Context **[Tree]** (admin>certificate convert-file)

Full Context admin certificate convert-file

Description This command converts imported certificates and keys in the cf3:/system-pki directory between secure and legacy format.

Parameters *filename* — Specifies an existing filename, up to 95 characters.

output-file-name — Specifies the output file name, up to 95 characters. If the output filename already exists, and the **force** keyword is not selected, the system prompts to proceed or abort.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

format — Specifies the target format.

Values secure — Specifies the enhanced secure format
legacy — Specifies the legacy format

force — Forces the conversion even if there is an existing file with the same output filename.

Platforms All

7.207 cookie

cookie

Syntax **cookie** [*cookie1*] [*cookie2*]
no cookie

Context **[Tree]** (config>service>epipe>spoke-sdp>egress>l2tpv3 cookie)
[Tree] (config>service>epipe>spoke-sdp>ingress>l2tpv3 cookie)

Full Context configure service epipe spoke-sdp egress l2tpv3 cookie
configure service epipe spoke-sdp ingress l2tpv3 cookie

Description This command configures the RX/TX cookie for L2TPv3 spoke SDPs for Epipe services. The RX cookie must match the configured TX cookie on a far-end node, while the TX cookie must match the configured RX cookie on a far-end node. If a mismatch is detected between the configured (far-end binding cookie) to what is received by the local IP address of the SDP a flag is set and must be manually cleared by an operator.

The purpose of the cookie is to provide validation against misconfiguration of service endpoints, and to ensure that the right service egress is being used.

One egress cookie and up to two ingress cookies may be configured per spoke SDP binding. One or two cookies can be configured for matching ingress packets from the far-end node, in order to support cookie rollover without dropping packets. When a cookie is not configured, SR OS assumes a value of 00:00:00:00:00:00:00:00.

A cookie is not mandatory. An operator may delete an egress cookie or either or both ingress cookies.

Default no cookie1 cookie2

Parameters *cookie1* — Specifies the first cookie, in the form of a 64-bit colon-separated hex value.

cookie2 — Specifies the second cookie, in the form of a 64-bit colon-separated hex value.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cookie

Syntax **cookie** *cookie1-value* [*cookie2-value*]
no cookie

Context **[Tree]** (config>mirror>mirror-dest>spoke-sdp>egress>l2tpv3 cookie)
[Tree] (config>mirror>mirror-dest>spoke-sdp>ingress>l2tpv3 cookie)
[Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp>ingress>l2tpv3 cookie)

Full Context configure mirror mirror-dest remote-source spoke-sdp ingress l2tpv3 cookie
configure mirror mirror-dest spoke-sdp egress l2tpv3 cookie
configure mirror mirror-dest spoke-sdp ingress l2tpv3 cookie

Description This command configures the RX/TX cookie for L2TPv3 spoke SDPs for the mirror destination. The command can configure L2TPv3 a single cookie for the egress spoke SDP or one or two cookies for the remote source ingress spoke SDP.

The purpose of the cookie is to provide validation against misconfiguration of service endpoints, and to ensure that the right service egress is being used.

When a cookie is not configured, SR OS assumes a value of 00:00:00:00:00:00:00:00. A cookie is not mandatory. An operator may delete the egress cookie or either or both ingress cookies.

Parameters *cookie1-value* — Specifies a 64-bit colon separated hex value.

Values xx-xx-xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx:xx:xx

cookie2-value — Specifies a second 64-bit colon separated hex value.

Values xx-xx-xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx:xx:xx

Platforms All

7.208 cookie-length

cookie-length

Syntax **cookie-length** {**4** | **8** | **default**}
no cookie-length

Context **[Tree]** (config>router>l2tp>l2tpv3 cookie-length)
[Tree] (config>service>vprn>l2tp>l2tpv3 cookie-length)
[Tree] (config>service>vprn>l2tp>group>l2tpv3 cookie-length)

Full Context configure router l2tp l2tpv3 cookie-length
configure service vprn l2tp group l2tpv3 cookie-length
configure service vprn l2tp l2tpv3 cookie-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the length of the optional cookie field.

The **no** form of this command returns the **cookie-length** to a default of **none**.

Default no cookie-length

Parameters **4** — Specifies the cookie length as 4 bytes.

8 — Specifies the cookie length as 8 bytes.

default — When specified within the **config>service>vprn>l2tp>group>l2tpv3** context, this is referencing to the **cookie-length** configuration within the **config>service>vprn>l2tp>l2tpv3** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.209 coordinates

coordinates

Syntax **coordinates** *coordinates*
no coordinates

Context **[Tree]** (config>system coordinates)

Full Context configure system coordinates

Description This command creates a text string that identifies the system coordinates for the device location. For example, the command **coordinates** "*37.390 -122.0550*" is read as latitude 37.390 north and longitude 122.0550 west.

Only one set of coordinates can be configured. If multiple coordinates are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Parameters *coordinates* — Specifies the coordinates describing the device location character string. The string may be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. If the coordinates are subsequently used by an algorithm that locates the exact position of this node then the string must match the requirements of the algorithm.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.210 copy

copy

Syntax **copy** *source-name* **to** *dest-name*

Context **[Tree]** (config>service>mrp copy)

Full Context configure service mrp copy

Description This command copies existing MRP policy list entries for a specific policy name to another policy name. The **copy** command is a configuration level maintenance tool used to create a new MRP policy using an existing MRP policy.

An error will occur if the destination policy name exists.

Parameters *source-name* — Identifies the source MRP policy from which the copy command will attempt to copy. The MRP policy with this name must exist for the command to be successful.

dest-name — Identifies the destination MRP policy to which the copy command will attempt to copy. If the MRP policy with dest-name exist within the system an error message is generated.

Platforms All

copy

Syntax **copy**

Context **[Tree]** (config>qos copy)

Full Context configure qos copy

Description Commands in this context copy existing QoS policy entries for a QoS policy-id to another QoS policy-id.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Platforms All

copy

Syntax **copy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter copy)

Full Context configure filter copy

Description This command copies existing filter list entries for a specific filter ID to another filter ID. The **copy** command is a configuration level maintenance tool used to create new filters using existing filters. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword. If **overwrite** is not specified, an error will occur if the destination policy ID exists.

Platforms All

copy

Syntax **copy** *source-file-url dest-file-url* [**force**] [**no-redirect**] [**client-tls-profile** *profile*] [**proxy** *proxy-url*]

Context [Tree] (file copy)

Full Context file copy

Description This command copies a file or all files in a directory from a source URL to a destination URL. At least one of the specified URLs should be a local URL. The optional wildcard (*) can be used to copy multiple files that share a common (partial) prefix and/or (partial) suffix.

When a file is copied to a destination with the same file name, the original file is overwritten by the new file specified in the operation. The following prompt appears if the destination file already exists:

"Overwrite destination file (y/n)?"

For example:

To copy a file named **srcfile** in a directory called test on cf2 in slot B to a file called **destfile** in a directory called production on cf1 in slot A, the syntax is:

```
sr1>file cf2:\ # copy cf2-B/test/srcfile cf1-A/production/destfile
```

To FTP a file named **121201.cfg** in directory mydir stored on cf1 in slot A to a network FTP server with IP address 192.0.2.79 in a directory called backup with a destination file name of **121201.cfg,** the FTP syntax is:

```
copy cf1-A/mydir/121201.cfg 192.0.2.79/backup/121201.cfg
```

Parameters *source-file-url* — Specifies the location of the source file or directory to be copied.

Values

local-url	[*cflash-id*/][*file-path*] up to 200 characters, including cflash-id directory length 99 chars max each

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-url	[{ftp:// | tftp:// | http:// | https://}*login*:*pswd*@*remote-locn*/][*file-path*]
	up to 247 characters
	directory length up to 199 characters
remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
	x:x:x:x:x:x:d.d.d.d[-*interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

dest-file-url — Specifies the destination of the copied file or directory.

force — Specifies to force an immediate copy of the specified file(s). Executes the command without displaying a user prompt message. This command also automatically accepts HTTP redirects unless overridden by the **no-redirect** parameter.

profile — Specifies the TLS client profile configured under **config**>**system**>**security**>**tls**>**client-tls-profile** to use.

proxy-url — Specifies the URL of an HTTP proxy. For example, http://proxy.mydomain.com:8000. This URL must be an HTTP URL and not an HTTPS URL.

no-redirect — Specifies to automatically refuse any HTTP redirects without prompting the user.

Platforms All

copy

Syntax **copy** [*line*]

Context **[Tree]** (candidate copy)

Full Context candidate copy

Description This command copies the selected CLI node (which includes all sub-branches) into a temporary buffer that can be used for a subsequent insert. The contents of the temporary buffer are deleted when the operator exits the candidate edit mode.

Parameters *line* — Specifies which line to copy.

Values line, offset, **first**, **edit-point**, **last**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

line — absolute line number

offset — relative line number to the current edit point. Prefixed with '+' or '-'.

first — keyword to indicate the first line

edit-point — keyword to indicate the current edit point

last — keyword to indicate the last line that is not 'exit'

copy

Syntax **copy** {**user** *source-user* | *profile source-profile*} **to** *destination* [**overwrite**]

Context **[Tree]** (config>system>security copy)

Full Context configure system security copy

Description This command copies a profile or user from a source profile to a destination profile.

Parameters *source-profile* — Specifies an existing profile to copy.

dest-profile — Specifies the copied profile is copied to the destination profile.

overwrite — Specifies that the destination profile configuration is overwritten with the copied source profile configuration. A profile is not overwritten if the **overwrite** command is not specified.

Platforms All

7.211 copy-config

copy-config

Syntax [**no**] **copy-config**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization copy-config)

Full Context configure system security profile netconf base-op-authorization copy-config

Description This command enables the NETCONF copy-config operation.

The **no** form of this command disables the operation.

Default no copy-config

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

7.212 copy-traffic-class-upon-decapsulation

copy-traffic-class-upon-decapsulation

Syntax [**no**] **copy-traffic-class-upon-decapsulation**

Context **[Tree]** (config>ipsec>tnl-temp copy-traffic-class-upon-decapsulation)
[Tree] (config>router>if>ipsec>ipsec-tunnel copy-traffic-class-upon-decapsulation)
[Tree] (config>service>ies>interface>ipsec>ipsec-tunnel copy-traffic-class-upon-decapsulation)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel copy-traffic-class-upon-decapsulation)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel copy-traffic-class-upon-decapsulation)

Full Context configure ipsec tunnel-template copy-traffic-class-upon-decapsulation
configure router interface ipsec ipsec-tunnel copy-traffic-class-upon-decapsulation
configure service ies interface ipsec ipsec-tunnel copy-traffic-class-upon-decapsulation
configure service vprn interface ipsec ipsec-tunnel copy-traffic-class-upon-decapsulation
configure service vprn interface sap ipsec-tunnel copy-traffic-class-upon-decapsulation

Description This command copies the traffic class from the outer tunnel IP packet header to the payload IP packet header upon tunnel decapsulation (public to private direction).

The **no** form of this command disables the traffic copying.

Default copy-traffic-class-upon-decapsulation

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec tunnel-template copy-traffic-class-upon-decapsulation
- configure service vprn interface sap ipsec-tunnel copy-traffic-class-upon-decapsulation

VSR

- configure service vprn interface ipsec ipsec-tunnel copy-traffic-class-upon-decapsulation
- configure service ies interface ipsec ipsec-tunnel copy-traffic-class-upon-decapsulation
- configure router interface ipsec ipsec-tunnel copy-traffic-class-upon-decapsulation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.213 core-connectivity

core-connectivity

Syntax [**no**] **core-connectivity**

Context **[Tree]** (debug>service>id>stp core-connectivity)

Full Context debug service id stp core-connectivity

Description This command enables STP debugging for core connectivity.

The **no** form of the command disables debugging.

Platforms All

7.214 core-mvpn

core-mvpn

Syntax [**no**] **core-mvpn** *service-id*

Context **[Tree]** (config>service>vprn>mvpn>rpf-select core-mvpn)

Full Context configure service vprn mvpn rpf-select core-mvpn

Description This command enables context for VRF extranet mapping for C-instance receivers in this receiver MVPN instance to multicast streams in the specified P-instance core MVPN instance.

Platforms All

7.215 cores

cores

Syntax **cores** *core-count*
no cores

Context **[Tree]** (config>esa>vm cores)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure esa vm cores

Description This command configures the number of CPU physical cores to be allocated to the ESA-VM instance. If an invalid value is configured for the number of cores, the VM remains in a failed state.

The **no** form of this command removes the core allocation. To modify the number of cores, you must use the **no core** command first.

Parameters *core-count* — Specifies the number of cores.

Values 0 to 128

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

7.216 correlation-id

correlation-id

Syntax **x-interfaces**

Context **[Tree]** (config>li>x-interfaces correlation-id)

Full Context configure li x-interfaces correlation-id

Description Commands in this context configure the origin of the correlation identifiers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.217 count

count

Syntax **count** *value*
no count

Context **[Tree]** (config>service>mac-notification count)

Full Context configure service mac-notification count

Description This command configures how often MAC notification messages are sent.

Parameters *value* — Specifies, in seconds, how often MAC notification messages are sent

Values 1 to 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

count

Syntax **count** *value*
no count

Context **[Tree]** (config>service>vpls>mac-notification count)

Full Context configure service vpls mac-notification count

Description This command configures how often MAC notification messages are sent.

Parameters *value* — Specifies, in seconds, how often MAC notification messages are sent

Values 1 to 10

Default Inherits the chassis level configuration from **config>service>mac-notification**

Platforms All

count

Syntax **count** *number*
no count

Context **[Tree]** (config>system>cron>sched count)

Full Context configure system cron schedule count

Description This command configures the total number of times a CRON “interval” schedule is run. For example, if the interval is set to 600 and the count is set to 4, the schedule runs 4 times at 600 second intervals.

Default no count

Parameters *number* — Specifies the number of times the schedule is run.

Values 1 to 65535

Default 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.218 cpe-check

cpe-check

Syntax **cpe-check** *cpe-ip-address*
no cpe-check [*cpe-ip-address*]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect cpe-check)
[Tree] (config>service>vprn>static-route-entry>next-hop cpe-check)

Full Context configure service vprn static-route-entry indirect cpe-check
configure service vprn static-route-entry next-hop cpe-check

Description This command enables CPE-check and specifies the IP address of the target CPE device.

This option initiates a background ICMP ping test to the configured target IP address. The IP address can either be an IPv4 address for IPv4 static routes or an IPv6 address for IPv6 static routes. The target-ip-address cannot be in the same subnet as the static route subnet itself to avoid possible circular references. This option is mutually exclusive with BFD support on a given static route.

The **no** form of this command disables the **cpe-check** option.

Default no cpe-check

Parameters *cpe-ip-address* — Specifies the IP address of the CPE device.

Platforms All

cpe-check

Syntax **cpe-check** *cpe-ip-address*
no cpe-check [*cpe-ip-address*]

Context **[Tree]** (config>router>static-route-entry>indirect cpe-check)
[Tree] (config>router>static-route-entry>next-hop cpe-check)

Full Context configure router static-route-entry indirect cpe-check
configure router static-route-entry next-hop cpe-check

Description This command enables CPE-check and specifies the IP address of the target CPE device.

This option initiates a background ICMP ping test to the configured target IP address. The IP address can either be an IPv4 address for IPv4 static routes or an IPv6 address for IPv6 static routes. The target-ip-address cannot be in the same subnet as the static route subnet itself to avoid possible circular references. This option is mutually exclusive with BFD support on a given static route.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the **cpe-check** option.

Default no cpe-check

Parameters *cpe-ip-address* — Specifies the IP address of the CPE device.

Platforms All

7.219 cpe-ping

cpe-ping

Syntax **cpe-ping service** *service-id* **destination** *ip-address* **source** *ip-address* [**source-mac** *ieee-address*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**ttl** *vc-label-ttl*] [**count** *send-count*] [**return-control**] [**interval** *interval*]

Context [Tree] (oam cpe-ping)
[Tree] (config>saa>test>type cpe-ping)

Full Context configure saa test type cpe-ping
oam cpe-ping

Description This ping utility determines the IP connectivity to a CPE within a specified VPLS service.

Parameters *service-id* — Specifies the service ID of the service to diagnose or manage.

Values

service-id:	1 to 2147483647
svc-name:	64 characters maximum

destination *ip-address* — Specifies the IP address to be used as the destination for performing an OAM ping operations.

Values a.b.c.d

source *ip-address* — Specifies an unused IP address in the same network that is associated with the VPLS or PBB Epipe.

Values a.b.c.d

ieee-address — Specifies the source MAC address that is sent to the CPE. If not specified or set to 0, the MAC address configured for the CPM or CFM is used. This parameter is not applicable to CPE ping on Epipes.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc-name — Specifies the forwarding class of the MPLS echo request encapsulation.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile state of the MPLS echo request encapsulation for VPLS and the ARP packet for PBB Epipe and Epipe VLLs.

Default out

vc-label-ttl — Specifies the TTL value in the VC label for the OAM MAC request, expressed as a decimal integer.

Values 1 to 255

Default 255

send-count — Specifies the number of messages to send to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must have expired before the next message request is sent.

Values 1 to 100

Default 1

return-control — Specifies the MAC OAM reply to a data plane MAC OAM request be sent using the control plane instead of the data plane. This parameter is only valid for VPLS services.

interval — Specifies the *interval* parameter in seconds, expressed as a decimal integer. This parameter is used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the *interval* is set to 1 second where the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

Platforms All

7.220 cpipe

cpipe

Syntax **cpipe** *service-id* [**customer** *customer-id*] [**vpn** *vpn-id*] [**vc-type** {**satop-e1** | **satop-t1** | [**vc-switching**] | **cesopsn** | **cesopsn-cas**}] [**vc-switching**] [**test**] [**create**] [**name** *name*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no cpipe *service-id*

Context [Tree] (config>service cpipe)

Full Context configure service cpipe

Description This command configures a Circuit Emulation Services instance.

When creating a service, you must enter the **customer** keyword and specify a *customer-id* to associate the service with a customer. The *customer-id* must already exist, having been created using the **customer** command in the **service** context. After a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and re-created with a new customer association.

After a service is created, the use of the **customer** *customer-id* parameter is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified results in an error.

By default, no services exist until they are explicitly created with this command.

The **no** form of this command deletes the service instance with the specified *service-id*. The service cannot be deleted until the service has been shutdown.

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every router on which this service is defined.

Values *service-id*: 1 to 2147483647

svc-name: Specifies an existing service name up to 64 characters in length.

customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN ID. If this parameter is not specified, the VPN ID uses the same service ID number.

Values 1 to 2147483647

Default null (0)

vc-type — The vc-type defines the type of unstructured or structured circuit emulation service to be configured.

Values **satop-e1**: Unstructured E1 circuit emulation service.

satop-t1: Unstructured DS1 circuit emulation service.

cesopsn: Basic structured N*64 kb/s circuit emulation service.

cesopsn-cas: Structured N*64 kb/s circuit emulation service with signaling.

Default satop-e1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vc-switching — Specifies if the pseudowire switching signaling is used for the spoke SDPs configured in this service.

test — Specifies a unique test service type for the service context which contains only a SAP configuration. The test service can be used to test the throughput and performance of a path for MPLS-TP PWs. This parameter applies to the 7450 ESS and 7750 SR only.

create — Keyword used to create the service. The **create** keyword requirement can be enabled/disabled in the **environment**>**create** context.

name *name* — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Values *name*: up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.221 cpm-filter

cpm-filter

Syntax **cpm-filter**

Context **[Tree]** (config>system>security cpm-filter)

Full Context configure system security cpm-filter

Description Commands in this context configure a CPM filter. A CPM filter is a hardware filter done by the P chip on the CPM and CFM that applies to all the traffic going to the CPM CPU. It can be used to drop, accept packets, as well as allocate dedicated hardware queues for the traffic.

The **no** form of this command disables the CPM filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.222 cpm-http-redirect

cpm-http-redirect

Syntax **cpm-http-redirect**

Context **[Tree]** (config>system cpm-http-redirect)

Full Context configure system cpm-http-redirect

Description Commands in this context configure **cpm-http-redirect** settings for enabling or disabling the **optimized-mode**.

Platforms All

7.223 cpm-queue

cpm-queue

Syntax **cpm-queue**

Context **[Tree]** (config>system>security cpm-queue)

Full Context configure system security cpm-queue

Description Commands in this context configure a CPM queue.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.224 cpr-window-size

cpr-window-size

Syntax **cpr-window-size** *window-size*

Context **[Tree]** (config>port>dwdm>coherent cpr-window-size)

Full Context configure port dwdm coherent cpr-window-size

Description This command configures the window size used for carrier phase recovery.

Default 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *window-size* — Indicates the number of symbols used for carrier phase recovery algorithm of the receiver. When this parameter is changed, the link bounces because the receiver needs to be reconfigured.

Values 2, 4, 8, 16, 32, 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.225 cpu-alarm

cpu-alarm

Syntax **cpu-alarm high-threshold** *high-percentage* **low-threshold** *low-percentage*
no cpu-alarm

Context **[Tree]** (config>li>x-interfaces>x3>alarms cpu-alarm)

Full Context configure li x-interfaces x3 alarms cpu-alarm

Description This command configures the thresholds for raising the CPU alarm. The low threshold value must be configured with a smaller value than the high threshold.

The **no** form of this command reverts to the default values.

Parameters *high-percentage* — Specifies the high threshold value, as a percentage.

Values 1 to 100

Default 100

low-percentage — Specifies the low threshold value, as a percentage.

Values 0 to 99

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.226 cpu-protection

cpu-protection

Syntax **cpu-protection**

Context **[Tree]** (config>sys>security cpu-protection)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security cpu-protection

Description Commands in this context configure CPU protection policies.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**] | [**eth-cfm-monitoring** [**aggregate**][**car**]] | [**ip-src-monitoring**]
no cpu-protection

Context **[Tree]** (config>service>ies>if>sap cpu-protection)
[Tree] (config>service>ies>if>spoke-sdp cpu-protection)
[Tree] (config>service>ies>sub-if>grp-if>sap cpu-protection)
[Tree] (config>service>vprn>if>sap cpu-protection)
[Tree] (config>service>vprn>if>spoke-sdp cpu-protection)
[Tree] (config>service>vprn>sub-if>grp-if>sap cpu-protection)
[Tree] (config>service>vpls>sap cpu-protection)

Full Context configure service ies interface sap cpu-protection
configure service ies interface spoke-sdp cpu-protection
configure service ies subscriber-interface group-interface sap cpu-protection
configure service vpls sap cpu-protection
configure service vprn interface sap cpu-protection
configure service vprn interface spoke-sdp cpu-protection
configure service vprn subscriber-interface group-interface sap cpu-protection

Description This command assigns an existing CPU protection policy to the SAP or interface. The CPU protection policies are configured in the **config**>**sys**>**security**>**cpuprotection**>**policy** *cpu-protection-policy-id* context.

If no CPU-protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of this command removes the association of the CPU protection policy from the associated SAP or interface configuration and reverts to the default policy values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.

Parameters **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-src-monitoring — Enables per SAP + IP source address rate limiting for certain protocol packets using the per-source-rate and include-protocols from the associated cpu-protection policy. The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In Layer 3 aggregation scenarios all packets from all subscribers behind the same aggregation router arrives with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

eth-cfm-monitoring — Enables the Ethernet Connectivity Fault Management cpu-protection extensions on the associated SAP, SDP, or template.

aggregate — applies the rate limit to the sum of the per-peer packet rates.

car — (Committed Access Rate (CAR) causes Eth-CFM packets to be ignored when enforcing the overall-rate.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s

- configure service ies subscriber-interface group-interface sap cpu-protection
- configure service vprn subscriber-interface group-interface sap cpu-protection

7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

- configure service ies interface spoke-sdp cpu-protection
- configure service ies interface sap cpu-protection
- configure service vprn interface sap cpu-protection
- configure service vpls sap cpu-protection
- configure service vprn interface spoke-sdp cpu-protection

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**] | [**eth-cfm-monitoring** [**aggregate**][**car**]]
no cpu-protection

Context **[Tree]** (config>service>epipe>sap cpu-protection)
[Tree] (config>service>epipe>spoke-sdp cpu-protection)
[Tree] (config>service>ipipe>sap cpu-protection)
[Tree] (config>service>template>vpls-sap-template cpu-protection)
[Tree] (config>service>vpls>mesh-sdp cpu-protection)
[Tree] (config>service>vpls>sap cpu-protection)
[Tree] (config>service>vpls>spoke-sdp cpu-protection)

Full Context configure service epipe sap cpu-protection
configure service epipe spoke-sdp cpu-protection
configure service ipipe sap cpu-protection
configure service template vpls-sap-template cpu-protection
configure service vpls mesh-sdp cpu-protection
configure service vpls sap cpu-protection
configure service vpls spoke-sdp cpu-protection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Use this command to apply a specific CPU protection policy to the associated SAP, SDP or template. If the mac-monitoring keyword is given then per-MAC-rate limiting should be performed, using the per-source-rate from the associated CPU protection policy.

The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-protection-policy-id* context.

If no CPU protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of this command reverts to the default values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

Parameters **mac-monitoring** — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

eth-cfm-monitoring — Enables the Ethernet Connectivity Fault Management cpu-protection extensions on the associated SAP/SDP/template.

aggregate — applies the rate limit to the sum of the per-peer packet rates.

car — (Committed Access Rate) Ignores Eth-CFM packets when enforcing overall-rate.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

cpu-protection

Syntax **cpu-protection** *policy-id*
no cpu-protection

Context **[Tree]** (config>router>interface cpu-protection)
[Tree] (config>service>ies>interface cpu-protection)
[Tree] (config>service>ies>video-interface cpu-protection)
[Tree] (config>service>vpls>video-interface cpu-protection)
[Tree] (config>service>vprn>interface cpu-protection)
[Tree] (config>service>vprn>network-interface cpu-protection)
[Tree] (config>service>vprn>video-interface cpu-protection)

Full Context configure router interface cpu-protection
configure service ies interface cpu-protection
configure service ies video-interface cpu-protection
configure service vpls video-interface cpu-protection
configure service vprn interface cpu-protection
configure service vprn network-interface cpu-protection
configure service vprn video-interface cpu-protection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command assigns an existing CPU protection policy to the associated interface. For these interface types, the per-source rate limit is not applicable.

The CPU protection policies are configured in the **config>sys>security>cpu-protection>policy** *cpu-protection-policy-id* context.

If no CPU-protection policy is assigned to an interface, then the default policy is used to limit the overall-rate. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of this command reverts to the default values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

no cpu-protection (for video interfaces)

Parameters *policy-id* — Specifies an existing CPU protection policy.

Values 1 to 255

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

- configure service vprn video-interface cpu-protection
- configure service ies video-interface cpu-protection
- configure service vpls video-interface cpu-protection

7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

- configure service vprn interface cpu-protection
- configure service vprn network-interface cpu-protection
- configure service ies interface cpu-protection
- configure router interface cpu-protection

cpu-protection

Syntax **cpu-protection** *policy-id* [**mac-monitoring**] [**ip-src-monitoring**]
no cpu-protection

Context **[Tree]** (config>subscr-mgmt>msap-policy cpu-protection)

Full Context configure subscriber-mgmt msap-policy cpu-protection

Description Use this command to apply a specific CPU protection policy to the associated MSAP policy. The specified CPU protection policy is automatically applied to any MSAPs that are create using the MSAP policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If no CPU protection policy is assigned to a SAP, then a default policy is used to limit the overall-rate according to the default policy. The default policy is policy number 254 for access interfaces, 255 for network interfaces and no policy for video interfaces.

The **no** form of this command reverts to the default values.

Default cpu-protection 254 (for access interfaces)

cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the msap-policy to the default policies as shown above.

Parameters *policy-id* — Specifies an existing CPU protection policy.

Values 1 to 255

mac-monitoring — Enables per SAP + source MAC address rate limiting using the per-source-rate from the associated cpu-protection policy.

ip-src-monitoring — Enables per SAP + IP source address rate limiting for certain protocol packets using the per-source-rate and included-protocols from the associated cpu-protection policy. The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In Layer 3 aggregation scenarios all packets from all subscribers behind the same aggregation router arrives with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s

cpu-protection

Syntax **cpu-protection**
cpu-protection *policy-id* [**ip-src-monitoring**] [**mac-monitoring**]

Context **[Tree]** (config>subscr-mgmt>sap-template cpu-protection)

Full Context configure subscriber-mgmt sap-template cpu-protection

Description This command assigns an existing CPU protection policy to the SAP or interface.

CPU protection policies are configured in the **config>sys>security>cpu-protection** context.

Default cpu-protection 254

Parameters *policy-id* — Specifies an existing CPU protection policy is assigned to the SAP or interface.

Values 1 to 255

ip-src-monitoring — Specifies to enable IP source monitoring.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-monitoring — Specifies to enable MAC monitoring.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s

7.227 crc

crc

Syntax **crc** {**16** | **32**}

Context **[Tree]** (config>port>sonet-sdh>path crc)

Full Context configure port sonet-sdh path crc

Description A 16 bit CRC can only be configured on an OC-3 channel, all other channel speeds must use a 32 bit CRC except for the paths configured with encap-type atm at OC3 speed.

Default crc 16 for OC-3, DS-1, DS-3 crc 32 for OC-12, OC-48, ATM-OC12/3, AT-MOC-3, and so on

Note: The CRC default is 32 when the encap-type is set to ATM and also, the default cannot be changed when the encap-type is set to ATM.

Parameters **16** — Use 16 bit checksum for the associated port/channel.

32 — Use 32 bit checksum for the associated port/channel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

crc

Syntax **crc** {**16** | **32**}

Context **[Tree]** (config>port>tdm>ds1>channel-group crc)
[Tree] (config>port>tdm>ds3 crc)
[Tree] (config>port>tdm>e1>channel-group crc)
[Tree] (config>port>tdm>e3 crc)

Full Context configure port tdm ds1 channel-group crc
configure port tdm ds3 crc
configure port tdm e1 channel-group crc
configure port tdm e3 crc

Description This command configures the precision of the cyclic redundancy check (CRC).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default crc 16 for non-ATM channel groups configured under DS-1, E-1 and for non-ATM E-3 and DS-3 channel/ports.

crc 32 for ATM channel-groups configured under DS-1 and E-1, and for ATM E-3 and DS-3 channels/ports. The default cannot be changed.

Parameters **16** — Uses 16 bit checksum for the associated port/channel.

32 — Uses 32 bit checksum for the associated port/channel.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

7.228 crc-monitor

crc-monitor

Syntax **crc-monitor**

Context **[Tree]** (config>port>ethernet crc-monitor)

Full Context configure port ethernet crc-monitor

Description This command configures Ethernet CRC Monitoring parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

7.229 create

create

Syntax [**no**] **create**

Context **[Tree]** (environment create)

Full Context environment create

Description By default, the **create** command is required to create a new OS entity.

The **no** form of the command disables requiring the **create** keyword.

Default create

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.230 create-mpls-tunnel

create-mpls-tunnel

Syntax [**no**] **create-mpls-tunnel**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action create-mpls-tunnel)

Full Context configure router policy-options policy-statement entry action create-mpls-tunnel

Description This command enables the creation of an MPLS tunnel to the BGP next-hop. It is supported for the following address families:

- vpn-ipv4
- vpn-ipv6
- evpn
- label-ipv4
- label-ipv6
- ipv4
- ipv6

The **no** form of the command disables the creation of an MPLS tunnel.

Default no create-mpls-tunnel

Platforms All

7.231 create-subscription

create-subscription

Syntax [**no**] **create-subscription**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization create-subscription)

Full Context configure system security profile netconf base-op-authorization create-subscription

Description This command enables the NETCONF create-subscription operation in the default user profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **base-op-authorization create-subscription** configuration is not pre-emptive, which means that it is checked only at the time of the initial subscription. Configuration changes to the **base-op-authorization** do not cancel any in-progress subscriptions and operators who successfully subscribed continue to receive messages.

The **no** form of this command disables the operation.

Default no create-subscription

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

7.232 create-udp-tunnel

create-udp-tunnel

Syntax **create-udp-tunnel**
no create-udp-tunnel

Context **[Tree]** (config>router>policy-options>policy-statement>default-action create-udp-tunnel)
[Tree] (config>router>policy-options>policy-statement>entry>action create-udp-tunnel)

Full Context configure router policy-options policy-statement default-action create-udp-tunnel
configure router policy-options policy-statement entry action create-udp-tunnel

Description This command instructs the router to create an MPLS-over-UDP tunnel upon receiving BGP routes that match the import policy.

Default no create-udp-tunnel

Platforms All

7.233 credential

credential

Syntax **credential**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>client-db>client credential)

Full Context configure ipsec client-db client credential

Description Commands in this context configure the parameters used to authenticate peers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.234 credit-control-policy

credit-control-policy

Syntax **credit-control-policy** *policy-name* [**create**]
credit-control-policy diameter *policy-name*
no credit-control-policy *policy-name*

Context [Tree] (config>subscr-mgmt credit-control-policy)

Full Context configure subscriber-mgmt credit-control-policy

Description This command creates, configures or deletes a credit control policy.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the policy name, up to 32 characters.

create — Keyword used to create the credit control policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

credit-control-policy

Syntax **credit-control-policy** *policy-name*
no credit-control-policy

Context [Tree] (config>subscr-mgmt>sla-prof credit-control-policy)

Full Context configure subscriber-mgmt sla-profile credit-control-policy

Description This command configures the credit policy for this SLA profile.

Default no credit-control-policy

Parameters *policy-name* — Specifies the credit control policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.235 credit-control-quota

credit-control-quota

Syntax [**no**] **credit-control-quota**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes credit-control-quota)

Full Context configure aaa isa-radius-policy acct-include-attributes credit-control-quota

Description This command includes any unconsumed volume quota in the Alc-Credit-Control-Quota attribute.

The **no** form of this command excludes the Alc-Credit-Control-Quota attribute.

Default no credit-control-quota

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.236 credit-control-server

credit-control-server

Syntax **credit-control-server radius**
no credit-control-server

Context **[Tree]** (config>subscr-mgmt>credit-control-policy credit-control-server)

Full Context configure subscriber-mgmt credit-control-policy credit-control-server

Description This command configures the credit control server to use. In case of RADIUS, the servers defined in the authentication policy are used. For Diameter, the peers defined in the specified Diameter policy are used.

The **no** form of this command reverts to the default.

Default credit-control-server radius

Parameters **radius** — Specifies to use the RADIUS authentication servers defined in the RADIUS authentication policy in the group interface to report credit usage and obtain new credit.

diameter *policy-name* — Specifies to use the diameter peers specified in the diameter policy to report credit usage and obtain new credit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.237 credit-exhaust-threshold

credit-exhaust-threshold

Syntax **credit-exhaust-threshold** *threshold-percentage*
no credit-exhaust-threshold

Context **[Tree]** (config>subscr-mgmt>cat-map credit-exhaust-threshold)

Full Context configure subscriber-mgmt category-map credit-exhaust-threshold

Description This command specifies the credit exhaust threshold considered to act.

The **no** form of this command reverts the configured value to the default.

Default credit-exhaust-threshold 100

Parameters *threshold-percentage* — Specifies the percentage to use for the credit exhaust threshold.

Values 50 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.238 credit-mcs-interval

credit-mcs-interval

Syntax **credit-mcs-interval** *interval*
no credit-mcs-interval

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx credit-mcs-interval)

Full Context configure subscriber-mgmt diameter-application-policy gx credit-mcs-interval

Description This command configures the usage monitoring between the redundant chassis that is synchronized periodically per Gx session, from the active Gx session to the standby Gx session.

The **no** form of this command reverts to the default value.

Default credit-mcs-interval 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *interval* — Specifies the interval time, in minutes, between synchronization moments for syncing volume to the multi-chassis redundant chassis in case of Gx usage monitoring on a CCI that belongs to a multi-chassis redundant host.

Values 5 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.239 credit-type

credit-type

Syntax **credit-type** {**volume** | **time**}
no credit-type

Context **[Tree]** (config>subscr-mgmt>cat-map credit-type)

Full Context configure subscriber-mgmt category-map credit-type

Description This command specifies whether volume or time based accounting is performed.

The **no** form of this command reverts to the default.

Default credit-type volume

Parameters **volume** — Specifies volume-based accounting.

time — Specifies time-based accounting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.240 credit-type-override

credit-type-override

Syntax **credit-type-override** {**volume** | **time**}
no credit-type-override

Context **[Tree]** (config>subscr-mgmt>cat-map>category credit-type-override)

Full Context configure subscriber-mgmt category-map category credit-type-override

Description This command overrides the **credit-type** configured in the **config>subscr-mgmt>cat-map** context for the given category.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters **volume** — If different than the value specified in the **credit-type** command, the value overrides the credit-type.

time — If different than the value specified in the **credit-type** command, the value overrides the credit-type.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.241 credits

credits

Syntax **credits** [**lowercase** *credits*] [**uppercase** *credits*] [**numeric** *credits*] [**special-character** *credits*]
no credits

Context **[Tree]** (config>system>security>password>complexity-rules credits)

Full Context configure system security password complexity-rules credits

Description The maximum credits given for usage of the different character classes in the local passwords.

The **no** form of this command resets to default.

Default no credits

Parameters *credits* — Specifies the number of credits that can be used for each characters class.

Values 0 to 10

Platforms All

7.242 criteria-overrides

criteria-overrides

Syntax **criteria-overrides**

Context **[Tree]** (config>service>apipe>sap>ingress criteria-overrides)
[Tree] (config>service>cpipe>sap>ingress criteria-overrides)
[Tree] (config>service>epipe>sap>ingress criteria-overrides)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>fpipe>sap>ingress criteria-overrides)
[Tree] (config>service>ies>if>sap>ingress criteria-overrides)
[Tree] (config>service>ipipe>sap>ingress criteria-overrides)
[Tree] (config>service>vpls>sap>ingress criteria-overrides)
[Tree] (config>service>vprn>if>sap>ingress criteria-overrides)

Full Context configure service apipe sap ingress criteria-overrides
configure service cpipe sap ingress criteria-overrides
configure service epipe sap ingress criteria-overrides
configure service fpipe sap ingress criteria-overrides
configure service ies interface sap ingress criteria-overrides
configure service ipipe sap ingress criteria-overrides
configure service vpls sap ingress criteria-overrides
configure service vprn interface sap ingress criteria-overrides

Description Commands in this context configure IPv4 and IPv6 criteria overrides.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls sap ingress criteria-overrides
- configure service ies interface sap ingress criteria-overrides
- configure service ipipe sap ingress criteria-overrides
- configure service cpipe sap ingress criteria-overrides
- configure service epipe sap ingress criteria-overrides
- configure service vprn interface sap ingress criteria-overrides
- configure service fpipe sap ingress criteria-overrides

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress criteria-overrides

7.243 critical-event

critical-event

Syntax [**no**] **critical-event**

Context [Tree] (config>port>ethernet>efm-oam>link-mon>local-sf-action>info-notification critical-event)

Full Context configure port ethernet efm-oam link-monitoring local-sf-action info-notification critical-event

Description This command sets the critical event Flag field in the Information OAMPDU when the local signal failure (sf-threshold) threshold is reached. This is maintained in all subsequent Information OAM PDUs until the situation is cleared.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Interactions: The signal failure threshold triggers these actions.

Default no critical-event

Platforms All

critical-event

Syntax **critical-event local-port-action** {**log-only** | **out-of-service**}

Context **[Tree]** (config>port>ethernet>efm-oam>peer-rdi-rx critical-event)

Full Context configure port ethernet efm-oam peer-rdi-rx critical-event

Description This command defines how to react to the reception of a critical event Flag field set in the informational OAMPDU.

Default critical-event local-port-action out-of-service

Parameters **local-port-action** — Defines whether or not the local port will be affected when a critical event is received from a peer.

log-only — Keyword that prevents the port from being affected when the local peer receives a critical event. The critical event will be logged but the port will remain operational.

out-of-service — Keyword that causes the port to enter a non-operation down state with a port state of link up. The error is logged upon reception of critical event. The port is not available to service data but continues to carry Link OAM traffic to ensure the link is monitored.

Platforms All

7.244 crl-expiration-warning

crl-expiration-warning

Syntax **crl-expiration-warning** *hours* [**repeat** *repeat-hours*]
no crl-expiration-warning

Context **[Tree]** (config>system>security>pki crl-expiration-warning)

Full Context configure system security pki crl-expiration-warning

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies when the systems issues a **BeforeExp** message before a CRL expires. For example, with **certificate-expiration-warning 5**, the system issues a **BeforeExp** message 5 hours before a CRL expires. An optional **repeat** *repeat-hour* parameter enables the system to repeat the **BeforeExp** message every hour until the CRL expires.

If the user only wants **AfterExp**, then **certificate-expiration-warning 0** can be used to achieve this.

BeforeExp and **AfterExp** warnings can be cleared in following cases:

- The CRL is reloaded by the **admin certificate reload** command. In this case, if the reloaded file is not expired, then **AfterExp** is cleared. And, if the reloaded file is outside of configured warning window, then the **BeforeExp** is also cleared.
- When the **ca-profile** is shutdown, then **BeforeExp** and **AfterExp** of corresponding certificates are cleared.
- When **no crl-expiration-warning** command is configured, then all existing **BeforeExp** and **AfterExp** are cleared.
- Users may change the configuration of the **crl-expiration-warning** so that certain CRL are no longer in the warning window. **BeforeExp** of corresponding CRL are cleared.
- If the system time changes so that the new time causes the CRL to no longer be in the warning window, then **BeforeExp** is cleared. If the new time causes an expired CRL to come non-expired, then **AfterExp** is cleared.

Default no crl-expiration-warning

Parameters *hours* — Specifies the amount of time before a CRL expires when system issues **BeforeExp**

Values 0 to 8760

repeat-hour — Specifies that the system repeats **BeforeExp** every repeat-hour

Values 0 to 8760

Platforms All

7.245 crl-file

crl-file

Syntax **crl-file** *filename*
no crl-file

Context **[Tree]** (config>system>security>pki>ca-profile crl-file)

Full Context configure system security pki ca-profile crl-file

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the name of a file in cf3:\system-pki\crl as the Certification Revoke List file of the **ca-profile**.

Notes:

- The system performs following checks against configured crl-file when a **no shutdown** command is issued:
  - A valid cert-file of the ca-profile must be already configured.
  - Configured crl-file must be a DER formatted CRLv2 file.
  - All non-optional fields defined in section 5.1 of RFC5280 must exist and conform to the RFC5280 defined format.
  - Check the version field to see if its value is 0x1.
  - Delta CRL Indicator must not exist (delta CRL is not supported).
  - CRL's signature must be verified by using the cert-file of ca-profile.

  If any of above checks fail, the **no shutdown** command fails.
- Changing or removing the **crl-file** is only allowed when the **ca-profile** is in a **shutdown** state.

The **no** form of this command removes the filename from the configuration.

Parameters *filename* — Specifies the name of CRL file stored in cf3:\system-pki\crl.

Platforms All

7.246 crl-update

crl-update

Syntax **crl-update ca** *ca-profile-name*

Context **[Tree]** (admin>certificate crl-update)

Full Context admin certificate crl-update

Description This command manually triggers the Certificate Revocation List file (CRL) update for the specified ca-profile.

Using this command requires shutting down the **auto-crl-update**.

Parameters *ca-profile-name* — Specifies the name of the Certificate Authority profile.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.247 crl-urls

crl-urls

Syntax **crl-urls**

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update crl-urls)

Full Context configure system security pki ca-profile auto-crl-update crl-urls

Description Commands in this context configure **crl-urls** parameters. The system allows up to eight URL entries to be configured and tries each URL in order and stop when a qualified CRL is successfully downloaded. A qualified CRL is a valid CRL signed by the CA and is more recent than the existing CRL.

If none of the configured URLs returns a qualified CRL, then:

- If the schedule-type is next-update-based, system will wait for configure retry-interval before it start from beginning of the list again.
- If the schedule-type is periodic, then system will wait till next periodic update time.

If the user wants to manually stop the download, shutting down of auto-crl-retrieval could be used to achieve this.

Platforms All

7.248 cron

cron

Syntax **cron**

Context **[Tree]** (config>system cron)

Full Context configure system cron

Description This command creates the context to create scripts, script parameters and schedules which support the Service Assurance Agent (SAA) functions.

CRON features are saved to the configuration file on both primary and backup control modules. If a control module switchover occurs, CRON events are restored when the new configuration is loaded. If a control module switchover occurs during the execution of a cron script, the failover behavior will be determined by the contents of the script.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cron

Syntax **cron**

Context **[Tree]** (config>system>security>cli-script>authorization cron)

Full Context configure system security cli-script authorization cron

Description Commands in this context configure authorization for the Cron job-scheduler.

Platforms All

7.249 cross-connect

cross-connect

Syntax [**no**] **cross-connect**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state cross-connect)

Full Context configure subscriber-mgmt wlan-gw ue-query state cross-connect

Description This command enables matching on cross-connected UEs.

The **no** form of this command disables matching on cross-connected UEs, unless all state matching is disabled.

Default no cross-connect

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.250 csf-enable

csf-enable

Syntax [**no**] **csf-enable**

Context **[Tree]** (config>lag>eth-cfm>mep csf-enable)
[Tree] (config>port>ethernet>eth-cfm>mep csf-enable)

Full Context configure lag eth-cfm mep csf-enable
configure port ethernet eth-cfm mep csf-enable

Description This command configures the reception of Client Signal Fail (CSF) message parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

csf-enable

Syntax [**no**] **csf-enable**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep csf-enable)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep csf-enable)
[Tree] (config>service>ies>if>sap>eth-cfm>mep csf-enable)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep csf-enable)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm csf-enable)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep csf-enable)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep csf-enable)
[Tree] (config>service>vpls>sap>eth-cfm>mep csf-enable)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep csf-enable)
[Tree] (config>service>vprn>if>sap>eth-cfm>mep csf-enable)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep csf-enable)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep csf-enable)

Full Context configure service epipe sap eth-cfm mep csf-enable
configure service epipe spoke-sdp eth-cfm mep csf-enable
configure service ies interface sap eth-cfm mep csf-enable
configure service ies interface spoke-sdp eth-cfm mep csf-enable
configure service ies subscriber-interface group-interface sap eth-cfm csf-enable
configure service ies subscriber-interface group-interface sap eth-cfm mep csf-enable
configure service vpls mesh-sdp eth-cfm mep csf-enable
configure service vpls sap eth-cfm mep csf-enable
configure service vpls spoke-sdp eth-cfm mep csf-enable
configure service vprn interface sap eth-cfm mep csf-enable
configure service vprn interface spoke-sdp eth-cfm mep csf-enable
configure service vprn subscriber-interface group-interface sap eth-cfm mep csf-enable

Description Commands in this context configure the reception and local processing of ETH-CSF frames.

The **no** form of this command disables the reception of Client Signal Fail (CSF) message parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep csf-enable
- configure service vprn subscriber-interface group-interface sap eth-cfm mep csf-enable

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service epipe sap eth-cfm mep csf-enable
- configure service vpls sap eth-cfm mep csf-enable
- configure service vprn interface sap eth-cfm mep csf-enable
- configure service ies interface sap eth-cfm mep csf-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe spoke-sdp eth-cfm mep csf-enable
- configure service ies interface spoke-sdp eth-cfm mep csf-enable
- configure service vpls spoke-sdp eth-cfm mep csf-enable
- configure service vprn interface spoke-sdp eth-cfm mep csf-enable
- configure service vpls mesh-sdp eth-cfm mep csf-enable

7.251 csnp-authentication

csnp-authentication

Syntax [**no**] **csnp-authentication**

Context **[Tree]** (config>service>vprn>isis csnp-authentication)
[Tree] (config>service>vprn>isis>level csnp-authentication)

Full Context configure service vprn isis csnp-authentication
configure service vprn isis level csnp-authentication

Description This command enables authentication of individual ISIS packets of complete sequence number PDUs (CSNP) type for the VPRN instance.

Platforms All

csnp-authentication

Syntax [**no**] **csnp-authentication**

Context **[Tree]** (config>router>isis csnp-authentication)
[Tree] (config>router>isis>level csnp-authentication)

Full Context configure router isis csnp-authentication
configure router isis level csnp-authentication

Description This command enables authentication of individual IS-IS packets of complete sequence number PDUs (CSNP) type.

The **no** form of this command suppresses authentication of CSNP packets.

Default csnp-authentication

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.252 csnp-interval

csnp-interval

Syntax **csnp-interval** *seconds*
no csnp-interval

Context **[Tree]** (config>service>vprn>isis>if csnp-interval)

Full Context configure service vprn isis interface csnp-interval

Description This command configures the time interval, in seconds, to send complete sequence number (CSN) PDUs from the interface. IS-IS must send CSN PDUs periodically.

The **no** form of this command reverts to the default value.

Default csnp-interval 10 — CSN PDUs are sent every 10 seconds for LAN interfaces.

csnp-interval 5 — CSN PDUs are sent every 5 seconds for point-to-point interfaces.

Parameters *seconds* — The time interval, in seconds between successive CSN PDUs sent from this interface expressed as a decimal integer.

Values 1 to 65535

Platforms All

csnp-interval

Syntax **csnp-interval** *seconds*
no csnp-interval

Context **[Tree]** (config>router>isis>interface csnp-interval)

Full Context configure router isis interface csnp-interval

Description This command configures the time interval, in seconds, to send complete sequence number (CSN) PDUs from the interface. IS-IS must send CSN PDUs periodically.

The **no** form of this command reverts to the default value.

Default csnp-interval 10 — CSN PDUs are sent every 10 seconds for LAN interfaces.

csnp-interval 5 — CSN PDUs are sent every 5 seconds for point-to-point interfaces.

Parameters *seconds* — Specifies the time interval, in seconds, between successive CSN PDUs sent from this interface expressed as a decimal integer.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

7.253 cspf

cspf

Syntax [**no**] **cspf**

Context **[Tree]** (debug>router>isis cspf)

Full Context debug router isis cspf

Description This command enables debugging for IS-IS cspf.

The **no** form of the command disables debugging.

Platforms All

cspf

Syntax **cspf** [*ip-address*]
no cspf

Context **[Tree]** (debug>router>ospf cspf)

Full Context debug router ospf cspf

Description This command enables debugging for an OSPF constraint-based shortest path first (CSPF).

Parameters *ip-address* — Specifies the IP address for the range used for CSPF.

Platforms All

7.254 cspf-on-loose-hop

cspf-on-loose-hop

Syntax [**no**] **cspf-on-loose-hop**

Context **[Tree]** (config>router>mpls cspf-on-loose-hop)

Full Context configure router mpls cspf-on-loose-hop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the option to do CSPF calculations until the next loose hop or the final destination of LSP on LSR. On receiving a PATH message on LSR and processing of all local hops in the received ERO, if the next hop is loose, then the LSR node will first do a CSPF calculation until the next loose hop. On successful completion of CSPF calculation, ERO in PATH message is modified to include newly calculated intermediate hops and propagate it forward to the next hop. This allows setting up inter-area LSPs based on ERO expansion method.

Note: The LSP may fail to set up if this option is enabled on an LSR that is not an area border router and receives a PATH message without proper next loose hop in ERO. The 'cspf-on-loose-hop' configuration is allowed to change dynamically and applied to new LSP setup after change.

Default no cspf-on-loose-hop

Platforms All

7.255 cumulative-factor

cumulative-factor

Syntax [**no**] **cumulative-factor** *cumulative-factor*

Context **[Tree]** (config>service>vpls>mac-move>primary-ports cumulative-factor)
[Tree] (config>service>vpls>mac-move>secondary-ports cumulative-factor)
[Tree] (config>service>template>vpls-template>mac-move>primary-ports cumulative-factor)
[Tree] (config>service>template>vpls-template>mac-move>secondary-ports cumulative-factor)

Full Context configure service template vpls-template mac-move primary-ports cumulative-factor
configure service template vpls-template mac-move secondary-ports cumulative-factor
configure service vpls mac-move primary-ports cumulative-factor
configure service vpls mac-move secondary-ports cumulative-factor

Description This command defines a factor defining how many mac-relearn measurement periods can be used to measure mac-relearn rate. The rate must be exceeded during the defined number of consecutive periods before the corresponding port is blocked by the mac-move feature. The cumulative-factor of primary ports must be higher than cumulative-factor of secondary ports.

Default cumulative-factor 2 — secondary ports

cumulative-factor 3 — primary ports

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *factor* — Specifies the factor defining the number of mac-relearn measurement periods can be used to measure mac-relearn rate

Values 2 to 10

Platforms All

7.256 cups

cups

Syntax [**no**] **cups**

Context **[Tree]** (config>subscr-mgmt>sla-profile>control cups)

Full Context configure subscriber-mgmt sla-profile control cups

Description This command enables a session that is set up with remote CUPS control plane handling to use this SLA profile.

The **no** form of this command disables a session that is set up with remote CUPS control-plane handling from using this SLA profile.

Default no cups

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

cups

Syntax [**no**] **cups**

Context **[Tree]** (config>subscr-mgmt>sub-profile>control cups)

Full Context configure subscriber-mgmt sub-profile control cups

Description This command enables a session that is set up with remote CUPS control plane handling to use this subscriber profile.

The **no** form of this command disables a session that is set up with remote CUPS control-plane handling from using this subscriber profile.

Default no cups

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.257 current-hop-limit

current-hop-limit

Syntax **current-hop-limit** *limit*
no current-hop-limit

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv current-hop-limit)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv current-hop-limit)
[Tree] (config>service>vprn>router-advert>if current-hop-limit)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv current-hop-limit)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv current-hop-limit)
[Tree] (config>subscr-mgmt>rtr-adv-plcy current-hop-limit)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements current-hop-limit
configure service ies subscriber-interface ipv6 router-advertisements current-hop-limit
configure service vprn router-advertisement interface current-hop-limit
configure service vprn subscriber-interface group-interface ipv6 router-advertisements current-hop-limit
configure service vprn subscriber-interface ipv6 router-advertisements current-hop-limit
configure subscriber-mgmt router-advertisement-policy current-hop-limit

Description This command configures the hop limit to be advertised.

The **no** form of this command returns the command to the default setting.

Default current-hop-limit 64

Parameters *limit* — Specifies the default value to be placed in the current hop limit field in router advertisement policies sent.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface ipv6 router-advertisements current-hop-limit
- configure subscriber-mgmt router-advertisement-policy current-hop-limit
- configure service ies subscriber-interface group-interface ipv6 router-advertisements current-hop-limit
- configure service ies subscriber-interface ipv6 router-advertisements current-hop-limit
- configure service vprn subscriber-interface ipv6 router-advertisements current-hop-limit

All

- configure service vprn router-advertisement interface current-hop-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

current-hop-limit

Syntax **current-hop-limit** *number*
no current-hop-limit

Context **[Tree]** (config>router>router-advert>if current-hop-limit)

Full Context configure router router-advertisement interface current-hop-limit

Description This command configures the current-hop-limit in the router advertisement messages. It informs the nodes on the subnet about the hop-limit when originating IPv6 packets.

Default current-hop-limit 64

Parameters *number* — Specifies the hop limit.

Values 0 to 255. A value of zero means there is an unspecified number of hops.

Platforms All

7.258 custom-buffer-mode

custom-buffer-mode

Syntax [**no**] **custom-buffer-mode**

Context **[Tree]** (config>port>sonet-sdh>path>atm custom-buffer-mode)

Full Context configure port sonet-sdh path atm custom-buffer-mode

Description This command configures ATM port custom buffer parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

7.259 custom-option

custom-option

Syntax **custom-option** *option-number* **address** [*ip-address*]
custom-option *option-number* **address** *ipv6-address* [*ipv6-address*]
custom-option *option-number* **domain** [*domain-string*]
custom-option *option-number* **hex** *hex-string*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

custom-option *option-number* **string** *ascii-string*
no custom-option *option-number*

Context **[Tree]** (config>router>dhcp>server>pool>options custom-option)
[Tree] (config>router>dhcp>server>pool>subnet>options custom-option)
[Tree] (config>service>vprn>dhcp>server>pool>options custom-option)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options custom-option)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>options custom-option)

Full Context configure router dhcp local-dhcp-server pool options custom-option
configure router dhcp local-dhcp-server pool subnet options custom-option
configure service vprn dhcp local-dhcp-server pool options custom-option
configure subscriber-mgmt local-user-db ipoe host options custom-option
configure subscriber-mgmt local-user-db ppp host options custom-option

Description This command configures specific DHCP options. The options defined here can overrule options in the local user database.

The **no** form of the removes the custom option parameters from the configuration.

Parameters *option-number* — Specifies up to four option numbers that the DHCP server uses to send the identification strings to the DHCP client.

Values 1 to 254

ip-address — Specifies the IP address of a host.

Values a.b.c.d

ipv6-address — Specifies the IPv6 address of a host. Applicable to DHCP6 only.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

domain-string — Specifies the domain name, up to 127 characters.

hex-string — Specifies the hex value of this option.

Values 0x0 to 0xFFFFFFFF (up to 254 hex nibbles)

ascii-string — Specifies the value of this option, up to 127 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

custom-option

Syntax **custom-option** *option-number* **address** [*ipv6-address*]
custom-option *option-number* **domain** [*domain-string*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

custom-option *option-number* **hex** *hex-string*
custom-option *option-number* **string** *ascii-string*
no custom-option *option-number*

Context [Tree] (config>router>dhcp6>server>defaults>options custom-option)
[Tree] (config>router>dhcp6>server>pool>options custom-option)
[Tree] (config>router>dhcp6>server>pool>prefix>options custom-option)
[Tree] (config>service>vprn>dhcp6>server>pool>options custom-option)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix>options custom-option)
[Tree] (config>service>vprn>dhcp6>server>pool>options custom-option)

Full Context configure router dhcp6 local-dhcp-server defaults options custom-option
configure router dhcp6 local-dhcp-server pool options custom-option
configure router dhcp6 local-dhcp-server pool prefix options custom-option
configure service vprn dhcp6 local-dhcp-server pool options custom-option
configure service vprn dhcp6 local-dhcp-server pool prefix options custom-option

Description This command configures specific DHCP6 options. The options defined here can overrule options in the local user database.

The **no** form of the removes the custom option parameters from the configuration.

Parameters *option-number* — Specifies up to four option numbers that the DHCP6 server uses to send the identification strings to the DHCP6 client.

Values 1 to 254

ipv6-address — Specifies the IPv6 address of a host.

Values

:ipv6-address	x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

domain-string — Specifies the domain name, up to 127 characters.

hex-string — Specifies the hex value of this option.

Values 0x0 to 0xFFFFFFFF (up to 254 hex nibbles)

ascii-string — Specifies the value of this option, up to 127 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router dhcp6 local-dhcp-server pool prefix options custom-option
- configure service vprn dhcp6 local-dhcp-server pool prefix options custom-option
- configure service vprn dhcp6 local-dhcp-server pool options custom-option
- configure router dhcp6 local-dhcp-server pool options custom-option

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router dhcp6 local-dhcp-server defaults options custom-option

custom-option

Syntax **custom-option** *protocol option-number* **address** *ip-address*
custom-option p*rotocol option-number* **hex** *hex-string*
custom-option *protocol option-number* **string** *ascii-string*
no custom-option *protocol option-number*

Context **[Tree]** (config>subscr-mgmt>ppp-policy>options custom-option)

Full Context configure subscriber-mgmt ppp-policy ppp-options custom-option

Description This command provides the ability to configure custom PPP options.

Note: Standard options such as the DNS name is returned from DHCP or RADIUS and be converted to PPP automatically. Compression is not supported.

The **no** form of this command removes the custom options from the configuration.

Parameters *protocol* — Specifies a protocol for the custom option.

Values lcp, ipcp, ipv6cp

option-number — Assigns an identifying number for the custom option.

Values 0 to 255

ip-address — Specifies the IP address in the a.b.c.d format.

ascii-string — Specifies an ASCII format string for the custom option up to 127 characters.

hex-string — Specifies a hex value for the custom option.

Values [0x0 to 0xFFFFFF (up to 254 hex nibbles)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

custom-option

Syntax **custom-option** *option-number* **address** [*ip-address*]
custom-option *option-number* **hex** *hex-string*
custom-option *option-number* **string** *ascii-string*
no custom-option *option-number*

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool>options custom-option)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt vrgw brg brg-profile dhcp-pool options custom-option

Description This command configures DHCP options.

Parameters *option-number* — Specifies the number of this DHCP option.

ip-address — Specifies the IP address of this option. Up to 4 addresses can be assigned.

hex-string — Specifies the hex value of this option.

Values 0x0 to 0xFFFFFFFF (maximum 254 hex nibbles)

ascii-string — Specifies an ASCII value of this option.

Values 127 characters maximum

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

7.260 custom-protocol

custom-protocol

Syntax **custom-protocol** *custom-protocol-id* **ip-protocol-num** *protocol-id* [**create**]
custom-protocol *custom-protocol-id*
no custom-protocol *custom-protocol-id*

Context **[Tree]** (config>app-assure>group>policy custom-protocol)

Full Context configure application-assurance group policy custom-protocol

Description This command creates and enters configuration context for custom protocols. Custom protocols allow the creation of TCP and UDP-based custom protocols (based on the *ip-protocol-num* option) that employ pattern-match at offset in protocol signature definition.

Operator-configurable custom-protocols are evaluated ahead of any Nokia-provided protocol signature in order of **custom-protocol-id** (the lower ID is matched first in case of flow matching multiple custom-protocols) within the context the protocol is defined.

Custom protocols must be created before they can be used in application definition but do not have to be enabled. To reference a custom protocol in application definition, or any other CLI configuration one must use protocol name that is a concatenation of “custom_” and <custom-protocol-id>, (for example custom_01, custom_02 ... custom_10, and so on). This concatenation is also used when reporting custom protocol statistics.

Parameters *custom-protocol-id* — Specifies the index into the protocol list that defines a custom protocol for application assurance.

Values 1 to 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

protocol-id — Specifies the IP protocol to match against for the custom protocol.

Values 6, 17, Protocol numbers accepted in DHB, keywords: tcp, udp

create — Mandatory keyword used when creating custom protocol. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.261 custom-record

custom-record

Syntax [**no**] **custom-record**

Context **[Tree]** (config>subscr-mgmt>acct-plcy custom-record)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record

Description Commands in this context configure the layout and setting for a custom accounting record associated with this accounting policy.

The **no** form of this command reverts the configured values to the defaults.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

custom-record

Syntax [**no**] **custom-record**

Context **[Tree]** (config>log>acct-policy custom-record)

Full Context configure log accounting-policy custom-record

Description Commands in this context configure the layout and setting for a custom accounting record associated with this accounting policy.

The **no** form of this command reverts the configured values to the defaults.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7.262 custom-x-header

custom-x-header

Syntax **custom-x-header** *x-header-name*
no custom-x-header

Context **[Tree]** (config>app-assure>group>url-filter>icap custom-x-header)

Full Context configure application-assurance group url-filter icap custom-x-header

Description This command configures the url-filter ICAP policy to include a new x-header field; the content of the x-header is populated based on AQP url-filter action which can optionally specify the ASO characteristic value to include in the x-header.

Default no custom-x-header

Parameters *x-header-name* — Specifies the name of the x-header added to the ICAP request.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

7.263 customer

customer

Syntax **customer** *customer-id* [**create**] [**name** *name*]
no customer *customer-id*

Context **[Tree]** (config>service customer)

Full Context configure service customer

Description This command creates a customer ID and customer context used to associate information with a particular customer. Services can later be associated with this customer at the service level.

Each *customer-id* must be unique. The **create** keyword must follow each new **customer** *customer-id* entry.

Enter an existing **customer** *customer-id* (without the *create* keyword) to edit the customer's parameters.

An optional customer **name** can be specified and is tied to the **customer-name** in the customer context (setting either **customer-name** or **name** will cause the other to change as well).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes a *customer-id* and all associated information. Before removing a *customer-id*, all references to that customer in all services must be deleted or changed to a different customer ID.

Default customer 1 always exists on the system and cannot be deleted.

Parameters *customer-id* — Specifies the ID number to be associated with the customer, expressed as an integer.

Values *customer-id*: 1 to 2147483647
customer-name: 64 characters maximum

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the **create** keyword.

name *name* — This parameter configures an optional customer name, up to 64 characters in length, which adds a name identifier to a given customer to then use that customer name in configuration references as well as display and use customer names in show commands throughout the system. This helps the service provider/ administrator to identify and manage services within the SR OS platforms.

All services are required to assign a customer ID to initially create a customer. However, either the customer ID or the customer name can be used to identify and reference a given customer once it is initially created.

If a name is not specified at creation time, then SR OS assigns a string version of the *customer-id* as the name.

Values *name*: 64 characters maximum

Platforms All

7.264 customer-id-range

customer-id-range

Syntax **customer-id-range start** *customer-id* **end** *customer-id*
no customer-id-range

Context **[Tree]** (config>service>md-auto-id customer-id-range)

Full Context configure service md-auto-id customer-id-range

Description This command specifies the range of IDs used by SR OS to automatically assign an ID to customers that are created in model-driven interfaces without an ID explicitly specified by the user or client.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A customer created with an explicitly-specified ID cannot use an ID in this range. In the classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed, which causes any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **config>service md-auto-id** command for further details.

Default no customer-id-range

Parameters **start** *customer-id* — Specifies the lower value of the ID range. The value must be less than or equal to the **end** value.

Values 2 to 2147483647

end *customer-id* — Specifies the upper value of the ID range. The value must be greater than or equal to the **start** value.

Values 2 to 2147483647

Platforms All

7.265 cut-through-packets

cut-through-packets

Syntax **cut-through-packets** *cut-through-packets*

Context **[Tree]** (debug>app-assure>group>traffic-capture>record cut-through-packets)

Full Context debug application-assurance group traffic-capture record cut-through-packets

Description This command records cut-through packet conditions.

Parameters *cut-through-packets* — Indicates whether to capture cut-through only packets or cut-through and other packets, or to exclude them all together.

Values exclude, include, only

Default include

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8 d Commands

8.1 d-path-length-ignore

d-path-length-ignore

Syntax [**no**] **d-path-length-ignore**

Context **[Tree]** (config>router>bgp>path-selection d-path-length-ignore)
[Tree] (config>service>vprn>bgp>path-selection d-path-length-ignore)
[Tree] (config>service>vprn d-path-length-ignore)

Full Context configure router bgp best-path-selection d-path-length-ignore
configure service vprn bgp best-path-selection d-path-length-ignore
configure service vprn d-path-length-ignore

Description This command enables and disables the ability of the router to ignore D-PATH domain segment length during best-path selection. At the base router level (or **vprn**>**bgp** level for PE-CE routers), this command allows BGP to ignore the D-PATH domain segment length for best-path selection purposes. The D-PATH length is ignored when comparing two VPN routes or two IFL routes within the same RD. However, these VPN/IFL routes are processed in Main-BGP instance.

At the VPRN router level, this command allows the VPRN RTM to ignore the D-PATH domain segment length for best path selection purposes (for routes in VPRN). The user can control whether the D-PATH length is considered when two VPN routes with different RDs are compared.

Best-path selection for EVPN-IFF routes against other owners (for example, EVPN-IFL or IPVPN) still relies on RTM preference. When EVPN-IFF RTM preference matches the RTM preference of another BGP owner, the existing RTM selection applies and D-PATH is not considered, irrespective of the **d-path-length-ignore** configuration.

The **no** form of this command disables the ability to ignore the D-PATH domain segment length.

Default no d-path-length-ignore

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.2 dack-timeout

dack-timeout

Syntax **dack-timeout** *dack-timeout*
no dack-timeout

Context **[Tree]** (config>app-assure>group>tcp-optimizer dack-timeout)

Full Context configure application-assurance group tcp-optimizer dack-timeout

Description This command configures a delayed ACK (DACK) timeout for the TCP optimizer. By entering this command a default of 200 ms timeout is enabled for delayed acknowledgment. This value is not configurable.

The **no** form of this command disables the delayed acknowledgment timeout.

Default no dack-timeout

Parameters *dack-timeout* — Specifies the delayed acknowledgment timeout in ms.

Default 200

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.3 dad-disable

dad-disable

Syntax [**no**] **dad-disable**

Context **[Tree]** (config>router>if>ipv6 dad-disable)
[Tree] (config>service>ies>if>ipv6 dad-disable)
[Tree] (config>service>vprn>if>ipv6 dad-disable)

Full Context configure router interface ipv6 dad-disable
configure service ies interface ipv6 dad-disable
configure service vprn interface ipv6 dad-disable

Description This command disables duplicate address detection (DAD) on a per-interface basis. This prevents the router from performing a DAD check on the interface. All IPv6 addresses of an interface with DAD disabled, immediately enter a preferred state, without checking for uniqueness on the interface. This is useful for interfaces which enter a looped state during troubleshooting and operationally disable themselves when the loop is detected, requiring manual intervention to clear the DAD violation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command turns off **dad-disable** on the interface.

Default no dad-disable

Platforms All

8.4 dad-snooping

dad-snooping

Syntax [**no**] **dad-snooping**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>nd dad-snooping)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>nd dad-snooping)

Full Context configure service ies subscriber-interface group-interface ipv6 nd dad-snooping
configure service vprn subscriber-interface group-interface ipv6 nd dad-snooping

Description This command allows the router to populate the neighbor discovery table through snooping subscribers' duplicate address detection messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.5 damp-peer-oscillations

damp-peer-oscillations

Syntax **damp-peer-oscillations** [**idle-hold-time** *initial-wait second-wait max-wait*] [**error-interval** *minutes*]

Context **[Tree]** (config>service>vprn>bgp damp-peer-oscillations)
[Tree] (config>service>vprn>bgp>group damp-peer-oscillations)
[Tree] (config>service>vprn>bgp>group>neighbor damp-peer-oscillations)

Full Context configure service vprn bgp damp-peer-oscillations
configure service vprn bgp group damp-peer-oscillations
configure service vprn bgp group neighbor damp-peer-oscillations

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls how long a BGP peer session remains in the idle-state after some type of error causes the session to reset. In the idle state, BGP does not initiate or respond to attempts to establish a new session. Repeated errors that occur a short while after each session reset cause longer and longer hold times in the idle state. This command supports the DampPeerOscillations FSM behavior described in section 8.1 of RFC 4271, *A Border Gateway Protocol 4 (BGP-4).*

The default behavior, which applies when no damp-peer-oscillations is configured, is to immediately transition out of the idle-state after every reset.

Default no damp-peer-oscillations

Parameters *initial-wait* — Specifies the amount of time, in minutes, that a session remains in the idle-state after it has been stable for a while.

Values 0 to 2048

Default 0

second-wait — Specifies the period of time, in minutes, that is doubled after each repeated session failure that occurs within a relatively short span of time.

Values 0 to 2048

Default 5

max-wait — Specifies the maximum amount of time, in minutes, that a session remains in the idle-state after it has experienced repeated instability.

Values 0 to 2048

Default 60

minutes — Specifies the interval of time, in minutes after a session reset, during which the session must be error-free in order to reset the penalty counter and return to idle-hold-time to initial-wait.

Values 0 to 2048

Default 30

Platforms All

damp-peer-oscillations

Syntax **damp-peer-oscillations** [**idle-hold-time** *initial-wait second-wait max-wait*] [**error-interval** *minutes*]

Context **[Tree]** (config>router>bgp damp-peer-oscillations)
[Tree] (config>router>bgp>group damp-peer-oscillations)
[Tree] (config>router>bgp>group>neighbor damp-peer-oscillations)

Full Context configure router bgp damp-peer-oscillations
configure router bgp group damp-peer-oscillations
configure router bgp group neighbor damp-peer-oscillations

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls how long a BGP peer session remains in the idle-state after some type of error causes the session to reset. In the idle state, BGP does not initiate or respond to attempts to establish a new session. Repeated errors that occur a short while after each session reset cause longer and longer hold times in the idle state. This command supports the DampPeerOscillations FSM behavior described in section 8.1 of RFC 4271, *A Border Gateway Protocol 4 (BGP-4).*

The default behavior, which applies when no damp-peer-oscillations is configured, is to immediately transition out of the idle-state after every reset.

Default no damp-peer-oscillations

Parameters *initial-wait* — The amount of time, in minutes, that a session remains in the idle-state after it has been stable for a while.

Values 0 to 2048

Default 0

second-wait — A period of time, in minutes, that is doubled after each repeated session failure that occurs within a relatively short span of time.

Values 1 to 2048

Default 5

max-wait — The maximum amount of time, in minutes, that a session remains in the idle-state after it has experienced repeated instability.

Values 1 to 2048

Default 60

minutes — The interval of time, in minutes after a session reset, during which the session must be error-free in order to reset the penalty counter and return from idle-hold-time to initial-wait.

Values 0 to 2048

Default 30

Platforms All

8.6 dampening

dampening

Syntax **dampening**

Context **[Tree]** (config>port>ethernet dampening)

Full Context configure port ethernet dampening

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure exponential port dampening for an Ethernet port.

Exponential Port Dampening (EPD) reduces the number of physical link transitions reported to upper layer protocols, potentially reducing upper layer protocol churn caused by a faulty link. Penalties are added against a port whenever the port's physical link state transitions from a link up state to a link down state. When the penalties exceed a configurable threshold, port-up and port-down transitions are no longer advertised to upper layers and the port's operational state will remain down until the penalty amount drops below a configurable reuse threshold. Each transition of link up state to link down state increments the accumulated penalty value by 1000. The accumulated penalties for a port are reduced at an exponential decay rate according to a configurable half-life parameter.

Platforms All

8.7 damping

damping

Syntax [**no**] **damping**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy damping)

Full Context configure subscriber-mgmt bgp-peering-policy damping

Description This command enables BGP route damping for learned routes which are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route the policy definition.

The **no** form of this command used at the global level disables route damping.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

Half-life:	15 minutes
Max-suppress:	60 minutes
Suppress-threshold:	3000
Reuse-threshold	750

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

damping

Syntax [**no**] **damping**

Context **[Tree]** (config>service>vprn>bgp damping)
[Tree] (config>service>vprn>bgp>group damping)
[Tree] (config>service>vprn>bgp>group>neighbor damping)

Full Context configure service vprn bgp damping
configure service vprn bgp group damping
configure service vprn bgp group neighbor damping

Description This command enables BGP route damping for learned routes which are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route policy definition.

The **no** form of this command used at the global level disables route damping.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

Half-life: 15 minutes

Max-suppress: 60 minutes

Suppress-threshold: 3000

Reuse-threshold: 750

Default no damping — Learned route damping is disabled.

Platforms All

damping

Syntax [**no**] **damping**

Context **[Tree]** (config>router>bgp damping)
[Tree] (config>router>bgp>group damping)
[Tree] (config>router>bgp>group>neighbor damping)

Full Context configure router bgp damping
configure router bgp group damping

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group neighbor damping

Description This command enables BGP route damping for learned routes which are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route policy definition.

The **no** form of this command used at the global level reverts route damping.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

- Half-life: 15 minutes
- Max-suppress: 60 minutes
- Suppress-threshold: 3000
- Reuse-threshold: 750

Default no damping

Platforms All

damping

Syntax [**no**] **damping** *name*

Context **[Tree]** (config>router>policy-options damping)

Full Context configure router policy-options damping

Description This command creates a context to configure a route damping profile to use in route policy entries.

The **no** form of this command deletes the named route damping profile.

Default no damping

Parameters *name* — Specifies the damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

damping

Syntax **damping** {*name* | **none**}
no damping

Context **[Tree]** (config>router>policy-options>policy-statement>default-action damping)
[Tree] (config>router>policy-options>policy-statement>entry>action damping)

Full Context configure router policy-options policy-statement default-action damping
configure router policy-options policy-statement entry action damping

Description This command configures a damping profile used for routes matching the route policy statement entry.

If no damping criteria is specified, the default damping profile is used.

The **no** form of this command removes the damping profile associated with the route policy entry.

Default no damping

Parameters *name* — The damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end"," @variable@end", or "start@variable@".

The *name* specified must already be defined.

none — Disables route damping for the route policy.

Platforms All

8.8 data

data

Syntax **data** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no data

Context **[Tree]** (debug>router>pim data)

Full Context debug router pim data

Description This command enables debugging for PIM data exception.

The **no** form of this command disables PIM data exception debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *grp-ip-address* — Debugs information associated with the specified data exception.

Values multicast group address (ipv4, ipv6)

ip-address — Debugs information associated with the specified data exception.

Values source address (ipv4, ipv6)

detail — Debugs detailed IP data exception information.

Platforms All

8.9 data-bearer

data-bearer

Syntax [**no**] **data-bearer** *data-bearer-id*

Context **[Tree]** (config>router>lmp>te-link data-bearer)

Full Context configure router lmp te-link data-bearer

Description This command creates a data bearer assigned to a TE Link. Only one data bearer may be configured within a given TE Link.

Default no data-bearer

Parameters *data-bearer-id* — Specifies the ID of the data bearer.

Values 1 to 4294967295

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.10 data-delay-interval

data-delay-interval

Syntax **data-delay-interval** *seconds*
no data-delay-interval

Context **[Tree]** (config>service>vpls>provider-tunnel>inclusive data-delay-interval)

Full Context configure service vpls provider-tunnel inclusive data-delay-interval

Description This command configures the I-PMSI data delay timer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This delay timer is intended to allow time for the RSVP control plane to signal and bring up the S2L sub-LSP to each destination PE participating in the VPLS/B-VPLS service. The delay timer is started as soon as the P2MP LSP instance becomes operationally up after the user performed a 'no shutdown' under the inclusive node, i.e., as soon as the first S2L sub-LSP is up. In general, it is started when the P2MP LSP instance transitions from the operationally down state to the up state.

For a mLDP P2MP LSP, the delay timer is started as soon as the P2MP FEC corresponding to the I-PMSI is resolved and installed at the root node. The user must factor in the value configured in the data-delay-interval at the root node any delay configured in IGP-LDP sync timer (**config**>**router**>**if**>**ldp-sync-timer**) on interfaces over the network. This is because the mLDP P2MP LSP may move to a different interface at the expiry of this timer since the routing upstream of the LDP Label Mapping message may change when this timer expires and the interface metric is restored.

At the expiry of this timer, the VPLS/B-VPLS will begin forwarding of BUM packets over the P2MP LSP instance even if not all the S2L paths are up.

The **no** version of this command re-instates the default value for this delay timer.

Parameters *seconds* — Specifies the delay time value in seconds

Values 3 to 180

Default 15

Platforms All

data-delay-interval

Syntax **data-delay-interval** *value*
no data-delay-interval

Context **[Tree]** (config>service>vprn>mvpn>pt>selective data-delay-interval)

Full Context configure service vprn mvpn provider-tunnel selective data-delay-interval

Description This command specifies the interval, in seconds, before a PE router connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.

This command is not applicable to multi-stream S-PMSI.

The **no** form of this command reverts the value to the default.

Default data-delay-interval 3

Parameters *value* — Specifies the data delay interval, in seconds.

Values 3 to 180

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

data-delay-interval

Syntax **data-delay-interval** *value*
no data-delay-interval

Context **[Tree]** (config>router>gtm>provider-tunnel>selective data-delay-interval)

Full Context configure router gtm provider-tunnel selective data-delay-interval

Description This command specifies the interval, in seconds, before a PBR connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.

This command is not applicable to multi-stream S-PMSIs.

The **no** form of this command reverts the value to the default.

Default data-delay-interval 3

Parameters *value* — Specifies the data delay interval, in seconds.

Values 3 to 180

Default 3

Platforms All

8.11 data-encapsulation

data-encapsulation

Syntax [**no**] **data-encapsulation**

Context **[Tree]** (config>service>vprn>msdp data-encapsulation)

Full Context configure service vprn msdp data-encapsulation

Description This command configures a rendezvous point (RP) using Multicast Source Discovery Protocol (MSDP) to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages.

Default data-encapsulation

Platforms All

data-encapsulation

Syntax [**no**] **data-encapsulation**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>msdp data-encapsulation)

Full Context configure router msdp data-encapsulation

Description This command configures a rendezvous point (RP) using Multicast Source Discovery Protocol (MSDP) to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages.

Default data-encapsulation

Platforms All

8.12 data-threshold

data-threshold

Syntax **data-threshold** {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*} *s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
data-threshold *c-grp-ipv6-addr/prefix-length s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
no data-threshold {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}
no data-threshold *c-grp-ipv6-addr/prefix-length*

Context [Tree] (config>service>vprn>mvpn>pt>selective data-threshold)

Full Context configure service vprn mvpn provider-tunnel selective data-threshold

Description This command specifies the data rate threshold that triggers the switch from the inclusive provider tunnel to the selective provider tunnel for (C-S, C-G) within the group range. Optionally, PE thresholds for creating/deleting ng-MVPN S-PMSI may also be specified. Omitting the PE thresholds, preserves the currently set value (or defaults if never set). Multiple statements (one per a unique group) are allowed in the configuration.

This command is not applicable to multi-stream S-PMSI.

The **no** form of this command removes the values from the configuration.

Default no data-threshold

Parameters *group-address/mask* — Specifies a multicast group address and netmask length.

c-grp-ip-addr/mask | *c-grp-ip-addr netmask* — Specifies an IPv4 multicast group address and netmask length or network mask.

c-grp-ipv6-addr/prefix-length — Specifies an IPv6 multicast group address and prefix length.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

s-pmsi-threshold — Specifies the rate, in kb/s. If the rate for a (C-S, C-G)) within the specified group range exceeds the threshold, traffic for the (C-S, C-G) is switched to the selective provider tunnel. Threshold 0 is supported. When threshold 0 is configured, the (C-S, C-G) switches to S-PMSI as soon as it is learned in the MVPN and without traffic flowing for that (C-S, C-G).

s-pmsi-threshold-add — Specifies the number of receiver PEs for creating S-PMSI. When the number of receiver PEs for a given multicast group configuration is non-zero and below the threshold and BW threshold is satisfied, S-PMSI is created.

s-pmsi-threshold-delete — Specifies the number of receiver PEs for deleting S-PMSI. When the number of receiver PEs for a given multicast group configuration is above the threshold, S-PMSI is deleted and the multicast group is moved to I-PMSI or a wildcard S-PMSI. It is recommended that the delete threshold be significantly larger than the add threshold, to avoid re-signaling of S-PMSI as the receiver PE count fluctuates.

Values

c-grp-ip-addr	: multicast group address a.b.c.d
mask	[4 to 32]
netmask	: a.b.c.d (network bits all 1 and host bits all 0)
s-pmsi-threshold	: [0 to 4294967294] (threshold in kb/s)
c-grp-ipv6-addr	: multicast ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D prefix-length [1 to 128]
pe-threshold-add:	[1 to 65535], if never specified, 65535 is used (add threshold always met)
pe-threshold-delete:	[2 to 65535], if never specified, 65535 is used (delete threshold never met)

Platforms All

data-threshold

Syntax **data-threshold** {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*} *s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
data-threshold *c-grp-ipv6-addr/prefix-length s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
no data-threshold {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}
no data-threshold *c-grp-ipv6-addr/prefix-length*

Context **[Tree]** (config>router>gtm>provider-tunnel>selective data-threshold)

Full Context configure router gtm provider-tunnel selective data-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the data rate threshold that triggers the switch from the inclusive provider tunnel to the selective provider tunnel for (C-S, C-G) within the group range. Optionally, PBR thresholds for creating or deleting NG-MVPN S-PMSI may also be specified. Omitting the PBR thresholds preserves currently set values (or defaults if never set). Multiple statements (one per a unique group) are allowed in the configuration.

This command is not applicable to multi-stream S-PMSIs.

The **no** form of this command removes the values from the configuration.

Default no data-threshold

Parameters *c-grp-ip-addr*/*mask* | *c-grp-ip-addr netmask* — Specifies an IPv4 multicast group address and netmask length or network mask.

Values mask: 4 to 32

c-grp-ipv6-addr/*prefix-length* — Specifies an IPv6 multicast group address and prefix length.

s-pmsi-threshold — Specifies the rate, in kb/s. If the rate for a (C-S, C-G) within the specified group range exceeds the threshold, traffic for the (C-S, C-G) will be switched to the selective provider tunnel.

s-pmsi-threshold-add — Specifies the number of receiver PBRs for creating S-PMSI. When the number of receiver PBRs for a given multicast group configuration is non-zero and below the threshold and BW threshold is satisfied, S-PMSI is created.

s-pmsi-threshold-delete — Specifies the number of receiver PBRs for deleting S-PMSI. When the number of receiver PBRs for a given multicast group configuration is above the threshold, S-PMSI is deleted and the multicast group is moved to I-PMSI or a wildcard S-PMSI. It is recommended that the delete threshold be significantly larger than the add threshold to avoid re-signaling of S-PMSI as the receiver PBR count fluctuates.

Values

c-grp-ip-addr	multicast group address a.b.c.d
mask	4 to 32
netmask	a.b.c.d (network bits all 1 and host bits all 0)
s-pmsi-threshold	1 to 4294967294 (threshold in kb/s)
c-grp-ipv6-addr	multicast ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D prefix-length [1 to 128]
pe-threshold-add	1 to 65535 Default: 65535 (delete threshold always met)
pe-threshold-delete	2 to 65535 Default: 65535:(delete threshold always met)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.13 data-tlv-size

data-tlv-size

Syntax **data-tlv-size** *octets*
no data-tlv-size

Context **[Tree]** (config>oam-pm>session>ethernet>slm data-tlv-size)
[Tree] (config>oam-pm>session>ethernet>dmm data-tlv-size)

Full Context configure oam-pm session ethernet dmm data-tlv-size
configure oam-pm session ethernet slm data-tlv-size

Description This command allows the operator to add an optional Data TLV to PDU and increase the frame on the wire by the specified amount. Note that this command only configures the size of the padding added to the PDU, and does not configure the total size of the frame on the wire.

The **no** form of this command removes the optional TLV.

Parameters *octets* — Specifies the size, in octets, of the optional Data TLV.

Values 0, 3 to 2000

Default 0

Platforms All

8.14 data-trigger

data-trigger

Syntax **data-trigger**

Context **[Tree]** (config>service>vprn>sub-if>grp-if data-trigger)
[Tree] (config>service>ies>sub-if>grp-if data-trigger)

Full Context configure service ies subscriber-interface group-interface data-trigger
configure service vprn subscriber-interface group-interface data-trigger

Description Commands in this context configure data-triggered subscriber management entities.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.15 data-triggered

data-triggered

Syntax [**no**] data-triggered

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host-mgmt>mac-learning-options data-triggered)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host-mgmt>mac-learning-options data-triggered)

Full Context configure service ies subscriber-interface group-interface sap static-host-mgmt mac-learning-options data-triggered
configure service vprn subscriber-interface group-interface sap static-host-mgmt mac-learning-options data-triggered

Description This command enables learning of MAC addresses from data packets.

The **no** form of this command disables learning of MAC addresses from data packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

data-triggered

Syntax [**no**] **data-triggered**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state data-triggered)

Full Context configure subscriber-mgmt wlan-gw ue-query state data-triggered

Description This command enables matching on UEs currently in a data-triggered state. This query only filters UEs that are currently authenticating due to a data trigger, not UEs that were originally authenticated due to data trigger, such as those in an ESM, DSM, or portal state.

The **no** form of this command disables matching on UEs in a data-triggered state, unless all state matching is disabled.

Default no data-triggered

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.16 data-triggered-ue-creation

data-triggered-ue-creation

Syntax [**no**] **data-triggered-ue-creation**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range data-triggered-ue-creation)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range data-triggered-ue-creation)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range data-triggered-ue-creation
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range data-triggered-ue-creation

Description This command enables data-triggered subscriber creation for WIFI subscribers. Data-triggered UE creation is currently only supported for UDP and TCP packets.

The **no** form of this command disables the data-triggered subscriber creation for WIFI subscribers.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.17 data-triggers

data-triggers

Syntax [**no**] **data-triggers**

Context **[Tree]** (debug>dynsvc data-triggers)

Full Context debug dynamic-services data-triggers

Description Commands in this context configure dynamic services data trigger capture SAP debugging. The **no** form of this command removes all dynamic services data trigger capture SAP debug configurations.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.18 database

database

Syntax **database** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no database

Context **[Tree]** (debug>service>id>pim-snooping database)

Full Context debug service id pim-snooping database

Description This command enables or disables debugging for the PIM database.

Parameters *grp-ip-address* — Debugs information associated with all PIM modules

Values multicast group address (IPv4 or IPv6) or zero

ip-address — Debugs information associated with the specified database

Platforms All

8.19 database-export

database-export

Syntax **database-export** [**identifier** *id*] [**bgp-ls-identifier** *bgp-ls-id*]
no database-export

Context **[Tree]** (config>router>isis database-export)

Full Context configure router isis database-export

Description This command enables the population of the extended TE Database (TE-DB) with the link-state information from a given IGP instance.

The extended TE-DB is used as a central point for importing all link-state information, link, node, and prefix, from IGP instances on the router or the vSROS controller of the NSP and to exporting it to BGP-LS on the router and to Java-VM proxy on the vSROS controller. This information includes the IGP, TE, and the SR information, prefix SID sub-TLV, adjacency SID sub-TLV, and router SR capability TLV.

The **no** form of this command disables database exportation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **identifier** — This parameter is used to uniquely identify the IGP instance in the BGP-LS NLRI when a router has interfaces participating in multiple IGP instances. This parameter defaults to the IGP instance ID assigned by SR OS. However, given that the concept of instance ID defined in IS-IS (RFC 6822) is unique within a routing domain while the one specified for OSPF is local subnet significant (RFC 6549), the user can remove any overlap by configuring the new **identifier** value to be unique within a given IGP domain when this router sends the IGP link-state information using BGP-LS.

id — Specifies an entry ID to export.

Values 0 to 18446744073709551615

bgp-ls-identifier — This parameter is used, along with the Autonomous System Number (ASN) to correlate the BGP-LS NLRI advertisements of multiples BGP-LS speakers of the same IGP domain. If an NRC-P network domain has multiple IGP domains, BGP-LS speakers within each IGP domain must be configured with the same unique {bgp-ls-identifier, asn} tuple.

The BGP-LS identifier is optional and is only sent in a BGP-LS NLRI if configured in the IGP instance of an IGP domain.

Note that if this IGP instance participates in traffic engineering with RSVP-TE or SR-TE, the **traffic-engineering** option is not strictly required because enabling the extended TE-DB populates this information automatically. It is, however, recommended to enable it to make the configuration consistent with other routers in the network that do not require the enabling of the extended TE-DB.

bgp-ls-id — Specifies a BGP LS ID to export.

Values 0 to 4294967295

Platforms All

database-export

Syntax **database-export** [**identifier** *id*] [**bgp-ls-identifier** *bgp-ls-id*]
no database-export

Context **[Tree]** (config>router>ospf database-export)
[Tree] (config>router>ospf3 database-export)

Full Context configure router ospf database-export
configure router ospf3 database-export

Description This command enables the population of the extended TE Database (TE-DB) with the link-state information from a given IGP instance.

The extended TE-DB is used as a central point for importing all link-state information, link, node, and prefix, from IGP instances on the router or the vSROS controller of the NSP and to exporting it to BGP-LS on the router and to Java-VM proxy on the vSROS controller. This information includes the IGP, TE, and the SR information, prefix SID sub-TLV, adjacency SID sub-TLV, and router SR capability TLV.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables database exportation.

Default no database-export

Parameters **identifier** — Identifies the IGP instance in the BGP-LS NLRI when a router has interfaces participating in multiple IGP instances. This parameter defaults to the IGP instance ID assigned by SR OS. The concept of instance ID specified for OSPF is local subnet significant (RFC 6549). The user can remove router specific overlap by configuring the new **identifier** value to be unique within a given IGP domain when this router sends the IGP link-state information using BGP-LS.

id — Specifies an entry ID to export.

Values 0 to 18446744073709551615

bgp-ls-identifier — This parameter is used, along with the Autonomous System Number (ASN), to correlate the BGP-LS NLRI advertisements of multiples BGP-LS speakers of the same IGP domain. If an NRC-P network domain has multiple IGP domains, BGP-LS speakers within each IGP domain must be configured with the same unique {bgp-ls-identifier, asn} tuple.

The BGP-LS identifier is optional and is only sent in a BGP-LS NLRI if configured in the IGP instance of an IGP domain.

Note that if this IGP instance participates in traffic engineering with RSVP-TE or SR-TE, the **traffic-engineering** option is not strictly required because enabling the extended TE-DB populates this information automatically. It is, however, recommended to enable it to make the configuration consistent with other routers in the network that do not require the enabling of the extended TE-DB.

bgp-ls-id — Specifies a BGP LS ID to export.

Values 0 to 4294967295

Platforms All

8.20 database-export-exclude

database-export-exclude

Syntax [**no**] **database-export-exclude**

Context **[Tree]** (config>router>isis>level database-export-exclude)

Full Context configure router isis level database-export-exclude

Description This command allows the user to prune the IGP link-state information of a specific IS-IS level from being exported into the extended TE-DB.

The no form of this command returns to the default behavior inherited from the database-export command at the IS-IS instance level.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

database-export-exclude

Syntax [**no**] **database-export-exclude**

Context **[Tree]** (config>router>ospf>area database-export-exclude)

Full Context configure router ospf area database-export-exclude

Description This command allows the user to prune the IGP link-state information of a specific OSPF level or OSPF area from being exported into the extended TE-DB. The **no** form of this command returns to the default behavior inherited from the database-export command at the IS-IS or OSPF instance level.

Default no database-export-exclude

Platforms All

8.21 datapath-cpu-high-wmark

datapath-cpu-high-wmark

Syntax **datapath-cpu-high-wmark** *high-watermark*
datapath-cpu-high-wmark max

Context **[Tree]** (config>app-assure datapath-cpu-high-wmark)

Full Context configure application-assurance datapath-cpu-high-wmark

Description This command configures the system-wide high watermark threshold as a percentage of the per-ISA datapath core CPU utilization, where an alarm will be raised by the agent. CPU usage is the average usage across all datapath cores.

Default datapath-cpu-high-wmark 95

Parameters *high-watermark* — Specifies the high watermark for datapath CPU usage alarms.

Values 1 to 100

max — Disables the high watermark for datapath CPU usage alarms

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.22 datapath-cpu-low-wmark

datapath-cpu-low-wmark

Syntax **datapath-cpu-low-wmark** *low-watermark*

Context **[Tree]** (config>app-assure datapath-cpu-low-wmark)

Full Context configure application-assurance datapath-cpu-low-wmark

Description This command configures the system-wide low watermark threshold as a percentage of the per-ISA datapath core CPU utilization, where an alarm will be raised by the agent. CPU usage is the average usage across all datapath cores.

Default datapath-cpu-low-wmark 90

Parameters *low-watermark* — Specifies the low watermark for datapath CPU usage alarms.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.23 day-of-month

day-of-month

Syntax **day-of-month** {*day-number* [..*day-number*] **all**}
no day-of-month

Context **[Tree]** (config>system>cron>sched day-of-month)

Full Context configure system cron schedule day-of-month

Description This command specifies which days of the month that the schedule will occur. Multiple days of the month can be specified. When multiple days are configured, each of them will cause the schedule to trigger. If a day-of-month is configured without configuring month, weekday, hour, and minute, the event will not execute.

Using the **weekday** command as well as the **day-of-month** command will cause the script to run twice. For example, consider that today is Monday January 1. If Tuesday January 5 is configured, the script will run on Tuesday (tomorrow) as well as January 5 (Friday).

The **no** form of this command removes the specified day-of-month from the list.

Default no day-of-month

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *day-number* — Specifies the positive integers specify the day of the month counting from the first of the month. The negative integers specify the day of the month counting from the last day of the month. For example, configuring **day-of-month -5, 5** in a month that has 31 days will specify the schedule to occur on the 27th and 5th of that month.

Integer values must map to a valid day for the month in question. For example, February 30 is not a valid date.

Values 1 to 31, -31 to -1 (maximum 62 day-numbers)

all — Specifies all days of the month.

Platforms All

8.24 db

db

Syntax **db** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no db

Context **[Tree]** (debug>router>pim db)

Full Context debug router pim db

Description This command enables debugging for PIM database.

The **no** form of this command disables PIM database debugging.

Parameters *grp-ip-address* — Debugs information associated with the specified database.

Values multicast group address (ipv4, ipv6) or zero

ip-address — Debugs information associated with the specified database.

Values source address (ipv4, ipv6)

detail — Debugs detailed IP database information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.25 dbw-accounting

dbw-accounting

Syntax [**no**] **dbw-accounting**

Context **[Tree]** (config>router>rsvp dbw-accounting)

Full Context configure router rsvp dbw-accounting

Description This command enables dark bandwidth accounting and enters the context to configure the associated parameters. When dark bandwidth accounting is enabled, the system polls the dark bandwidth counters, performs sample and average rate computations, and generates IGP-TE updates if required. To enable dark bandwidth accounting, auxiliary MPLS statistics must first be enabled using the command **config>router>mpls>aux-stats**.

The **no** form of this command disables dark bandwidth accounting, resets all global parameters to their default values, and results in an immediate IGP-TE update for which dark bandwidth is null.

Default no dbw-accounting

8.26 dbw-down-threshold

dbw-down-threshold

Syntax **dbw-down-threshold** *percent-change* [**bw** *absolute-change*]
no dbw-down-threshold

Context **[Tree]** (config>router>rsvp>interface dbw-down-threshold)

Full Context configure router rsvp interface dbw-down-threshold

Description This command sets the minimum change (in percent of the latest advertised value) above which an decrease in MRLB (IS-IS TE sub-TLV 10) or MRB (OSPF TE sub-TLV 7) triggers an IGP-TE update. This configuration only applies to a change in MRLB or MRB caused by dark bandwidth. Other events affecting MRLB/MRB (such as the change of the subscription factor or the loss of link in a LAG over which the RSVP interface is defined) trigger an immediate TE update, regardless of the importance of the impact.

Optionally, the threshold can also be expressed as an absolute value. In this case, the evaluation of the change is made using the percent change and the absolute change. An IGP-TE update is sent if both thresholds are crossed. Changing this parameter in the course of dark bandwidth accounting does not affect the accounting cycle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, the multiplier inherits the global value, unless it is specifically set using this command. The **no** form of this command sets this parameter to inherit the value of the corresponding global parameter.

Parameters *percent-change* — Specifies the minimum decrease in MRLB/MRB, expressed in percent.

Values 0 to 100

absolute-change — Specifies the minimum decrease in MRLB/MRB, expressed in Mb/s.

Values 0 to 1000000

8.27 dbw-multiplier

dbw-multiplier

Syntax **dbw-multiplier** *percent*

Context **[Tree]** (config>router>rsvp>dbw-accounting dbw-multiplier)

Full Context configure router rsvp dbw-accounting dbw-multiplier

Description This command sets the dark bandwidth multiplier to the specified value. Choosing 0% will lead to no IGP-TE updates based on dark bandwidth evolution being sent. Changing this parameter in the course of dark bandwidth accounting does not affect the accounting cycle.

Default dbw-multiplier 100

Parameters *percent* — Specifies the multiplier, expressed in percent.

Values 0 to 1000

dbw-multiplier

Syntax **dbw-multiplier** *percent*
no dbw-multiplier

Context **[Tree]** (config>router>rsvp>interface dbw-multiplier)

Full Context configure router rsvp interface dbw-multiplier

Description This command sets the dark bandwidth multiplier to the specified value. Choosing 0% will lead to no IGP-TE updates based on dark bandwidth evolution being sent. Changing this parameter in the course of dark bandwidth accounting does not affect the accounting cycle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, the multiplier inherits the global value, unless it is specifically set using this command. The **no** form of this command sets this parameter to inherit the value of the corresponding global parameter.

Parameters *percent* — Specifies the multiplier, expressed in percent.

Values 0 to 1000

8.28 dbw-up-threshold

dbw-up-threshold

Syntax **dbw-up-threshold** *percent-change* [**bw** *absolute-change*]
no dbw-up-threshold

Context **[Tree]** (config>router>rsvp>interface dbw-up-threshold)

Full Context configure router rsvp interface dbw-up-threshold

Description This command sets the minimum change (in percent of the latest advertised value) above which an increase in MRLB (IS-IS TE sub-TLV 10) or MRB (OSPF TE sub-TLV 7) triggers an IGP-TE update. This configuration only applies to a change in MRLB or MRB caused by dark bandwidth. Other events affecting MRLB/MRB (such as the change of the subscription factor or the loss of link in a LAG over which the RSVP interface is defined) trigger an immediate TE update, regardless of the importance of the impact.

Optionally, the threshold can also be expressed as an absolute value. In this case, the evaluation of the change uses the percent change and the absolute change. An IGP-TE update is sent if both thresholds are crossed. Changing this parameter in the course of dark bandwidth accounting does not affect the accounting cycle.

By default, the multiplier inherits the global value, unless it is specifically set using this command. The **no** form of this command sets this parameter to inherit the value of the corresponding global parameter.

Parameters *percent-change* — Specifies the minimum increase in MRLB/MRB, expressed in percent.

Values 0 to 100

absolute-change — Specifies the minimum increase in MRLB/MRB, expressed in Mb/s.

Values 0 to 1000000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.29 ddm-events

ddm-events

Syntax [**no**] **ddm-events**

Context **[Tree]** (config>port ddm-events)

Full Context configure port ddm-events

Description This command enables Digital Diagnostic Monitoring (DDM) events for the port.

The **no** form of this command disables DDM events.

Platforms All

8.30 de-1-out-profile

de-1-out-profile

Syntax [**no**] **de-1-out-profile**

Context **[Tree]** (config>qos>sap-ingress>fc de-1-out-profile)

Full Context configure qos sap-ingress fc de-1-out-profile

Description This command, when enabled on a parent forwarding class, applies a color profile mode to the packets stored in the queue associated with this forwarding class. The queue associated with the parent forwarding class must be of type **profile-mode**.

When this QoS policy is applied to the ingress of a Frame Relay VLL SAP, the system will treat the received FR frames with DE bit set as out-of-profile, regardless of their previous marking as the result of the default classification or on a match with an IP filter. It also adjusts the CIR of the ingress SAP queue to consider out-of-profile frames that were sent while the SAP queue was in the “< CIR” state of the bucket. This makes sure that the CIR of the SAP is achieved.

All received DE = 0 frames that are classified into this parent forwarding class or any of its subclasses have their profile unchanged by enabling this option. That is, the DE = 0 frame profile could be undetermined (default), in-profile, or out-of-profile as per previous classification. The DE = 0 frames that have a profile of undetermined will be evaluated by the system CIR marking algorithm and will be marked appropriately.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **priority** option, if used, has no effect. All FR VLL DE = 1 frames have their priority automatically set to low while DE = 0 frames have their priority set to high. Furthermore, DE = 1 frames have the drop-preference bit set in the internal header. The internal settings of the priority bit and of the drop-preference bit of the frame is independent of the use of the profile mode.

All other capabilities of the Fpipe service are maintained. This includes remarking of the DE bit on egress SAP, and FR PW control word on egress network port for the packets that were classified into “out-of-profile” at ingress SAP.

This **de-1-out-profile** keyword has an effect when applied to the ingress of a SAP that is part of an Fpipe service. It can also be used on the ingress of an Epipe or VPLS SAP.

The **no** form of this command disables the color profile mode of operation on all SAPs to which this ingress QoS policy is applied.

Default no de-1-out-profile

Platforms All

8.31 de-mark

de-mark

Syntax **de-mark** [**force** *de-value*]
no demark

Context **[Tree]** (config>qos>sap-egress>fc de-mark)

Full Context configure qos sap-egress fc de-mark

Description This command is used to explicitly define the marking of the DE bit for **fc** *fc-name* according to the inplus-profile/in-profile or out-of-profile/exceed-profile status of the packet (*fc-name* may be used to identify the dot1p-value).

If no DE value is present, the default values are used for the marking of the DE bit; for example, 0 for inplus-profile or in-profile packets, 1 for out-of-profile or exceed-profile packets. For more information, refer to the *IEEE 802.1ad-2005 standard*.

In the PBB case, for a Backbone SAP (B-SAP) and for packets originated from a local I-VPLS/PBB-Epipe, the command dictates the marking of the DE bit for both the BVID and ITAG.

If this command is not used, the DE bit should be preserved if an ingress TAG exist; otherwise, set to zero.

If the DE value is included in the command line, this value is to be used for all the packets of this forwarding class regardless of their profile status.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The commands **de-mark-inner** and **de-mark-outer** take precedence over the **de-mark** command if both are specified in the same policy.

Parameters *de-value* — Specifies the DE marking value.

Values 0 or 1

Platforms All

de-mark

Syntax **de-mark** [**force** *de-value*]
no de-mark

Context **[Tree]** (config>qos>network>egress>fc de-mark)

Full Context configure qos network egress fc de-mark

Description This command is used to explicitly define the marking of the DE bit for **fc** *fc-name* according to the inplus-profile or in-profile and out-of-profile or exceed-profile status of the packet (*fc-name* may be used to identify the dot1p value).

Parameters *de-value* — Specifies that this value is to be used for all the packets of this forwarding class regardless of their profile status.

If no DE value is present, the default values are used for the marking of the DE bit; that is, 0 for inplus-profile and in-profile packets, 1 for out-of-profile and exceed-profile packets. For more information, refer to the *IEEE 802.1ad-2005 standard*.

In the PBB case, use the following rules for a network port (B-SDP):

- the outer VID follows the rules for regular SDP
- for packets originating from a local I-VPLS/PBB-Epipe, this command dictates the marking of the DE bit for both the outer (link level) BVID and ITAG; if the command is not used, the DE bit is set to zero.
- for transit packets (B-SAP/B-SDP to B-SDP), the related ITAG bits are preserved, the same as for BVID.

Values 0, 1

Platforms All

8.32 de-mark-inner

de-mark-inner

Syntax **de-mark-inner** [**force** *de-value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no de-mark-inner

Context [Tree] (config>qos>sap-egress>fc de-mark-inner)

Full Context configure qos sap-egress fc de-mark-inner

Description This command is used to explicitly define the marking of the DE bit in the inner VLAN tag for **fc** *fc-name* on a QinQ SAP, according to the in- and out-of-profile status of the packet.

If no DE value is present, the default values are used for the marking of the DE bit; for example, 0 for inplus-profile or in-profile packets, 1 for out-of-profile or exceed-profile packets. For more information, refer to the *IEEE 802.1ad-2005 standard*.

If the DE value is included in the command line, this value is used for all the inner tags of packets of this forwarding class, regardless of their profile status.

This command takes precedence over the **de-mark** command if both are specified in the same policy and over the default action.

The configuration of **qinq-mark-top-only** under the SAP egress takes precedence over the use of the **de-mark-inner** in the policy. That is, the inner VLAN tag is not remarked when **qinq-mark-top-only** is configured (the marking used for the inner VLAN tag is based on the current default, which is governed by the marking of the packet received at the ingress to the system).

If no de-mark commands are used, the DE bit is preserved if an ingress inner tag exists; otherwise, set to 0.

Remarking the inner DE bit is not supported based on the profile result of egress policing.

Parameters *de-value* — Specifies the DE marking value.

Values 0 or 1

Platforms All

8.33 de-mark-outer

de-mark-outer

Syntax **de-mark-outer** [**force** *de-value*]
no de-mark-outer

Context [Tree] (config>qos>sap-egress>fc de-mark-outer)

Full Context configure qos sap-egress fc de-mark-outer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to explicitly define the marking of the DE bit in the outer or single VLAN tag on a qinq or dot1q SAP, respectively, according to the in, out, or exceed-profile status of the packet.

If no DE value is present, the default values are used for the marking of the DE bit; for example, 0 for inplus-profile/in-profile packets, 1 for out-of-profile/exceed-profile packets. For more information, refer to the *IEEE 802.1ad-2005 standard*.

If the DE value is included in the command line, this value is used for all the outer or single tags of packets of this forwarding class, regardless of their profile status.

In the PBB case, for a Backbone SAP (B-SAP) and for packets originated from a local I-VPLS/PBB-Epipe, the command dictates the marking of the DE bit for both the BVID and ITAG.

This command takes precedence over the **de-mark** command if both are specified in the same policy and over the default action.

If no de-mark commands are used, the DE bit is preserved if an ingress outer or single tag exists; otherwise, set to 0.

Parameters *de-value* — Specifies the DE marking value.

Values 0 or 1

Platforms All

8.34 dead-interval

dead-interval

Syntax **dead-interval** *seconds*
no dead-interval

Context **[Tree]** (config>service>vprn>ospf>area>if dead-interval)
[Tree] (config>service>vprn>ospf>area>virtual-link dead-interval)
[Tree] (config>service>vprn>ospf3>area>if dead-interval)
[Tree] (config>service>vprn>ospf3>area>virtual-link dead-interval)
[Tree] (config>service>vprn>ospf>area>sham-link dead-interval)

Full Context configure service vprn ospf area interface dead-interval
configure service vprn ospf area sham-link dead-interval
configure service vprn ospf area virtual-link dead-interval
configure service vprn ospf3 area interface dead-interval
configure service vprn ospf3 area virtual-link dead-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the time, in seconds, that OSPF waits before declaring a neighbor router down. If no Hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the Hello interval.

The **no** form of this command reverts to the default value.

Default dead-interval 40

Special Cases **OSPF Interface —** If the configured **dead-interval** applies to an interface, then all nodes on the subnet must have the same dead interval.

Virtual Link — If the configured **dead-interval** applies to a virtual link, then the interval on both termination points of the virtual link must have the same dead interval.

Sham-link — If the configured **dead-interval** applies to a sham-link, then the interval on both endpoints of the sham-link must have the same dead interval.

Parameters *seconds* — The dead interval expressed as a decimal integer.

Values 2 to 65535 seconds

Platforms All

dead-interval

Syntax **dead-interval** *seconds*
no dead-interval

Context **[Tree]** (config>router>ospf>area>interface dead-interval)
[Tree] (config>router>ospf>area>virtual-link dead-interval)
[Tree] (config>router>ospf3>area>interface dead-interval)
[Tree] (config>router>ospf3>area>virtual-link dead-interval)

Full Context configure router ospf area interface dead-interval
configure router ospf area virtual-link dead-interval
configure router ospf3 area interface dead-interval
configure router ospf3 area virtual-link dead-interval

Description This command configures the time, in seconds, that OSPF waits before declaring a neighbor router down. If no hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the hello interval.

The **no** form of this command reverts to the default value.

Default dead-interval 40

Special Cases **OSPF Interface —** If the **dead-interval** configured applies to an interface, then all nodes on the subnet must have the same dead interval.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Virtual Link — If the **dead-interval** configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same dead interval.

Parameters *seconds* — The dead interval expressed in seconds.

Values 2 to 65535

Platforms All

8.35 dead-timer

dead-timer

Syntax **dead-timer** *seconds*
no dead-timer

Context **[Tree]** (config>router>pcep>pcc dead-timer)
[Tree] (config>router>pcep>pce dead-timer)

Full Context configure router pcep pcc dead-timer
configure router pcep pce dead-timer

Description This command configures the PCEP session dead timer value, which is the amount of time a PCEP speaker (PCC or PCE) will wait after the receipt of the last PCEP message before declaring its peer down.

The keep-alive mechanism is asymmetric, meaning that each PCEP speaker can propose a different dead timer value to its peer to use to detect session timeout.

The **no** form of the command returns the dead timer to the default value.

Default dead-timer 120

Parameters *seconds* — the dead timer value, in seconds

Values 1 to 255

Platforms All

8.36 debounce

debounce

Syntax [**no**] **debounce**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>redundancy>mc>peer>mcr>ring>in-band-control-path debounce)
[Tree] (config>redundancy>mc>peer>mc>l3-ring>in-band-control-path debounce)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring in-band-control-path debounce
configure redundancy multi-chassis peer mc-ring ring in-band-control-path debounce

Description This command enables the inband control path debouncing. The **no** form of this command disables inband control path debouncing.

The **no** form of this command reverts to the default.

Default debounce

Platforms All

debounce

Syntax **debounce** *occurrences* [**within** *seconds*]
no debounce

Context [Tree] (config>log>event-trigger>event>trigger-entry debounce)

Full Context configure log event-trigger event trigger-entry debounce

Description This command configures when to trigger, for example after one or more event occurrences. The number of occurrences of an event can be bounded by a time window or left open.

The **no** form of this command removes the debounce configuration.

Parameters *occurrences* — Specifies the number of times an event must occur for EHS to trigger a response.

Values 2 to 15

within *seconds* — Specifies the time window within which a specific event must occur a number of times equivalent to the specified *occurrences* for EHS to trigger a response.

Values 1 to 604800

Platforms All

8.37 debug

debug

Syntax **debug**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug)

Full Context debug

Description Commands in this context specify debugging options.

Platforms All

8.38 debug-output

debug-output

Syntax [**no**] **debug-output**

Context [Tree] (config>call-trace>trace-profile debug-output)

Full Context configure call-trace trace-profile debug-output

Description This command enables output to the debug log. Traced messages are decoded as text and sent to debug logging. This allows for real-time debugging but is not recommended on live systems because of the decode overhead.

This command disables logging to the compact flash. The **debug-output** and **live-output** commands are mutually exclusive.

The **no** form of this command disables output to the debug log.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.39 debug-save

debug-save

Syntax **debug-save** [*file-url*]

Context [Tree] (admin debug-save)

Full Context admin debug-save

Description This command saves existing debug configuration (configuration done under the debug branch of CLI). Debug configurations are not saved by the **admin save** command and not preserved across a node reboot or CPM switchover. The **debug-save** command makes the debug configuration available for the operator to execute after a reboot by using the **exec** command or after a CPM switchover by using the **switchover-exec** command, if desired.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *file-url* — Specifies the file URL location to save the debug configuration. If no file-url is specified then the debug configuration is saved at the same location as the standard configuration file (**bof>primary-config/bof>secondary-config**/**bof>tertiary-config**) with the same file name as the standard configuration file but with a .dbg suffix.

Note: IPv6-address applies only to 7750 SR and 7950 XRS.

Values

file url	local-url | remote-url: 255 chars max
local-url	[*cflash-id/*][*file-path*] 200 chars max, including cflash-id *file-path* 199 chars max
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*] 255 chars max directory length 99 chars max each
remote-locn	{hostname | ipv4-address | [ipv6-address]}
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - 32 chars max, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

8.40 decrypt-key

decrypt-key

Syntax **decrypt-key** *key* | *hash-key* | *hash2-key* [**hash** | **hash2** | **custom**]
no decrypt-key

Context **[Tree]** (config>app-assure>group>url-list decrypt-key)

Full Context configure application-assurance group url-list decrypt-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description In case the file is encrypted this command is used to configure the decryption key used to read the file.

The **no** form of this command removes the url-list object.

Default no decrypt-key

Parameters *key* | *hash-key* | *hash2-key* — Specifies the Application-Assurance url-list decryption key.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.41 def-app-profile

def-app-profile

Syntax **def-app-profile** *app-profile-name*
no def-app-profile

Context [Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt def-app-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-app-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt def-app-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-app-profile)
[Tree] (config>service>vpls>sap>sub-sla-mgmt def-app-profile)
[Tree] (config>subscriber-mgmt>msap-policy>sub-sla-mgmt def-app-profile)

Full Context configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-app-profile
configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-app-profile
configure service vpls sap sub-sla-mgmt def-app-profile
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt def-app-profile
configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-app-profile
configure subscriber-mgmt msap-policy sub-sla-mgmt def-app-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the default application profile to be used by a subscriber host.

The **no** form of this command removes the application profile name from the configuration.

Parameters *app-profile-name* — Specifies an existing application profile to be mapped to the subscriber profile by default up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt msap-policy sub-sla-mgmt def-app-profile
- configure service vprn subscriber-interface group-interface sap sub-sla-mgmt def-app-profile
- configure service vpls sap sub-sla-mgmt def-app-profile
- configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-app-profile

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-app-profile
- configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-app-profile

def-app-profile

Syntax **def-app-profile** *profile-name*
no def-app-profile

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm def-app-profile)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm def-app-profile)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt def-app-profile
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt def-app-profile

Description This command configures the default application profile.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

def-app-profile

Syntax **def-app-profile** *app-profile-name*
no def-app-profile

Context **[Tree]** (config>app-assure>group>transit-ip-policy def-app-profile)

Full Context configure application-assurance group transit-ip-policy def-app-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a default application profile.

Default no def-app-profile

Parameters *app-profile-name* — Specifies the application profile name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.42 def-instance-sharing

def-instance-sharing

Syntax **def-instance-sharing** {**per-sap** | **per-session**}

Context **[Tree]** (config>subscr-mgmt>sla-prof def-instance-sharing)

Full Context configure subscriber-mgmt sla-profile def-instance-sharing

Description This command configures the default SPI sharing method for IPoE or PPPoE sessions from the same subscriber, having the same SLA profile associated, that are active on the same SAP. SPI sharing can be per-SAP or a dedicated SPI per-session.

Default def-instance-sharing per-sap

Parameters **per-sap** — Specifies that IPoE or PPP sessions from the same subscriber, having the same SLA profile associated, and active on the same SAP share an SPI.

per-session — Specifies that IPoE or PPP sessions from the same subscriber, having the same SLA profile associated, and active on the same SAP obtain a dedicated SPI per session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.43 def-inter-dest-id

def-inter-dest-id

Syntax **def-inter-dest-id string** *string*
def-inter-dest-id {**use-top-q** | **use-vpi**}
no def-inter-dest-id

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt def-inter-dest-id)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt def-inter-dest-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>subscr-mgmt>msap-policy>sub-sla-mgmt def-inter-dest-id)

Full Context configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-inter-dest-id
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt def-inter-dest-id
configure subscriber-mgmt msap-policy sub-sla-mgmt def-inter-dest-id

Description This command specifies a default destination string for all subscribers associated with the SAP. The command also accepts the **use-top-q** flag that automatically derives the string based on the top most delineating Dot1Q tag from the SAP's encapsulation.

The **no** form of this command removes the default subscriber identification string from the configuration.

Parameters *string* — A RADIUS VSA (Alc-Int-Dest-Id-Str, type 28) obtained during the subscriber authentication phase contains the destination string name that is matched against the string defined under the Vport. In this fashion the subscriber host is associated with the corresponding Vport.

Alternatively, the destination string can be defined in LUDB.

use-top-q — This is applicable only to Ethernet ports.

use-vpi — VP Identifier (VPI) is used to make the association between the subscriber and the Vport automatically.

The control plane is aware of the VPI during the session initiation phase. This VPI is used to make the association between the host and the Vport with the same name (VPI number).

Note: In this case the Vport name under the **configure>port>sonet-sdh>path>access>egress** context must be the VPI number.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

def-inter-dest-id

Syntax **def-inter-dest-id** {**string** *string* | **use-top-q**}
no def-inter-dest-id

Context [Tree] (config>service>vpls>sap>sub-sla-mgmt def-inter-dest-id)

Full Context configure service vpls sap sub-sla-mgmt def-inter-dest-id

Description This command specifies a default destination string for all subscribers associated with the SAP. The command also accepts the **use-top-q** flag that automatically derives the string based on the top most delineating Dot1Q tag from the SAP's encapsulation.

The **no** form of this command removes the default subscriber identification string from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no def-sub-id

Default no def-inter-dest-id

Parameters **use-top-q** — Specifies to derive the string based on the top most delineating Dot1Q tag from the SAP's encapsulation

string *string* — Specifies the subscriber identification applicable for a subscriber host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.44 def-recv-evpn-encap

def-recv-evpn-encap

Syntax **def-recv-evpn-encap** {**mpls** | **vxlan**}
no def-recv-evpn-encap

Context **[Tree]** (config>router>bgp>group>neighbor def-recv-evpn-encap)
[Tree] (config>router>bgp>group def-recv-evpn-encap)

Full Context configure router bgp group def-recv-evpn-encap
configure router bgp group neighbor def-recv-evpn-encap

Description This command defines how the BGP will treat a received EVPN route without RC5512 BGP encapsulation extended community. If no encapsulation is received, BGP will validate the route as MPLS or VXLAN depending on how this command is configured.

Default no def-recv-evpn-encap

Parameters **mpls** — Specifies that **mpls** is the default encapsulation value in the case where no RFC5512 extended community is received in the incoming BGP-EVPN route.

vxlan — Specifies that **vxlan** is the default encapsulation value.

Platforms All

8.45 def-sla-profile

def-sla-profile

Syntax **def-sla-profile** *default-sla-profile-name*
no def-sla-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt def-sla-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-sla-profile)
[Tree] (config>service>vpls>sap>sub-sla-mgmt def-sla-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt def-sla-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-sla-profile)
[Tree] (config>subscr-mgmt>msap-policy>sub-sla-mgmt def-sla-profile)

Full Context
configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-sla-profile
configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sla-profile
configure service vpls sap sub-sla-mgmt def-sla-profile
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt def-sla-profile
configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sla-profile
configure subscriber-mgmt msap-policy sub-sla-mgmt def-sla-profile

Description
This command specifies a default SLA profile for this SAP. The SLA profile must be defined prior to associating the profile with a SAP in the config>subscr-mgmt>sla-profile context.

If a subscriber is not explicitly associated with an SLA profile during the authentication phase, a default profile will be assigned to it.

The **no** form of this command removes the default SLA profile from the SAP configuration.

Parameters
default-sla-profile-name — Specifies a default SLA profile for this SAP.

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt msap-policy sub-sla-mgmt def-sla-profile
- configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-sla-profile
- configure service vpls sap sub-sla-mgmt def-sla-profile
- configure service vprn subscriber-interface group-interface sap sub-sla-mgmt def-sla-profile

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sla-profile
- configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sla-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.46 def-sub-id

def-sub-id

Syntax **def-sub-id use-auto-id**
def-sub-id use-sap-id
def-sub-id string *sub-id*
no def-sub-id

Context **[Tree]** (config>subscr-mgmt>msap-policy>sub-sla-mgmt def-sub-id)
[Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt def-sub-id)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt def-sub-id)
[Tree] (config>service>vpls>sap>sub-sla-mgmt def-sub-id)

Full Context configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-sub-id
configure service vpls sap sub-sla-mgmt def-sub-id
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt def-sub-id
configure subscriber-mgmt msap-policy sub-sla-mgmt def-sub-id

Description This command specifies the explicit default sub-id for dynamic subscriber hosts (including ARP hosts) in case that the sub-id string is not supplied through RADIUS or LUDB.

The sub-id is assigned to a new subscriber host in the following order of priority:

- RADIUS
- LUDB
- Explicit default – The **def-sub-id** command is used to explicitly set the *sub-id* name of the host as one of the following:
  - The SAP ID to which the new host is associated
  - An explicit string
  - An auto-generated string consisting of the concatenated subscriber identification fields defined under the **subscr-mgmt**>**auto-sub-id-key** node. The fields are taken in the order in which they are configured and are separated by a ‘|‘character. The subscriber host identification fields are separately defined for IPoE and PPPoE host types.
- Implicit default – If the sub-id string is not returned via RADIUS or LUDB and there is no def-sub-id configured, the *sub-id* name is generated as a random 10 character encoded string based on the auto-sub-id-keys. This 10 characters encoded string is unique per chassis as well as in dual-homed environment. It is generated based on auto-sub-id-keys. If auto-sub-id-keys are not explicitly configured, the default ones are:
  - mac, sap-id, or session-id for PPP type hosts
  - mac or sap-id for IPoE type hosts.

This command does not apply to static subscribers.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **use-sap-id** — Specifies the sub-id name-id on which the original request for host creation arrived (DHCP Discover, or PADI or ARP Request).

sub-id — Explicitly configured sub-id name up to 32 characters.

use-auto-id — Specifies the concatenated string of auto-sub-id-keys separated by a "| " character.

Default no def-sub-id

Implicit default If the *sub-id string* is not supplied through RADIUS, LUDB, or **def-sub-id** configuration, then a random 10 character encoded sub-id name is generated. This random sub-id name is based on the subscriber identification keys defined under the **subscr-mgmt**>**auto-sub-id-key** node. In case that the auto-sub-id-keys are not defined explicitly, the default ones are:

- mac, sap-id, or session-id for PPPoE type hosts
- mac or sap-id for IPoE type hosts

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

def-sub-id

Syntax **def-sub-id string** *sub-id*
def-sub-id use-auto-id
no def-sub-id

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-sub-id)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-sub-id)

Full Context configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sub-id
configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sub-id

Description This command configures the default subscriber ID. The default is used if no other source (like RADIUS) provides a subscriber identification string.

Parameters *sub-id* — Specifies the default subscriber identification up to 32 characters.

use-auto-id — Specifies that the auto-generated subscriber identification string, is used as the default subscriber identification string.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.47 def-sub-profile

def-sub-profile

Syntax **def-sub-profile** *default-subscriber-profile-name*

Context **[Tree]** (config>subscr-mgmt>msap-policy>sub-sla-mgmt def-sub-profile)

Full Context configure subscriber-mgmt msap-policy sub-sla-mgmt def-sub-profile

Description This command specifies a default subscriber profile for an MSAP.

A subscriber profile defines the aggregate QoS for all hosts within a subscriber context. This is done through the definition of the egress and ingress scheduler policies that govern the aggregate SLA for subscriber using the subscriber profile.

The **no** form of this command removes the default SLA profile from the SAP configuration.

Parameters *default-sub-profile* — Specifies a default subscriber profile for this SAP up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

def-sub-profile

Syntax **def-sub-profile** *default-subscriber-profile-name*

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt def-sub-profile)
[Tree] (config>service>ies>if>sap>sub-sla-mgmt def-sub-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-sub-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters>sub-sla-mgmt def-sub-profile)

Full Context configure service ies interface sap sub-sla-mgmt def-sub-profile
configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-sub-profile
configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sub-profile
configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sub-profile

Description This command specifies a default subscriber profile for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscr-mgmt>sub-profile** context.

A subscriber profile defines the aggregate QoS for all hosts within a subscriber context. This is done through the definition of the egress and ingress scheduler policies that govern the aggregate SLA for subscriber using the subscriber profile. Subscriber profiles also allow for specific SLA profile definitions when the default definitions from the subscriber identification policy must be overridden.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the default SLA profile from the SAP configuration.

Parameters *default-sub-profile* — Specifies a default subscriber profile for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscr-mgmt>sub-profile** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap sub-sla-mgmt def-sub-profile

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sub-profile
- configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt def-sub-profile

def-sub-profile

Syntax **def-sub-profile** *default-subscriber-profile-name*

Context **[Tree]** (config>service>vpls>sap>sub-sla-mgmt def-sub-profile)

Full Context configure service vpls sap sub-sla-mgmt def-sub-profile

Description This command specifies a default subscriber profile for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscr-mgmt>sub-profile** context.

A subscriber profile defines the aggregate QoS for all hosts within a subscriber context. This is done through the definition of the egress and ingress scheduler policies that govern the aggregate SLA for subscriber using the subscriber profile. Subscriber profiles also allow for specific SLA profile definitions when the default definitions from the subscriber identification policy must be overridden.

The **no** form of this command removes the default SLA profile from the SAP configuration.

Parameters *default-sub-profile* — Specifies a default subscriber profile for this SAP. The subscriber profile must be defined prior to associating the profile with a SAP in the **config>subscr-mgmt>sub-profile** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.48 default

default

Syntax [**no**] **default**

Context **[Tree]** (config>log>accounting-policy default)

Full Context configure log accounting-policy default

Description This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.

If no access accounting policy is defined on a SAP, accounting records are produced in accordance with the default access policy. If no default access policy is created, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

If no network accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one access accounting policy ID can be designated as the default access policy. Likewise, only one network accounting policy ID can be designated as the default network accounting policy.

The record name must be specified prior to assigning an accounting policy as default.

If a policy is configured as the default policy, then a **no default** command must be issued before a new default policy can be configured.

The **no** form of this command removes the default policy designation from the policy ID. The accounting policy will be removed from all SAPs or network ports that do not have this policy explicitly defined.

Platforms All

8.49 default-accounting-server-policy

default-accounting-server-policy

Syntax **default-accounting-server-policy** *policy-name*
no default-accounting-server-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>radius-proxy>server default-accounting-server-policy)
[Tree] (config>service>vprn>radius-proxy>server default-accounting-server-policy)

Full Context configure router radius-proxy server default-accounting-server-policy
configure service vprn radius-proxy server default-accounting-server-policy

Description This command specifies the default radius-server-policy for RADIUS accounting. This policy is used when there is no specific match based on username.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the name of the default RADIUS server policy associated with this RADIUS Proxy server for accounting purposes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.50 default-action

default-action

Syntax **default-action** {**bypass-host-creation** | **drop**}
no default-action

Context [Tree] (config>filter>dhcp-filter default-action)

Full Context configure filter dhcp-filter default-action

Description This command specifies the default action for DHCP filters when no entries match.

The **no** form of this command reverts to the default.

Parameters **bypass-host-creation** — Specifies to bypass ESM host creation options.

drop — Specifies to drop and not process the DHCP message.

Platforms All

default-action

Syntax **default-action bypass-host-creation** [**na**] [**pd**]
default-action drop
no default-action

Context [Tree] (config>filter>dhcp6-filter default-action)

Full Context configure filter dhcp6-filter default-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the default action for DHCP6 filters when no entries match.

The **no** form of this command reverts to the default.

Parameters **bypass-host-creation** — Specifies to bypass ESM host creation options.

Values **na** — Bypasses the DHCP NA hosts creation.
pd — Bypasses the DHCP PD hosts creation.

drop — Specifies to drop and not process the DHCP6 message.

Platforms All

default-action

Syntax **default-action** {**drop** | **forward**}
no default-action

Context **[Tree]** (config>subscr-mgmt>isa-filter default-action)
[Tree] (config>subscr-mgmt>isa-filter>ipv6 default-action)

Full Context configure subscriber-mgmt isa-filter default-action
configure subscriber-mgmt isa-filter ipv6 default-action

Description This command specifies what should happen to packets that do not match any of the configured entries.

The **no** form of this command reverts to the default value.

Default default-action drop

Parameters **drop** — Specifies that packets matching the filter entry are dropped.

forward — Specifies that packets matching the filter entry are forwarded.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action** {**block** | **allow**}

Context **[Tree]** (config>service>mrp>mrp-policy default-action)

Full Context configure service mrp mrp-policy default-action

Description This command specifies the action to be applied to the MMRP attributes (Group B-MACs) whose ISIDs do not match the specified criteria in all of the entries of the mrp-policy.

When multiple **default-action** commands are entered, the last command will overwrite the previous command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default default-action allow

Parameters **block** — Specifies that all MMRP attributes will not be declared or registered unless there is a specific mrp-policy entry which causes them to be allowed on this SAP or SDP.

allow — Specifies that all MMRP attributes will be declared and registered unless there is a specific mrp-policy entry which causes them to be blocked on this SAP or SDP.

Platforms All

default-action

Syntax **default-action** {**drop** | **forward**}
no default-action

Context **[Tree]** (config>service>vprn>log>filter default-action)

Full Context configure service vprn log filter default-action

Description The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.

When multiple **default-action** commands are entered, the last command overwrites the previous command.

The **no** form of this command reverts the default action to the default value (forward).

Default default-action forward — The events which are not explicitly dropped by an event filter match are forwarded.

Parameters **drop** — The events which are not explicitly forwarded by an event filter match are dropped.

forward — The events which are not explicitly dropped by an event filter match are forwarded.

Platforms All

default-action

Syntax **default-action** {**permit** | **deny**} [**event-log** *event-log-name*]

Context **[Tree]** (config>app-assure>group>sess-fltr default-action)

Full Context configure application-assurance group session-filter default-action

Description This command specifies the default action to take for packets that do not match any filter entries.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts the default action to the default value (forward).

Default default-action deny

Parameters **deny** — Indicates that packets matching the criteria are denied.

permit — Indicates that packets matching the criteria are permitted.

event-log-name — Specifies the event log name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action direction** *direction* [**create**]
no default-action direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-fltr>msg default-action)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type default-action

Description This command configures a TCA for the counter capturing hits for the specified GTP filter default action. A default action TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action direction** *direction* [**create**]
no default-action direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-fltr>msg-gtpv2 default-action)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type-gtpv2 default-action

Description This command configures a TCA for the counter capturing hits due to the default action specified for the GTPv2 message type filter. A default action TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action direction** *direction* [**create**]
no default-action direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-fltr>imsi-apn default-action)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter imsi-apn default-action

Description This command configures a TCA for the counter capturing hits for the specified GTP IMSI-APN filter default action. A default action TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

default-action

Syntax **default-action direction** *direction* [**create**]

Context **[Tree]** (config>app-assure>group>statistics>tca>sctp-fltr>ppid default-action)

Full Context configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid default-action

Description This command configures a TCA for the counter capturing hits for the specified SCTP filter default PPID. A default action TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-action

Syntax **default-action direction** *direction* [**create**]
no default-action direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>session-filter default-action)

Full Context configure application-assurance group statistics threshold-crossing-alert session-filter default-action

Description This command configures a TCA for the counter capturing hits for the specified session filter default action. A default action TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action** {**permit** | **deny**}

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>imsi-apn-fltr default-action)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter default-action

Description This command configures the default action for the IMSI-APN filter.

Default default-action permit

Parameters **permit** — Specifies to permit packets that do not match any message entries.

deny — Specifies to deny packets that do not match any message entries.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action** {**permit** | **deny**}

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>msg default-action)
[Tree] (config>app-assure>group>gtp>gtp-fltr>msg-gtpv2 default-action)

Full Context configure application-assurance group gtp gtp-filter message-type default-action
configure application-assurance group gtp gtp-filter message-type-gtpv2 default-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the default action for all GTP message types.

Default default-action permit

Parameters **permit** — Specifies to permit packets that do not match any message entries.

deny — Specifies to deny packets that do not match any message entries.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action** {**permit** | **deny**}

Context **[Tree]** (config>app-assure>group>sctp-fltr>ppid default-action)

Full Context configure application-assurance group sctp-filter ppid default-action

Description This command configures the default action for all SCTP PPIDs.

Default default-action permit

Parameters **permit** — Specifies to permit packets that do not match any PPID entries.

deny — Specifies to deny packets that do not match any PPID entries.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action allow**
default-action block-all
default-action block-http-redirect *http-redirect-name*
no default-action

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action>url-filter default-action)

Full Context configure application-assurance group policy app-qos-policy entry action url-filter default-action

Description This command configures the default action to take when the ICAP server is unreachable.

Default no default-action

Parameters **allow** — Allows all requests.

block-all — Blocks all requests.

block-http-redirect *http-redirect-name* — Blocks and redirects requests.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-action

Syntax **default-action** {**dnat** | **forward**} [**ip-address** *ip-address*]

Context **[Tree]** (config>service>nat>nat-classifier default-action)

Full Context configure service nat nat-classifier default-action

Description This command specifies the default action to take for packets in this nat-classifier. The default-action will apply to packet that do not match any configured criteria within nat-classifier. The **no** form of this command equals action forward.

Default default-action forward

Parameters **dnat** — Performs the DNAT function. The destination IP address of the packet traversing the router in the direction from inside to outside is replaced by the configured IP address. Destination port is not translated. In the opposite direction (from outside to inside), the source address in the returning packet is restored to the original value.

forward — The forward action will ensure that the packet is transparently passed through the nat-classifier.

ip-address *ip-address* — The destination IP address that will replace the original IP address in the packet traveling from inside to outside.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

default-action

Syntax **default-action** {**accept** | **discard**}

Context **[Tree]** (config>router>mcac>policy default-action)

Full Context configure router mcac policy default-action

Description This command specifies the action to be applied to multicast streams (channels) when the streams do not match any of the multicast addresses defined in the MCAC policy.

When multiple default-action commands are entered, the last command will overwrite the previous command.

Default default-action discard

Parameters **accept** — Specifies multicast streams (channels) not defined in the MCAC policy will be accepted.

discard — Specifies multicast streams (channels) not defined in the MCAC policy will be dropped.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-action

Syntax **default-action fc** *fc-name* **profile** {**in** | **out**}

Context **[Tree]** (config>qos>network>ingress default-action)

Full Context configure qos network ingress default-action

Description This command defines or edits the default action to be taken for packets that have an undefined DSCP or MPLS EXP bit set. The **default-action** command specifies the forwarding class to which such packets are assigned.

Multiple default-action commands will overwrite each previous default-action command.

Default default-action fc be profile out

Parameters *fc-name* — Specifies the forwarding class name. All packets with DSCP value or MPLS EXP or dot1p bits that are not defined will be placed in this forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out} — All packets that are assigned to this forwarding class will be considered in-profile or out-of-profile based on this command. In case of congestion, the in-profile packets are preferentially queued over the out-of-profile packets.

Values in, out

Platforms All

default-action

Syntax **default-action** {**drop** | **forward**}

Context **[Tree]** (config>filter>ip-filter default-action)
[Tree] (config>filter>ipv6-filter default-action)
[Tree] (config>filter>mac-filter default-action)

Full Context configure filter ip-filter default-action
configure filter ipv6-filter default-action
configure filter mac-filter default-action

Description This command defines the default action to be applied to packets not matching any entry in this ACL filter policy or to packets for that match a PBF/PBR filter entry for which the PBF/PBR target is down and **pbr-down-action-override** per-entry is set to **filter-default-action**.

Default default-action drop

Parameters **drop** — Specifies the default action is to drop a packet.

forward — Specifies the default action is to forward a packet.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-action

Syntax **default-action** {**drop** | **forward**}
no default-action

Context **[Tree]** (config>log>filter default-action)

Full Context configure log filter default-action

Description The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.

When multiple **default-action** commands are entered, the last command overwrites the previous command.

The **no** form of this command reverts the default action to the default value (forward).

Default default-action forward

Parameters **drop** — The events which are not explicitly forwarded by an event filter match are dropped.

forward — The events which are not explicitly dropped by an event filter match are forwarded.

Platforms All

default-action

Syntax **default-action** {**permit** | **deny** | **deny-host-unreachable**}

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter default-action)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter default-action)
[Tree] (config>system>security>mgmt-access-filter>mac-filter default-action)

Full Context configure system security management-access-filter ip-filter default-action
configure system security management-access-filter ipv6-filter default-action
configure system security management-access-filter mac-filter default-action

Description This command creates the default action for management access in the absence of a specific management access filter match.

The **default-action** is applied to a packet that does not satisfy any match criteria in any of the management access filters. Whenever management access filters are configured, the **default-action** must be defined.

Parameters **permit** — Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.

deny — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

deny-host-unreachable — Specifies that packets not matching the selection criteria be denied access and that an ICMP host unreachable message will be issued.

The **deny-host-unreachable** only applies to ip-filter and ipv6filter.

Platforms All

default-action

Syntax **default-action** {**accept** | **drop**}

Context **[Tree]** (config>system>security>cpm-filter default-action)

Full Context configure system security cpm-filter default-action

Description This command specifies the action to take on the traffic when there are no filter entry matches. If there are no filter entries defined, the packets received are either dropped or forwarded based on that default action.

Default default-action accept

Parameters **accept** — Specifies that packets matching the filter entry are forwarded.

drop — Specifies that packets matching the filter entry are dropped.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

default-action

Syntax **default-action** {**deny-all** | **permit-all** | **none** | **read-only-all**}

Context **[Tree]** (config>system>security>profile default-action)

Full Context configure system security profile default-action

Description This command specifies the default action to be applied when no match conditions are met.

Parameters **deny-all** — Sets the default of the profile to deny access to all commands.

permit-all — Sets the default of the profile to permit access to all commands.

Note: In classic CLI but not in MD-CLI the **permit-all** parameter does not change access to **security** commands. Specific entries must be created in a command authorization profile in order to give access to **security** commands. The system populated “administrative” profile contains rules to access **security** commands.

none — Sets the default of the profile to no-action. This option is useful to assign multiple profiles to a user.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For example, if a user is a member of two profiles and the default action of the first profile is **permit-all**, then the second profile is never evaluated because the **permit-all** is executed first. Set the first profile default action to **none** and if no match conditions are met in the first profile, then the second profile is evaluated. If the default action of the last profile is **none** and no explicit match is found, then the command is denied.

read-only-all — Sets the default of the profile to allow read-only access to all commands.

Platforms All

default-action

Syntax **default-action** {**accept** | **next-entry** | **next-policy** | **drop** | **reject**}
no default-action

Context **[Tree]** (config>router>policy-options>policy-statement default-action)

Full Context configure router policy-options policy-statement default-action

Description Commands in this context configure actions to apply to routes that do not match any entries of a route policy statement.

The **no** form of this command deletes the **default-action** context for the policy statement.

Default no default-action

Parameters **accept** — Specifies that routes not matched by any entry should be allowed or accepted. This parameter provides a context for modifying route properties.

next-entry — Specifies that routes not matched by any entry should be evaluated by the next sequential entry in the policy chain, after route properties are possibly modified by the default action of the current policy.

next-policy — Specifies that routes not matched by any entry should be evaluated by the next sequential policy in the policy chain, after route properties are possibly modified by the default action of the current policy.

drop — Specifies that routes not matched by any entry should be disallowed or rejected. This parameter provides a context for modifying route properties.

reject — Specifies that routes not matched by any entry should be disallowed or rejected. This parameter does not provide a context for modifying route properties.

Platforms All

default-action

Syntax **default-action allow**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-action block-all
default-action block-http-redirect *http-redirect-name*
no default-action

Context [Tree] (config>app-assure>group>url-filter>icap default-action)
[Tree] (config>app-assure>group>url-filter>web-service default-action)
[Tree] (config>app-assure>group>url-filter>local-filtering default-action)

Full Context configure application-assurance group url-filter icap default-action
configure application-assurance group url-filter local-filtering default-action
configure application-assurance group url-filter web-service default-action

Description This command configures a default action for the URL filter. The default action takes effect when the URL filter cannot be used. This may happen in the following scenarios.

- In the case of a local URL list, when the URL list is shutdown or the file is not loaded due to an error.
- In the case of ICAP or web filtering, when all TCP connections are busy or down.

The **no** form of this command removes the **default-action** for the URL filter.

Default no default-action

Parameters **allow** — Specifies to allows traffic.

block-all — Specifies to block traffic.

block-http-redirect *http-redirect-name* — Specifies to block traffic and redirect the user to an information page, which can be different than the page the user is redirected to when the site they attempted to access was found in the URL filter; this page is configured using the **config**>**aa**>**group**>**url-filter**>**http-redirect** command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.51 default-authentication-server-policy

default-authentication-server-policy

Syntax **default-authentication-server-policy** *policy-name*
no default-authentication-server-policy

Context [Tree] (config>router>radius-proxy>server default-authentication-server-policy)
[Tree] (config>service>vprn>radius-proxy>server default-authentication-server-policy)

Full Context configure router radius-proxy server default-authentication-server-policy
configure service vprn radius-proxy server default-authentication-server-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the default radius-server-policy for RADIUS authentication. This policy is used when there is no specific match based on username.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the name of the default RADIUS server policy associated with this RADIUS proxy server for authentication purposes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.52 default-brg-profile

default-brg-profile

Syntax **default-brg-profile** *profile-name*
no default-brg-profile

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-ranges>range>vrgw>brg default-brg-profile)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>brg default-brg-profile)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>brg default-brg-profile)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-ranges>range>vrgw>brg default-brg-profile)
[Tree] (config>service>vprn>sub-if>grp-if>brg default-brg-profile)
[Tree] (config>service>ies>sub-if>grp-if>brg default-brg-profile)

Full Context configure service ies subscriber-interface group-interface brg default-brg-profile
configure service ies subscriber-interface group-interface wlan-gw ranges range brg default-brg-profile
configure service ies subscriber-interface group-interface wlan-gw vlan-ranges range vrgw brg default-brg-profile
configure service vprn subscriber-interface group-interface brg default-brg-profile
configure service vprn subscriber-interface group-interface wlan-gw ranges range brg default-brg-profile
configure service vprn subscriber-interface group-interface wlan-gw vlan-ranges range vrgw brg default-brg-profile

Description This command indicates that the default BRG profile must be used for new BRGs. This profile can be overridden by RADIUS.

Parameters *profile-name* — Specifies the name of the brg-profile to be applied.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.53 default-category-map

default-category-map

Syntax **default-category-map** *category-map-name*
no default-category-map

Context **[Tree]** (config>subscr-mgmt>credit-control-policy default-category-map)

Full Context configure subscriber-mgmt credit-control-policy default-category-map

Description This command configures the default category map.

The **no** form of this command reverts to the default.

Parameters *category-map-name* — Specifies the category map name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.54 default-charging-group

default-charging-group

Syntax **default-charging-group** *charging-group-name*
no default-charging-group

Context **[Tree]** (config>app-assure>group>policy default-charging-group)

Full Context configure application-assurance group policy default-charging-group

Description This command associates a charging group to any applications or app-groups that are not explicitly assigned to a charging group, for an application assurance policy.

The **no** form of this command deletes the default charging group from the configuration.

Default no default-charging-group

Parameters *charging-group-name* — A string of up to 32 characters uniquely identifying an existing charging group in the system.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.55 default-credit

default-credit

Syntax **default-credit volume** *credits* [**bytes** | **kilobytes** | **megabytes** | **gigabytes**]
default-credit time *seconds*
no default-credit

Context **[Tree]** (config>subscr-mgmt>cat-map>category default-credit)

Full Context configure subscriber-mgmt category-map category default-credit

Description This command configures the default credit values for RADIUS credit control and Diameter Gy application credit control.

For RADIUS credit control, this command configures the default time or volume credit for this category. The default credit is used during initial setup when no quota is received from the RADIUS server.

For Diameter Gy credit control, this command specifies the interim credit assigned to this category (rating group) when Extended Failure Handling (EFH) is enabled. This command is ignored when EFH is disabled.

The **no** form of this command reverts to the default.

Parameters **volume** *credits* [**bytes** | **kilobytes** | **megabytes** | **gigabytes**] — Specifies the default value for the volume credit and the unit in which the default value is expressed.

Values 1 to 4294967295 (minimum 1 byte)

time *seconds* — Specifies the default value for the time credit, in seconds.

Values 1 to 4294967295 (minimum 1 second)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.56 default-dnat-ip-address

default-dnat-ip-address

Syntax **default-dnat-ip-address** *ip-address*
no default-dnat-ip-address

Context **[Tree]** (config>service>nat>nat-classifier default-dnat-ip-address)

Full Context configure service nat nat-classifier default-dnat-ip-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the IP address to substitute for the destination IP address of the packets

Default no default-dnat-ip-address

Parameters *ip-address* — Specifies the default DNAP IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.57 default-dns

default-dns

Syntax **default-dns** *ip-address* [**secondary** *ip-address*]
no default-dns

Context **[Tree]** (config>service>ies>sub-if default-dns)
[Tree] (config>service>vprn>sub-if default-dns)

Full Context configure service ies subscriber-interface default-dns
configure service vprn subscriber-interface default-dns

Description This command configures last resort IP DNS addresses that can be used for name resolution by IPoE hosts (IA_NA, IA_PD and SLAAC) and PPPoE hosts (IA_NA, IA_PD and SLAAC).

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IP address of the primary DNS server.

secondary *ip-address* — Specifies the IP address of the secondary DNS server (optional).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

default-dns

Syntax **default-dns** *ipv6-address* [**secondary** *ipv6-address*]
no default-dns

Context **[Tree]** (config>service>ies>sub-if>ipv6 default-dns)
[Tree] (config>service>vprn>sub-if>ipv6 default-dns)

Full Context configure service ies subscriber-interface ipv6 default-dns
configure service vprn subscriber-interface ipv6 default-dns

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures last resort IPv6 DNS addresses that can be used for name resolution by IPoEv6 hosts (IA_NA, IA_PD and SLAAC) and PPPoEv6 hosts (IA_NA, IA_PD and SLAAC).

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the IPv6 address of the primary DNS server.

secondary *ipv6-address* — Specifies the IPv6 address of the secondary DNS server (optional).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.58 default-domain

default-domain

Syntax **default-domain** *dns-name*
no default-domain

Context **[Tree]** (config>service>vprn>dns default-domain)

Full Context configure service vprn dns default-domain

Description This command configures the DNS domain name to be added in DNS retries when a DNS query is not replied or an empty DNS reply is received.

The **no** form of this command prevents DNS retries when the DNS query is not replied or an empty DNS reply is received.

Parameters *dns-name* — Specifies the name of the default domain, up to 255 characters. Allowed values for characters are alphabetical (A-Z), numeric (0-9), the minus sign (-), and the period (.). For example, “3gpp-network.org”.

Platforms All

default-domain

Syntax **default-domain**

Context **[Tree]** (config>eth-cfm default-domain)

Full Context configure eth-cfm default-domain

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure MIP creation parameters per index (**bridge-identifier** *bridge-id* **vlan** *vlan-id*) if the MIP creation statement exists as part of the service connection. The mip creation statement must be present on the connection before any configuration can occur for a MIP under this context. The determining factor for MIP creation is based on the authoritative properties of the **eth-cfm domain association** configuration. The individual indexes in this table are used for MIP creation only when the association context is not authoritative; this includes the lack of association for a matching index.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.59 default-fc

default-fc

Syntax **default-fc** *fc-name*
no default-fc

Context **[Tree]** (config>qos>sap-ingress default-fc)

Full Context configure qos sap-ingress default-fc

Description This command configures the default forwarding class for the policy. In the event that an ingress packet does not match a higher priority (more explicit) classification command, the default forwarding class or subclass will be associated with the packet. Unless overridden by an explicit forwarding class classification rule, all packets received on an ingress SAP using this ingress QoS policy will be classified to the default forwarding class. Optionally, the default ingress enqueuing priority for the traffic can be overridden as well.

The default forwarding class is best effort (be). The **default-fc** settings are displayed in the **show configuration** and **save** output regardless of inclusion of the **detail** keyword.

Default default-fc “be”

Parameters *fc-name* — Specify the forwarding class name for the queue. The value given for *fc-name* must be one of the predefined forwarding classes in the system.

The subclass-name parameter is optional and used with the fc-name parameter to define a preexisting subclass. The fc-name and subclass-name parameters must be separated by a period (dot). If subclass-name does not exist in the context of fc -name, an error will occur. If subclass-name is removed using the **no fc** *fc-name.subclass-name* **force** command, the **default-fc** command will automatically drop the *subclass-name* and only use *fc-name* (the parent forwarding class for the subclass) as the forwarding class.

Values

fc: *class*[.*subclass*]
class: be, l2, af, l1, h2, ef, h1, nc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

subclass: 29 characters max

Platforms All

8.60 default-filter-action

default-filter-action

Syntax **default-filter-action** *default-action*

Context **[Tree]** (debug>app-assure>group>http-host>filter default-filter-action)

Full Context debug application-assurance group http-host-recorder filter default-filter-action

Description This command configures the recorder filter default action to either record or no-record. This parameter applies to http-host values not matching any expressions defined in the filter context.

Parameters *default-action* — Specifies the default action.

Values record, no-record

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.61 default-group-interface

default-group-interface

Syntax **default-group-interface** *ip-int-name* **service-id** *service-id*
default-group-interface *ip-int-name* **service-name** *svc-name*
no default-group-interface

Context **[Tree]** (config>router>l2tp>group>ppp default-group-interface)
[Tree] (config>router>l2tp>group>tunnel>ppp default-group-interface)
[Tree] (config>service>vprn>l2tp>group>ppp default-group-interface)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp default-group-interface)

Full Context configure router l2tp group ppp default-group-interface
configure router l2tp group tunnel ppp default-group-interface
configure service vprn l2tp group ppp default-group-interface
configure service vprn l2tp group tunnel ppp default-group-interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the group interface where the PPP sessions are established when the authentication server does not specify the group interface.

The **no** form of this command removes the interface name or service ID from the configuration.

Parameters *ip-int-name* — Specifies an IP interface name, up to 32 characters.

service-id *service-id* — Specifies an existing service identification number.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **default-group-interface** *ip-int-name* **service-name** *svc-name* variant can be used in all configuration modes.

Values {*id* | *svc-name*}

id:	1 to 2147483647
svc-name:	up to 64 characters (*svc-name* is an alias for input only. The *svc-name* gets replaced with an id automatically by SR OS in the configuration).

service-name *svc-name* — Specifies an existing service name up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.62 default-gtp-tunnel-endpoint-limit

default-gtp-tunnel-endpoint-limit

Syntax **default-gtp-tunnel-endpoint-limit direction** *direction* [**create**]
no default-gtp-tunnel-endpoint-limit direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter default-gtp-tunnel-endpoint-limit)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter default-gtp-tunnel-endpoint-limit

Description This command configures a TCA for the counter capturing drops due to the GTP endpoint limits create requests exceeding the configured allowed limit (set by the **default-tunnel-endpoint-limit** command). A default-gtp-tunnel-endpoint-limit drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**). The **create** keyword is mandatory when creating a TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Keyword used to create the TCA.

8.63 default-host

default-host

Syntax **default-host** *ipv4-prefix/mask* | *ipv6-prefix/prefix-length* **next-hop** *ipv4-address* | *ipv6-address*
no default-host *ipv4-prefix/mask* | *ipv6-prefix/prefix-length*

Context [Tree] (config>service>ies>sub-if>grp-if>sap default-host)
[Tree] (config>service>vprn>sub-if>grp-if>sap default-host)

Full Context configure service ies subscriber-interface group-interface sap default-host
configure service vprn subscriber-interface group-interface sap default-host

Description This command configures the default-host. More than one default host can be configured per SAP.

The **no** form of this command removes the values from the configuration.

Parameters *ipv4prefix/prefix-length* — Specifies an IPv4 prefix and prefix length.

Values

ipv4-prefix	a.b.c.d (host bits must be 0
prefix-length	0 to 32

ipv6-prefix/prefix-length — Specifies an IPv6 prefix and prefix length.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0 to FFFF]H d - [0 to 255]D
prefix-length	- [0 to 128]

next-hop — Assigns the next hop IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.64 default-instance

default-instance

Syntax [**no**] **default-instance**

Context **[Tree]** (config>service>vprn>isis>if default-instance)

Full Context configure service vprn isis interface default-instance

Description This command enables a non-MI capable router to establish an adjacency and operate with an SR OS in a non-zero instance. If the router does not receive IID-TLVs, it will establish an adjacency in a single instance. Instead of establishing an adjacency in the standard instance 0, the router will establish an adjacency in the configured non-zero instance. The router will then operate in the configured non-zero instance so that it appears to be in the standard instance 0 to its neighbor. This feature is supported on point-to-point interfaces, broadcast interfaces are not supported.

The **no** form of this command disables the functionality so that the router can only establish adjacencies in the standard instance 0.

Default no default-instance

Platforms All

default-instance

Syntax [**no**] **default-instance**

Context **[Tree]** (config>router>isis>interface default-instance)

Full Context configure router isis interface default-instance

Description This command enables a non-MI capable router to establish an adjacency and operate with a router in a non-zero instance. If the router does not receive IID-TLVs, it will establish an adjacency in a single instance. Instead of establishing an adjacency in the standard instance 0, the router will establish an adjacency in the configured non-zero instance. The router will then operate in the configured non-zero instance so that it appears to be in the standard instance 0 to its neighbor. This feature is supported on point-to-point interfaces, broadcast interfaces are not supported.

This feature must be configured on the router connected to non-MI capable routers and on all other SR OS routers in the area, so that they receive non-MI LSPs in the correct instance and not in the base instance.

The **no** form of this command disables the functionality so that the router can only establish adjacencies in the standard instance 0.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no default-instance

Platforms All

8.65 default-ipv4-multicast-metric

default-ipv4-multicast-metric

Syntax **default-ipv4-multicast-metric** *metric*
no default-ipv4-multicast-metric

Context **[Tree]** (config>service>vprn>isis>level default-ipv4-multicast-metric)

Full Context configure service vprn isis level default-ipv4-multicast-metric

Description This command configures the default metric to be used for the IS-IS interface in the IPv4 multicast topology (MT3).

The **no** form of this command deletes the specified default metric and reverts to using the system default of 10.

Default default-ipv4-multicast-metric 10

Parameters *metric* — Specifies the default metric for interfaces in the IPv4 multicast topology (MT3).

Values 1 to 16777215

Platforms All

default-ipv4-multicast-metric

Syntax **default-ipv4-multicast-metric** *metric*
no default-ipv4-multicast-metric

Context **[Tree]** (config>router>isis>level default-ipv4-multicast-metric)

Full Context configure router isis level default-ipv4-multicast-metric

Description This command configures the default metric to be used for the IS-IS interface in the IPv4 multicast topology (MT3).

The **no** form of this command deletes the specified default metric and reverts to using the system default of 10.

Default default-ipv4-multicast-metric 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — Specifies the default metric for interfaces in the IPv4 multicast topology (MT3).

Values 1 to 16777215

Platforms All

8.66 default-ipv6-multicast-metric

default-ipv6-multicast-metric

Syntax **default-ipv6-multicast-metric** *metric*
no default-ipv6-multicast-metric

Context **[Tree]** (config>service>vprn>isis>level default-ipv6-multicast-metric)

Full Context configure service vprn isis level default-ipv6-multicast-metric

Description This command configures the default metric to be used for the IS-IS interface in the IPv6 multicast topology (MT4).

The **no** form of this command deletes the specified default metric and reverts to using the system default of 10.

Default default-ipv6-multicast-metric 10

Parameters *metric* — Specifies the default metric for interfaces in the IPv4 multicast topology (MT4).
1 to 16777215

default-ipv6-multicast-metric

Syntax **default-ipv6-multicast-metric** *metric*
no default-ipv6-multicast-metric

Context **[Tree]** (config>router>isis>level default-ipv6-multicast-metric)

Full Context configure router isis level default-ipv6-multicast-metric

Description This command configures the default metric to be used for the IS-IS interface in the IPv6 multicast topology (MT4).

The **no** form of this command deletes the specified default metric and reverts to using the system default of 10.

Default default-ipv6-multicast-metric 10

Parameters *metric* — Specifies the default metric for interfaces in the IPv4 multicast topology (MT4).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

1 to 16777215

Platforms All

8.67 default-ipv6-unicast-metric

default-ipv6-unicast-metric

Syntax **default-ipv6-unicast-metric** *ipv6 metric*
no default-ipv6-unicast-metric

Context **[Tree]** (config>service>vprn>isis>level default-ipv6-unicast-metric)

Full Context configure service vprn isis level default-ipv6-unicast-metric

Description This command specifies the default metric for IPv6 unicast.

Default default-ipv6-unicast-metric 10

Parameters *ipv6-metric* — Specifies the default metric for IPv6 unicast.

Values 1 to 16777215

Platforms All

default-ipv6-unicast-metric

Syntax **default-ipv6-unicast-metric** *ipv6 metric*
no default-ipv6-unicast-metric

Context **[Tree]** (config>router>isis>level default-ipv6-unicast-metric)

Full Context configure router isis level default-ipv6-unicast-metric

Description This command specifies the default metric for IPv6 unicast.

The **no** form of this command reverts to the default value.

Default default-ipv6-unicast-metric 10

Parameters *ipv6-metric* — Specifies the default metric for IPv6 unicast.

Values 1 to 16777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.68 default-label-preference

default-label-preference

Syntax **default-label-preference** [**ebgp** *ebgp label preference*] [**ibgp** *ibgp label preference*]
no default-label-preference

Context **[Tree]** (config>router>bgp default-label-preference)
[Tree] (config>router>bgp>group default-label-preference)
[Tree] (config>router>bgp>group>neighbor default-label-preference)

Full Context configure router bgp default-label-preference
configure router bgp group default-label-preference
configure router bgp group neighbor default-label-preference

Description This command specifies a route-table preference value to use for EBGP or IBGP routes carrying labeled-unicast prefixes and received from peers covered by the context of the command. Route-table preference comes into play when the route-table has multiple routes for the same IP prefix. In this case the route with the numerically lowest preference value is usually the route that is activated and installed into the IP FIB. By default all BGP routes have a route-table preference value of 170.

This command overrides the preference value assigned by the **label-preference** command; that other command does not distinguish between EBGP and IBGP routes. Overriding happens even when the default-label-preference value is inherited from a higher level of configuration and competes with an explicitly configured label-preference value at a lower level of configuration in the BGP hierarchy.

Note: The preference value assigned by the **default-label-preference** command can always be overwritten by a route policy entry that accepts the route with a **preference** command in the action.

The **no** form of the command lets BGP route-table preference for labeled-unicast routes to be controlled by other means.

Default no default-label-preference

Parameters *ebgp label preference* — Specifies the EBGP default preference label value.

Values 0 to 255

ibgp label preference — Specifies the IBGP default preference label value.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.69 default-metric

default-metric

Syntax **default-metric** *metric*
no default-metric

Context **[Tree]** (config>aaa>route-downloader default-metric)

Full Context configure aaa route-downloader default-metric

Description This command sets the default metric that routes imported by the RTM will acquire.

The **no** form of this command removes the metric.

Default default-metric 2

Parameters *metric* — Specifies the default metric of the routes imported.

Values 0 to 254

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

default-metric

Syntax **default-metric** *ipv4 metric*
no default-metric

Context **[Tree]** (config>service>vprn>isis>level default-metric)

Full Context configure service vprn isis level default-metric

Description This command specifies the configurable default metric used for all IS-IS interfaces on this level. This value is not used if a metric is configured for an interface.

Default default-metric 10

Parameters *ipv4 metric* — Specifies the default metric for IPv4 unicast.

Values 1 to 16777214

Platforms All

default-metric

Syntax **default-metric** *metric*
no default-metric

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>ospf>area>stub default-metric)
[Tree] (config>service>vprn>ospf3>area>stub default-metric)

Full Context configure service vprn ospf area stub default-metric
configure service vprn ospf3 area stub default-metric

Description This command configures the metric used by the area border router (ABR) for the default route into a stub area. The default metric should only be configured on an ABR of a stub area. An ABR generates a default route if the area is a **stub** area.

The **no** form of this command reverts to the default value.

Default default-metric 1

Parameters *metric* — The metric expressed as a decimal integer for the default route cost to be advertised into the stub area.

Values 1 to 16777214

Platforms All

default-metric

Syntax **default-metric** *ipv4 metric*
no default-metric

Context [Tree] (config>router>isis>level default-metric)

Full Context configure router isis level default-metric

Description This command specifies the configurable default metric used for all IS-IS interfaces on this level. This value is not used if a metric is configured for an interface.

The **no** form of this command reverts to the default value.

Default default-metric 10

Parameters *ipv4 metric* — Specifies the default metric for IPv4 unicast.

Values 1 to 16777214

Platforms All

default-metric

Syntax **default-metric** *metric*
no default-metric

Context [Tree] (config>router>ospf>area>stub default-metric)
[Tree] (config>router>ospf3>area>stub default-metric)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ospf area stub default-metric
configure router ospf3 area stub default-metric

Description This command configures the metric used by the area border router (ABR) for the default route into a stub area.

The default metric should only be configured on an ABR of a stub area.

An ABR generates a default route if the area is a **stub** area.

The **no** form of this command reverts to the default value.

Default default-metric 1

Parameters *metric* — Specifies the metric expressed as a decimal integer for the default route cost to be advertised into the stub area.

Values 1 to 16777214

Platforms All

8.70 default-msap-policy

default-msap-policy

Syntax **default-msap-policy** *policy-name*
no default-msap-policy

Context **[Tree]** (config>service>vpls>sap default-msap-policy)

Full Context configure service vpls sap default-msap-policy

Description This command specifies the default managed SAP policy to use to create MSAPs when the response from the RADIUS server does not specify a managed SAP policy.

The *policy-name* parameter is only valid for a SAP with the keywords **capture-sap** specified in the SAP's configuration. The **capture-sap** keyword in the SAP configuration captures the SAP where triggering packets is sent to the CPM. Non-triggering packets captured by the capture SAP is dropped.

The managed SAP policy must already be defined in the **config>subscr-mgmt>msap-policy** context.

The **no** form of this command removes the policy-name from the configuration.

Parameters *policy-name* — Specifies an existing default managed SAP policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.71 default-pap-password

default-pap-password

Syntax **default-pap-password** *password* [**hash** | **hash2** | **custom**]
no default-pap-password

Context **[Tree]** (config>subscr-mgmt>ppp-policy default-pap-password)

Full Context configure subscriber-mgmt ppp-policy default-pap-password

Description This command configures the default PAP password for RADIUS authentication when the Password-Length=0 in the PAP Authenticate-Request.

RADIUS authentication cannot be initiated when the Password-Length=0 in the PAP Authenticate-Request and no default-pap-password is configured. The PPP session terminates in this case.

Parameters *password* — Specifies a default PAP password up to 64 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.72 default-path

default-path

Syntax **default-path** *path-name*

Context **[Tree]** (config>router>mpls>lsp-template default-path)

Full Context configure router mpls lsp-template default-path

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description A default path binding must be provided before the LSP template can be used for signaling LSP. The LSP template must be shutdown to modify default-path binding.

Parameters *path-name* — Configures the default path binding

Platforms All

8.73 default-peer

default-peer

Syntax [**no**] **default-peer**

Context **[Tree]** (config>aaa>diam>node>peer default-peer)

Full Context configure aaa diameter node peer default-peer

Description This command designates a peer as a default peer. Traffic that is destined to realms that are not associated with locally configured peers, is sent to the default-peer. In effect, the default peer becomes a default route for Diameter realms.

This command is mandatory in multi-chassis redundancy where the inter-chassis peer is designated as default peer. Then, the SR with no open connections towards agents or servers, forwards all traffic to the inter-peer which maintains, as part of MCS, open connections with agents and servers.

The **no** form of this command reverts to the default.

Default no default-peer

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

default-peer

Syntax **default-peer**
no default-peer

Context **[Tree]** (config>service>vprn>msdp>group>peer default-peer)
[Tree] (config>service>vprn>msdp>peer default-peer)

Full Context configure service vprn msdp group peer default-peer
configure service vprn msdp peer default-peer

Description Using the default peer mechanism, a peer can be selected as the default Multicast Source Discovery Protocol (MSDP) peer. As a result, all source-active messages from the peer will be accepted without the usual peer-reverse-path-forwarding (RPF) check.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The MSDP peer-RPF check is different from the normal multicast RPF checks. The peer-RPF check is used to stop source-active messages from looping. A router validates source-active messages originated from other routers in a deterministic fashion.

A set of rules is applied in order to validate received source-active messages, and the first rule that applies determines the peer-RPF neighbor. All source-active messages from other routers are rejected. The rules applied to source-active messages originating at Router S received at Router R from Router N are as follows:

- If Router N and router S are one and the same, then the message is originated by a direct peer-RPF neighbor and will be accepted.
- If Router N is a configured peer, or a member of the Router R mesh group then its source-active messages are accepted.
- If Router N is the Border Gateway Protocol (BGP) next hop of the active multicast RPF route toward Router S then Router N is the peer-RPF neighbor and its source-active messages are accepted.
- If Router N is an external BGP peer of Router R and the last autonomous system (AS) number in the BGP AS-path to Router S is the same as Router N's AS number, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N uses the same next hop as the next hop to Router S, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N fits none of the above rules, then Router N is not a peer-RPF neighbor, and its source-active messages are rejected.

Default no default-peer

Platforms All

default-peer

Syntax [**no**] **default-peer**

Context **[Tree]** (config>router>msdp>peer default-peer)
[Tree] (config>router>msdp>group>peer default-peer)

Full Context configure router msdp group peer default-peer
configure router msdp peer default-peer

Description Using the default peer mechanism, a peer can be selected as the default Multicast Source Discovery Protocol (MSDP) peer. As a result, all source-active messages from the peer will be accepted without the usual peer-reverse-path-forwarding (RPF) check.

The MSDP peer-RPF check is different from the normal multicast RPF checks. The peer-RPF check is used to stop source-active messages from looping. A router validates source-active messages originated from other routers in a deterministic fashion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A set of rules is applied in order to validate received source-active messages, and the first rule that applies determines the peer-RPF neighbor. All source-active messages from other routers are rejected. The rules applied to source-active messages originating at Router S received at Router R from Router N are as follows:

- If Router N and router S are one and the same, then the message is originated by a direct peer-RPF neighbor and will be accepted.
- If Router N is a configured peer, or a member of the Router R mesh group then its source-active messages are accepted.
- If Router N is the Border Gateway Protocol (BGP) next hop of the active multicast RPF route toward Router S then Router N is the peer-RPF neighbor and its source-active messages are accepted.
- If Router N is an external BGP peer of Router R and the last autonomous system (AS) number in the BGP AS-path to Router S is the same as Router N's AS number, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N uses the same next hop as the next hop to Router S, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N fits none of the above rules, then Router N is not a peer-RPF neighbor, and its source-active messages are rejected.

Default no default-peer (No default peer is established and all active source messages must be RPF checked)

Platforms All

8.74 default-pool

default-pool

Syntax **default-pool** *pool-name*
no default-pool

Context **[Tree]** (config>service>ies>sub-if>grp-if>local-address-assignment default-pool)
[Tree] (config>service>ies>sub-if>local-address-assignment default-pool)
[Tree] (config>service>vprn>sub-if>grp-if>local-address-assignment default-pool)
[Tree] (config>service>vprn>sub-if>local-address-assignment default-pool)

Full Context configure service ies subscriber-interface group-interface local-address-assignment default-pool
configure service ies subscriber-interface local-address-assignment default-pool
configure service vprn subscriber-interface group-interface local-address-assignment default-pool
configure service vprn subscriber-interface local-address-assignment default-pool

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command references a default DHCP address pool for local PPPoX pool management in case that the pool-name is not returned via Radius or LUDB.

Parameters *pool-name* — Specifies the name of the local DHCP server pool.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.75 default-preference

default-preference

Syntax **default-preference** [**ebgp** *ebgp preference*] [**ibgp** *ibgp preference*]
no default-preference

Context **[Tree]** (config>router>bgp default-preference)
[Tree] (config>router>bgp>group default-preference)
[Tree] (config>router>bgp>group>neighbor default-preference)

Full Context configure router bgp default-preference
configure router bgp group default-preference
configure router bgp group neighbor default-preference

Description This command specifies a route-table preference value to use for EBGP or IBGP routes carrying unlabeled prefixes and received from peers covered by the context of the command. Route-table preference comes into play when the route-table has multiple routes for the same IP prefix. In this case, the route with the numerically lowest preference value is usually the route that is activated and installed into the IP FIB. By default all BGP routes have a route-table preference value of 170.

This command overrides the preference value assigned by the **preference** command; that other command does not distinguish between EBGP and IBGP routes. Overriding happens even when the default-preference value is inherited from a higher level of configuration and competes with an explicitly configured preference value at a lower level of configuration in the BGP hierarchy.

Note: The preference value assigned by the **default-preference** command can always be overwritten by a route policy entry that accepts the route with a **preference** command in the action.

The **no** form of the command lets BGP route-table preference to be controlled by other means.

Default no default-preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ebgp preference* — Specifies the EBGP default preference value.

Values 0 to 255

ibgp preference — Specifies the IBGP default preference value.

Values 0 to 255

Platforms All

8.76 default-priority

default-priority

Syntax **default-priority** {**high** | **low**}
no default-priority

Context **[Tree]** (config>qos>sap-ingress default-priority)

Full Context configure qos sap-ingress default-priority

Description This command configures the default enqueuing priority for all packets received on an ingress SAP using this policy. To change the default priority for the policy, the **fc-name** must be defined whether it is being changed or not.

Default default-priority low

Parameters **high** — Setting the enqueuing parameter to **high** for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

low — Setting the enqueuing parameter to **low** for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Platforms All

8.77 default-profile

default-profile

Syntax **default-profile** *profile-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no default-profile

Context [Tree] (config>app-assure>group>url-filter>web-service default-profile)

Full Context configure application-assurance group url-filter web-service default-profile

Description This command configures the default category profile to use when no category profile is explicitly selected for the subscriber.

The **no** form of this command removes the selected default profile configuration.

Default no default-profile

Parameters *profile-name* — Specifies a configured category profile to use as the default profile name, up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.78 default-result

default-result

Syntax **default-result** {**revoked** | **good**}
no default-result

Context [Tree] (config>service>ies>if>ipsec>ipsec-tunnel>dyn>cert>status-verify default-result)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn>cert>status-verify default-result)
[Tree] (config>service>ies>if>sap>ipsec-gw>cert>status-verify default-result)
[Tree] (config>service>vprn>if>sap>ipsec-gw>cert>status-verify default-result)
[Tree] (config>service>vprn>if>sap>ipsec-tun>dyn>cert>status-verify default-result)
[Tree] (config>router>if>ipsec>ipsec-tun>dyn>cert>status-verify default-result)
[Tree] (config>ipsec>trans-mode-prof>dyn>cert>status-verify default-result)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying cert default-result
configure router interface ipsec ipsec-tunnel dynamic-keying cert status-verify default-result
configure service ies interface ipsec ipsec-tunnel dynamic-keying cert status-verify default-result
configure service ies interface sap ipsec-gw cert status-verify default-result
configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert status-verify default-result
configure service vprn interface sap ipsec-gw cert status-verify default-result
configure service vprn interface sap ipsec-tunnel dynamic-keying cert status-verify default-result

Description This command specifies the default certificate revocation status that is used result when both the primary and secondary CSV methods fail to verify the status.

Default default-result revoked

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **good** — Specifies that the certificate is considered as acceptable.

revoked — Specifies that the certificate is considered as revoked.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ipsec-gw cert status-verify default-result
- configure service vprn interface sap ipsec-tunnel dynamic-keying cert status-verify default-result
- configure service vprn interface sap ipsec-gw cert status-verify default-result

VSR

- configure service ies interface ipsec ipsec-tunnel dynamic-keying cert status-verify default-result
- configure router interface ipsec ipsec-tunnel dynamic-keying cert status-verify default-result
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert status-verify default-result

8.79 default-retail-svc-id

default-retail-svc-id

Syntax **default-retail-svc-id** *service-id*
no default-retail-svc-id

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>vlan-tag-ranges default-retail-svc-id)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-tag-ranges default-retail-svc-id)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges default-retail-svc-id
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges default-retail-svc-id

Description This command specifies the id of default retail service if there is no match found in VLAN to retail map configuration (specified by the **vlan** command). For DSM and migrant, this command is only applicable for non-NAT stacks.

Parameters *service-id* — Specifies the identifier of the retail service to be used by default of a value in the retail service map of this interface.

Values 1 to 2147483650
svc-name: up to 64 characters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-retail-svc-id

Syntax **default-retail-svc-id** *service-id*

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges default-retail-svc-id)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges default-retail-svc-id)

Full Context configure service ies subscriber-interface group-interface wlan-gw ranges default-retail-svc-id
configure service vprn subscriber-interface group-interface wlan-gw ranges default-retail-svc-id

Description This command configures the default retailer service for WIFI users.

8.80 default-route-tag

default-route-tag

Syntax **default-route-tag** *tag*
no default-route-tag

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls default-route-tag)
[Tree] (config>service>epipe>bgp-evpn>srv6 default-route-tag)
[Tree] (config>service>epipe>bgp-evpn>vxlan default-route-tag)
[Tree] (config>service>vpls>bgp-evpn>vxlan default-route-tag)
[Tree] (config>service>vpls>bgp-evpn>mpls default-route-tag)
[Tree] (config>service>vprn>bgp-evpn>mpls default-route-tag)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 default-route-tag)

Full Context configure service epipe bgp-evpn mpls default-route-tag
configure service epipe bgp-evpn segment-routing-v6 default-route-tag
configure service epipe bgp-evpn vxlan default-route-tag
configure service vpls bgp-evpn mpls default-route-tag
configure service vpls bgp-evpn vxlan default-route-tag
configure service vprn bgp-evpn mpls default-route-tag
configure service vprn bgp-ivpn segment-routing-v6 default-route-tag

Description This command configures a route tag that EVPN and IP-VPN use when sending a route to the BGP application (for the corresponding service and BGP instance). If the corresponding BGP EVPN instance is enabled, the command cannot be changed. Additionally, EVPN services can add tags to routes with **proxy-arp/nd>evpn-route-tag** or the route table tag (added using the import policy). Only one tag is passed from EVPN to the BGP for matching on export policies. In case of a conflict with other route tags pushed by EVPN, the default route tag has the least priority.

The following are examples of the conflict priority handling:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If a service is configured with both **default-route-tag** *X* and **proxy-arp>evpn-route-tag** *Y*, EVPN uses route tag *Y* when sending EVPN proxy-arp routes to the BGP RIB for advertisement.
- If a given IP-prefix route is tagged in the route-table with tag *A* and the R-VPLS, in which the route is advertised, uses *B* as the **default-route-tag**, then EVPN keeps tag *A* when sending the route to the BGP RIB.

The **default-route-tag** configuration is only supported on EVPN and IP-VPN service routes. The route tag for ES and AD per-ES routes is always zero.

The **no** form of this command removes the **default-route-tag** (that is, it sets the route tag to zero).

Default no default-route-tag

Parameters *tag* — Specifies the route tag.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service epipe bgp-evpn segment-routing-v6 default-route-tag

All

- configure service vpls bgp-evpn vxlan default-route-tag
- configure service vprn bgp-evpn mpls default-route-tag
- configure service epipe bgp-evpn vxlan default-route-tag
- configure service epipe bgp-evpn mpls default-route-tag
- configure service vpls bgp-evpn mpls default-route-tag

default-route-tag

Syntax **default-route-tag** *tag*
no default-route-tag

Context **[Tree]** (config>service>vprn>isis default-route-tag)

Full Context configure service vprn isis default-route-tag

Description This command configures the route tag for default route for the router or VPRN service.

Parameters *tag* — Assigns a default tag.

Values 1 — 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

default-route-tag

Syntax **default-route-tag** *tag*
no default-route-tag

Context **[Tree]** (config>router>isis default-route-tag)

Full Context configure router isis default-route-tag

Description This command configures the route tag for default route.

Parameters *tag* — Assigns a default tag.

Values 1 to 4294967295

Platforms All

8.81 default-route-target

default-route-target

Syntax [**no**] **default-route-target**

Context **[Tree]** (config>router>bgp>group default-route-target)
[Tree] (config>router>bgp>group>neighbor default-route-target)

Full Context configure router bgp group default-route-target
configure router bgp group neighbor default-route-target

Description This command originates the default RTC route (zero prefix length) towards the selected peers.

Default no default-route-target

Platforms All

8.82 default-router

default-router

Syntax **default-router** *ip-address* [*ip-address*]
no default-router

Context **[Tree]** (config>router>dhcp>server>pool>subnet>options default-router)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>dhcp6>server>pool>subnet default-router)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options default-router)

Full Context configure router dhcp local-dhcp-server pool subnet options default-router
configure service vprn dhcp6 server pool subnet default-router
configure subscriber-mgmt local-user-db ipoe host options default-router

Description This command configures the IP address of the default router for a DHCP client. Up to four IP addresses can be specified.

The **no** form of this command removes the address(es) from the configuration.

Parameters *ip-address* — Specifies up to four default router IP addresses. Each address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.83 default-sap

default-sap

Syntax [**no**] **default-sap**

Context [Tree] (config>service>vpls>sap>managed-vlan-list default-sap)

Full Context configure service vpls sap managed-vlan-list default-sap

Description This command adds a default SAP to the managed VLAN list.

The **no** form of this command removes the default SAP to the managed VLAN list.

Platforms All

8.84 default-secure-service

default-secure-service

Syntax **default-secure-service** *service-id* **interface** *ip-int-name*
no default-secure-service

Context [Tree] (config>service>ies>if>sap>ipsec-gateway default-secure-service)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>sap>ipsec-gateway default-secure-service)

Full Context configure service ies interface sap ipsec-gateway default-secure-service
configure service vprn interface sap ipsec-gateway default-secure-service

Description This command specifies a service ID or service name of the default security service used by this SAP IPsec gateway.

Parameters *service-id* — Specifies a default secure service.

Values *service-id*: 1 to 2147483647*svc-name:* An existing service name up to 64 characters.

ip-int-name — The name of private IPsec tunnel interface.

8.85 default-set

default-set

Syntax **default-set** *set-id*
no default-set

Context [Tree] (config>router>mpls>class-forwarding-policy default-set)

Full Context configure router mpls class-forwarding-policy default-set

Description This command configures the default forwarding set.

Parameters *set-id* — Specifies the class forwarding set.

Values 1 to 4 (in system profile None/A)
1 to 6 (in system profile B)

Platforms All

8.86 default-tag

default-tag

Syntax **default-tag** *tag*
no default-tag

Context [Tree] (config>aaa>route-downloader default-tag)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa route-downloader default-tag

Description This command sets the default tag that routes processed by the AAA route downloader will take.

Note: Any route received with a specific tag retains the specific tag. The tag value is passed to the Route Table Manager and is available as match condition on the export statement of other routing protocols.

The **no** form of this command reverts to the default.

Default default-tag 0

Parameters *tag* — Specifies the default tag of the routes imported.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.87 default-tunnel-endpoint-limit

default-tunnel-endpoint-limit

Syntax **default-tunnel-endpoint-limit** *default-endpoint*
no default-tunnel-endpoint-limit

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>gtp-tunnel-database default-tunnel-endpoint-limit)

Full Context configure application-assurance group gtp gtp-filter gtp-tunnel-database default-tunnel-endpoint-limit

Description This command configures the maximum number of GTP endpoints requested in GTP-C messages by using, for example, the PDP Context Create message type.

The **validate-gtp-tunnels** command must be enabled before using this command.

The **no** form of this command sets the limit to 4294967295 (the maximum number of GTP endpoints supported by AA FW minus one).

Default no default-tunnel-endpoint-limit

Parameters *default-endpoint* — Specifies the limit.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.88 default-tunnel-template

default-tunnel-template

Syntax **default-tunnel-template** *ipsec-template-identifier*
no default-tunnel-template

Context **[Tree]** (config>service>ies>if>sap>ipsec-gateway default-tunnel-template)
[Tree] (config>service>vprn>if>sap>ipsec-gateway default-tunnel-template)

Full Context configure service ies interface sap ipsec-gateway default-tunnel-template
configure service vprn interface sap ipsec-gateway default-tunnel-template

Description This command configures a default tunnel policy template for the gateway.

8.89 default-user-name

default-user-name

Syntax **default-user-name** *ppp-username*
no default-user-name

Context **[Tree]** (config>subscr-mgmt>ppp-policy default-user-name)

Full Context configure subscriber-mgmt ppp-policy default-user-name

Description This command configures the default username for authentication when not provided in PAP/CHAP authentication (no Name field in CHAP Response message or Peer-Id-Length=0 in PAP Authenticate-Request).

The PPP session terminates when no username is provided in PAP/CHAP authentication and no default-user-name is configured.

Parameters *ppp-username* — Specifies a default username up to 253 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.90 default-value

default-value

Syntax **default-value** *value-name*
no default-value

Context **[Tree]** (config>app-assure>group>policy>aso>char default-value)

Full Context configure application-assurance group policy app-service-options characteristic default-value

Description This command assigns one of the characteristic values as default.

When a default value is specified, app-profile entries that do not explicitly include this characteristic inherit the default value and use it as part of the AQP match criteria based on that app-profile.

A default-value is required for each characteristic. This is evaluated at commit time.

The **no** form of this command removes the default value for the characteristic.

Parameters *value-name* — Specifies the name of an existing characteristic value.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.91 defaults

defaults

Syntax **defaults**

Context **[Tree]** (config>router>dhcp6>server defaults)

Full Context configure router dhcp6 local-dhcp-server defaults

Description Commands in this context configure server default timer and option parameters. These can be overridden on a per-pool and per-prefix basis.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

defaults

Syntax **defaults**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>gtp>apn-policy>apn defaults)

Full Context configure subscriber-mgmt gtp apn-policy apn defaults

Description Commands in this context configure default parameters for the GTP connection that can be used when the parameters are not returned in authentication.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.92 delay

delay

Syntax **delay**

Context [Tree] (config>router>if>if-attribute delay)

Full Context configure router interface if-attribute delay

Description Commands in this context configure or apply delay interface attributes such as static delay.

Platforms All

delay

Syntax **delay** *interval*

Context [Tree] (config>system>management-interface>cli>md-cli>environment>progress-indicator delay)

Full Context configure system management-interface cli md-cli environment progress-indicator delay

Description This command sets the delay before the progress indicator is displayed in the MD-CLI.

Default delay 500

Parameters *interval* — Specifies the delay interval, in milliseconds.

Values 1 to 10000

Platforms All

delay

Syntax **delay** *delay-measurement-type*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>test-oam>link-meas>template delay)

Full Context configure test-oam link-measurement measurement-template delay

Description This command configures the type of delay measurement statistic used in both the sample window and aggregate sample window.

The **no** form of this command reverts to the default value.

Default delay min

Parameters *delay-measurement-type* — Specifies the type of delay measurement that is used for comparison and reporting.

Values **min** — Keyword to take the minimum of a series of measurements for comparison and reporting.

max — Keyword to take the maximum of a series of measurements for comparison and reporting.

avg — Keyword to compute the average of a series of measurements for comparison and reporting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.93 delay-event

delay-event

Syntax **delay-event** {**forward** | **backward** | **round-trip**} **lowest-bin** *bin-number* **threshold***raise-threshold* [**clear** *clear-threshold*]

no delay-event {**forward** | **backward** | **round-trip**}

Context [Tree] (config>oam-pm>bin-group>bin-type delay-event)

Full Context configure oam-pm bin-group bin-type delay-event

Description This command sets the bin number, the threshold and the direction that is monitored to determine if a delay metric threshold crossing event has occurred or has cleared. It requires a bin number, a rising threshold value and a direction. If the *clear-threshold* value is not specified, the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and without regard to any previous window. When a raise threshold is reached, the log event is generated. Each unique threshold can only be raised once for the threshold within measurement interval. If the optional clear threshold is specified, the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

carried forward to following measurement intervals. If a threshold crossing event is raised another is not raised until a measurement interval completes, and the clear threshold has not been exceeded. A clear event is raised under that condition. In general, alarms are generated when there is a state change. The thresholds configured are applied to the count in specified bin and all higher number bins.

The **no** form of this command removes thresholding for this delay metric. The complete command must be configured in order to remove the specific threshold.

Parameters **forward** — Specifies the threshold is applied to the forward direction bin.

backward — Specifies the threshold is applied to the backward direction bin.

round-trip — Specifies the threshold is applied to the roundtrip direction bin.

bin-number — Specifies the number of the bin that the threshold is applied to. This bin and all higher bins are monitored to determine if the sum total results in these bins have reached or crossed the configured threshold.

Values 0 to 9

raise-threshold — Specifies the rising numerical value in the range that determines when the event is to be generated, when value reached.

Values 1 to 864000

clear-threshold — Specifies an optional numerical value in the range threshold used to indicate stateful behavior that allows the operator to configure a lower value than the rising threshold that determines when the clear event should be generated. Clear is generated when the end of measurement interval count is less than or equal to the configured value. If this option is not configured the behavior is stateless. Zero means no results can exist in the lower bin or any higher.

Values 0 to 863999

Default Clear threshold disabled

Platforms All

8.94 delay-event-exclusion

delay-event-exclusion

Syntax **delay-event-exclusion** {**forward** | **backward** | **round-trip**} **lowest-bin** *bin-number*
no delay-event-exclusion {**forward** | **backward** | **round-trip**}

Context **[Tree]** (config>oam-pm>bin-group>bin-type delay-event-exclusion)

Full Context configure oam-pm bin-group bin-type delay-event-exclusion

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This optional command allows results from probes that map to the specified bin and higher bins to be excluded from the TCA count. The TCA count is used to determine if a threshold has been reached by the event monitoring function. Individual counters are incremented in the bin, but the counts in the specified bin and higher bins are not included in the TCA threshold computation. A **delay-event** must be configured in the same direction, and the **lowest-bin** configured as part of the **delay-event-exclusion** command must be higher than the lowest bin specified by the corresponding **delay-event** command.

The bin group allows this optional command to be added, modified, or deleted while tests are actively referencing the bin group. The bin group does not need to be shut down during **delay-event-exclusion** configuration. If the values are modified while the active tests are executing, all configured TCAs for the specified direction within the bin group enters a pending (p) state until the start of the next measurement interval. Any existing stateful TCAs that were raised are cleared without creating a log event, and no further processing for the affected TCAs occur in the active window. Depending on timing, the pending state may continue past the adjacent measurement interval until the start of the following measurement interval.

The **no** form of this command does not exclude any values from the configured TCA threshold.

Default no delay-event-exclusion forward

no delay-event-exclusion backward

no delay-event-exclusion round-trip

Parameters **forward** — Specifies the forward direction bin.

backward — Specifies the backward direction bin.

round-trip — Specifies the round-trip direction bin.

bin-number — Specifies the number of the lowest bin that the exclusion is applied to. This bin and all higher bins are excluded from the **delay-event** (TCA) count. If no bin numbers are configured, this command is ignored.

Values 1 to 9

Platforms All

8.95 delay-events

delay-events

Syntax [**no**] **delay-events**

Context **[Tree]** (config>oam-pm>session>measurement-interval>event-mon delay-events)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure oam-pm session measurement-interval event-mon delay-events

Description This enables the monitoring of all configured delay events. Adding this functionality starts the monitoring of the configured delay events at the start of the next measurement interval. If the function is removed using the **no** command, all monitoring of configured delay events, logging, and recording of new events for that session are suspended. Any existing events at the time of the shut down are maintained until the active measurement window in which the removal was performed has completed. The state of this monitoring function can be changed without having to shutdown all the tests in the session.

The **no** form of this command disables the monitoring of all configured delay events.

8.96 delay-selection

delay-selection

Syntax **delay-selection {static | dynamic | static-preferred | dynamic-preferred}**
no delay-selection

Context **[Tree]** (config>router>if>if-attr>delay delay-selection)

Full Context configure router interface if-attribute delay delay-selection

Description This command selects the delay source to be advertised by the IGP for this interface.

The **no** form of this command reverts to the default value.

Default delay-selection static-preferred

Parameters **static** — Keyword to use only statically configured delay and ignore dynamic delay measurements generated by **link-measurement**.

dynamic — Keyword to use only dynamic delay measurements generated by **link-measurement** and ignore statically configured delay.

static-preferred — Keyword to prefer the configured static delay over the dynamic delay. If static delay is not configured, the delay reported using **link-measurement** is used.

dynamic-preferred — Keyword to prefer the dynamic reported delay over the statically configured delay. If no dynamic delay has been reported using **link-measurement**, the statically configured delay is used.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.97 delay-start-time

delay-start-time

Syntax **delay-start-time** *delay*
no delay-start-time

Context **[Tree]** (config>subscr-mgmt>acct-plcy delay-start-time)

Full Context configure subscriber-mgmt radius-accounting-policy delay-start-time

Description It is recommended to only use this command when **session-accounting** is used. By default, a dual stack subscriber generates a RADIUS accounting interim message for each new host update (IPv4, IPv6 WAN, and IPv6 PD). This command delays the trigger of a RADIUS accounting start message and allows all hosts to connect first. When the delay timer expires, a single RADIUS accounting start message containing all the host currently connected to the BNG is sent to the server. Subsequent host connections will trigger interim-updates if host-update is enabled on session-accounting. For all other accounting modes, this command will delay the trigger of an accounting start when a host connects.

The **no** form of this command reverts to the default.

Default no delay-start-time

Parameters *delay* — Specifies the accounting start delay, in seconds.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.98 delay-template

delay-template

Syntax **delay-template** *delay-template-name*
no delay-template

Context **[Tree]** (config>oam-pm>session>ethernet>dmm delay-template)

Full Context configure oam-pm session ethernet dmm delay-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a reference to a **config>oam-pm>streaming delay-template** for the Ethernet DMM test. It is possible to include a delay template reference that is not configured under **config>oam-pm>streaming**. In this case, the streaming of the results is not in effect. Refer to the **config>oam-pm>streaming delay-template** command for session to template interaction behaviors.

The **no** form of this command deletes the delay template from the test.

Default no delay-template

Parameters *delay-template-name* — Specifies the delay template name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

delay-template

Syntax **delay-template** *delay-template-name*
no delay-template

Context **[Tree]** (config>oam-pm>session>ip>twamp-light delay-template)

Full Context configure oam-pm session ip twamp-light delay-template

Description This command specifies a reference to a **config>oam-pm>streaming delay-template** for the IP TWAMP LIGHT test. It is possible to include a delay template reference that is not configured under **config>oam-pm>streaming**. In this case, streaming of results are not in effect. Refer to the **config>oam-pm>streaming delay-template** command for session to template interaction behaviors.

The **no** form of this command deletes the delay template from the test.

Default no delay-template

Parameters *delay-template-name* — Specifies the delay template name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

delay-template

Syntax **delay-template** *delay-template-name*
no delay-template

Context **[Tree]** (config>oam-pm>session>mpls>dm delay-template)

Full Context configure oam-pm session mpls dm delay-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a reference to a **config>oam-pm>streaming delay-template** for the MPLS DM test. It is possible to include a delay template reference that is not configured under **config>oam-pm>streaming**. In this case, streaming of results are not in effect. Refer to the **config>oam-pm>streaming delay-template** command for session to template interaction behaviors.

The **no** form of this command deletes the delay template from the test.

Default no delay-template

Parameters *delay-template-name* — Specifies the delay template name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

delay-template

Syntax **delay-template** *template-name* [**create**]
no delay-template *template-name*

Context **[Tree]** (config>oam-pm>streaming delay-template)

Full Context configure oam-pm streaming delay-template

Description This command specifies a template for streaming delay metrics that can be referenced under the **oam-pm>session** technology delay style test.

The **delay-template** must be configured under the technology delay test **oam-pm>session** to allow the delay specific test to stream results using the configured template attributes.

The **no** form of this command deletes the specified delay template.

Parameters *template-name* — Specifies the template name, up to 64 characters.

create — Creates the template.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.99 delegated-ipv6-prefix

delegated-ipv6-prefix

Syntax [**no**] **delegated-ipv6-prefix**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute delegated-ipv6-prefix)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute delegated-ipv6-prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the generation of the **delegated-ipv6-prefix** RADIUS attribute.

The **no** form of this command disables the generation of the **delegated-ipv6-prefix** RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.100 delegated-prefix-length

delegated-prefix-length

Syntax **delegated-prefix-length** [**minimum** *prefix-length*] [**maximum** *prefix-length*]
no delegated-prefix-length

Context **[Tree]** (config>router>dhcp6>server>pool delegated-prefix-length)
[Tree] (config>service>vprn>dhcp6>server>pool delegated-prefix-length)

Full Context configure router dhcp6 local-dhcp-server pool delegated-prefix-length
configure service vprn dhcp6 local-dhcp-server pool delegated-prefix-length

Description This command configures the delegated prefix length that is used if the DHCPv6 client does not specify a prefix length hint.

The DHCPv6 client prefix length hint is limited by the range specified by the **minimum** and **maximum** parameters. If the hint is smaller than the minimum, the allocated prefix length is equal to the minimum length. If the hint is larger than the maximum, the allocated prefix length is equal to the maximum length.

The **no** form of this command reverts to the default.

Default delegated-prefix-length 64 minimum 48 maximum 64

Parameters *prefix-length* — Specifies the minimum or maximum allowed prefix length, in bits.

Values 48 to 127

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

delegated-prefix-length

Syntax **delegated-prefix-length** *bits*
delegated-prefix-length variable
no delegated-prefix-length

Context **[Tree]** (config>service>ies>sub-if>ipv6 delegated-prefix-length)
[Tree] (config>service>vprn>sub-if>ipv6 delegated-prefix-length)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface ipv6 delegated-prefix-length
configure service vprn subscriber-interface ipv6 delegated-prefix-length

Description This command configures the subscriber interface level setting for delegated prefix length. The delegated prefix length for a subscriber- interface can be either set to a fixed value that is explicitly configured under the subscriber interface CLI hierarchy or a variable value that can be obtained from various sources. This command can be changed only when no IPv6 prefixes are configured under the **subscriber-interface** context.

The **no** form of this command reverts to the default.

Default no delegated-prefix-length (the delegated prefix length is 64)

Parameters *bits* — Specifies the delegated prefix length in bits. This value is applicable to the entire subscriber interface. In case that the delegated prefix length is also supplied via other means (LUDB, RADIUS or DHCP Server), such supplied value must match the value configured under the **subscriber-interface** context. Otherwise, the prefix instantiation in the router fails.

Values 48 to 64

variable — Specifies that the delegated prefix value can be of any length between 48 to 64. The value itself can vary between the prefixes and is provided at the time of prefix instantiation. The order of priority for the source of the delegated prefix length is:

- LUDB
- RADIUS
- DHCPv6 server

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.101 delete

delete

Syntax **delete** *file-url* [**force**] [**no-redirect**] [**client-tls-profile** *profile*] [**proxy** *proxy-url*]

Context **[Tree]** (file delete)

Full Context file delete

Description This command deletes the specified file.

The optional wildcard (*) can be used to delete multiple files that share a common (partial) prefix and/or (partial) suffix. When the wildcard is entered, the following prompt displays for each file that matches the wildcard:

“Delete file <filename> (y/n)?”

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *file-url* — Specifies the file name to delete.

Values	
local-url	[*cflash-id*/][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp:// | http:// | https://}*login*:*pswd@remote-locn*/][*file-path*] up to 247 characters directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

force — Forces an immediate deletion of the specified file(s). The command **file delete * force** deletes all the wildcard matching files without displaying a user prompt message. This command also automatically accepts HTTP redirects unless overridden by the **no-redirect** parameter.

profile — Specifies the TLS client profile configured under **config**>**system**>**security**>**tls**>**client-tls-profile** to use.

proxy-url — Specifies the URL of an HTTP proxy. For example, http://proxy.mydomain.com:8000. This URL must be an HTTP URL and not an HTTPS URL.

no-redirect — Specifies to automatically refuse any HTTP redirects without prompting the user.

Platforms All

delete

Syntax **delete** [*line*]

Context **[Tree]** (candidate delete)

Full Context candidate delete

Description This command deletes the selected CLI node (which includes all sub-branches). The deleted lines are also copied into a temporary buffer that can be used for a subsequent insert.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *line* — Indicates which line to delete.

Values

line, offset, **first**, **edit-point**, **last**

line	absolute line number
offset	relative line number to current edit point. Prefixed with '+' or '-'
first	keyword - first line
edit-point	keyword - current edit point
last	keyword - last line that is not 'exit'

delete

Syntax **delete** [{*checkpoint-id* | **rescue** | **latest-rb**}]

Context **[Tree]** (admin>rollback delete)

Full Context admin rollback delete

Description This command deletes a rollback checkpoint and causes the suffixes to be adjusted (decremented) for all checkpoints older that the one that was deleted (to close the hole in the list of checkpoint files and create room to create another checkpoint).

If **config redundancy rollback-sync** is enabled, a rollback delete will also delete the equivalent checkpoint on the standby CF and shuffle the suffixes on the standby CF.

It is not advised to manually delete a rollback checkpoint (for example, using a **file delete** command). If a rollback checkpoint file is manually deleted without using the **admin rollback delete** command then the suffixes of the checkpoint files are not shuffled, nor is the equivalent checkpoint file deleted from the standby CF. This manual deletion creates a hole in the checkpoint file list until enough new checkpoints have been created to roll the hole off the end of the list.

Parameters *checkpoint-id* — An ID indicating a specific rollback checkpoint. A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback location) with *.rb.1 as the suffix, 2 for file *.rb.2, and so on.

Values 1 to 9

latest-rb — Specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file).

rescue — Deletes the rescue checkpoint. No checkpoint suffix numbers are changed.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.102 delete-config

delete-config

Syntax [**no**] **delete-config**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization delete-config)

Full Context configure system security profile netconf base-op-authorization delete-config

Description This command enables the NETCONF delete-config operation.

The **no** form of this command disables the operation.

Default no delete-config

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

8.103 delete-pending

delete-pending

Syntax [**no**] **delete-pending**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state delete-pending)

Full Context configure subscriber-mgmt wlan-gw ue-query state delete-pending

Description This command enables matching on UEs that are in a delete-pending state.

The **no** form of this command disables matching on UEs in a delete pending-state, unless all state matching is disabled.

Default no delete-pending

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.104 delivery-service

delivery-service

Syntax **delivery-service** *service-id*
delivery-service name *service-name*
no delivery-service

Context [Tree] (config>service>ies>if>sap>ip-tunnel delivery-service)
[Tree] (config>service>vprn>if>sap>ip-tunnel delivery-service)

Full Context configure service ies interface sap ip-tunnel delivery-service
configure service vprn interface sap ip-tunnel delivery-service

Description This command sets the delivery service for GRE encapsulated packets associated with a particular GRE tunnel. This is the IES or VPRN service where the GRE encapsulated packets are injected and terminated. The delivery service may be the same service that owns the private tunnel SAP associated with the GRE tunnel. The GRE tunnel does not come up until a valid delivery service is configured.

The **no** form of this command deletes the delivery-service from the GRE tunnel configuration.

Parameters *service-id* — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **delivery-service name** *service-name* variant can be used in all configuration modes.

Values {*id* | *svc-name*}

id:	1 to 2147483647
svc-name:	up to 64 characters (*svc-name* is an alias for input only. The *svc-name* gets replaced with an id automatically by SR OS in the configuration).

service-name — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

Values 1 to 64 characters

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.105 delta-consumed-agg-rate

delta-consumed-agg-rate

Syntax **delta-consumed-agg-rate percent** *percent-of-delta-consumed-agg-rate*
no delta-consumed-agg-rate

Context **[Tree]**
(config>qos>adv-config-policy>child-control>bandwidth-distribution>above-offered-allowance delta-consumed-agg-rate)

Full Context configure qos adv-config-policy child-control bandwidth-distribution above-offered-allowance delta-consumed-agg-rate

Description This command configures the percentage of the delta (from the beginning to the end of the current H-QoS below CIR or above CIR pass) of the aggregate rate consumed by its other members that can be given to a queue at the end of an H-QoS below CIR pass and above CIR pass. This command is only applicable when the port scheduler is configured to use the **above-offered-allowance-control** algorithm, otherwise it is ignored.

The **no** form of this command reverts the **delta-consumed-agg-rate percent** to its default value.

Default delta-consumed-agg-rate 20.00

Parameters *percent-of-delta-consumed-agg-rate* — Specifies the percentage of the delta (over the current H-QoS below CIR or above CIR pass) consumed aggregate rate that can be given to a queue.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.106 delta-consumed-higher-tier-rate

delta-consumed-higher-tier-rate

Syntax **delta-consumed-higher-tier-rate percent** *percent-of-delta-consumed-high-tier-rate*
no delta-consumed-higher-tier-rate

Context **[Tree]**
(config>qos>adv-config-policy>child-control>bandwidth-distribution>above-offered-allowance delta-consumed-higher-tier-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos adv-config-policy child-control bandwidth-distribution above-offered-allowance delta-consumed-higher-tier-rate

Description This command configures the percentage of the delta (from the beginning to the end of the current H-QoS below CIR or above CIR pass) of the higher tier rate consumed by its other members that can be given to a queue at the end of an H-QoS below CIR pass and above CIR pass. Higher tier refers to the Vport aggregate rate and port scheduler level, group, and maximum rates.

This command is only applicable when the port scheduler is configured to use the **above-offered-allowance-control** algorithm, otherwise it is ignored.

The **no** form of this command reverts the **delta-consumed-higher-tier-rate percent** to its default value.

Default delta-consumed-higher-tier-rate 5.00

Parameters *percent-of-delta-consumed-high-tier-rate* — Specifies the percentage of the delta (over the current H-QoS below CIR or above CIR pass) consumed higher tier rate that can be given to a queue.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.107 delta-in-use-limit

delta-in-use-limit

Syntax **delta-in-use-limit** *limit*
no delta-in-use-limit

Context **[Tree]** (config>vrrp>policy delta-in-use-limit)

Full Context configure vrrp policy delta-in-use-limit

Description This command sets a lower limit on the virtual router in-use priority that can be derived from the delta priority control events.

Each *vrrp-priority-id* places limits on the delta priority control events to define the in-use priority of the virtual router instance. Setting this limit prevents the sum of the delta priority events from lowering the in-use priority value of the associated virtual router instances below the configured value.

The limit has no effect on explicit priority control events. Explicit priority control events are controlled by setting the in-use priority to any value between 1 and 254.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Only non-owner virtual router instances can be associated with VRRP priority control policies and their priority control events.

Once the total sum of all delta events is calculated and subtracted from the base **priority** of the virtual router instance, the result is compared to the **delta-in-use-limit** value. If the result is less than the limit, the **delta-in-use-limit** value is used as the virtual router in-use priority value. If an explicit priority control event overrides the delta priority control events, the **delta-in-use-limit** has no effect.

Setting the limit to a higher value than the default of 1 limits the effect of the delta priority control events on the virtual router instance base **priority** value. This allows for multiple priority control events while minimizing the overall effect on the in-use priority.

Changing the *in-use-priority-limit* causes an immediate re-evaluation of the in-use priority values for all virtual router instances associated with this *vrrp-policy-id* based on the current sum of all active delta control policy events.

The **no** form of the command reverts to the default value.

Default delta-in-use-limit 1 — Specifies the lower limit of 1 for the in-use priority, as modified, by delta priority control events.

Parameters *limit* — Specifies the lower limit of the in-use priority base, as modified by priority control policies. The *in-use-priority-limit* has the same range as the non-owner virtual router instance base-priority parameter. If the result of the total delta priority control events minus the virtual router instances base-priority, is less than the *in-use-priority-limit*, the *in-use-priority-limit* value is used as the virtual router instances in-use priority value.

Setting the *in-use-priority-limit* to a value equal to or larger than the virtual router instance *base-priority* prevents the delta priority control events from having any effect on the virtual router instance in-use priority value.

Values 1 to 254

Platforms All

8.108 dent-threshold

dent-threshold

Syntax **dent-threshold** *threshold*
no dent-threshold

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd dent-threshold)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip dent-threshold)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd dent-threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd dent-threshold
configure mcast-management multicast-info-policy video-policy video-interface pip dent-threshold
configure mcast-management multicast-info-policy video-policy video-interface sd dent-threshold

Description This command sets the threshold value below which the FCC server will dent/drop unicast data sent to the FCC client during a fast channel change. Within the RTP extension header, the packet priority (PRI) (2 bits) and the fine-grained priority (FPRI) (3 bits) indicate the "importance" of the frame as to how essential it is to the video stream.

This parameter is only applicable if the FCC server mode is **dent**.

The **no** form of the command returns the parameter to the default value.

Default dent-threshold 16 (only B frames are dropped)

Parameters *threshold* — Specifies the threshold value is used by the FCC server to compare with the concatenation of the PRI and FPRI to determine whether to send the packet to the FCC client. If the PRI and FPRI expressed as a decimal integer is greater than or equal to the threshold value, the packet will be sent.

Values 1 to 31

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

8.109 deny-list

deny-list

Syntax **[no] deny-list** *deny-list-name*

Context **[Tree]** (config>app-assure>group>url-filter>local-filtering deny-list)

Full Context configure application-assurance group url-filter local-filtering deny-list

Description This command adds a **deny-list** URL list to the local URL filter policy.

The **no** form of this command removes the URL list object.

Default no deny-list

Parameters *deny-list-name* — Specifies the URL list name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.110 depleted-event

depleted-event

Syntax [**no**] **depleted-event**

Context **[Tree]** (config>service>vprn>dhcp6>server>pool>prefix>thresholds>minimum-free depleted-event)
[Tree] (config>router>dhcp6>server>pool>prefix>thresholds>minimum-free depleted-event)

Full Context configure router dhcp6 local-dhcp-server pool prefix thresholds minimum-free depleted-event
configure service vprn dhcp6 local-dhcp-server pool prefix thresholds minimum-free depleted-event

Description This command enables the system to send out a warning when the prefix with a configured length is no longer available in the provisioned prefix.

For example:

```
prefix 2001:0:0:ffe0::/50 pd wan-host create
   thresholds
       minimum-free prefix-length 64
           depleted-event
```

With the above configuration, the system will send out a warning when there is no available /64 that can be allocated out of 2001:0:0:ffe0::/50.

The **no** form of this command disables the warnings.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

depleted-event

Syntax [**no**] **depleted-event**

Context **[Tree]** (config>service>vprn>dhcp6>server>pool>thresholds>minimum-free depleted-event)
[Tree] (config>router>dhcp6>server>pool>thresholds>minimum-free depleted-event)

Full Context configure router dhcp6 local-dhcp-server pool thresholds minimum-free depleted-event
configure service vprn dhcp6 local-dhcp-server pool thresholds minimum-free depleted-event

Description This command enables the system to send out warnings when the prefix with the configured length is no longer available in the pool.

The **no** form of this command disables the warnings.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.111 derived-id

derived-id

Syntax **derived-id** *derived-id-string*
no derived-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident derived-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-ident derived-id)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification derived-id
configure subscriber-mgmt local-user-db ppp host host-identification derived-id

Description This command configures an ASCII string that uniquely identifies a host and is derived by a Python script from packet content available during a DHCP transaction or PPPoE session establishment.

Note: This command is only used when **derived-id** is configured as one of the **match-list** parameters.

The **no** form of this command removes the derived-id from the configuration.

Parameters *derived-id-string* — Specifies the host ID to be derived by a python script from DHCP or PPPoE packets, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.112 description

description

Syntax **description** *tiny-description-string*
no description

Context **[Tree]** (config>ipsec>static-sa description)

Full Context configure ipsec static-sa description

Description This command configures a text description that is stored in the configuration file. The text string is associated with a configuration context to identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *tiny-description-string* — Specifies the description character string. Allowed values are any string, up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

description

Syntax **description** *short-description-string*
no description

Context **[Tree]** (config>bmp>station description)
[Tree] (config>router>bgp description)
[Tree] (config>router>bgp>group description)
[Tree] (config>router>bgp>group>neighbor description)
[Tree] (config>card>fp>ingress>access>queue-group description)
[Tree] (config>card>fp>ingress>network>queue-group description)
[Tree] (config>eth-tunnel>path>eth-cfm>mep description)
[Tree] (config>fwd-path-ext>fpe description)
[Tree] (config>lag>link-map-profile description)
[Tree] (config>port>ethernet>access>egr>qgrp description)
[Tree] (config>port>ethernet>access>egr>vport description)
[Tree] (config>port>ethernet>access>ing>qgrp description)
[Tree] (config>port>ethernet>eth-cfm>mep description)
[Tree] (config>port>ethernet>network>egr>qgrp description)
[Tree] (config>port>ethernet>egress>hs-sec-shaper description)
[Tree] (config>port-xc>pxc description)
[Tree] (config>qos>fp-resource-policy description)
[Tree] (config>redundancy>multi-chassis>peer description)
[Tree] (config>connection-profile description)
[Tree] (config>service>apipe description)
[Tree] (config>service>apipe>endpoint description)
[Tree] (config>service>cpipe description)
[Tree] (config>service>cpipe>endpoint description)
[Tree] (config>service>epipe description)
[Tree] (config>service>epipe>spoke-sdp description)
[Tree] (config>service>epipe>endpoint description)
[Tree] (config>service>fpipe description)
[Tree] (config>service>fpipe>endpoint description)
[Tree] (config>service>ipipe description)
[Tree] (config>service>ipipe>endpoint description)
[Tree] (config>service>ipipe>spoke-sdp description)
[Tree] (config>eth-tunnel>path description)
[Tree] (config>filter>dhcp-filter description)
[Tree] (config>ipsec>client-db description)
[Tree] (config>ipsec>client-db>client description)
[Tree] (config>ipsec>ike-policy description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>ipsec>tnl-temp description)
[Tree] (config>isa>ipsec-group description)
[Tree] (config>isa>tunnel-group description)
[Tree] (config>qos>hw-agg-shap-sched-plcy description)
[Tree] (config>router>dhcp>server description)
[Tree] (config>router>dhcp>server>pool description)
[Tree] (config>router>dhcp6>server description)
[Tree] (config>router>dhcp6>server>pool description)
[Tree] (config>service>ies>aarp-interface>spoke-sdp description)
[Tree] (config>service>ies>if>dhcp description)
[Tree] (config>service>ies>if>ipv6>dhcp6-relay description)
[Tree] (config>service>ies>if>sap>eth-cfm>mep description)
[Tree] (config>service>ies>if>sap>ip-tunnel description)
[Tree] (config>service>ies>if>spoke-sdp description)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep description)
[Tree] (config>service>ies>sub-if>dhcp description)
[Tree] (config>service>ies>sub-if>grp-if>dhcp description)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep description)
[Tree] (config>service>ies>sub-if>grp-if>srrp description)
[Tree] (config>service>ies>sub-if>grp-if>ppp description)
[Tree] (config>service>ies>sub-if>grp-if>pppoe description)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>relay description)
[Tree] (config>service>vpls>sap>ipoe-session description)
[Tree] (config>service>vprn>if>dhcp description)
[Tree] (config>service>vprn>if>sap description)
[Tree] (config>service>vprn>if>sap>ip-tunnel description)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel description)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay description)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe description)
[Tree] (config>subscr-mgmt>loc-user-db description)
[Tree] (config>subscr-mgmt>ppp-policy description)
[Tree] (config>subscr-mgmt>acct-plcy description)
[Tree] (config>subscr-mgmt>rip-plcy description)
[Tree] (config>filter>gre-tun-tmp description)
[Tree] (config>filter>ip-exception description)
[Tree] (config>filter>ip-exception>entry description)
[Tree] (config>filter>ip-filter description)
[Tree] (config>filter>ip-filter>entry description)
[Tree] (config>filter>ipv6-filter description)
[Tree] (config>filter>ipv6-filter>entry description)
[Tree] (config>filter>ipv6-exception description)
[Tree] (config>filter>ipv6-exception>entry description)
[Tree] (config>filter>log description)
[Tree] (config>filter>mac-filter description)
[Tree] (config>filter>mac-filter>entry description)
[Tree] (config>filter>redirect-policy description)
[Tree] (config>filter>redirect-policy>destination description)
[Tree] (config>filter>match-list>ip-prefix-list description)
[Tree] (config>filter>match-list>ipv6-prefix-list description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>filter>match-list>port-list description)
[Tree] (config>filter>match-list>protocol-list description)
[Tree] (config>qos>match-list>ip-prefix-list description)
[Tree] (config>qos>match-list>ipv6-prefix-list description)
[Tree] (config>qos>match-list>port-list description)
[Tree] (config>qos>network-queue description)
[Tree] (config>qos>policer-control-policy description)
[Tree] (config>qos>policer-control-policy>tier>arbiter description)
[Tree] (config>qos>post-policer-mapping description)
[Tree] (config>router>fad>flex-algo description)
[Tree] (config>router>if>dhcp description)
[Tree] (config>router>if>eth-cfm>mep description)
[Tree] (config>router>if>vrrp description)
[Tree] (config>router>network-domains>network-domain description)
[Tree] (config>router>origin-validation>rpki-session description)
[Tree] (config>router>pcp-server>server description)
[Tree] (config>router>route-next-hop-policy>template description)
[Tree] (config>router>mcac>if-policy description)
[Tree] (config>router>mcac>policy description)
[Tree] (config>router>mcac>policy>bundle description)
[Tree] (config>router>rip description)
[Tree] (config>router>rip>group description)
[Tree] (config>router>rip>group>neighbor description)
[Tree] (config>router>ripng description)
[Tree] (config>router>ripng>group description)
[Tree] (config>router>ripng>group>neighbor description)
[Tree] (config>router>static-route-entry>black-hole description)
[Tree] (config>router>static-route-entry>indirect description)
[Tree] (config>router>static-route-entry>next-hop description)
[Tree] (config>service>ies description)
[Tree] (config>subscr-mgmt>gtp>peer-profile description)
[Tree] (config>service>sdp>binding>pw-port description)
[Tree] (config>service>vpls>endpoint description)
[Tree] (config>service>vprn>aarp-interface>spoke-sdp description)
[Tree] (config>service>vprn>bgp description)
[Tree] (config>service>vprn>bgp>group description)
[Tree] (config>service>vprn>bgp>group>neighbor description)
[Tree] (config>service>vprn>l2tp description)
[Tree] (config>service>vprn>red-if>spoke-sdp description)
[Tree] (config>service>vprn>rip description)
[Tree] (config>service>vprn>rip>group description)
[Tree] (config>service>vprn>rip>group>neighbor description)
[Tree] (config>service>vprn>ripng description)
[Tree] (config>service>vprn>ripng>group description)
[Tree] (config>service>vprn>ripng>group>neighbor description)
[Tree] (config>service>vprn>spoke-sdp description)
[Tree] (config>service>vprn>static-route-entry>black-hole description)
[Tree] (config>service>vprn>static-route-entry>indirect description)
[Tree] (config>service>vprn>static-route-entry>next-hop description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>static-route-entry>grt description)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel description)
[Tree] (config>subscr-mgmt>git description)
[Tree] (config>subscr-mgmt>pfcp-association description)
[Tree] (config>subscr-mgmt>sap-template description)
[Tree] (config>system>bluetooth>device description)
[Tree] (config>system>cron>sched description)
[Tree] (config>system>grpc-tunnel>destination-group description)
[Tree] (config>system>grpc-tunnel>tunnel description)
[Tree] (config>system>management-interface>remote-management>manager description)
[Tree] (config>system>persistence>ancp description)
[Tree] (config>system>persistence>dhcp-server description)
[Tree] (config>system>persistence>nat-fwd description)
[Tree] (config>system>persistence>python-policy-cache description)
[Tree] (config>system>persistence>sub-mgmt description)
[Tree] (config>system>script-control>script description)
[Tree] (config>system>satellite>eth-sat description)
[Tree] (config>system>satellite>local-forward description)
[Tree] (config>system>satellite>local-forward>sap description)
[Tree] (config>system>satellite>port-template description)
[Tree] (config>system>satellite>tdm-sat description)
[Tree] (config>system>software-repository description)
[Tree] (config>ipsec>trans-mode-prof description)

Full Context

configure bmp station description
configure card fp ingress access queue-group description
configure card fp ingress network queue-group description
configure connection-profile description
configure eth-tunnel path description
configure eth-tunnel path eth-cfm mep description
configure filter dhcp-filter description
configure filter gre-tunnel-template description
configure filter ip-exception description
configure filter ip-exception entry description
configure filter ip-filter description
configure filter ip-filter entry description
configure filter ipv6-exception description
configure filter ipv6-exception entry description
configure filter ipv6-filter description
configure filter ipv6-filter entry description
configure filter log description
configure filter mac-filter description
configure filter mac-filter entry description
configure filter match-list ip-prefix-list description
configure filter match-list ipv6-prefix-list description
configure filter match-list port-list description
configure filter match-list protocol-list description
configure filter redirect-policy description
configure filter redirect-policy destination description
configure fwd-path-ext fpe description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure ipsec client-db client description
configure ipsec client-db description
configure ipsec ike-policy description
configure ipsec tunnel-template description
configure ipsec ipsec-transport-mode-profile description
configure isa ipsec-group description
configure isa tunnel-group description
configure lag link-map-profile description
configure port ethernet access egress queue-group description
configure port ethernet access egress vport description
configure port ethernet access ingress queue-group description
configure port ethernet egress hs-secondary-shaper description
configure port ethernet eth-cfm mep description
configure port ethernet network egress queue-group description
configure port-xc pxc description
configure qos fp-resource-policy description
configure qos hw-agg-shaper-scheduler-policy description
configure qos match-list ip-prefix-list description
configure qos match-list ipv6-prefix-list description
configure qos match-list port-list description
configure qos network-queue description
configure qos policer-control-policy description
configure qos policer-control-policy tier arbiter description
configure qos post-policer-mapping description
configure redundancy multi-chassis peer description
configure router bgp description
configure router bgp group description
configure router bgp group neighbor description
configure router dhcp local-dhcp-server description
configure router dhcp local-dhcp-server pool description
configure router dhcp6 local-dhcp-server description
configure router dhcp6 local-dhcp-server pool description
configure router flexible-algorithm-definitions flex-algo description
configure router interface dhcp description
configure router interface eth-cfm mep description
configure router interface vrrp description
configure router mcac if-policy description
configure router mcac policy bundle description
configure router mcac policy description
configure router network-domains network-domain description
configure router origin-validation rpki-session description
configure router pcp-server server description
configure router rip description
configure router rip group description
configure router rip group neighbor description
configure router ripng description
configure router ripng group description
configure router ripng group neighbor description
configure router route-next-hop-policy template description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router static-route-entry black-hole description
configure router static-route-entry indirect description
configure router static-route-entry next-hop description
configure service apipe description
configure service apipe endpoint description
configure service cpipe description
configure service cpipe endpoint description
configure service epipe description
configure service epipe endpoint description
configure service epipe spoke-sdp description
configure service fpipe description
configure service fpipe endpoint description
configure service ies aarp-interface spoke-sdp description
configure service ies description
configure service ies interface dhcp description
configure service ies interface ipv6 dhcp6-relay description
configure service ies interface sap eth-cfm mep description
configure service ies interface sap ip-tunnel description
configure service ies interface spoke-sdp description
configure service ies interface spoke-sdp eth-cfm mep description
configure service ies subscriber-interface dhcp description
configure service ies subscriber-interface group-interface dhcp description
configure service ies subscriber-interface group-interface ppp description
configure service ies subscriber-interface group-interface pppoe description
configure service ies subscriber-interface group-interface sap eth-cfm mep description
configure service ies subscriber-interface group-interface srrp description
configure service ies subscriber-interface ipv6 dhcp6 relay description
configure service ipipe description
configure service ipipe endpoint description
configure service ipipe spoke-sdp description
configure service sdp binding pw-port description
configure service vpls endpoint description
configure service vpls sap ipoe-session description
configure service vprn aarp-interface spoke-sdp description
configure service vprn bgp description
configure service vprn bgp group description
configure service vprn bgp group neighbor description
configure service vprn interface dhcp description
configure service vprn interface sap description
configure service vprn interface sap ip-tunnel description
configure service vprn interface sap ipsec-tunnel description
configure service vprn l2tp description
configure service vprn redundant-interface spoke-sdp description
configure service vprn rip description
configure service vprn rip group description
configure service vprn rip group neighbor description
configure service vprn ripng description
configure service vprn ripng group description
configure service vprn ripng group neighbor description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn spoke-sdp description
configure service vprn static-route-entry black-hole description
configure service vprn static-route-entry grt description
configure service vprn static-route-entry indirect description
configure service vprn static-route-entry ipsec-tunnel description
configure service vprn static-route-entry next-hop description
configure service vprn subscriber-interface group-interface pppoe description
configure service vprn subscriber-interface ipv6 dhcp6 relay description
configure subscriber-mgmt radius-accounting-policy description
configure subscriber-mgmt group-interface-template description
configure subscriber-mgmt gtp peer-profile description
configure subscriber-mgmt local-user-db description
configure subscriber-mgmt pfcp-association description
configure subscriber-mgmt ppp-policy description
configure subscriber-mgmt rip-policy description
configure subscriber-mgmt sap-template description
configure system bluetooth device description
configure system cron schedule description
configure system grpc-tunnel destination-group description
configure system grpc-tunnel tunnel description
configure system management-interface remote-management manager description
configure system persistence ancp description
configure system persistence dhcp-server description
configure system persistence nat-port-forwarding description
configure system persistence python-policy-cache description
configure system persistence subscriber-mgmt description
configure system satellite eth-sat description
configure system satellite local-forward description
configure system satellite local-forward sap description
configure system satellite port-template description
configure system satellite tdm-sat description
configure system script-control script description
configure system software-repository description

Description This command configures a text description that is stored in the configuration file. The text string is associated with a configuration context to identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default no description

Parameters *short-description-string* — Specifies the description entered as a character string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep description

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure eth-tunnel path eth-cfm mep description
- configure eth-tunnel path description
- configure service ies interface spoke-sdp eth-cfm mep description
- configure system satellite eth-sat description
- configure service fpipe endpoint description
- configure system satellite port-template description
- configure system satellite local-forward sap description
- configure system software-repository description
- configure router interface eth-cfm mep description
- configure port ethernet eth-cfm mep description
- configure qos match-list port-list description
- configure service ies interface sap eth-cfm mep description
- configure service cpipe description
- configure service fpipe description
- configure system satellite local-forward description
- configure service cpipe endpoint description

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt group-interface-template description
- configure router dhcp local-dhcp-server pool description
- configure router dhcp6 local-dhcp-server pool description
- configure service ies subscriber-interface group-interface srrp description
- configure system persistence dhcp-server description
- configure subscriber-mgmt pfcp-association description
- configure subscriber-mgmt local-user-db description
- configure service vprn redundant-interface spoke-sdp description
- configure subscriber-mgmt rip-policy description
- configure service ies subscriber-interface group-interface dhcp description
- configure subscriber-mgmt sap-template description
- configure service ies subscriber-interface group-interface pppoe description
- configure subscriber-mgmt ppp-policy description
- configure service vprn subscriber-interface ipv6 dhcp6 relay description
- configure router dhcp local-dhcp-server description
- configure system persistence subscriber-mgmt description
- configure router dhcp6 local-dhcp-server description
- configure subscriber-mgmt radius-accounting-policy description
- configure service vpls sap ipoe-session description
- configure service ies subscriber-interface ipv6 dhcp6 relay description
- configure service ies subscriber-interface dhcp description
- configure service ies subscriber-interface group-interface ppp description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn subscriber-interface group-interface pppoe description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos policer-control-policy tier arbiter description
- configure card fp ingress network queue-group description
- configure card fp ingress access queue-group description
- configure qos post-policer-mapping description
- configure qos policer-control-policy description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies aarp-interface spoke-sdp description
- configure service vprn aarp-interface spoke-sdp description
- configure ipsec ipsec-transport-mode-profile description
- configure ipsec client-db description
- configure isa tunnel-group description
- configure system persistence nat-port-forwarding description
- configure service vprn interface sap ipsec-tunnel description
- configure ipsec tunnel-template description
- configure ipsec ike-policy description
- configure router pcp-server server description

7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

- configure qos fp-resource-policy description

7450 ESS, 7750 SR-7/12/12e

- configure connection-profile description

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure system satellite tdm-sat description

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe endpoint description
- configure service apipe description

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt gtp peer-profile description

7750 SR-1, 7750 SR-s

- configure qos hw-agg-shaper-scheduler-policy description
- configure system bluetooth device description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7750 SR-7/12/12e

- configure port ethernet egress hs-secondary-shaper description

All

- configure router ripng description
- configure service vprn spoke-sdp description
- configure router mcac policy description
- configure router bgp group description
- configure system grpc-tunnel destination-group description
- configure router route-next-hop-policy template description
- configure filter gre-tunnel-template description
- configure bmp station description
- configure service epipe endpoint description
- configure filter match-list port-list description
- configure filter ip-filter entry description
- configure service vprn static-route-entry ipsec-tunnel description
- configure qos match-list ip-prefix-list description
- configure filter mac-filter entry description
- configure service ies interface ipv6 dhcp6-relay description
- configure port-xc pxc description
- configure filter redirect-policy destination description
- configure service ies interface dhcp description
- configure router static-route-entry black-hole description
- configure port ethernet access egress queue-group description
- configure router mcac if-policy description
- configure service ipipe spoke-sdp description
- configure router rip group neighbor description
- configure fwd-path-ext fpe description
- configure service vprn interface sap ip-tunnel description
- configure router static-route-entry next-hop description
- configure service vprn ripng group description
- configure filter ipv6-filter entry description
- configure port ethernet network egress queue-group description
- configure router ripng group neighbor description
- configure lag link-map-profile description
- configure service vpls endpoint description
- configure service vprn static-route-entry black-hole description
- configure service vprn static-route-entry indirect description
- configure service epipe description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router mcac policy bundle description
- configure router network-domains network-domain description
- configure system management-interface remote-management manager description
- configure port ethernet access ingress queue-group description
- configure filter ip-filter description
- configure redundancy multi-chassis peer description
- configure service vprn bgp description
- configure service vprn ripng group neighbor description
- configure service vprn rip description
- configure service ipipe description
- configure filter match-list protocol-list description
- configure service vprn static-route-entry next-hop description
- configure router bgp group neighbor description
- configure qos match-list ipv6-prefix-list description
- configure service vprn static-route-entry grt description
- configure filter log description
- configure service ies interface sap ip-tunnel description
- configure system cron schedule description
- configure filter ipv6-filter description
- configure service ies interface spoke-sdp description
- configure service ies description
- configure qos network-queue description
- configure service epipe spoke-sdp description
- configure service vprn interface sap description
- configure filter mac-filter description
- configure service vprn bgp group neighbor description
- configure router rip description
- configure port ethernet access egress vport description
- configure system persistence python-policy-cache description
- configure router ripng group description
- configure filter dhcp-filter description
- configure router bgp description
- configure router interface dhcp description
- configure service vprn ripng description
- configure system grpc-tunnel tunnel description
- configure service ipipe endpoint description
- configure system persistence ancp description
- configure service vprn rip group description
- configure filter match-list ip-prefix-list description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure filter match-list ipv6-prefix-list description
- configure router static-route-entry indirect description
- configure router rip group description
- configure router flexible-algorithm-definitions flex-algo description
- configure router origin-validation rpki-session description
- configure system script-control script description
- configure filter redirect-policy description
- configure service vprn interface dhcp description
- configure service vprn bgp group description
- configure service vprn rip group neighbor description

VSR

- configure filter ipv6-exception entry description
- configure filter ipv6-exception description
- configure filter ip-exception entry description
- configure filter ip-exception description

description

Syntax **description** *short-description-string*
no description

Context **[Tree]** (config>service>vpls>sap description)
[Tree] (config>service>vpls>wlan-gw description)
[Tree] (config>service>vprn description)
[Tree] (config>service>vprn>if>sap>ip-tunnel description)
[Tree] (config>service>mac-list description)
[Tree] (config>service>vpls description)
[Tree] (config>service>vpls>gsmp>group description)
[Tree] (config>service>vpls>gsmp>group>neighbor description)
[Tree] (config>service>vpls>igmp-snooping>mvr description)
[Tree] (config>service>vpls>split-horizon-group description)
[Tree] (config>service>vpls>mesh-sdp description)
[Tree] (config>service>vpls>spoke-sdp description)
[Tree] (config>service>vpls>sap>dhcp description)
[Tree] (config>service>vpls>mld-snooping>mvr description)
[Tree] (config>subscr-mgmt>accu-stats-policy description)
[Tree] (config>subscr-mgmt>authentication-policy description)
[Tree] (config>subscr-mgmt>host-tracking description)
[Tree] (config>subscr-mgmt>pim-policy description)
[Tree] (config>subscr-mgmt>sla-profile description)
[Tree] (config>subscr-mgmt>sub-ident-pol description)
[Tree] (config>subscr-mgmt>sub-profile description)
[Tree] (config>subscr-mgmt>mld-policy description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>sap description)
[Tree] (config>service>vprn>sub-if>grp-if>srrp description)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session description)
[Tree] (config>service>vprn>sub-if>grp-if>arp-host description)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt description)
[Tree] (config>service>vprn>sub-if>grp-if>wpp description)
[Tree] (config>service>vprn>gsmp>group description)
[Tree] (config>service>vprn>gsmp>group>neighbor description)
[Tree] (config>subscr-mgmt>cat-map description)
[Tree] (config>subscr-mgmt>ipoe-session-policy description)
[Tree] (config>subscr-mgmt>diam-appl-plcy description)
[Tree] (config>subscr-mgmt>credit-cntrl-plcy description)
[Tree] (config>subscr-mgmt>host-lockout-plcy description)
[Tree] (config>subscr-mgmt>sub-mcac-policy description)
[Tree] (config>aaa>route-downloader description)
[Tree] (config>aaa>diam-peer-plcy description)
[Tree] (config>aaa>wpp>portal-groups>portal-group description)
[Tree] (config>port>ethernet>access>egress description)
[Tree] (config>subscr-mgmt>cat-map>category description)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry description)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry description)
[Tree] (config>call-trace>trace-profile description)
[Tree] (config>aaa>diam>node description)
[Tree] (config>aaa>l2tp-acct-plcy description)
[Tree] (config>mcast-mgmt>bandwidth-policy description)
[Tree] (config>mcast-mgmt>multicast-info-policy description)
[Tree] (config>mcast-mgmt>mcast-rprt-dest description)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle description)
[Tree] (config>card>fp>ingress>mcast-mgmt description)
[Tree] (config>python>py-policy description)
[Tree] (config>python>python-script description)
[Tree] (config>aaa>radius-script-policy description)
[Tree] (config>service>dynsvc>policy description)
[Tree] (config>service>dynsvc>ladb description)
[Tree] (config>service>dynsvc>ladb>user description)
[Tree] (config>subscr-mgmt>isa-svc-chain>evpn description)
[Tree] (config>subscr-mgmt>isa-svc-chain>vas-filter description)
[Tree] (config>aaa>acct-on-off-grp description)
[Tree] (config>aaa>radius-srv-plcy description)
[Tree] (config>isa>wlan-gw-group description)
[Tree] (config>router>radius-server>server description)
[Tree] (config>router>radius-proxy>server description)
[Tree] (config>service>vprn>radius-proxy>server description)
[Tree] (config>service>vprn>radius-server>server description)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw description)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw description)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters description)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters description)
[Tree] (config>subscr-mgmt>isa-filter description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>subscr-mgmt>isa-filter>ipv6>entry description)
[Tree] (config>subscr-mgmt>isa-filter>entry description)
[Tree] (config>subscr-mgmt>isa-policer description)
[Tree] (config>app-assure>aarp description)
[Tree] (config>app-assure>group description)
[Tree] (config>app-assure>group>statistics>aa-sub description)
[Tree] (config>app-assure>group>cflowd>collector description)
[Tree] (config>app-assure>group>cflowd>collector description)
[Tree] (config>app-assure>group>cflowd>direct-export>collector description)
[Tree] (config>app-assure>group>certificate-profile description)
[Tree] (config>app-assure>group>dns-ip-cache description)
[Tree] (config>app-assure>group>event-log>syslog description)
[Tree] (config>app-assure>group>gtp>gtp-filter description)
[Tree] (config>app-assure>group>http-enrich description)
[Tree] (config>app-assure>group>http-error-redirect description)
[Tree] (config>app-assure>group>http-notification description)
[Tree] (config>app-assure>group>http-redirect description)
[Tree] (config>app-assure>group>ip-prefix-list description)
[Tree] (config>app-assure>group>policer description)
[Tree] (config>app-assure>group>policer>tod-override description)
[Tree] (config>app-assure>group>policy>app-filter>entry description)
[Tree] (config>app-assure>group>policy>app-group description)
[Tree] (config>app-assure>group>policy>application description)
[Tree] (config>app-assure>group>policy>app-profile description)
[Tree] (config>app-assure>group>policy>app-qos-policy>entry description)
[Tree] (config>app-assure>group>policy>aqp>entry>action>url-filter description)
[Tree] (config>app-assure>group>policy>charging-group description)
[Tree] (config>app-assure>group>policy>custom-protocol description)
[Tree] (config>app-assure>group>policy>transit-ip-policy description)
[Tree] (config>app-assure>group>port-list description)
[Tree] (config>app-assure>group>sctp-filter description)
[Tree] (config>app-assure>group>session-filter description)
[Tree] (config>app-assure>group>session-filter>entry description)
[Tree] (config>app-assure>group>tcp-validate description)
[Tree] (config>app-assure>group>transit-prefix-policy description)
[Tree] (config>app-assure>group>url-filter description)
[Tree] (config>app-assure>group>url-filter>icap>server description)
[Tree] (config>app-assure>group>url-filter>web-service>profile description)
[Tree] (config>app-assure>group>url-list description)
[Tree] (config>app-assure>protocol description)
[Tree] (config>app-assure>rad-acct-plcy description)
[Tree] (config>isa description)
[Tree] (config>isa>aa-group description)
[Tree] (config>system>persistence>application-assurance description)
[Tree] (config>aaa>isa-radius-plcy description)
[Tree] (config>isa>nat-group description)
[Tree] (config>router>firewall>domain>prefix description)
[Tree] (config>router>nat>inside>subscriber-id description)
[Tree] (config>router>nat>outside>pool description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>nat>outside>pool>address-range description)
[Tree] (config>router>vrgw>lanext description)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext description)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network description)
[Tree] (config>service>ipfix>ipfix-export-policy description)
[Tree] (config>service>nat>firewall-policy description)
[Tree] (config>service>nat>map-domain>mapping-rule description)
[Tree] (config>service>nat>nat-classifier description)
[Tree] (config>service>nat>nat-classifier>entry description)
[Tree] (config>service>nat>nat-policy description)
[Tree] (config>service>nat>pcp-server-policy description)
[Tree] (config>service>nat>up-nat-policy description)
[Tree] (config>service>upnp>upnp-policy description)
[Tree] (config>service>vprn>firewall>domain>prefix description)
[Tree] (config>service>vprn>nat>outside>pool>address-range description)
[Tree] (config>service>vprn>nat>outside>pool description)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext description)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network description)
[Tree] (config>subscr-mgmt>vrgw>brg>brg-profile description)
[Tree] (config>subscr-mgmt>pppoe-client-policy description)
[Tree] (config>subscr-mgmt>vrgw>brg>brg-profile description)
[Tree] (config>macsec>connectivity-association description)
[Tree] (config>pw-port description)
[Tree] (config>esa description)
[Tree] (config>esa>vm description)
[Tree] (config>mirror>mirror-dest description)
[Tree] (config>mirror>mirror-dest>endpoint description)
[Tree] (config>li>log>log-id description)
[Tree] (config>li>li-filter>li-mac-filter description)
[Tree] (config>li>li-filter>li-mac-filter>entry description)
[Tree] (config>li>li-filter>li-ip-filter description)
[Tree] (config>li>li-filter>li-ip-filter>entry description)
[Tree] (config>li>li-filter>li-ipv6-filter description)
[Tree] (config>li>li-filter>li-ipv6-filter>entry description)
[Tree] (config>li>li-filter-block-reservation>li-reserved-block description)
[Tree] (config>li>x-interfaces>lics>lic description)
[Tree] (config>service>vprn>ip-mirror-interface>spoke-sdp description)
[Tree] (config>oam-pm>bin-group description)
[Tree] (config>oam-pm>session description)
[Tree] (config>oam-pm>streaming>delay-template description)
[Tree] (config>saa>test description)
[Tree] (config>test-oam>twamp>server>prefix description)
[Tree] (config>router>twamp-light>reflector>prefix description)
[Tree] (config>service>vprn>twamp-light>reflector>prefix description)
[Tree] (config>router>twamp-light>reflector description)
[Tree] (config>service>vprn>twamp-light>reflector description)
[Tree] (config>qos>sap-egress description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>qos>sap-egress>ip-criteria>entry description)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry description)
[Tree] (config>qos>sap-egress>policer description)
[Tree] (config>qos>sap-ingress description)
[Tree] (config>qos>sap-ingress>ip-criteria>entry description)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry description)
[Tree] (config>qos>sap-ingress>mac-criteria>entry description)
[Tree] (config>qos>sap-ingress>policer description)
[Tree] (config>qos>mc-fr-profile-egress description)
[Tree] (config>qos>mc-fr-profile-ingress description)
[Tree] (config>qos>network description)
[Tree] (config>qos>network>egress>ip-criteria>entry description)
[Tree] (config>qos>network>egress>ipv6-criteria>entry description)
[Tree] (config>qos>network>ingress>ip-criteria>entry description)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry description)
[Tree] (cfg>qos>qgrps>egr>qgrp description)
[Tree] (cfg>qos>qgrps>ing>qgrp description)
[Tree] (cfg>qos>qgrps>egr>qgrp>policer description)
[Tree] (cfg>qos>qgrps>ing>qgrp>policer description)
[Tree] (config>cflowd>collector description)
[Tree] (config>vrrp>policy description)
[Tree] (config>router>policy-options>policy-statement description)
[Tree] (config>router>policy-options>policy-statement>entry description)
[Tree] (config>test-oam>link-meas>template description)
[Tree] (config>subscr-mgmt>steering-profile description)

Full Context

configure qos queue-group-templates egress queue-group description
configure qos queue-group-templates egress queue-group policer description
configure qos queue-group-templates ingress queue-group description
configure qos queue-group-templates ingress queue-group policer description
configure aaa acct-on-off-group description
configure aaa diameter node description
configure aaa diameter-peer-policy description
configure aaa isa-radius-policy description
configure aaa l2tp-accounting-policy description
configure aaa radius-script-policy description
configure aaa radius-server-policy description
configure aaa route-downloader description
configure aaa wpp portal-groups portal-group description
configure application-assurance aarp description
configure application-assurance group certificate-profile description
configure application-assurance group cflowd collector description
configure application-assurance group cflowd direct-export collector description
configure application-assurance group description
configure application-assurance group dns-ip-cache description
configure application-assurance group event-log syslog description
configure application-assurance group gtp gtp-filter description
configure application-assurance group http-enrich description
configure application-assurance group http-error-redirect description
configure application-assurance group http-notification description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group http-redirect description
configure application-assurance group ip-prefix-list description
configure application-assurance group policer description
configure application-assurance group policer tod-override description
configure application-assurance group policy app-filter entry description
configure application-assurance group policy app-group description
configure application-assurance group policy app-profile description
configure application-assurance group policy app-qos-policy entry description
configure application-assurance group policy application description
configure application-assurance group policy app-qos-policy entry action url-filter description
configure application-assurance group policy charging-group description
configure application-assurance group policy custom-protocol description
configure application-assurance group policy transit-ip-policy description
configure application-assurance group port-list description
configure application-assurance group sctp-filter description
configure application-assurance group session-filter description
configure application-assurance group session-filter entry description
configure application-assurance group statistics aa-sub description
configure application-assurance group tcp-validate description
configure application-assurance group transit-prefix-policy description
configure application-assurance group url-filter description
configure application-assurance group url-filter icap server description
configure application-assurance group url-filter web-service profile description
configure application-assurance group url-list description
configure application-assurance protocol description
configure application-assurance radius-accounting-policy description
configure call-trace trace-profile description
configure card fp ingress mcast-management description
configure cflowd collector description
configure esa description
configure esa vm description
configure isa aa-group description
configure isa description
configure isa nat-group description
configure isa wlan-gw-group description
configure li li-filter li-ip-filter description
configure li li-filter li-ip-filter entry description
configure li li-filter li-ipv6-filter description
configure li li-filter li-ipv6-filter entry description
configure li li-filter li-mac-filter description
configure li li-filter li-mac-filter entry description
configure li li-filter-block-reservation li-reserved-block description
configure li log log-id description
configure li x-interfaces lics lic description
configure macsec connectivity-association description
configure mcast-management bandwidth-policy description
configure mcast-management multicast-info-policy bundle description
configure mcast-management mcast-reporting-dest description
configure mcast-management multicast-info-policy description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure mirror mirror-dest description
configure mirror mirror-dest endpoint description
configure oam-pm bin-group description
configure oam-pm session description
configure oam-pm streaming delay-template description
configure port ethernet access egress description
configure pw-port description
configure python python-policy description
configure python python-script description
configure qos mc-fr-profile-egress description
configure qos mc-fr-profile-ingress description
configure qos network description
configure qos network egress ip-criteria entry description
configure qos network egress ipv6-criteria entry description
configure qos network ingress ip-criteria entry description
configure qos network ingress ipv6-criteria entry description
configure qos sap-egress description
configure qos sap-egress ip-criteria entry description
configure qos sap-egress ipv6-criteria entry description
configure qos sap-egress policer description
configure qos sap-ingress description
configure qos sap-ingress ip-criteria entry description
configure qos sap-ingress ipv6-criteria entry description
configure qos sap-ingress mac-criteria entry description
configure qos sap-ingress policer description
configure router firewall domain prefix description
configure router nat inside subscriber-id description
configure router nat outside pool address-range description
configure router nat outside pool description
configure router policy-options policy-statement description
configure router policy-options policy-statement entry description
configure router radius-proxy server description
configure router radius-server server description
configure router twamp-light reflector description
configure router twamp-light reflector prefix description
configure router vrgw lanext description
configure saa test description
configure service dynamic-services local-auth-db description
configure service dynamic-services local-auth-db user-name description
configure service dynamic-services dynamic-services-policy description
configure service ies subscriber-interface group-interface sap-parameters description
configure service ies subscriber-interface group-interface wlan-gw description
configure service ies subscriber-interface group-interface wlan-gw ranges range vrgw lanext description
configure service ies subscriber-interface group-interface wlan-gw ranges range vrgw lanext network description
configure service ipfix ipfix-export-policy description
configure service mac-list description
configure service nat firewall-policy description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service nat map-domain mapping-rule description
configure service nat nat-classifier description
configure service nat nat-classifier entry description
configure service nat nat-policy description
configure service nat pcp-server-policy description
configure service nat up-nat-policy description
configure service upnp upnp-policy description
configure service vpls description
configure service vpls gsmp group description
configure service vpls gsmp group neighbor description
configure service vpls igmp-snooping mvr description
configure service vpls mesh-sdp description
configure service vpls mld-snooping mvr description
configure service vpls sap description
configure service vpls sap dhcp description
configure service vpls split-horizon-group description
configure service vpls spoke-sdp description
configure service vpls wlan-gw description
configure service vprn description
configure service vprn firewall domain prefix description
configure service vprn gsmp group description
configure service vprn gsmp group neighbor description
configure service vprn interface sap ip-tunnel description
configure service vprn ip-mirror-interface spoke-sdp description
configure service vprn nat outside pool address-range description
configure service vprn nat outside pool description
configure service vprn radius-proxy server description
configure service vprn radius-server server description
configure service vprn subscriber-interface group-interface arp-host description
configure service vprn subscriber-interface group-interface ipoe-session description
configure service vprn subscriber-interface group-interface sap description
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt description
configure service vprn subscriber-interface group-interface sap-parameters description
configure service vprn subscriber-interface group-interface srrp description
configure service vprn subscriber-interface group-interface wlan-gw description
configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext description
configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext network description
configure service vprn subscriber-interface group-interface wpp description
configure service vprn twamp-light reflector description
configure service vprn twamp-light reflector prefix description
configure subscriber-mgmt accu-stats-policy description
configure subscriber-mgmt authentication-policy description
configure subscriber-mgmt category-map category description
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry description
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt category-map description
configure subscriber-mgmt credit-control-policy description
configure subscriber-mgmt diameter-application-policy description
configure subscriber-mgmt host-lockout-policy description
configure subscriber-mgmt host-tracking description
configure subscriber-mgmt ipoe-session-policy description
configure subscriber-mgmt isa-filter description
configure subscriber-mgmt isa-filter entry description
configure subscriber-mgmt isa-filter ipv6 entry description
configure subscriber-mgmt isa-policer description
configure subscriber-mgmt isa-service-chaining evpn description
configure subscriber-mgmt isa-service-chaining vas-filter description
configure subscriber-mgmt mld-policy description
configure subscriber-mgmt pim-policy description
configure subscriber-mgmt pppoe-client-policy description
configure subscriber-mgmt sla-profile description
configure subscriber-mgmt steering-profile description
configure subscriber-mgmt sub-ident-policy description
configure subscriber-mgmt sub-mcac-policy description
configure subscriber-mgmt sub-profile description
configure subscriber-mgmt vrgw brg brg-profile description
configure system persistence application-assurance description
configure test-oam link-measurement measurement-template description
configure test-oam twamp server prefix description
configure vrrp policy description

Description This command configures a text description that is stored in the configuration file. The text string is associated with a configuration context to identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Parameters *short-description-string* — Specifies the description character string. Allowed values are any string, up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure subscriber-mgmt sub-mcac-policy description

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn twamp-light reflector prefix description
- configure test-oam link-measurement measurement-template description
- configure router twamp-light reflector description
- configure router twamp-light reflector prefix description
- configure li x-interfaces lics lic description
- configure oam-pm streaming delay-template description
- configure qos mc-fr-profile-ingress description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure test-oam twamp server prefix description
- configure service vprn twamp-light reflector description
- configure qos mc-fr-profile-egress description

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service dynamic-services local-auth-db description
- configure aaa diameter-peer-policy description
- configure service vprn subscriber-interface group-interface sap description
- configure aaa wpp portal-groups portal-group description
- configure subscriber-mgmt isa-filter entry description
- configure subscriber-mgmt pim-policy description
- configure subscriber-mgmt isa-filter description
- configure subscriber-mgmt category-map category description
- configure subscriber-mgmt category-map description
- configure service vprn subscriber-interface group-interface srrp description
- configure call-trace trace-profile description
- configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry description
- configure subscriber-mgmt isa-filter ipv6 entry description
- configure service dynamic-services dynamic-services-policy description
- configure subscriber-mgmt accu-stats-policy description
- configure aaa diameter node description
- configure subscriber-mgmt sub-profile description
- configure subscriber-mgmt sla-profile description
- configure subscriber-mgmt credit-control-policy description
- configure subscriber-mgmt ipoe-session-policy description
- configure aaa radius-script-policy description
- configure service vprn subscriber-interface group-interface ipoe-session description
- configure subscriber-mgmt vrgw brg brg-profile description
- configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry description
- configure subscriber-mgmt isa-policer description
- configure subscriber-mgmt steering-profile description
- configure subscriber-mgmt mld-policy description
- configure subscriber-mgmt pppoe-client-policy description
- configure aaa route-downloader description
- configure subscriber-mgmt diameter-application-policy description
- configure router radius-server server description
- configure aaa acct-on-off-group description
- configure subscriber-mgmt host-lockout-policy description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router radius-proxy server description
- configure aaa radius-server-policy description
- configure subscriber-mgmt authentication-policy description
- configure service dynamic-services local-auth-db user-name description
- configure service vprn radius-server server description
- configure service vprn radius-proxy server description
- configure subscriber-mgmt sub-ident-policy description
- configure aaa l2tp-accounting-policy description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

- configure esa description
- configure esa vm description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-ingress policer description
- configure qos queue-group-templates egress queue-group policer description
- configure qos queue-group-templates ingress queue-group policer description
- configure qos sap-egress policer description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure application-assurance group description
- configure application-assurance group session-filter description
- configure service vprn nat outside pool description
- configure isa nat-group description
- configure application-assurance group url-list description
- configure application-assurance group policy app-filter entry description
- configure application-assurance group cflowd collector description
- configure application-assurance group http-notification description
- configure application-assurance group policy custom-protocol description
- configure system persistence application-assurance description
- configure subscriber-mgmt isa-service-chaining evpn description
- configure application-assurance group url-filter web-service profile description
- configure service nat pcp-server-policy description
- configure router nat outside pool description
- configure application-assurance group port-list description
- configure service vprn nat outside pool address-range description
- configure application-assurance group http-enrich description
- configure application-assurance group gtp gtp-filter description
- configure application-assurance group event-log syslog description
- configure application-assurance group policy application description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure application-assurance group url-filter description
- configure application-assurance group ip-prefix-list description
- configure application-assurance aarp description
- configure application-assurance group http-redirect description
- configure application-assurance group http-error-redirect description
- configure service nat nat-classifier entry description
- configure application-assurance group dns-ip-cache description
- configure router nat outside pool address-range description
- configure application-assurance group tcp-validate description
- configure aaa isa-radius-policy description
- configure application-assurance group url-filter icap server description
- configure service nat nat-policy description
- configure application-assurance group cflowd direct-export collector description
- configure application-assurance group sctp-filter description
- configure subscriber-mgmt isa-service-chaining vas-filter description
- configure application-assurance group session-filter entry description
- configure application-assurance group transit-prefix-policy description
- configure application-assurance group policy app-profile description
- configure application-assurance radius-accounting-policy description
- configure application-assurance group policy app-qos-policy entry description
- configure application-assurance group policy charging-group description
- configure service upnp upnp-policy description
- configure service nat nat-classifier description
- configure application-assurance group policer description
- configure application-assurance group policer tod-override description
- configure application-assurance group policy app-group description
- configure service nat up-nat-policy description
- configure application-assurance group certificate-profile description

7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

- configure mcast-management bandwidth-policy description

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure isa wlan-gw-group description
- configure service vprn firewall domain prefix description
- configure service nat firewall-policy description
- configure service ies subscriber-interface group-interface sap-parameters description
- configure service vprn subscriber-interface group-interface sap-parameters description
- configure service vpls wlan-gw description
- configure router firewall domain prefix description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure qos network ingress ipv6-criteria entry description
- configure service vpls mesh-sdp description
- configure qos queue-group-templates egress queue-group description
- configure service vprn interface sap ip-tunnel description
- configure li log log-id description
- configure qos sap-ingress description
- configure oam-pm bin-group description
- configure service vpls sap dhcp description
- configure qos queue-group-templates ingress queue-group description
- configure service vpls split-horizon-group description
- configure pw-port description
- configure service vprn ip-mirror-interface spoke-sdp description
- configure qos sap-egress description
- configure service vpls spoke-sdp description
- configure service vpls gsmp group description
- configure li li-filter li-ipv6-filter description
- configure qos network egress ipv6-criteria entry description
- configure service vpls gsmp group neighbor description
- configure mcast-management multicast-info-policy bundle description
- configure li li-filter li-ipv6-filter entry description
- configure service vprn gsmp group description
- configure macsec connectivity-association description
- configure qos sap-ingress ip-criteria entry description
- configure service vpls description
- configure mirror mirror-dest description
- configure li li-filter li-mac-filter description
- configure python python-policy description
- configure mirror mirror-dest endpoint description
- configure router policy-options policy-statement description
- configure qos sap-egress ip-criteria entry description
- configure cflowd collector description
- configure service vpls igmp-snooping mvr description
- configure router policy-options policy-statement entry description
- configure mcast-management mcast-reporting-dest description
- configure oam-pm session description
- configure li li-filter li-ip-filter entry description
- configure qos sap-ingress mac-criteria entry description
- configure qos sap-ingress ipv6-criteria entry description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn description
- configure qos network description
- configure qos network ingress ip-criteria entry description
- configure service mac-list description
- configure qos sap-egress ipv6-criteria entry description
- configure service vprn gsmp group neighbor description
- configure li li-filter li-ip-filter description
- configure li li-filter li-mac-filter entry description
- configure python python-script description
- configure li li-filter-block-reservation li-reserved-block description
- configure service vpls sap description
- configure mcast-management multicast-info-policy description
- configure service ipfix ipfix-export-policy description
- configure qos network egress ip-criteria entry description
- configure vrrp policy description
- configure service vpls mld-snooping mvr description
- configure saa test description

VSR

- configure service nat map-domain mapping-rule description

description

Syntax **description** *short-description-string*
no description

Context **[Tree]** (config>connection-profile-vlan description)
[Tree] (config>service>cust description)
[Tree] (config>service>cust>multi-service-site description)
[Tree] (config>service>mrp>mrp-policy description)
[Tree] (config>service>mrp>mrp-policy>entry description)
[Tree] (config>service>pw-template description)
[Tree] (config>service>pw-template>split-horizon-group description)
[Tree] (config>service>sdp description)
[Tree] (config>eth-ring description)
[Tree] (config>eth-ring>path description)
[Tree] (config>eth-ring>path>eth-cfm>mep description)
[Tree] (config>grp-encryp>encryp-keygrp description)
[Tree] (config>isa>video-group description)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>video description)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video description)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video description)
[Tree] (config>service>ies>video-interface description)
[Tree] (config>service>vpls>video-interface description)
[Tree] (config>service>vprn>video-interface description)
[Tree] (config>service>ies>video-interface>channel description)
[Tree] (config>service>vprn>video-interface>channel description)
[Tree] (config>qos>adv-config-policy description)
[Tree] (config>qos>atm-td-profile description)
[Tree] (config>qos>hs-attachment-policy description)
[Tree] (config>qos>hs-pool-policy description)
[Tree] (config>qos>hs-port-pool-policy description)
[Tree] (config>qos>hs-scheduler-policy description)
[Tree] (config>qos>mlppp-profile-egress description)
[Tree] (config>qos>mlppp-profile-ingress description)
[Tree] (config>qos>port-scheduler-policy description)
[Tree] (config>qos>scheduler-policy description)
[Tree] (config>qos>scheduler-policy>tier>scheduler description)
[Tree] (config>qos>shared-queue description)
[Tree] (config>qos>slope-policy description)
[Tree] (config>log>event-handling>handler>action-list>entry description)
[Tree] (config>log>filter description)
[Tree] (config>log>filter>entry description)
[Tree] (config>log>log-id description)
[Tree] (config>log>accounting-policy description)
[Tree] (config>log>event-handling>handler description)
[Tree] (config>log>event-trigger>event description)
[Tree] (config>log>event-trigger>event>trigger-entry description)
[Tree] (config>log>file-id description)
[Tree] (config>log>syslog description)
[Tree] (config>log>snmp-trap-group description)
[Tree] (cfg>sys>sec>cpm>mac-filter>entry description)
[Tree] (config>system>security>mgmt-access-filter>ip-filter>entry description)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry description)
[Tree] (config>sys>security>cpm-filter>ip-filter>entry description)
[Tree] (config>sys>security>cpm-filter>ipv6-filter>entry description)
[Tree] (config>system>security>dist-cpu-protection>policy description)
[Tree] (config>system>security>keychain description)
[Tree] (config>system>security>keychain>direction>bi>entry description)
[Tree] (config>system>security>keychain>direction>uni>receive>entry description)
[Tree] (config>system>security>keychain>direction>uni>send>entry description)
[Tree] (config>system>security>pki>ca-profile description)
[Tree] (config>sys>security>cpu-protection>policy description)
[Tree] (config>system>security>mgmt-access-filter>mac-filter>entry description)
[Tree] (config>system>security>user>public-keys>ecdsa>ecdsa-key description)
[Tree] (config>system>security>user>public-keys>rsa>rsa-key description)
[Tree] (config>system>telemetry>destination-group description)
[Tree] (config>system>telemetry>persistent-subscriptions>subscription description)
[Tree] (config>system>telemetry>sensor-groups>sensor-group description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context

configure system security cpm-filter mac-filter entry description
configure connection-profile-vlan description
configure eth-ring description
configure eth-ring path description
configure eth-ring path eth-cfm mep description
configure group-encryption encryption-keygroup description
configure isa video-group description
configure log accounting-policy description
configure log event-handling handler action-list entry description
configure log event-handling handler description
configure log event-trigger event description
configure log event-trigger event trigger-entry description
configure log file-id description
configure log filter description
configure log filter entry description
configure log log-id description
configure log snmp-trap-group description
configure log syslog description
configure mcast-management multicast-info-policy bundle channel source-override video description
configure mcast-management multicast-info-policy bundle channel video analyzer description
configure mcast-management multicast-info-policy bundle channel video description
configure mcast-management multicast-info-policy bundle video description
configure qos adv-config-policy description
configure qos atm-td-profile description
configure qos hs-attachment-policy description
configure qos hs-pool-policy description
configure qos hs-port-pool-policy description
configure qos hs-scheduler-policy description
configure qos mlppp-profile-egress description
configure qos mlppp-profile-ingress description
configure qos port-scheduler-policy description
configure qos scheduler-policy description
configure qos scheduler-policy tier scheduler description
configure qos shared-queue description
configure qos slope-policy description
configure service customer description
configure service customer multi-service-site description
configure service ies video-interface channel description
configure service ies video-interface description
configure service mrp mrp-policy description
configure service mrp mrp-policy entry description
configure service pw-template description
configure service pw-template split-horizon-group description
configure service sdp description
configure service vpls video-interface description
configure service vprn video-interface channel description
configure service vprn video-interface description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security cpm-filter ip-filter entry description
configure system security cpm-filter ipv6-filter entry description
configure system security cpu-protection policy description
configure system security dist-cpu-protection policy description
configure system security keychain description
configure system security keychain direction bi entry description
configure system security keychain direction uni receive entry description
configure system security keychain direction uni send entry description
configure system security management-access-filter ip-filter entry description
configure system security management-access-filter ipv6-filter entry description
configure system security management-access-filter mac-filter entry description
configure system security pki ca-profile description
configure system security user public-keys ecdsa ecdsa-key description
configure system security user public-keys rsa rsa-key description
configure system telemetry destination-group description
configure system telemetry persistent-subscriptions subscription description
configure system telemetry sensor-groups sensor-group description

Description This command configures a text description that is stored in the configuration file. The text string is associated with a configuration context to identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description is associated with the configuration context.

Parameters *short-description-string* — Specifies the description character string. Allowed values are any string, up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure eth-ring path description
- configure system security cpm-filter ip-filter entry description
- configure system security cpm-filter mac-filter entry description
- configure eth-ring description
- configure system security cpm-filter ipv6-filter entry description
- configure eth-ring path eth-cfm mep description
- configure qos mlppp-profile-ingress description
- configure qos mlppp-profile-egress description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure group-encryption encryption-keygroup description

7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

- configure isa video-group description
- configure service vprn video-interface description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn video-interface channel description
- configure service ies video-interface description
- configure service ies video-interface channel description
- configure mcast-management multicast-info-policy bundle channel video analyzer description
- configure service vpls video-interface description

7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

- configure system security cpu-protection policy description

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure qos atm-td-profile description

7750 SR-7/12/12e

- configure qos hs-scheduler-policy description
- configure qos hs-port-pool-policy description
- configure qos hs-attachment-policy description
- configure qos hs-pool-policy description

All

- configure system security keychain description
- configure log event-trigger event trigger-entry description
- configure service sdp description
- configure log file-id description
- configure system security management-access-filter ip-filter entry description
- configure log log-id description
- configure qos shared-queue description
- configure service mrp mrp-policy entry description
- configure service customer description
- configure connection-profile-vlan description
- configure service pw-template split-horizon-group description
- configure log event-handling handler description
- configure log snmp-trap-group description
- configure service customer multi-service-site description
- configure system security user public-keys rsa rsa-key description
- configure system telemetry persistent-subscriptions subscription description
- configure qos scheduler-policy tier scheduler description
- configure log filter description
- configure log filter entry description
- configure qos adv-config-policy description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure system security management-access-filter mac-filter entry description
- configure log event-trigger event description
- configure system telemetry sensor-groups sensor-group description
- configure system security pki ca-profile description
- configure log event-handling handler action-list entry description
- configure system telemetry destination-group description
- configure system security dist-cpu-protection policy description
- configure system security management-access-filter ipv6-filter entry description
- configure qos port-scheduler-policy description
- configure qos scheduler-policy description
- configure service mrp mrp-policy description
- configure log syslog description
- configure system security user public-keys ecdsa ecdsa-key description
- configure log accounting-policy description
- configure qos slope-policy description

description

Syntax **description** *medium-description-string*
no description

Context **[Tree]** (config>service>ies>interface>sap description)
[Tree] (config>service>ies>sub-if>grp-if>sap description)
[Tree] (config>port>sonet-sdh>path description)
[Tree] (config>port>tdm>ds1>channel-group description)
[Tree] (config>port>tdm>ds3 description)
[Tree] (config>port>tdm>e1>channel-group description)
[Tree] (config>port>tdm>e3 description)
[Tree] (config>service>apipe>sap description)
[Tree] (config>service>cpipe>sap description)
[Tree] (config>service>epipe>sap description)
[Tree] (config>service>fpipe>sap description)
[Tree] (config>service>ipipe>sap description)
[Tree] (config>service>ies>aarp-interface description)
[Tree] (config>gmpls-tun-grp description)

Full Context configure gmpls-tun-grp description
configure port sonet-sdh path description
configure port tdm ds1 channel-group description
configure port tdm ds3 description
configure port tdm e1 channel-group description
configure port tdm e3 description
configure service apipe sap description
configure service cpipe sap description
configure service epipe sap description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service fpipe sap description
configure service ies aarp-interface description
configure service ies interface sap description
configure service ies subscriber-interface group-interface sap description
configure service ipipe sap description

Description This command configures a text description that is stored in the configuration file. The text string is associated with a configuration context to identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default no description

Parameters *medium-description-string* — Specifies the description character string. Allowed values are any string, up to 160 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap description
- configure service cpipe sap description
- configure port sonet-sdh path description

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies aarp-interface description

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group description
- configure port tdm e1 channel-group description
- configure port tdm ds3 description
- configure port tdm e3 description

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap description

7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure gmpls-tun-grp description

All

- configure service ies interface sap description
- configure service ipipe sap description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap description

description

Syntax **description** *medium-description-string*
no description

Context **[Tree]** (config>service>ies>aa-interface>sap description)
[Tree] (config>service>vprn>aa-interface>sap description)

Full Context configure service ies aa-interface sap description
configure service vprn aa-interface sap description

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of this command removes the string from the configuration.

Parameters *medium-description-string* — Specifies the text string to describe the entity, up to 160 characters. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

description

Syntax **description** *long-description-string*
no description

Context **[Tree]** (config>service>vprn>isis>link-group description)
[Tree] (config>open-flow>of-switch description)
[Tree] (config>router>isis>link-group description)

Full Context configure open-flow of-switch description
configure router isis link-group description
configure service vprn isis link-group description

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default no description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *long-description-string* — Specifies the description character string. Allowed values are any string, up to 255-256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

description

Syntax **description** *long-description-string*
no description

Context **[Tree]** (config>router>if description)
[Tree] (config>port description)
[Tree] (config>lag description)
[Tree] (config>service>ies>aa-interface description)
[Tree] (config>service>ies>interface description)
[Tree] (config>service>ies>redundant-interface description)
[Tree] (config>service>ies>sub-if description)
[Tree] (config>service>ies>sub-if>grp-if description)
[Tree] (config>service>vpls>interface description)
[Tree] (config>service>vprn>aa-interface description)
[Tree] (config>service>vprn>aarp-interface description)
[Tree] (config>service>vprn>if description)
[Tree] (config>service>vprn>ip-mirror-interface description)
[Tree] (config>service>vprn>nw-if description)
[Tree] (config>service>vprn>red-if description)
[Tree] (config>service>vprn>subscriber-interface description)
[Tree] (config>service>vprn>sub-if>grp-if description)

Full Context configure lag description
configure port description
configure router interface description
configure service ies aa-interface description
configure service ies interface description
configure service ies redundant-interface description
configure service ies subscriber-interface description
configure service ies subscriber-interface group-interface description
configure service vpls interface description
configure service vprn aa-interface description
configure service vprn aarp-interface description
configure service vprn interface description
configure service vprn ip-mirror-interface description
configure service vprn network-interface description
configure service vprn redundant-interface description
configure service vprn subscriber-interface group-interface description
configure service vprn subscriber-interface description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Parameters *long-description-string* — Specifies the description character string. Allowed values are any string up to 255-256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface description
- configure service vprn redundant-interface description
- configure service vprn subscriber-interface description
- configure service ies redundant-interface description
- configure service vprn subscriber-interface group-interface description
- configure service ies subscriber-interface group-interface description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies aa-interface description
- configure service vprn aarp-interface description
- configure service vprn aa-interface description

All

- configure lag description
- configure port description
- configure service ies interface description
- configure service vprn interface description
- configure service vprn network-interface description
- configure router interface description
- configure service vpls interface description
- configure service vprn ip-mirror-interface description

description

Syntax **description** *medium-description-string*
no description

Context **[Tree]** (config>eth-tunnel description)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure eth-tunnel description

Description This command adds a text description for the eth-tunnel.

The **no** form of this command removes the text description.

Default Eth-tunnel

Parameters *medium-description-string* — Specifies the text description up to 160 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

description

Syntax **description** *description-string*
no description

Context **[Tree]** (config>service>vsd>domain description)

Full Context configure service vsd domain description

Description This command provides a description for a vsd-domain. This description must be added before the domain is activated using the **no shutdown** command.

Parameters *description-string* — Specifies the text for the description.

Platforms All

description

Syntax **description** *description-string*
no description

Context **[Tree]** (config>isa>lns-group description)
[Tree] (config>port-policy description)
[Tree] (config>subscr-mgmt>up-resiliency>fsg-template description)

Full Context configure isa lns-group description
configure port-policy description
configure subscriber-mgmt up-resiliency fate-sharing-group-template description

Description This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The **no** form of the command removes the string from the configuration.

Parameters *string* — Specifies the description character string. Allowed values are any string composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on.), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt up-resiliency fate-sharing-group-template description

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure port-policy description
- configure isa lns-group description

description

Syntax [**no**] **description**

Context **[Tree]** (config>service>nat>pcp-server-policy>option description)

Full Context configure service nat pcp-server-policy option description

Description This command enables/disables support for the **description** option.

Default no description

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

description

Syntax **description** *description-string*
no description

Context **[Tree]** (config>bfd>seamless-bfd>reflector description)

Full Context configure bfd seamless-bfd reflector description

Description This command specifies a description of a S-BFD reflector.

Parameters *description-string* — Specifies the S-BFD reflector description.

Platforms All

description

Syntax **description** *description-string*
no description

Context **[Tree]** (config>system>alarm-contact-input description)

Full Context configure system alarm-contact-input description

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a text description of an alarm contact input pin. The description is stored in the CLI configuration file. It indicates the usage or attribute of the pin, and helps the user to identify the purpose of the pin. The description is included in the log event when the pin changes state.

The **no** form of this command reverts the description string to the default.

Parameters *description-string* — Specifies a printable character string, up to 80 characters.

Default "Pin *x*", where *x* is the alarm contact input pin number.

Platforms 7750 SR-a

8.113 descriptor-type

descriptor-type

Syntax **descriptor-type** *type*

Context **[Tree]** (config>qos>atm-td-profile descriptor-type)

Full Context configure qos atm-td-profile descriptor-type

Description This command is used to specify the type of the traffic descriptor profile as per ATM Forum Traffic Management Specification Version 4.1.

Default Table 41 lists the default values of descriptor type based on a service category.

Table 41 **Descriptor Type Default Values**

Service Category	Default Descriptor Type
CBR	P0_1
UBR	P0_1
UBR with MIR	P0_1
rt-VBR or nrt-VBR	P0_1andS0_1

Parameters *type* — Defines interpretation of traffic parameters that are specified for this profile.

Values P0_1, P0_1andS0_Tag, P0_1andS0, P0_1andS0_1

Table 42 describes these rules.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 42 **Descriptor Type Rate Interpretations**

Descriptor Type	Rates Interpretation	Applicable Service Categories
P0_1	PIR applies to CLP=0 and CLP=1 cell flows	CBR, UBR, UBR with MIR
P0_1andS0_1	PIR applies to CLP=0 and CLP=1 cell flows SCR applies to CLP=0 and CLP=1 cell flows	rt-VBR and nrt-VBR
P0_1andS0	PIR applies to CLP=0 and CLP=1 cell flows SCR applies to CLP=0 cell flow	rt-VBR and nrt-VBR

Setting the descriptor type to a value not compatible with the service category will generate an error.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

8.114 dest-class

dest-class

Syntax **dest-class** *dest-class*
no dest-class

Context [Tree] (config>router>policy-options>policy-statement>entry dest-class)
[Tree] (config>router>policy-options>policy-statement>default-action dest-class)

Full Context configure router policy-options policy-statement default-action dest-class
configure router policy-options policy-statement entry dest-class

Description This command specifies the policy accounting destination class index to associate with matched routes.

Default no dest-class

Parameters *dest-class* — Specifies the destination class.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.115 dest-global-id

dest-global-id

Syntax **dest-global-id** *dest-global-id*
no dest-global-id

Context **[Tree]** (config>router>mpls>lsp dest-global-id)

Full Context configure router mpls lsp dest-global-id

Description This optional command configures the MPLS-TP Global ID of the far end node of the MPLS-TP LSP. This command is only allowed for MPLS-TP LSPs. Global ID values of 0 indicate that the local node's configured global ID is used. If the local global-id is 0, then the dest-global-id must also be 0. The dest-global-id cannot be changed if an LSP is in use by an SDP.

Default dest-global-id 0

Parameters *dest-global-id* — Specifies the destination global ID.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.116 dest-ip

dest-ip

Syntax [**no**] **dest-ip** *ip-address*

Context **[Tree]** (config>service>ies>if>sap>ip-tunnel dest-ip)
[Tree] (config>service>vprn>if>sap>ip-tunnel dest-ip)
[Tree] (config>service>vprn>sap>ipsec-tunnel dest-ip)

Full Context configure service ies interface sap ip-tunnel dest-ip
configure service vprn interface sap ip-tunnel dest-ip
configure service vprn sap ipsec-tunnel dest-ip

Description This command configures a private IPv4 or IPv6 address of the remote tunnel endpoint. A tunnel can have up to 16 **dest-ip** commands. At least one **dest-ip** address is required in the configuration of a tunnel. A tunnel does not come up operationally unless all **dest-ip** addresses are reachable (part of a local subnet).

Unnumbered interfaces are not supported.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the destination IP of the tunnel.

Parameters *ip-address* — Specifies the private IPv4 or IPv6 address of the remote IP tunnel endpoint. If this remote IP address is not within the subnet of the IP interface associated with the tunnel then the tunnel will not come up.

Values

<ip-address>	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.117 dest-ip-addr

dest-ip-addr

Syntax **dest-ip-addr** *ip-addr***ess**
no dest-ip-addr

Context **[Tree]** (config>mcast-mgmt>mcast-rprt-dest dest-ip-addr)

Full Context configure mcast-management mcast-reporting-dest dest-ip-addr

Description This command specifies the IP address of the external node to which IGMP events are exported. The destination IP address can only be reachable from the global routing table (no vrf access).

The **no** form of this command removes the destination address from the configuration.

Parameters *ip-addr* — Specifies the IP address of the multicast reporting destination.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.118 dest-mac

dest-mac

Syntax **dest-mac** {**nearest-bridge** | **nearest-non-tpmr** | **nearest-customer**}

Context **[Tree]** (config>port>ethernet>lldp dest-mac)

Full Context configure port ethernet lldp dest-mac

Description This command configures destination MAC address parameters.

Default dest-mac nearest-bridge

Parameters **nearest-bridge** — Specifies to use the nearest bridge.

nearest-non-tpmr — Specifies to use the nearest non-Two-Port MAC Relay (TPMR).

nearest-customer — Specifies to use the nearest customer.

Platforms All

dest-mac

Syntax **dest-mac** *ieee-address*
no dest-mac

Context **[Tree]** (config>oam-pm>session>ethernet dest-mac)

Full Context configure oam-pm session ethernet dest-mac

Description This command defines the destination MAC address of the peer MEP and sets the destination MAC address in the layer two header to match. This must be a unicast address.

The **no** form of this command removes session parameter.

Parameters *ieee-address* — Specifies the Layer 2 unicast MAC address of the destination MEP.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.119 dest-mac-address

dest-mac-address

Syntax **dest-mac-address** *mac-address* [**create**]
no dest-mac-address *mac-address*

Context **[Tree]** (config>macsec>mac-policy dest-mac-address)

Full Context configure macsec mac-policy dest-mac-address

Description This command specifies the destination MAC address.

The **no** form of this command removes the MAC address.

Parameters *mac-address* — Specifies the value of the MAC address policy.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

create — Mandatory to create the configuration.

Platforms All

8.120 dest-mac-rewrite

dest-mac-rewrite

Syntax **dest-mac-rewrite** *ieee-address*
no dest-mac-rewrite

Context **[Tree]** (config>service>vpls>sap>egress dest-mac-rewrite)

Full Context configure service vpls sap egress dest-mac-rewrite

Description This commands enables the overwriting of a destination MAC address to an operator-configured value for all unicast packets egressing the specified SAP. The command is intended to be deployed with L2 PBF SAP redirect when a remote end of the SAP interface is an L3 interface with a MAC address different from the MAC address of the non-PBF-ed L3 interface. See Filter Policy in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide* for more details.

The **no** form disables the option.

Default no dest-mac-rewrite

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ieee-address* — Specifies the MAC address

Values 1xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
Cannot be all zeros

Platforms All

8.121 dest-realm

dest-realm

Syntax **dest-realm** *realm*
no dest-realm

Context **[Tree]** (debug>diameter dest-realm)

Full Context debug diameter dest-realm

Description This command restricts the output to a specific destination-realm.

The **no** form of this command disables debugging.

Parameters *realm* — Specifies the realm up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.122 dest-realm-learning

dest-realm-learning

Syntax [**no**] **dest-realm-learning**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx dest-realm-learning)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy dest-realm-learning)

Full Context configure subscriber-mgmt diameter-application-policy gx dest-realm-learning
configure subscriber-mgmt diameter-application-policy gy dest-realm-learning

Description This command configures destination realm learning that is used in outgoing Gx and Gy Credit Control Request (CCR) messages. Destination realm is a mandatory configuration parameter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured destination realm is always used in the initial CCR-I message. The consecutive request message of a Gx or Gy session can use the destination realm as learned from replies within a DIAMETER session (if learning is enabled), or they can ignore the realm from the reply and always use the configured destination realm in Gx and Gy request messages (learning is disabled).

The **no** form of this command ignores the realm from the reply.

Default dest-realm-learning

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.123 dest-tunnel-number

dest-tunnel-number

Syntax **dest-tunnel-number** *dest-tunnel-number*
no dest-tunnel-number

Context **[Tree]** (config>router>mpls>lsp dest-tunnel-number)

Full Context configure router mpls lsp dest-tunnel-number

Description This optional command configures the MPLS-TP tunnel number of the LSP at the far end node of the MPLS-TP LSP. This command is only allowed for MPLS-TP LSPs. If it is not entered, then the system will take the dest-tunnel-number to be the same as the src-tunnel-num for the LSP.

Default The default value is the configured *src-tunnel-num*.

Parameters *dest-tunnel-number* — Specifies the destination tunnel number.

Values 1 to 61440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.124 dest-udp-port

dest-udp-port

Syntax **dest-udp-port** *udp-port-number*
no dest-udp-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>oam-pm>session>ip dest-udp-port)

Full Context configure oam-pm session ip dest-udp-port

Description This command defines the destination UDP port on outbound TWAMP Light packets sent from the session controller. The destination UDP port must match the UDP port value configured on the TWAMP Light reflector that is responding to this specific TWAMP Light test.

The **no** form of this command removes the destination UDP port setting.

Parameters *udp-port-number* — Specifies the UDP source port.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dest-udp-port

Syntax **dest-udp-port** *port-number*

Context **[Tree]** (config>test-oam>link-meas>template>twl dest-udp-port)

Full Context configure test-oam link-measurement measurement-template twamp-light dest-udp-port

Description This command configures the destination UDP port used by the link measurement tests.

Default dest-udp-port 862

Parameters *port-number* — Specifies the destination UDP port copied into the UDP header of each Echo request packet launched for each link measurement test belonging to the specified template.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.125 destination

destination

Syntax **destination** *ip-address*
no destination

Context **[Tree]** (config>oam-pm>session>ip destination)

Full Context configure oam-pm session ip destination

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the destination IP address that is assigned to the TWAMP Light packets. The destination address must be included in the prefix list on the session reflector within the configured context in order to allow the reflector to process the inbound TWAMP Light packets.

The **no** form of this command removes the destination parameters.

Parameters *ip-address* — Specifies the IP address of the IP peer to which the packet is directed.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

destination

Syntax **destination** *ip-address* [**create**]
no destination *ip-address*

Context **[Tree]** (config>filter>redirect-policy destination)

Full Context configure filter redirect-policy destination

Description This command defines a destination in a redirect policy. More than one destination can be configured. Whether a destination IPv4/IPv6 address will receive redirected packets depends on the effective priority value after evaluation.

The most preferred destination is programmed in hardware as action forward next-hop. If all destinations are down (as determined by the supported tests), action forward is programmed in hardware. All destinations within a given policy must be either IPv4 or (exclusive) IPv6. The redirect policy with IPv4 destinations configured can only be used by IPv4 filter policies. The redirect policy with IPv6 destinations configured can only be used by IPv6 filter policies.

Default no destination

Parameters *ip-address* — Specifies the IPv4 address (in dotted decimal notation) or IPv6 address to send the redirected traffic to.

Values

IPv4 address:	ip-address: a.b.c.d
IPv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

destination

Syntax **destination memory** *num-entries*
destination syslog *syslog-id*
no destination

Context **[Tree]** (config>filter>log destination)

Full Context configure filter log destination

Description This command configures the destination for filter log entries for the filter log ID.

Filter logs can be sent to either memory (**memory**) or to an existing Syslog server definition (**syslog**).

If the filter log destination is **memory**, the maximum number of entries in the log must be specified.

The **no** form of the command deletes the filter log association.

Default destination memory 1000

Parameters **memory** *num-entries* — Specifies the destination of the filter log ID is a memory log. The *num-entries* value is the maximum number of entries in the filter log expressed as a decimal integer.

Values 10 to 50000

syslog *syslog-id* — Specifies the destination of the filter log ID is a Syslog server. The *syslog-id* parameter is the number of the Syslog server definition.

Values 1 to 10

Platforms All

destination

Syntax **destination** {*ip-address* | *fqdn*} **port** *port* [**create**]
no destination {*ip-address* | *fqdn*} **port** *port*

Context **[Tree]** (config>system>grpc-tunnel>destination-group destination)
[Tree] (config>system>telemetry>destination-group destination)

Full Context configure system grpc-tunnel destination-group destination
configure system telemetry destination-group destination

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a destination IP address and port for a specific destination within a destination group. Up to two destinations can be defined within a destination group. Each destination is an IPv4 address, an IPv6 address, or the Fully Qualified Domain Name (FQDN).

The **no** form of this command removes the destination from the destination group.

Parameters *ip-address* — Specifies the IPv4 address (in dotted decimal notation) or IPv6 address.

Values

IPv4 address:	ip-address: a.b.c.d	
IPv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0..FFFF]H
	d:	[0..255]D

fqdn — Specifies the FQDN.

port — Specifies the TCP destination port number.

Values 1 to 65535

create — Keyword used to create a destination.

Platforms All

destination

Syntax **destination** *ip-address*
no destination

Context **[Tree]** (config>router>if>if-attr>delay>dyn>twamp>ipv4 destination)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv4 destination

Description This command configures the unicast IPv4 destination address for the TWAMP Light test packet. When this command is not configured, the destination IPv4 address is auto-assigned for interfaces configured with a prefix length of 30 and 31. All other interface prefix lengths and unnumbered interfaces are unable to auto- assign the destination IPv4 address. If the interface does not use a prefix length of 30 or 31, the destination must be configured.

Deleting a configured destination removes the specified address and causes the source address to be auto-assigned for prefix length of 30 and 31.

Configuration modifications are allowed without administratively disabling the IPv4 protocol.

The **no** form of this command removes the IPv4 address from the configuration.

Default no destination

Parameters *ip-address* — Specifies the IPv4 destination address.

Values a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

destination

Syntax **destination** *ipv6-address*
no destination

Context **[Tree]** (config>router>if>if-attr>delay>dyn>twamp>ipv6 destination)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv6 destination

Description This command configures the IPv6 destination address of the TWAMP Light test packet. When this command is not configured, no destination address is present and an error is raised to prevent the transmission of the test packet.

The IPv6 protocol can be enabled without addressing. However, the test does not transmit packets.

The link local address must be in the form fe80::/60 in accordance with RFC 4291, *IP Version 6 Addressing Architecture*.

The **no** form of this command removes the IPv6 address from the configuration.

Default no destination

Parameters *ipv6-address* — Specifies the TWAMP Light IPv6 destination address

Values

ipv6-address:	x:x:x:x:x:x:x:x x - [0 to FFFF]H unicast and link local IPv6 address only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.126 destination-address

destination-address

Syntax [**no**] **destination-address** *ip-address*

Context **[Tree]** (config>filter>gre-tun-tmp>ipv4 destination-address)

Full Context configure filter gre-tunnel-template ipv4 destination-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines one or more destinations for the GRE IP header used to encapsulate the matching IPv4/IPv6 packet.

Traffic matching the associated IPv4 or IPv6 filter are hashed across all available destination address. If no destination address is available, then matching traffic follows the configured **pbr-down-action-override** action, if configured.

The **no** form of this command removes the specified destination IP address configuration from the associated GRE tunnel template.

Parameters *ip-address* — Specifies up to 16 IPv4 addresses to be used as the destination address.

Platforms All

destination-address

Syntax **destination-address** *ip-address*
no destination-address

Context **[Tree]** (config>service>ies>if>ping-template destination-address)
[Tree] (config>service>vprn>if>ping-template destination-address)

Full Context configure service ies interface ping-template destination-address
configure service vprn interface ping-template destination-address

Description This command configures the address to where the ICMP echo requests are directed to test connectivity. The source of the ICMP echo request is the primary IPv4 address of the interface under which the ping-template is configured. The destination address must be on the same subnet as the source IP address. A configuration warning message displays if the primary IPv4 address and the destination are not on the same subnet, `INFO: PIP #2092 Ping template misconfiguration - destination-address and primary IP address should fall in the same subnet.` Unnumbered interfaces and loopback addresses are not supported.

The **config>service>ies|vprn>interface>ping-template** must be in the no shutdown state to remove or change the **destination-address** *ip-address*.

The **no** form of this command removes the destination address from the configuration.

Default none

Parameters *ip-address* — Specifies the destination address to where the ICMP echo requests are directed to test connectivity, in a.b.c.d format.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.127 destination-class

destination-class

Syntax **destination-class** *index*
no destination-class *index*
no destination-class all

Context **[Tree]** (config>router>policy-acct-template destination-class)

Full Context configure router policy-acct-template destination-class

Description Commands in this context create a destination class index for the template.

The **no** form of this command removes the index from the configuration.

Parameters *index* — Specifies the destination index value.

Values 1 to 255

all — Deletes all destination class indexes from this configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

destination-class

Syntax **destination-class** *dest-index*
no destination-class [*dest-index*]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect destination-class)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel destination-class)

Full Context configure service vprn static-route-entry indirect destination-class
configure service vprn static-route-entry ipsec-tunnel destination-class

Description This command configures the policy accounting destination-class index to be used when incrementing accounting statistic for traffic matching the associated static route.

The **no** form of this command removes the associated destination-class from the associated static route nexthop.

Default no destination-class

Parameters *dest-index* — The destination index integer value.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

destination-class

Syntax **destination-class** *dest-index*
no destination-class

Context **[Tree]** (config>filter>ip-filter>entry>match destination-class)
[Tree] (config>filter>ipv6-filter>entry>match destination-class)

Full Context configure filter ip-filter entry match destination-class
configure filter ipv6-filter entry match destination-class

Description This command configures the BGP destination-class value match criterion. Filtering egress traffic on **destination-class** requires the **destination-class-lookup** command to be enabled on the interface that the packet ingresses on.

The **no** form of the command removes the destination-class value match criterion.

Default no destination-class

Parameters *dest-index* — Specifies the destination index integer value.

Values 1 to 255

Platforms All

destination-class

Syntax **destination-class** *dest-index*
no destination-class [*dest-index*]

Context **[Tree]** (config>router>static-route-entry>indirect destination-class)
[Tree] (config>router>static-route-entry>next-hop destination-class)

Full Context configure router static-route-entry indirect destination-class
configure router static-route-entry next-hop destination-class

Description This command configures the policy accounting destination-class index to be used when incrementing accounting statistic for traffic matching the associated static route.

The **no** form of this command removes the associated destination-class from the associated static route next hop.

Default no destination-class

Parameters *dest-index* — Specifies the destination index integer value.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.128 destination-class-lookup

destination-class-lookup

Syntax [**no**] **destination-class-lookup**

Context **[Tree]** (config>service>ies>if>ingress destination-class-lookup)

Full Context configure service ies interface ingress destination-class-lookup

Description This command enables BGP destination-class lookup for packets on this interface ingress and is supported on FP3-based cards and later. It is used in combination with an IP filter or IPv6 filter **destination-class** to filter traffic egress of the router based on BGP destination classes.

The command is supported on network, IES, VPRN and R-VPLS interfaces. It is not supported on subscriber interfaces, tunnel interfaces or VPRN network interfaces.

Default no destination-class-lookup

Platforms All

destination-class-lookup

Syntax [**no**] **destination-class-lookup**

Context **[Tree]** (config>service>vprn>if>ingress destination-class-lookup)

Full Context configure service vprn interface ingress destination-class-lookup

Description This command enables BGP destination-class lookup for packets on this interface ingress and is supported on FP3-based cards and later. It is used in combination with an IP filter or IPv6 filter **destination-class** to filter traffic egress of the router based on BGP destination classes.

The command is supported on network, IES, VPRN and R-VPLS interfaces. It is not supported on subscriber interfaces, tunnel interfaces and VPRN network interfaces.

Default no destination-class-lookup

Platforms All

destination-class-lookup

Syntax [**no**] **destination-class-lookup**

Context **[Tree]** (config>router>if>ingress destination-class-lookup)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface ingress destination-class-lookup

Description This command enables BGP destination-class lookup for packets on this interface ingress. It is used in combination with an IP filter or IPv6 filter **destination-class** to filter traffic egress of the router based on BGP destination classes.

The command is supported on network, IES, VPRN and R-VPLS interfaces. It is not supported on subscriber interfaces, tunnel interfaces or VPRN network interfaces.

The **no** form of this command reverts to the default value.

Default no destination-class-lookup

Platforms All

8.129 destination-group

destination-group

Syntax **destination-group** *name* [**create**]
no destination-group *name*

Context **[Tree]** (config>system>grpc-tunnel destination-group)
[Tree] (config>system>telemetry destination-group)

Full Context configure system grpc-tunnel destination-group
configure system telemetry destination-group

Description Commands in this context configure commands for destination groups.

The **no** form of this command removes the destination group name.

Parameters *name* — Specifies the destination group name, up to 32 characters.

create — Keyword used to create a destination group.

Platforms All

destination-group

Syntax **destination-group** *name*
no destination-group

Context **[Tree]** (config>system>grpc-tunnel>tunnel destination-group)

Full Context configure system grpc-tunnel tunnel destination-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command assigns the specified destination group to a gRPC tunnel.

The **no** form of this command removes the specified destionation group from the gRPC tunnel.

Default no destination-group

Parameters *name* — Specifies the destination group name, up to 32 characters

Platforms All

destination-group

Syntax **destination-group** *name*
no destination-group

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription destination-group)

Full Context configure system telemetry persistent-subscriptions subscription destination-group

Description This command assigns an existing destination group to the specified persistent subscription. The assigned **destination-group** must already exist before the configured persistent subscription can be activated.

The **no** form of this command removes the destination group name from the persistent subscription.

Parameters *name* — Specifies the destination group name, up to 32 characters.

Platforms All

8.130 destination-host

destination-host

Syntax **destination-host** *destination-host-string*
no destination-host

Context **[Tree]** (config>aaa>diam-peer-plcy>peer destination-host)

Full Context configure aaa diameter-peer-policy peer destination-host

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Destination-Host AVP that is sent in CCR-I/U/T and RAA messages. If the destination host name is not explicitly set by configuration, it is learned from CCA or RAR messages. In other words, the origin host name received in the CCA or RAR message is used to populate or replace the destination host name for a session in SR OS node.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Parameters *destination-host-string* — Specifies the destination host name, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.131 destination-ip

destination-ip

Syntax [**no**] **destination-ip**

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>include destination-ip)

Full Context configure service nat syslog syslog-export-policy include destination-ip

Description This command includes the destination IP address in the flow log. The **destination-ip** is significant in Destination Based NAT (DNAT) where the foreign IP address is translated. A foreign IP address is the original IP address toward the destination node and in DNAT it is replaced by the **destination-ip**. More clearly, on the inside (private side), the IP address of the destination node is referred to as foreign IP (original destination IP), and once this address is translated by DNAT, it is referred to as destination IP (translated destination IP) on the outside (public side).

The **no** form of the command disables the feature.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.132 destination-port

destination-port

Syntax **destination-port** [*destination-port*]

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>collector destination-port)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service nat syslog syslog-export-policy collector destination-port

Description This command configures the destination port (collector port) to which UDP stream containing the syslog flow records are sent.

Default destination-port 514

Parameters *destination-port* — Specifies the destination port to which UDP streams are sent.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.133 destination-prefix

destination-prefix

Syntax **destination-prefix** *ip-prefix/length* [**nat-policy** *nat-policy-name*]
no destination-prefix *ip-prefix/length*

Context **[Tree]** (config>service>vprn>nat>inside destination-prefix)
[Tree] (config>router>nat>inside destination-prefix)

Full Context configure router nat inside destination-prefix
configure service vprn nat inside destination-prefix

Description This command configures a destination prefix. An (internal) static route will be created for this prefix. All traffic that hits this route will be subject to NAT. The system will not allow a destination-prefix to be configured if the configured nat-policy refers to an IP pool that resides in the same service (as this would result in a routing loop).

Parameters *ip-prefix* — Specifies the IP prefix; host bits must be zero (0).

Values a.b.c.d

length — Specifies the prefix length.

Values 0 to 32

nat-policy-name — Specifies the NAT policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

destination-prefix

Syntax [**no**] **destination-prefix**

Context **[Tree]** (config>cflowd>collector>aggregation destination-prefix)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure cflowd collector aggregation destination-prefix

Description This command specifies that the aggregation data is based on destination prefix information.

The **no** form removes this type of aggregation from the collector configuration.

Platforms All

8.134 destination-realm

destination-realm

Syntax **destination-realm** *destination-realm-string*
no destination-realm

Context **[Tree]** (config>aaa>diam-peer-plcy>peer destination-realm)

Full Context configure aaa diameter-peer-policy peer destination-realm

Description This command configures the destination-realm AVP that is sent in CCR-I/U/T and RAA messages. The destination realm name cannot be learned dynamically from the CCA or RAR messages and therefore it should be explicitly configured in SR OS node. Once configured, it cannot be changed while peers are open.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Parameters *destination-realm-string* — Specifies the destination realm name, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.135 destruct-timeout

destruct-timeout

Syntax **destruct-timeout** *destruct-timeout*
no destruct-timeout

Context **[Tree]** (config>router>l2tp destruct-timeout)
[Tree] (config>router>l2tp>group destruct-timeout)
[Tree] (config>router>l2tp>group>tunnel destruct-timeout)
[Tree] (config>service>vprn>l2tp destruct-timeout)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>l2tp>group destruct-timeout)
[Tree] (config>service>vprn>l2tp>group>tunnel destruct-timeout)

Full Context configure router l2tp destruct-timeout
configure router l2tp group destruct-timeout
configure router l2tp group tunnel destruct-timeout
configure service vprn l2tp destruct-timeout
configure service vprn l2tp group destruct-timeout
configure service vprn l2tp group tunnel destruct-timeout

Description This command configures the period of time that the data of a disconnected tunnel will persist before being removed.

The **no** form of this command removes the value from the configuration.

Default no destruct-timeout

Parameters *destruct-timeout* — Specifies the automatic removal of dynamic L2TP sessions, in seconds, that are no longer active.

Default no destruct-timeout

Values 60 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.136 detail-level

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context [Tree] (debug>router>ip>dhcp detail-level)
[Tree] (debug>router>ip>dhcp6 detail-level)
[Tree] (debug>router>local-dhcp-server detail-level)

Full Context debug router ip dhcp detail-level
debug router ip dhcp6 detail-level
debug router local-dhcp-server detail-level

Description This command debugs the DHCP tracing detail level.

Parameters **low** — Displays a low detail level for DHCP debugging.

medium — Displays a medium detail level for DHCP debugging.

high — Displays a high detail level for DHCP debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- debug router local-dhcp-server detail-level

All

- debug router ip dhcp detail-level
- debug router ip dhcp6 detail-level

detail-level

Syntax **detail-level** *detail-level*

Context **[Tree]** (debug>router>l2tp>assignment-id>packet detail-level)
[Tree] (debug>router>l2tp>group>packet detail-level)
[Tree] (debug>router>l2tp>packet detail-level)

Full Context debug router l2tp assignment-id packet detail-level
debug router l2tp group packet detail-level
debug router l2tp packet detail-level

Description This command configures the L2TP packet debugging level of detail.

Parameters *detail-level* — Specifies the detail level.

Values low, high

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context **[Tree]** (debug>service>id>ppp>packet detail-level)

Full Context debug service id ppp packet detail-level

Description This command specify the detail level of PPP packet debug output.

The **no** form of this command disables debugging.

Parameters **low** | **medium** | **high** — Specifies the detail level of PPP packet debug output.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

detail-level

Syntax **detail-level** *level*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>diameter detail-level)

Full Context debug diameter detail-level

Description This command configures the detail level of debug output.

The **no** form of this command disables debugging.

Parameters *level* — Specifies the detail level.

Values low, medium, high

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context [Tree] (debug>router>radius detail-level)

Full Context debug router radius detail-level

Description This command specifies the output detail level of command **debug router radius**.

Default detail-level medium

Parameters **low** — Specifies that the output includes packet type, server address, length, radius-server-policy name.

medium — Specifies all output in low level including the RADIUS attributes in the packet.

high — Specifies all output in medium level including the hex packet dump.

Platforms All

detail-level

Syntax **detail-level** *detail-level*

Context [Tree] (debug>router>wpp detail-level)
[Tree] (debug>router>wpp>packet detail-level)
[Tree] (debug>router>wpp>portal>packet detail-level)

Full Context debug router wpp detail-level
debug router wpp packet detail-level
debug router wpp portal packet detail-level

Description This command specifies the detail level of WPP packet debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *detail-level* — specifies the detail level of WPP packet debugging.

Values high — Specifies a high detail level for WPP packet debugging
low — Specifies a low detail for WPP packet debugging

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg>pppoe-client>brg-id detail-level)

Full Context debug subscriber-mgmt vrgw brg pppoe-client brg-id detail-level

Description This command specifies the amount of detail present in debugging the specified PPPoE client.

Default detail-level high

Parameters **low** — Specifies a low level of detail during debugging.

medium — Specifies a medium level of detail during debugging.

high — Specifies a high level of detail during debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context **[Tree]** (debug>service>id>igmp-snooping detail-level)

Full Context debug service id igmp-snooping detail-level

Description This command enables and configures the IGMP tracing detail level.

The **no** form of this command disables the IGMP tracing detail level.

Platforms All

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context **[Tree]** (debug>service>id>mld detail-level)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug service id mld-snooping detail-level

Description This command enables and configures the MLD tracing detail level.

The **no** form of this command disables the MLD tracing detail level.

Platforms All

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context **[Tree]** (debug>service>id>dhcp detail-level)

Full Context debug service id dhcp detail-level

Description This command configures the DHCP tracing detail level.

The **no** form of the command disables debugging.

Parameters **low** — Displays a low detail level for DHCP debugging.

medium — Displays a medium detail level for DHCP debugging.

high — Displays a high detail level for DHCP debugging.

Platforms All

detail-level

Syntax **detail-level** *detail-level*

Context **[Tree]** (debug>router>pcp>pcp-server>packet detail-level)

Full Context debug router pcp pcp-server packet detail-level

Description This command configures the packet debugging level of detail.

Parameters *detail-level* — Specifies the detail level.

Values low, high

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.137 detailed-acct-attributes

detailed-acct-attributes

Syntax [**no**] **detailed-acct-attributes**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include detailed-acct-attributes)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute detailed-acct-attributes

Description This command enables detailed reporting of per queue and per policer octet and packet counters using RADIUS VSAs. Enabled by default. It can be enabled simultaneously with aggregate counters (std-acct-attributes).

The **no** form of this command excludes the detailed counter VSAs from the RADIUS accounting messages.

Default detailed-acct-attributes

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.138 detect

detect

Syntax **detect num-moves** *num-moves* **window** *minutes*

Context **[Tree]** (config>service>vpls>bgp-evpn>mac-duplication detect)

Full Context configure service vpls bgp-evpn mac-duplication detect

Description The **mac-duplication** featured is always enabled by default. This command modifies the default behavior. **mac-duplication** monitors the number of moves of a MAC address for a period of time (window).

Default detect num-moves 5 window 3

Parameters *num-moves* — Identifies the number of MAC moves in a VPLS service. The counter is incremented when a specified MAC is locally relearned in the FDB or flushed from the FDB due to the reception of a better remote EVPN route for that MAC.

Values 3 to 10

Default 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

minutes — Specifies the length of the window in minutes.

Values 1 to 15

Default 3

Platforms All

8.139 detect-seen-ip

detect-seen-ip

Syntax [**no**] **detect-seen-ip**

Context **[Tree]** (config>app-assure>group>transit-ip-policy detect-seen-ip)

Full Context configure application-assurance group transit-ip-policy detect-seen-ip

Description This command enables the detection of transit subscribers based on the IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.140 detection-time

detection-time

Syntax **detection-time** *seconds*
no detection-time

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>protocol>dynamic-parameters detection-time)

Full Context configure system security dist-cpu-protection policy protocol dynamic-parameters detection-time

Description When a dynamic enforcing policer is instantiated, it remains allocated until at least a contiguous conforming period of detection-time passes.

Default detection-time 30

Parameters *seconds* — Specifies the detection time.

Values 1 to 128000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

detection-time

Syntax **detection-time** *seconds*

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>static-policer detection-time)

Full Context configure system security dist-cpu-protection policy static-policer detection-time

Description When a policer is declared as in an “exceed” state, it remains as exceeding until a contiguous conforming period of **detection-time** passes. The **detection-time** only starts after the exceed-action hold-down is complete. If the policer detects another exceed during the detection count down then a hold-down is once again triggered before the policer re-enters the detection time (that is, the countdown timer starts again at the configured value). During the hold-down (and the detection-time), the policer is considered as in an “exceed” state.

Default detection-time 30

Parameters *seconds* — Specifies the detection time.

Values 1 to 128000

Platforms All

8.141 deterministic

deterministic

Syntax **deterministic**

Context **[Tree]** (config>service>vprn>nat>inside deterministic)
[Tree] (config>router>nat>inside deterministic)

Full Context configure router nat inside deterministic
configure service vprn nat inside deterministic

Description Commands in this context configure deterministic NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

deterministic

Syntax **deterministic**

Context **[Tree]** (config>service>vprn>nat>outside>pool deterministic)

Full Context configure service vprn nat outside pool deterministic

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures deterministic NAT for this pool.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.142 deterministic-med

deterministic-med

Syntax [**no**] **deterministic-med**

Context **[Tree]** (config>service>vprn>bgp>best-path-selection deterministic-med)

Full Context configure service vprn bgp best-path-selection deterministic-med

Description This command controls how the BGP decision process compares routes on the basis of MED. When **deterministic-med** is configured, BGP groups paths that are equal up to the MED comparison step based on neighbor AS, and then compares the best path from each group to arrive at the overall best path. This change to the BGP decision process makes best path selection completely deterministic in all cases. Without **deterministic-med**, the overall best path selection is sometimes dependent on the order of the route arrival because of the rule that MED cannot be compared in routes from different neighbor AS.

Default no deterministic-med

Platforms All

deterministic-med

Syntax [**no**] **deterministic-med**

Context **[Tree]** (config>router>bgp>best-path-selection deterministic-med)

Full Context configure router bgp best-path-selection deterministic-med

Description This command controls how the BGP decision process compares routes on the basis of MED. When **deterministic-med** is configured, BGP groups paths that are equal up to the MED comparison step based on neighbor AS, and then compares the best path from each group to arrive at the overall best path. This change to the BGP decision process makes best path selection completely deterministic in all cases. Without **deterministic-med**, the overall best path selection is sometimes dependent on the order of the route arrival because of the rule that MED cannot be compared in routes from different neighbor AS.

Default no deterministic-med

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.143 deterministic-script

deterministic-script

Syntax **deterministic-script**

Context **[Tree]** (config>service>nat deterministic-script)

Full Context configure service nat deterministic-script

Description This command configures the script generated for deterministic NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.144 device

device

Syntax **device** *ieee-address* [**create**]
no device *ieee-address*

Context **[Tree]** (config>system>bluetooth device)

Full Context configure system bluetooth device

Description This command is used to add and remove devices from the Bluetooth allowlist or to enter the context to configure the MAC. The router only accepts pairing requests with devices that are in the allowlist. The devices are identified through their IEEE 802 MAC addresses. There can be up to six devices defined in the allowlist.

The **create** keyword must be used to add a new device.

The **no** form of this command removes the indicated device from the allowlist.

Parameters *ieee-address* — Specifies the MAC address of the external Bluetooth device.

Values 6-byte unicast MAC address (*xx:xx:xx:xx:xx:xx* or *xx-xx-xx-xx-xx-xx*)

Platforms 7750 SR-1, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.145 device-label

device-label

Syntax **device-label** *name*
no device-label

Context **[Tree]** (config>system>management-interface>remote-management device-label)

Full Context configure system management-interface remote-management device-label

Description This command configures the metadata label that is supplied to all remote managers. This label can be used to group devices (network-nodes) that serve a common purpose or role.

If this command is also configured for a specific remote manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command causes an empty string to be used.

Parameters *name* — Specifies the device-label name, up to 64 characters.

Platforms All

device-label

Syntax **device-label** *name*
no device-label

Context **[Tree]** (config>system>management-interface>remote-management>manager device-label)

Full Context configure system management-interface remote-management manager device-label

Description This command configures the metadata label that is supplied to this remote manager. This label can be used to group devices (network-nodes) with a common purpose/role.

This command takes precedence over the same command configured in the global context (**config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command causes the device-label name to be inherited from the global context (**config**>**system**>**management-interface**>**remote-management)**.

Parameters *name* — Specifies the device-label name, up to 64 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.146 device-name

device-name

Syntax **device-name** *name*
no device-name

Context **[Tree]** (config>system>management-interface>remote-management device-name)

Full Context configure system management-interface remote-management device-name

Description This command configures a device name that is supplied to all remote managers. This name identifies the specified SR OS node in the network.

If this command is also configured for a specific manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command causes the system to use the default device name (system-name).

Default system-name

Parameters *name* — Specifies the device name, up to 64 characters.

Platforms All

device-name

Syntax **device-name** *name*
no device-name

Context **[Tree]** (config>system>management-interface>remote-management>manager device-name)

Full Context configure system management-interface remote-management manager device-name

Description This command configures a device name that is supplied to the specific manager. This name identifies the specified SR OS node in the network.

This command takes precedence over the same command configured in the global context **(config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command causes the device name to be inherited from the global context (**config**>**system**>**management-interface**>**remote-management)**.

Default system-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the device name, up to 64 characters.

Platforms All

8.147 df-bit-lac

df-bit-lac

Syntax **df-bit-lac** {**always** | **never**}
no df-bit-lac

Context **[Tree]** (config>router>l2tp df-bit-lac)
[Tree] (config>service>vprn>l2tp df-bit-lac)

Full Context configure router l2tp df-bit-lac
configure service vprn l2tp df-bit-lac

Description By default, the LAC df-bit-lac is always set and sends all L2TP packets with the DF bit set to 1. The DF bit is configurable to allow downstream routers to fragment the L2TP packets. The LAC itself will not fragment L2TP packets. L2TP packets that have a larger MTU size than what the LAC egress ports allows are dropped.

The **no** form of this command reverts to the default.

Default df-bit-lac always

Parameters **always** — Specifies that the LAC sends all L2TP packets with the DF bit set to 1.

never — Specifies that the LAC sends all L2TP packets with the DF bit set to 0.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

df-bit-lac

Syntax **df-bit-lac** {**always** | **never** | **default**}
no df-bit-lac

Context **[Tree]** (config>router>l2tp>group df-bit-lac)
[Tree] (config>router>l2tp>group>tunnel df-bit-lac)
[Tree] (config>service>vprn>l2tp>group df-bit-lac)
[Tree] (config>service>vprn>l2tp>group>tunnel df-bit-lac)

Full Context configure router l2tp group df-bit-lac
configure router l2tp group tunnel df-bit-lac
configure service vprn l2tp group df-bit-lac
configure service vprn l2tp group tunnel df-bit-lac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description By default, the LAC df-bit-lac is set to default and sends all L2TP packets with the DF bit set to 1. The DF bit is configurable to allow downstream routers to fragment the L2TP packets. The LAC will not fragment L2TP packets. L2TP packets that have a larger MTU size than what the LAC egress ports allows are dropped. The configuration of the df-bit can be overridden at different levels: l2tp, tunnel, and group. The configuration at the tunnel level overrides the configuration on both the group and l2tp levels. The configuration at the group level overrides the configuration on l2tp.

The **no** form of this command reverts to the default.

Default df-bit-lac default

Parameters **always** — Specifies that the LAC sends all L2TP packets with the DF bit set to 1.

never — Specifies that the LAC sends all L2TP packets with the DF bit set to 0.

default — Follows the DF-bit configuration specified on upper levels.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.148 dh-group

dh-group

Syntax **dh-group** {**1** | **2** | **5** | **14** | **15** | **19** | **20** | **21**}

Context **[Tree]** (config>ipsec>ike-transform dh-group)

Full Context configure ipsec ike-transform dh-group

Description This command specifies the Diffie-Hellman group to be used in this IKE transform instance.

Default dh-group 2 (1024-bit — More Modular Exponential (MODP))

Parameters **dh-group {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21}** — Specifies which Diffie-Hellman group to use for calculating session keys. More bits provide a higher level of security, but require more processing. Three groups are supported with IKE-v1:

Group 1: 768 bits
Group 2: 1024 bits
Group 5: 1536 bits
Group 14: 2048 bits
Group 15: 3072 bits
Group 19: P-256 ECC Curve, 256 bits
Group 20: P-384 ECC Curve, 384 bits
Group 21: P-512 ECC Curve, 512 bits

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.149 dhcp

dhcp

Syntax **dhcp**

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only-sap-parameters dhcp)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp

Description Commands in this context configure DHCP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp

Syntax **dhcp**

Context **[Tree]** (config>service>ies>if dhcp)
[Tree] (config>service>ies>sub-if dhcp)
[Tree] (config>service>ies>sub-if>grp-if dhcp)
[Tree] (config>service>vpls>sap dhcp)
[Tree] (config>service>vpls>spoke-sdp dhcp)
[Tree] (config>service>vpls>mesh-sdp dhcp)
[Tree] (config>service>vprn dhcp)
[Tree] (config>service>vprn>if dhcp)
[Tree] (config>service>vprn>sub-if dhcp)
[Tree] (config>service>vprn>sub-if>grp-if dhcp)

Full Context configure service ies interface dhcp
configure service ies subscriber-interface dhcp
configure service ies subscriber-interface group-interface dhcp
configure service vpls mesh-sdp dhcp
configure service vpls sap dhcp
configure service vpls spoke-sdp dhcp
configure service vprn dhcp
configure service vprn interface dhcp
configure service vprn subscriber-interface dhcp
configure service vprn subscriber-interface group-interface dhcp

Description Commands in this context configure DHCP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn dhcp
- configure service vprn subscriber-interface group-interface dhcp
- configure service ies subscriber-interface group-interface dhcp
- configure service vprn subscriber-interface dhcp
- configure service ies subscriber-interface dhcp

All

- configure service ies interface dhcp
- configure service vpls mesh-sdp dhcp
- configure service vprn interface dhcp
- configure service vpls spoke-sdp dhcp
- configure service vpls sap dhcp

dhcp

Syntax [**no**] **dhcp** [**interface** *ip-int-name*]
[**no**] **dhcp mac** *ieee-address*
[**no**] **dhcp sap** *sap-id*

Context **[Tree]** (debug>router>ip dhcp)

Full Context debug router ip dhcp

Description This command enables DHCP debugging.

The **no** form of this command disables debugging.

Parameters *ip-int-name* — Specifies the name of the IP interface, up to 32 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

ieee-address — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

sap-id — Specifies the physical port identifier portion of the SAP definition.

Platforms All

dhcp

Syntax **dhcp** *type* **direction** {**ingress** | **egress**} **script** *script*
no dhcp *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy dhcp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure python python-policy dhcp

Description This command specifies the Python script for the specified DHCPv4 packet type in the specified direction.

Multiple **dhcp** command configurations are allowed in the same Python policy.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type of the event.

Values discover, offer, request, decline, ack, nak, release, inform, force-renew, lease-query, lease-unassigned, lease-unknown, lease-active

direction {**ingress** | **egress**} — Specifies whether the packet is being received by the system or being sent by the system.

script *script* — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

dhcp

Syntax **dhcp**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges dhcp)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges dhcp)

Full Context configure service ies subscriber-interface group-interface wlan-gw ranges dhcp
configure service vprn subscriber-interface group-interface wlan-gw ranges dhcp

Description Commands in this context create DHCP configuration for WLAN-GW ISA subscribers (such as migrant subscribers).

dhcp

Syntax [**no**] **dhcp**

Context **[Tree]** (debug>service>id dhcp)

Full Context debug service id dhcp

Description Commands in this context perform DHCP debugging.

The **no** form of the command disables DHCP debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dhcp

Syntax **dhcp**

Context **[Tree]** (config>app-assure>group>transit-ip-policy dhcp)

Full Context configure application-assurance group transit-ip-policy dhcp

Description This command enables dynamic DHCP-based management of transit aa-subs for the transit-ip-policy. This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dhcp

Syntax [**no**] **dhcp**

Context **[Tree]** (config>service>ies>if>sap>ipsec-gateway dhcp)
[Tree] (config>service>vprn>if>sap>ipsec-gateway dhcp)

Full Context configure service ies interface sap ipsec-gateway dhcp
configure service vprn interface sap ipsec-gateway dhcp

Description Commands in this context configure DHCPv4-based address assignment for IKEv2 remote-access tunnels.

The system acts as a DHCPv4 client on behalf of the IPsec client, and also a relay agent to relay DHCPv4 packets to the DHCPv4 server.

DHCPv4 DORA(Discovery/Offer/Request/Ack) exchange happens during IKEv2 remote-access tunnel setup. The system also supports standard renew.

In order to use this feature, the **relay-proxy** must be enabled on the corresponding interface (either the private interface or the interface that has the gi-address as the interface address).

Default no dhcp

dhcp

Syntax **dhcp**

Context **[Tree]** (config>router>if dhcp)

Full Context configure router interface dhcp

Description Commands in this context configure DHCP parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dhcp

Syntax **dhcp** [**include-user-class**] [**timeout** *timeout*]
dhcp client-id [**string** *ascii-string*] [**hex** *hex-string*] [**include-user-class**] [**timeout** *timeout*]
no dhcp

Context **[Tree]** (bof>autoconfigure>ipv4 dhcp)

Full Context bof autoconfigure ipv4 dhcp

Description This command configures the IPv4 DHCP client for OOB management. The OOB management IPv4 can be set using a DHCP server offer.

The **no** form of this command disables IPv4 DHCP OOB management.

Default no dhcp

Parameters **include-user-class** — Specifies to include Option 77 user class data in the offer.

client-id — Specifies to include the client ID for IPv4 Option 61 for auto-discovery. The identifier is opaque and is in string format. By default, this is the chassis serial number.

timeout — Specifies the DHCP offer timeout, in seconds.

Values 1 to 65535

Default 30

ascii-string — Specifies the string format for this option, up to 127 characters.

hex-string — Specifies the hexadecimal format for this option, up to 254 hex nibbles.

Values 0x0 to 0xFFFFFFFF

Platforms 7450 ESS-7, 7750 SR-1, 7750 SR-1e, 7750 SR-7, 7750 SR-s

dhcp

Syntax **dhcp** [**include-user-class**] [**timeout** *timeout*]
dhcp client-id *duid-type* [**string** *ascii-string*] [**hex** *hex-string*] [**include-user-class**] [**timeout** *timeout*]
no dhcp

Context **[Tree]** (bof>autoconfigure>ipv6 dhcp)

Full Context bof autoconfigure ipv6 dhcp

Description This command configures the IPv6 DHCP client for out-of-band (OOB) management. The OOB management IPv6 can be set using a DHCP server offer.

The **no** form of this command disables IPv6 DHCP client OOB management.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no dhcp

Parameters **include-user-class** — Specifies to include Option 15 user class data in the offer.

client-id — Specifies to include the client ID for IPv6 DHCP Option 1 for auto-discovery. The identifier is opaque and is in string format. By default, this is the chassis serial number.

seconds — Specifies the DHCP client ID timeout, in seconds.

Values 1 to 65535

duid-type — Specifies the type code of the server DUID.

Values duid-link-local, duid-enterprise

ascii-string — Specifies the string format for this option, up to 124 characters.

hex-string — Specifies the hexadecimal format for this option, up to 248 hex nibbles.

Values 0x0 to 0xFFFFFFFF

timeout — Specifies the DHCP offer timeout, in seconds.

Values 1 to 65535

Default 30

Platforms 7450 ESS-7, 7750 SR-1, 7750 SR-1e, 7750 SR-7, 7750 SR-s

dhcp

Syntax [**no**] **dhcp**

Context **[Tree]** (config>sys>security>cpu-protection>ip>included-protocols dhcp)

Full Context configure system security cpu-protection ip-src-monitoring included-protocols dhcp

Description This command includes the extracted IPv4 DHCP packets for ip-src-monitoring. IPv4 DHCP packets will be subject to the per-source-rate of CPU protection policies.

Default dhcp (Note this is different from the other protocols)

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

8.150 dhcp-client

dhcp-client

Syntax [**no**] **dhcp-client**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>router>l2tp>assignment-id>packet dhcp-client)
[Tree] (debug>router>l2tp>group>packet dhcp-client)
[Tree] (debug>router>l2tp>packet dhcp-client)
[Tree] (debug>router>l2tp>peer>packet dhcp-client)

Full Context debug router l2tp assignment-id packet dhcp-client
debug router l2tp group packet dhcp-client
debug router l2tp packet dhcp-client
debug router l2tp peer packet dhcp-client

Description This command enables debugging for DHCP client packet.

The **no** form of this command disables debugging for DHCP client packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp-client

Syntax **dhcp-client** [**terminate-only**]
no dhcp-client

Context [Tree] (debug>service>id>ppp>event dhcp-client)

Full Context debug service id ppp event dhcp-client

Description This command enable PPP event debug for DHCP client.

The **no** form of this command disables PPP event debugging for the DHCP client.

Parameters **terminate-only** — Enables debug for local terminated PPP session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp-client

Syntax [**no**] **dhcp-client**

Context [Tree] (debug>service>id>ppp>packet dhcp-client)

Full Context debug service id ppp packet dhcp-client

Description This command enables debugging for specific DHCP client packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp-client

Syntax **dhcp-client**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>pppoe dhcp-client)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe dhcp-client)

Full Context configure service ies subscriber-interface group-interface pppoe dhcp-client
configure service vprn subscriber-interface group-interface pppoe dhcp-client

Description Commands in this context configure the PPPoE-to-DHCP options.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.151 dhcp-filter

dhcp-filter

Syntax **dhcp-filter** *filter-id* [**create**]
no dhcp-filter

Context [Tree] (config>filter dhcp-filter)

Full Context configure filter dhcp-filter

Description Commands in this context create and configure the specified DHCP filter policy.

Parameters *filter-id* — Specifies the DHCP filter policy ID expressed as a decimal integer.

Values 1 to 65535

create — Keyword required to create the configuration context.

Platforms All

8.152 dhcp-leasetime-threshold

dhcp-leasetime-threshold

Syntax **dhcp-leasetime-threshold** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no dhcp-leasetime-threshold

Context [Tree] (config>system>persistence>options dhcp-leasetime-threshold)

Full Context configure system persistence options dhcp-leasetime-threshold

Description This command configures Dynamic Data Persistence (DDP) compact flash access optimization for DHCP leases.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The DHCP lease-time threshold controls the eligibility of a DHCP lease for persistency updates when no data other than the lease expiry time is to be updated. When the offered lease time of the DHCP lease is less than the configured threshold, the lease is flagged to skip persistency updates and will be installed with its full lease time upon a persistency recovery after a reboot.

The **dhcp-leasetime-threshold** command controls persistency updates for DHCPv4 and DHCPv6 leases for a DHCP relay or proxy and DHCPv4 leases for DHCP snooping (enabled with **subscriber-mgmt**) and a DHCP server (enabled with **dhcp-server**).

The **no** form of the command disables the DHCP lease time threshold.

Default no dhcp-leasetime-threshold

Parameters *days* — Specifies the threshold in days.

Values 0 to 7305

hours — Specifies the threshold in hours.

Values 0 to 23

minutes — Specifies the threshold in minutes.

Values 0 to 59

seconds — Specifies the threshold in seconds.

Values 0 to 59

Platforms All

dhcp-leasetime-threshold

Syntax **dhcp-leasetime-threshold** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no dhcp-leasetime-threshold

Context **[Tree]** (config>redundancy>multi-chassis>options>sub-mgmt dhcp-leasetime-threshold)

Full Context configure redundancy multi-chassis options sub-mgmt dhcp-leasetime-threshold

Description This command configures the DHCP lease time threshold to be eligible for MCS synchronization.

DHCP leases for the **sub-mgmt** MCS applications are eligible to skip synchronization if the committed lease time is less than the active threshold on a multi-chassis peer. The active threshold is the minimum value of the thresholds configured on the nodes at each end of a multi-chassis peer. The threshold is inactive when it is unconfigured on at least one end of the multi-chassis peer.

The **no** form of the command disables the DHCP lease time threshold.

Default no dhcp-leasetime-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

No threshold is active and all **sub-mgmt** DHCP leases are synchronized.

Parameters *days* — Specifies the threshold in days.

Values 0 to 1

hours — Specifies the threshold in hours.

Values 0 to 23

minutes — Specifies the threshold in minutes.

Values 0 to 59

seconds — Specifies the threshold in seconds.

Values 0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.153 dhcp-options

dhcp-options

Syntax [**no**] **dhcp-options**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute dhcp-options)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute dhcp-options

Description This command enables insertion of RADIUS VSA containing all DHCP options from DHCP discover (or DHCP request) message. The VSA contains all DHCP options in a form of the string. If required (the total length of all DHCP options exceeds 255B), multiple VSAs are included.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp-options

Syntax [**no**] **dhcp-options**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes dhcp-options)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes dhcp-options)

Full Context configure aaa isa-radius-policy acct-include-attributes dhcp-options
configure aaa isa-radius-policy auth-include-attributes dhcp-options

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables insertion of RADIUS VSA containing all dhcp-options from dhcp-discover (or dhcp-request) message. The VSA contains all dhcp-options in a form of the string. If required (the total length of all dhcp-options exceeds 255B), multiple VSAs are included.

Default no dhcp-options

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.154 dhcp-pool

dhcp-pool

Syntax **dhcp-pool**

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile dhcp-pool)

Full Context configure subscriber-mgmt vrgw brg brg-profile dhcp-pool

Description Commands in this context configure per-subscriber IPv4 address pool parameters to be used for address allocation. Pools for different subscribers can overlap. Specific pool parameters can be overridden by RADIUS.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.155 dhcp-python-policy

dhcp-python-policy

Syntax **dhcp-python-policy** *policy-name*
no dhcp-python-policy

Context **[Tree]** (config>service>vpls>sap dhcp-python-policy)

Full Context configure service vpls sap dhcp-python-policy

Description This command specifies the name of the Python policy. The Python policy is created in the **config>python>python-policy** *name* context.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies a Python policy name, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.156 dhcp-server

dhcp-server

Syntax **dhcp-server**

Context **[Tree]** (config>system>persistence dhcp-server)

Full Context configure system persistence dhcp-server

Description This command configures DHCP server persistence parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.157 dhcp-triggered

dhcp-triggered

Syntax [**no**] **dhcp-triggered**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state dhcp-triggered)

Full Context configure subscriber-mgmt wlan-gw ue-query state dhcp-triggered

Description This command enables matching on UEs currently in a DHCP-triggered state. This query only filters UEs that are currently authenticating due to a DHCP, DHCPv6, or RS trigger, not RADIUS-authenticated UEs in an ESM, DSM, or portal state that were originally authenticated due to a DHCP, DHCPv6, or RS trigger.

The **no** form of this command disables matching on UEs in a DHCP-triggered state, unless all state matching is disabled.

Default no dhcp-triggered

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.158 dhcp-user-db

dhcp-user-db

Syntax **dhcp-user-db** *local-user-db-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no dhcp-user-db

Context **[Tree]** (config>service>vpls>sap dhcp-user-db)

Full Context configure service vpls sap dhcp-user-db

Description This command enabled access to LUDB for DHCPv4 hosts under the capture SAP. The name of this local user database must match the name of local user database configured under the **config>service>vprn/ies>sub-if>group-if>dhcp** context.

Parameters *local-user-db* — Specifies the name of the local user database name up to 32 characters.

Platforms All

8.159 dhcp-vendor-class-id

dhcp-vendor-class-id

Syntax [**no**] **dhcp-vendor-class-id**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute dhcp-vendor-class-id)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute dhcp-vendor-class-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute dhcp-vendor-class-id
configure subscriber-mgmt authentication-policy include-radius-attribute dhcp-vendor-class-id

Description This command includes the [26-6527-36] Alc-DHCP-Vendor-Class-Id attribute in authentication or RADIUS accounting messages. The content of the DHCP Vendor-Class-Identifier option (60) is mapped in this attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp-vendor-class-id

Syntax [**no**] **dhcp-vendor-class-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes dhcp-vendor-class-id)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes dhcp-vendor-class-id)

Full Context configure aaa isa-radius-policy acct-include-attributes dhcp-vendor-class-id
configure aaa isa-radius-policy auth-include-attributes dhcp-vendor-class-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command includes the "[26-6527-36] Alc-DHCP-Vendor-Class-Id" attribute in authentication or RADIUS accounting messages. The content of the DHCP Vendor-Class-Identifier option (60) is mapped in this attribute.

Default no dhcp-vendor-class-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.160 dhcp6

dhcp6

Syntax **dhcp6**

Context **[Tree]** (config>service>vpls>spoke-sdp dhcp6)
[Tree] (config>service>vpls>mesh-sdp dhcp6)
[Tree] (config>service>vpls>sap dhcp6)
[Tree] (config>service>ies>if dhcp6)
[Tree] (config>service>vprn dhcp6)
[Tree] (config>service>vprn>interface dhcp6)
[Tree] (config>service>vprn>sub-if dhcp6)
[Tree] (config>service>vprn>sub-if>grp-if dhcp6)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 dhcp6)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 dhcp6)
[Tree] (config>service>ies>sub-if dhcp6)
[Tree] (config>service>ies>sub-if>grp-if dhcp6)

Full Context configure service ies interface dhcp6
configure service ies subscriber-interface dhcp6
configure service ies subscriber-interface group-interface dhcp6
configure service ies subscriber-interface group-interface ipv6 dhcp6
configure service vpls mesh-sdp dhcp6
configure service vpls sap dhcp6
configure service vpls spoke-sdp dhcp6
configure service vprn dhcp6
configure service vprn interface dhcp6
configure service vprn subscriber-interface dhcp6
configure service vprn subscriber-interface group-interface dhcp6
configure service vprn subscriber-interface group-interface ipv6 dhcp6

Description Commands in this context configure DHCPv6 parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dhcp6

Syntax **dhcp6**

Context **[Tree]** (config>system dhcp6)

Full Context configure system dhcp6

Description Commands in this context configure system-wide DHCPv6 parameters.

Platforms All

dhcp6

Syntax [**no**] **dhcp6** [*ip-int-name*]
[**no**] **dhcp6 client-identifier duid** *duid-hex-string* [**mask** *mask-hex-string*]
[**no**] **dhcp6 client-identifier link-layer-address** *lla-hex-string*
[**no**] **dhcp6 interface** *ip-int-name*
[**no**] **dhcp6 sap** *sap-id*

Context **[Tree]** (debug>router>ip dhcp6)

Full Context debug router ip dhcp6

Description This command enables DHCPv6 debugging with optional interface, SAP, and client-identifier match criteria to filter the debug output.

The **no** form of this command disables debugging.

Parameters *ip-int-name* — Specifies the name of an existing IP interface, up to 32 characters. Up to four DHCPv6 interface match criteria can be specified per routing instance.

client-identifier — Specifies a client identifier option match criteria.

duid *duid-hex-string* — Specifies a hexadecimal value for an opaque match on the client DUID in the client identifier option. When the actual length of the client DUID is longer than the length of the specified hex-string, only the left most octets are matched. Up to four DHCPv6 client-identifier match criteria can be specified per routing instance.

Values 0x0 to 0xFFFFFFFF (maximum 260 hex nibbles)

mask *mask-hex-string* — Specifies an optional substring match criteria. When a mask is specified, both hex-string lengths must be equal.

Values 0x0 to 0xFFFFFFFF (maximum 260 hex nibbles)

link-layer-address *lla-hex-string* — Specifies a hexadecimal value for a link layer address field match of a type 1 (DUID-LLT) or type 3 (DUID-LL) client DUID in the client identifier option. When the actual length of the link layer address field is longer than the length of the specified hex-string, only the left most octets are matched. Up to four DHCPv6 client-identifier match criteria can be specified per routing instance.

Values 0x0 to 0xFFFFFFFF (maximum 252 hex nibbles)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap-id — Specifies an existing SAP identifier. Up to four DHCPv6 SAP match criteria can be specified per routing instance.

Platforms All

dhcp6

Syntax **dhcp6** *type* **direction** {**ingress** | **egress**} **script** *script*
no dhcp6 *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy dhcp6)

Full Context configure python python-policy dhcp6

Description This command specifies the Python script for the specified DHCPv6 packet type in the specified direction.

Multiple **dhcps** command configurations are allowed in the same Python policy.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type of the event.

Values solicit, advertise, request, confirm, renew, rebind, reply, release, decline, reconfigure, info-request, relay-forward, relay-reply

direction {**ingress** | **egress**} — Specifies whether the event is incoming or outgoing.

script — Specifies the name of the Python script, up to 32 characters, that will be used to handle the specified message.

Platforms All

dhcp6

Syntax **dhcp6**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges dhcp6)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges dhcp6)

Full Context configure service ies subscriber-interface group-interface wlan-gw ranges dhcp6
configure service vprn subscriber-interface group-interface wlan-gw ranges dhcp6

Description Commands in this context create DHCPv6 configuration for WLAN-GW ISA subscribers.

dhcp6

Syntax [**no**] **dhcp6**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>ipsec-gateway dhcp6)
[Tree] (config>service>vprn>if>sap>ipsec-gateway dhcp6)

Full Context configure service ies interface sap ipsec-gateway dhcp6
configure service vprn interface sap ipsec-gateway dhcp6

Description Commands in this context configure DHCPv6-based address assignment for IKEv2 remote-access tunnels.

The system acts as a DHCPv6 client on behalf of the IPsec client, and also acts as a relay agent to relay DHCPv6 packets to the DHCPv6 server.

DHCPv6 exchange happens during IKEv2 remote-access tunnel setup. The system also supports standard renew.

Default no dhcp6

8.161 dhcp6-address

dhcp6-address

Syntax **dhcp6-address** *ipv6-address*
no dhcp6-address

Context [Tree] (config>subscr-mgmt>wlan-gw>ue-query dhcp6-address)

Full Context configure subscriber-mgmt wlan-gw ue-query dhcp6-address

Description This command enables matching on UEs with the specified DHCPv6 IA-NA address.

The **no** form of this command disables matching on the IA-NA address.

Default no dhcp6-address

Parameters *ipv6-address* — Specifies the IA-NA address.

Values	
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.162 dhcp6-filter

dhcp6-filter

Syntax **dhcp6-filter** *filter-id* [**create**]
no dhcp6-filter

Context **[Tree]** (config>filter dhcp6-filter)

Full Context configure filter dhcp6-filter

Description Commands in this context create and configure the specified DHCPv6 filter policy.

The **no** form of this command reverts to the default.

Parameters *filter-id* — Specifies the DHCPv6 filter policy ID expressed as a decimal integer.

Values 1 to 65535

create — Keyword required to create the configuration context.

Platforms All

8.163 dhcp6-options

dhcp6-options

Syntax [**no**] **dhcp6-options**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include dhcp6-options)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute dhcp6-options

Description This command copies DHCPv6 options from received DHCPv6 messages on ingress access and pass them to the RADIUS server in Accept-Request. The messages is carried in the RADIUS VSA Alc-ToServer-Dhcp6-Options.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dhcp6-options

Syntax [**no**] **dhcp6-options**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes dhcp6-options)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa isa-radius-policy acct-include-attributes dhcp6-options

Description If a DHCPv6 stack is active for a UE, this attribute defines if options received in the last DHCPv6 message should be reflected.

Default no dhcp6-options

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dhcp6-options

Syntax [**no**] **dhcp6-options**

Context **[Tree]** (config>aaa>isa-radius-plcy>auth-include-attributes dhcp6-options)

Full Context configure aaa isa-radius-policy auth-include-attributes dhcp6-options

Description If authentication was triggered by DHCPv6, this knob defines if options received in that DHCPv6 message should be reflected in the radius Access-Request.

Default no dhcp6-options

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.164 dhcp6-python-policy

dhcp6-python-policy

Syntax **dhcp6-python-policy** *policy-name*
no dhcp6-python-policy

Context **[Tree]** (config>service>vpls>sap dhcp6-python-policy)

Full Context configure service vpls sap dhcp6-python-policy

Description This command specified the Python policy for DHCPv6 packets sent/received on the capture SAP.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy name* — Specifies an existing Python policy name, up to 256 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.165 dhcp6-relay

dhcp6-relay

Syntax [**no**] **dhcp6-relay**

Context **[Tree]** (config>service>ies>if>ipv6 dhcp6-relay)
[Tree] (config>service>vprn>if>ipv6 dhcp6-relay)

Full Context configure service ies interface ipv6 dhcp6-relay
configure service vprn interface ipv6 dhcp6-relay

Description Commands in this context configure DHCPv6 relay parameters for the interface.

The **no** form of this command disables DHCPv6 relay.

Platforms All

8.166 dhcp6-server

dhcp6-server

Syntax [**no**] **dhcp6-server**

Context **[Tree]** (config>service>ies>if>ipv6 dhcp6-server)
[Tree] (config>service>vprn>if>ipv6 dhcp6-server)

Full Context configure service ies interface ipv6 dhcp6-server
configure service vprn interface ipv6 dhcp6-server

Description Commands in this context configure DHCPv6 server parameters for the interface.

The **no** form of this command disables the DHCP6 server.

Platforms All

8.167 dhcp6-user-db

dhcp6-user-db

Syntax **dhcp6-user-db** *local-user-db*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no dhcp6-user-db

Context **[Tree]** (config>service>vpls>sap dhcp6-user-db)

Full Context configure service vpls sap dhcp6-user-db

Description This command enabled access to LUDB for DHCPv6 hosts under the capture SAP. The name of this LUDB must match the name of the LUDB configured under the **config>service>vprn/ies>sub-if>grp-if>dhcp** hierarchy.

The **no** form of this command reverts to the default.

Parameters *local-user-db* — Specifies the name of the local-user-database, up to 32 characters.

Platforms All

8.168 dhcpv4-nat

dhcpv4-nat

Syntax **dhcpv4-nat**

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client dhcpv4-nat)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client dhcpv4-nat)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client dhcpv4-nat
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client dhcpv4-nat

Description This node enables address pools for DHCPv4 NAT inside addresses. This configuration is only available in wholesale interfaces.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.169 dhcpv6-client

dhcpv6-client

Syntax **dhcpv6-client**

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>pool-manager dhcpv6-client)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager dhcpv6-client)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the DHCPv6 client for the pool manager.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.170 diameter

diameter

Syntax **diameter** *type* **direction** {**ingress** | **egress**} **script** *script*
no diameter *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy diameter)

Full Context configure python python-policy diameter

Description This command specifies the Python script to use for the specified Diameter message type in the specified direction.

Multiple diameter command configurations are allowed in the same Python policy.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type.

Message type	Application	Direction
aaa – AA Answer	Nasreq	ingress
aar – AA Request	Nasreq	egress
asa – Abort Session Answer	Gx, Gy	egress
asr – Abort Session Request	Gx, Gy	ingress
cca – Credit Control Answer	Gx, Gy	ingress
ccr – Credit Control Request	Gx, Gy	egress
cea – Capabilities Exchange Answer	Base	ingress
cer – Capabilities Exchange Request	Base	egress
dpa – Disconnect Peer Answer	Base	ingress/egress
dpr – Disconnect Peer Request	Base	ingress/egress
dwa – Device Watchdog Answer	Base	ingress/egress
dwr – Device Watchdog Request	Base	ingress/egress
raa – Re-Authentication Answer	Gx, Gy	egress
rar – Re-Authentication Request	Gx, Gy	ingress

direction {**ingress** | **egress**} — Specifies if the message is incoming or outgoing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

script — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

diameter

Syntax **diameter**

Context **[Tree]** (config>aaa diameter)

Full Context configure aaa diameter

Description Commands in this context configure Diameter parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter

Syntax [**no**] **diameter**

Context **[Tree]** (debug diameter)

Full Context debug diameter

Description This command enables debugging for diameter.

The **no** form of this command disables debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter

Syntax **diameter**

Context **[Tree]** (config>app-assure>group>transit-ip diameter)

Full Context configure application-assurance group transit-ip-policy diameter

Description Commands in this context configure dynamic Diameter-based management of transit AA subs for the transit IP policy. This is mutually exclusive to other types of management of transit subs for a given transit IP policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.171 diameter-application-policy

diameter-application-policy

Syntax **diameter-application-policy** *policy-name*
no diameter-application-policy

Context **[Tree]** (config>service>vpls>sap diameter-application-policy)
[Tree] (config>service>ies>sub-if>grp-if diameter-application-policy)
[Tree] (config>service>vprn>sub-if>grp-if diameter-application-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host diameter-application-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host diameter-application-policy)

Full Context configure service ies subscriber-interface group-interface diameter-application-policy
configure service vpls sap diameter-application-policy
configure service vprn subscriber-interface group-interface diameter-application-policy
configure subscriber-mgmt local-user-db ipoe host diameter-application-policy
configure subscriber-mgmt local-user-db ppp host diameter-application-policy

Description This command applies the **diameter-application-policy** to the processing of the host attachment requests.

The **no** form of this command reverts to the default value.

Parameters *policy-name* — Specifies the name of the diameter policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter-application-policy

Syntax **diameter-application-policy** *application-policy-name* [**create**]
no diameter-application-policy *application-policy-name*

Context **[Tree]** (config>subscr-mgmt diameter-application-policy)

Full Context configure subscriber-mgmt diameter-application-policy

Description Commands in this context create and configure diameter application policy.

The **no** form of this command reverts to the default.

Parameters *application-policy-name* — Specifies the name of the diameter policy, up to 32 characters.

create — Specifies the keyword used to create a diameter application policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.172 diameter-auth-policy

diameter-auth-policy

Syntax **diameter-auth-policy** *name*
no diameter-auth-policy

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host diameter-auth-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host diameter-auth-policy)

Full Context configure subscriber-mgmt local-user-db ipoe host diameter-auth-policy
configure subscriber-mgmt local-user-db ppp host diameter-auth-policy

Description This command is used to configure the Diameter NASREQ application policy to use for authentication.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies the name of the Diameter NASREQ application policy, up to 32 characters, to use for authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter-auth-policy

Syntax **diameter-auth-policy** *diameter-authentication-policy-name*
no diameter-auth-policy

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn diameter-auth-policy)

Full Context configure subscriber-mgmt gtp apn-policy apn diameter-auth-policy

Description This command configures the Diameter authentication policy with which the GTP connection is authenticated.

The **no** form of this command removes the authentication policy. Only new session setups are affected.

Default no diameter-auth-policy

Parameters *diameter-authentication-policy-name* — Specifies the name of the authentication policy to be used, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

diameter-auth-policy

Syntax **diameter-auth-policy** *name*
no diameter-auth-policy

Context **[Tree]** (config>service>vpls>sap diameter-auth-policy)

Full Context configure service vpls sap diameter-auth-policy

Description This command is used to configure the Diameter NASREQ application policy to use for authentication.

The **no** form of this command reverts to the default value.

Parameters *name* — Specifies the name of the Diameter NASREQ application policy, up to 32 characters, to use for authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter-auth-policy

Syntax **diameter-auth-policy** *name*
no diameter-auth-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if diameter-auth-policy)
[Tree] (config>service>vprn>sub-if>grp-if diameter-auth-policy)

Full Context configure service ies subscriber-interface group-interface diameter-auth-policy
configure service vprn subscriber-interface group-interface diameter-auth-policy

Description This command is used to configure the Diameter NASREQ application policy to use for authentication.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies the name of the Diameter NASREQ application policy, up to 32 characters, to use for authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.173 diameter-node

diameter-node

Syntax **diameter-node** *origin-host-string* **destination-realm** *destination-realm-string*
no diameter-node

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>diam-appl-plcy diameter-node)

Full Context configure subscriber-mgmt diameter-application-policy diameter-node

Description This command configures the Diameter node for this Diameter application policy.

Parameters *origin-host-string* — Specifies the Origin-Host AVP used by this Diameter policy, up to 80 characters.

destination-realm-string — Specifies the Destination-Realm AVP used by this Diameter policy peer, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.174 diameter-peer

diameter-peer

Syntax **diameter-peer** *peer* [*psm-events*]
no diameter-peer

Context [Tree] (debug>diameter diameter-peer)

Full Context debug diameter diameter-peer

Description This command restricts output to a specific peer.

The **no** form of this command disables debugging.

Parameters *peer* — Specifies the peer, up to 32 characters.

psm-events — Specifies to restrict output to the peer's state machine (PSM).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter-peer

Syntax **diameter-peer** *peer* [**psm-events**]
no diameter-peer

Context [Tree] (debug>diam>diam-peer-plcy diameter-peer)

Full Context debug diameter diameter-peer-policy diameter-peer

Description This command restricts the debug output to messages on a specific peer within the diameter peer policy. Overrides the **debug>diam>diam-peer** debug command for the specified diameter peer policy. A single peer can be specified per diameter peer policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When no peer is specified at the diameter peer policy level, the debug output is restricted to the peer configured at the **debug>diam** level.

The **no** form of this command removes the peer from the **debug>diam>diam-peer-plcy** debug output.

Parameters *peer* — Specifies a peer name, up to 32 characters.

psm-events — Specifies to include Peer State Machine (PSM) events in the debug output.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.175 diameter-peer-policy

diameter-peer-policy

Syntax **diameter-peer-policy** *peer-policy-name* [**role** {**client** | **proxy**}] [**create**]
no diameter-peer-policy *peer-policy-name*

Context **[Tree]** (config>aaa diameter-peer-policy)

Full Context configure aaa diameter-peer-policy

Description This command is the foundation of the legacy Diameter base implementation in the SR OS node. It defines a Diameter client node in the SR OS and within, where the peering connections are defined. Various diameter applications (NASREQ, Gx, and Gy) can reference this policy.

This command applies only to the legacy Diameter base.

The **no** form of this command removes the Diameter node origin host string and destination realm from the configuration.

Parameters *peer-policy-name* — Specifies the peer policy name, up to 32 characters.

role client — Specifies that Diameter is configured as a client. The client initiates peering connections towards the server or Diameter proxy. Various applications such as NASREQ, Gx, and Gy are layered directly on top of the Diameter client.

Default role client

role proxy — Specifies that the SR OS node is configured as an intermediary Diameter node in dual-homed topology. In such topology, there are two Diameter proxy nodes placed between dual-homed Diameter clients on one side and Diameter server on the other. Diameter proxy can assume an active or standby state.

create — Keyword used to create the Diameter peer policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter-peer-policy

Syntax **diameter-peer-policy** *referenced-policy-name*
no diameter-peer-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if diameter-peer-policy)

Full Context configure service ies subscriber-interface group-interface diameter-peer-policy

Description This command is used by an application (DCCA, Gx, policy-management application, and so on) to reference a base diameter peer policy that the application will use.

The **no** form of this command reverts to the default.

Parameters *referenced-policy-name* — Specifies the name of the referenced policy.

diameter-peer-policy

Syntax **diameter-peer-policy** *peer-policy-name*
no diameter-peer-policy

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy diameter-peer-policy)

Full Context configure subscriber-mgmt diameter-application-policy diameter-peer-policy

Description The **diameter-peer-policy** command contain a legacy Diameter client node definition in SR OS is referenced by an application (NASREQ, Gx, and Gy). The application will then use this **diameter-peer-policy** to communicate with external Diameter nodes.

This command applies only to legacy implementations of Diameter base and it is mutually exclusive with the **diameter-node** command under the same hierarchy.

The **no** form of this command removes the peer policy name from the configuration.

Parameters *peer-policy-name* — Specifies the peer policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

diameter-peer-policy

Syntax **diameter-peer-policy** *policy*
no diameter-peer-policy *policy*

Context **[Tree]** (debug>diam diameter-peer-policy)

Full Context debug diameter diameter-peer-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command restricts the debug output to messages on peers of a specific diameter peer policy. Up to eight diameter peer policies can be specified.

The **no** form of this command removes the specified diameter peer policy and all debug statement under this policy from the debug configuration.

Parameters *policy* — Specifies the diameter peer policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.176 diameter-proxy

diameter-proxy

Syntax [**no**] **diameter-proxy**

Context **[Tree]** (configure>redundancy>multi-chassis>peer>sync diameter-proxy)

Full Context configure redundancy multi-chassis peer sync diameter-proxy

Description This command enables Diameter redundancy in dual-homed environment. This command is used to synchronize Diameter proxy parameters between two redundant SR OS nodes. The parameters that are synchronized are:

- chassis system MAC
- Diameter proxy states
- Origin-State-Id

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command disables Diameter redundancy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.177 diff

diff

Syntax **diff**

Context **[Tree]** (config>app-assure>group>policy diff)

Full Context configure application-assurance group policy diff

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command compares the newly configured policy against the operational policy.

8.178 diffserv-te

diffserv-te

Syntax **diffserv-te** [**mam** | **rdm**]
no diffserv-te

Context **[Tree]** (config>router>rsvp diffserv-te)

Full Context configure router rsvp diffserv-te

Description This command enabled Diff-Serv TE on the node.

When this command is enabled, IS-IS and OSPF will start advertising available bandwidth for each TE class configured under the diffserv-te node. This command will only have effect if the operator has already enabled TE at the IS-IS and/or OSPF routing protocol levels:

config>router>isis>traffic-engineering

and/or:

config>router>ospf>traffic-engineering

IGP will advertise for each RSVP interface in the system the available bandwidth in each TE class in the unreserved bandwidth TE parameter for that class. In addition, IGP will continue to advertise the existing Maximum Reservable Link Bandwidth TE parameter to mean the maximum bandwidth that can be booked on a given interface by all classes. The value advertised is adjusted with the link **subscription** *percentage* factor configured in the **config>router>rsvp>interface** context.

The user configures the following parameters for the operation of Diff-Serv:

- Definition of TE classes, TE Class = {Class Type (CT), LSP priority}.
- Mapping of the system forwarding classes to the Diff-Serv Class Type (CT).
- Configuration of the percentage of RSVP interface bandwidth each CT shares, that is, the Bandwidth Constraint (BC).

When Diff-Serv TE is enabled, the system will automatically enable the Max Allocation Model (MAM) Admission Control Policy. MAM represents the bandwidth constraint model for the admission control of an LSP reservation to a link. This is the only Admission Control Policy supported in this release.

Each CT shares a percentage of the Maximum Reservable Link Bandwidth through the user-configured Bandwidth Constraint (BC) for this CT. The Maximum Reservable Link Bandwidth is the link bandwidth multiplied by the RSVP interface subscription factor.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The sum of all BC values across all CTs will not exceed the Maximum Reservable Link Bandwidth. In other words, the following rule is enforced:

SUM (BCc) =< Max-Reservable-Bandwidth, 0 <= c <= 7

An LSP of class-type CTc, setup priority p, holding priority h (h=<p), and bandwidth B is admitted into a link if the following condition is satisfied:

B <= Unreserved Bandwidth for TE-Class[i]

where TE-Class [i] maps to < CTc , p > in the definition of the TE classes on the node. The bandwidth reservation is effected at the holding priority, that is, in TE-class [j] = <CTc, h>. Thus, the reserved bandwidth for CTc and the unreserved bandwidth for the TE classes using CTc are updated as follows:

Reserved(CTc) = Reserved(CTc) + B

Unreserved TE-Class [j] = BCc - SUM (Reserved(CTc,q)) for 0<= q <= h

Unreserved TE-Class [i] = BCc - SUM (Reserved(CTc,q)) for 0<= q <= p

The same is done to update the unreserved bandwidth for any other TE class making use of the same CTc. These new values are advertised to the rest of the network at the next IGP-TE flooding.

The Russian Doll Model (RDM) LSP admission control policy allows bandwidth sharing across Class Types. It provides a hierarchical model by which the reserved bandwidth of a CT is the sum of the reserved bandwidths of the numerically equal and higher CTs.

The RDM model is defined using the following equations:

SUM (Reserved (CTc)) <= BCb,

where the SUM is across all values of c in the range b <= c <= (MaxCT - 1), and BCb is the bandwidth constraint of CTb.

BC0= Max-Reservable-Bandwidth, so that

SUM (Reserved(CTc)) <= Max-Reservable-Bandwidth,

where the SUM is across all values of c in the range 0 <= c <= (MaxCT - 1).

When Diff-Serv is disabled on the node, this model degenerates into a single default CT internally with eight preemption priorities and a non-configurable BC equal to the Maximum Reservable Link Bandwidth. This would behave exactly like CT0 with eight preemption priorities and BC= Maximum Reservable Link Bandwidth if Diff-Serv was enabled.

The enabling or disabling of Diff-Serv TE on the system requires the RSVP and MPLS protocol be shutdown.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no diffserv-te

Parameters **mam** — Defines the default admission control policy for Diff-Serv LSPs.

rdm — Defines Russian doll model for the admission control policy of Diff-Serv LSPs.

Platforms All

8.179 digest-type

digest-type

Syntax **digest-type** {**default** | **none** | **md5** | **sha1**}
no digest-type

Context **[Tree]** (config>service>vprn>l2tp>l2tpv3 digest-type)
[Tree] (config>service>vprn>l2tp>group>l2tpv3 digest-type)

Full Context configure service vprn l2tp group l2tpv3 digest-type
configure service vprn l2tp l2tpv3 digest-type

Description This command configures the hashing algorithm used to calculate the message digest.

The **no** form of this command returns the **digest-type** to **none**.

Default no digest-type

Parameters **none** — Specifies that no digest should be used.

md5 — Specifies that the MD5 algorithm should be used.

sha1 — Specifies that the SHA1 algorithm should be used.

default — When specified within the **config>service>vprn>l2tp>group>l2tpv3** context, this is referencing to the **digest-type** configuration within the **config>service>vprn>l2tp>l2tpv3** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.180 digital-coherent-optics

digital-coherent-optics

Syntax [**no**] **digital-coherent-optics**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>transceiver digital-coherent-optics)

Full Context configure port transceiver digital-coherent-optics

Description This command specifies if a digital coherent optics module is used for this port.

The **no** form of this command specifies that the optical module used in this port is not a digital coherent optics module.

Default no digital-coherent-optics

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.181 dir

dir

Syntax **dir** [*file-url*] [**sort-order** {**d** | **n** | **s**}] [**reverse**]

Context [Tree] (file dir)

Full Context file dir

Description This command displays a list of files and subdirectories in a directory.

Parameters *file-url* — Specifies the path or directory name.

Use the *file-url* with the optional wildcard (*) to reduce the number of files to list.

sort-order {d | n | s} — Specifies the sort order.

Values d — date
n — name
s — size

reverse — Reverses the sort order.

Default Lists all files in the current working directory.

local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[*-interface*] *x:x:x:x:x:x:d.d.d.d*[*-interface*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	x - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Output The following output is an example of directory information.

Sample Output

```
A:cses-E12>file cf3:\ # dir
  - dir [<file-url>] [sort-order { d | n | s}] [reverse]

 <file-url>           : <local-url> | <remote-url>
                        local-url      - [<cflash-id>/][<file-path>]
                                         200 chars max, including cflash-id
                                         directory length 99 chars max each
                        remote-url     - [ftp://<login>:<pswd>@<remote-locn>/
                                         ][<file-path>]
                                         255 chars max
                                         directory length 99 chars max each
                        remote-locn    - [ <hostname> | <ipv4-address> |
                                         [<ipv6-address>]]
                        ipv4-address   - a.b.c.d
                        ipv6-address   - x:x:x:x:x:x:x:x[-interface]
                                         x:x:x:x:x:x:d.d.d.d[-interface]
                                         x - [0..FFFF]H
                                         d - [0..255]D
                                         interface - 32 chars max, for link
                                         local addresses
                        cflash-id      - cf1:|cf1-A:|cf1-B:|cf2:|cf2-A:|
                                         cf2-B:|cf3:|cf3-A:|cf3-B:
 < d | n | s>         : Sort order: d - date, n - name, s - size
 <reverse>            : keyword - reverse order
A:cses-E12>file cf3:\ # dir
```

Platforms All

8.182 direction

direction

Syntax **direction** *direction*

Context **[Tree]** (debug>router>l2tp>assignment-id>packet direction)
[Tree] (debug>router>l2tp>group>packet direction)
[Tree] (debug>router>l2tp>packet direction)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (debug>router>l2tp>peer>packet direction)

Full Context debug router l2tp assignment-id packet direction
debug router l2tp group packet direction
debug router l2tp packet direction
debug router l2tp peer packet direction

Description This command enables debugging for packet direction.

Parameters *direction* — Specifies the packet direction.

Values ingress, egress, both

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

direction

Syntax **direction** {**ingress** | **egress** | **both**}

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg>pppoe-client>brg-id direction)

Full Context debug subscriber-mgmt vrgw brg pppoe-client brg-id direction

Description This command specifies if debugging should only include ingress, egress or all messages.

Default direction both

Parameters **ingress** — Specifies that debugging only includes ingress messages.

egress — Specifies that debugging only includes egress messages.

both — Specifies that debugging includes both ingress and egress messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

direction

Syntax **direction** *ipsec-direction*
no direction

Context **[Tree]** (config>ipsec>static-sa direction)

Full Context configure ipsec static-sa direction

Description This command configures the direction for an IPsec manual SA.

The **no** form of this command reverts to the default value.

Default direction bidirectional

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipsec-direction* — Identifies the direction to which this static SA entry can be applied.

Values inbound, outbound, bidirectional

Platforms All

direction

Syntax **direction** *direction*

Context **[Tree]** (debug>router>pcp>pcp-server>packet direction)

Full Context debug router pcp pcp-server packet direction

Description This command enables debugging for packet direction.

Parameters *direction* — Specifies the packet direction.

Values ingress, egress, both

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

direction

Syntax **direction**

Context **[Tree]** (config>system>security>keychain direction)

Full Context configure system security keychain direction

Description This command specifies the data type that indicates the TCP stream direction to apply the keychain.

Platforms All

8.183 direction-bit

direction-bit

Syntax [**no**] **direction-bit**

Context **[Tree]** (config>mirror>mirror-dest>encap>layer-3-encap direction-bit)

Full Context configure mirror mirror-dest encap layer-3-encap direction-bit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to steal one bit from the intercept-id in the LI-Shim and use it to indicate the direction of traffic flow for an LI session. Using a direction bit may be used by a LI Mediation Gateway to distinguish between the two directions of traffic flow for an LI session when both directions share a common mirror-dest, intercept-id and session-id. If the direction bit is enabled then the Mirror Header Version (2 bit mhv) in the LI-Shim will be set to binary 01, and the next bit after the mhv is set to 0 for ingress traffic and 1 for egress traffic.

For NAT based LI, ingress means the traffic is arriving at the node from the subscriber host (applies to the 7450 ESS and 7750 SR).

No changes are allowed to the **direction-bit** configuration once a gateway is configured.

Platforms All

direction-bit

Syntax [**no**] **direction-bit**

Context **[Tree]** (config>li>mirror-dest-template>layer-3-encap direction-bit)

Full Context configure li mirror-dest-template layer-3-encap direction-bit

Description This command enables and disables the use of one bit from the interception ID field in the LI-Shim header to be used to indicate the direction of mirrored traffic flow for an LI session. An LI Mediation Gateway can use a direction bit to distinguish between the two directions of traffic flow for an LI session when both directions share a common mirror destination, interception ID, and session ID. If the direction bit is enabled, the Mirror Header Version (2-bit MHV) in the LI-Shim header will be set to binary 01, and the next bit after the MHV is set to 0 for ingress traffic and 1 for egress traffic.

For NAT-based LI, ingress traffic arrives at the node from the subscriber host. No changes are allowed to the direction bit configuration after a gateway is configured.

The **no** form of this command disables the use of the bit as a direction indicator.

Platforms All

8.184 disable

disable

Syntax [**no**] **disable**

Context **[Tree]** (config>call-trace>location disable)

Full Context configure call-trace location disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When configured, the specified compact flash will not be used by call-trace. The **no** form of this command enables the compact flash for use by call-trace.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.185 disable-4byte-asn

disable-4byte-asn

Syntax [**no**] **disable-4byte-asn**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy disable-4byte-asn)

Full Context configure subscriber-mgmt bgp-peering-policy disable-4byte-asn

Description This command disables the use of 4-byte ASNs. It can be configured at all 3 level of the hierarchy so it can be specified down to the per peer basis.

If this command is enabled 4-byte ASN support should not be negotiated with the associated remote peer.

The **no** form of this command resets the behavior to the default which is to enable the use of 4-byte ASN.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

disable-4byte-asn

Syntax [**no**] **disable-4byte-asn**

Context **[Tree]** (config>service>vprn>bgp disable-4byte-asn)
[Tree] (config>service>vprn>bgp>group disable-4byte-asn)
[Tree] (config>service>vprn>bgp>group>neighbor disable-4byte-asn)

Full Context configure service vprn bgp disable-4byte-asn
configure service vprn bgp group disable-4byte-asn
configure service vprn bgp group neighbor disable-4byte-asn

Description This command disables the use of 4-byte ASNs. It can be configured at all 3 level of the hierarchy so it can be specified down to the per peer basis.

If this command is enabled 4-byte ASN support should not be negotiated with the associated remote peer(s).

The **no** form of this command resets the behavior to the default which is to enable the use of 4-byte ASN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

disable-4byte-asn

Syntax [**no**] **disable-4byte-asn**

Context **[Tree]** (config>router>bgp disable-4byte-asn)
[Tree] (config>router>bgp>group disable-4byte-asn)
[Tree] (config>router>bgp>group>neighbor disable-4byte-asn)

Full Context configure router bgp disable-4byte-asn
configure router bgp group disable-4byte-asn
configure router bgp group neighbor disable-4byte-asn

Description This command disables the support of 4-byte ASNs. It can be configured at all three levels of the hierarchy so it can be specified down to the per-peer basis.

If this command is enabled, 4-byte ASN support should not be negotiated with the associated remote peers.

The **no** form of this command resets the behavior to the default which is to enable the support of 4-byte ASN.

Default no disable-4byte-asn

Platforms All

8.186 disable-aging

disable-aging

Syntax [**no**] **disable-aging**

Context **[Tree]** (config>service>vpls disable-aging)
[Tree] (config>service>vpls>sap disable-aging)
[Tree] (config>service>vpls>spoke-sdp disable-aging)
[Tree] (config>service>template>vpls-template disable-aging)
[Tree] (config>service>vpls>vxlan disable-aging)

Full Context configure service template vpls-template disable-aging
configure service vpls disable-aging
configure service vpls sap disable-aging
configure service vpls spoke-sdp disable-aging
configure service vpls vxlan disable-aging

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command disables MAC address aging across a VPLS service, on a VPLS service SAP or spoke-SDP, or VXLAN instance with static binds. Learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the VPLS forwarding database (FDB).

The **disable-aging** command turns off aging for local and remote learned MAC addresses. When **no disable-aging** is specified for a VPLS, aging can be disabled for specific SAPs, spoke-SDPs, and VXLAN instances (or any combination) by entering the **disable-aging** command at the appropriate level.

When the **disable-aging command** is entered at the VPLS level, the aging state of individual SAPs or SDPs or VXLAN instance is ignored.

The **no** form of this command enables aging on the VPLS service.

Default no disable-aging

Except for VXLAN instances, where the **disable-aging** is the default mode

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls vxlan disable-aging

All

- configure service vpls sap disable-aging
- configure service template vpls-template disable-aging
- configure service vpls disable-aging
- configure service vpls spoke-sdp disable-aging

disable-aging

Syntax [**no**] **disable-aging**

Context **[Tree]** (config>service>pw-template disable-aging)

Full Context configure service pw-template disable-aging

Description This command disables MAC address aging across a service.

The **no** form of this command enables aging.

Default no disable-aging

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.187 disable-capability-negotiation

disable-capability-negotiation

Syntax [**no**] **disable-capability-negotiation**

Context **[Tree]** (config>service>vprn>bgp>group disable-capability-negotiation)
[Tree] (config>service>vprn>bgp>group>neighbor disable-capability-negotiation)

Full Context configure service vprn bgp group disable-capability-negotiation
configure service vprn bgp group neighbor disable-capability-negotiation

Description This command disables the exchange of capabilities. When command is enabled and after the peering is flapped, any new capabilities are not negotiated and strictly supports IPv4 routing exchanges with that peer.

The **no** form of this command removes this command from the configuration and restores the normal behavior.

Default no disable-capability-negotiation

Platforms All

disable-capability-negotiation

Syntax [**no**] **disable-capability-negotiation**

Context **[Tree]** (config>router>bgp>group disable-capability-negotiation)
[Tree] (config>router>bgp>group>neighbor disable-capability-negotiation)

Full Context configure router bgp group disable-capability-negotiation
configure router bgp group neighbor disable-capability-negotiation

Description This command disables capability negotiation. When the command is enabled and after the peering is flapped, any new capabilities are not negotiated and will strictly support IPv4 routing exchanges with that peer.

The **no** form of this command removes this command from the configuration and restores the normal behavior.

Default no disable-capability-negotiation

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.188 disable-client-reflect

disable-client-reflect

Syntax [**no**] **disable-client-reflect**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy disable-client-reflect)

Full Context configure subscriber-mgmt bgp-peering-policy disable-client-reflect

Description This command disables the reflection of routes by the route reflector to the group or neighbor. This only disables the reflection of routes from other client peers. Routes learned from non-client peers are still reflected to all clients.

The **no** form re-enables client reflection of routes to all client peers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

disable-client-reflect

Syntax [**no**] **disable-client-reflect**

Context **[Tree]** (config>service>vprn>bgp disable-client-reflect)
[Tree] (config>service>vprn>bgp>group disable-client-reflect)
[Tree] (config>service>vprn>bgp>group>neighbor disable-client-reflect)

Full Context configure service vprn bgp disable-client-reflect
configure service vprn bgp group disable-client-reflect
configure service vprn bgp group neighbor disable-client-reflect

Description This command disables the reflection of routes by the route reflector to the group or neighbor. This only disables the reflection of routes from other client peers. Routes learned from non-client peers are still reflected to all clients.

The **no** form re-enables client reflection of routes.

Default no disable-client-reflect

Platforms All

disable-client-reflect

Syntax [**no**] **disable-client-reflect**

Context **[Tree]** (config>router>bgp disable-client-reflect)
[Tree] (config>router>bgp>group disable-client-reflect)
[Tree] (config>router>bgp>group>neighbor disable-client-reflect)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bgp disable-client-reflect
configure router bgp group disable-client-reflect
configure router bgp group neighbor disable-client-reflect

Description This command determines whether routes received from neighbors considered to be RR clients are reflected to other clients.

The **no** form enables client reflection of routes.

Default no disable-client-reflect

Platforms All

8.189 disable-communities

disable-communities

Syntax **disable-communities** [**standard**] [**extended**]
no disable-communities

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy disable-communities)

Full Context configure subscriber-mgmt bgp-peering-policy disable-communities

Description This command configures BGP to disable sending communities.

The **no** form of this command reverts to the default.

Parameters **standard** — Specifies standard communities that existed before VPRNs or 2547.

extended — Specifies BGP communities used were expanded after the concept of 2547 was introduced, to include handling the VRF target.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

disable-communities

Syntax **disable-communities** [**standard**] [**extended**] [**large**]
no disable-communities

Context **[Tree]** (config>service>vprn>bgp disable-communities)
[Tree] (config>service>vprn>bgp>group disable-communities)
[Tree] (config>service>vprn>bgp>group>neighbor disable-communities)

Full Context configure service vprn bgp disable-communities
configure service vprn bgp group disable-communities
configure service vprn bgp group neighbor disable-communities

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures BGP to disable sending standard, extended, or large communities to specific peers.

By default, all communities that are attached to a BGP route (any address family) are not stripped from the route when it is advertised to any type of peer: IBGP, EBGP or confed-EBGP.

Default no disable-communities

Parameters **standard** — Specifies that standard 4-byte communities should be removed.

extended — Specifies that 8-byte extended communities (of all types) should be removed.

large — Specifies that 12-byte large communities should be removed.

Platforms All

disable-communities

Syntax **disable-communities** [**standard**] [**extended**] [**large**]
no disable-communities

Context **[Tree]** (config>router>bgp disable-communities)
[Tree] (config>router>bgp>group disable-communities)
[Tree] (config>router>bgp>group>neighbor disable-communities)

Full Context configure router bgp disable-communities
configure router bgp group disable-communities
configure router bgp group neighbor disable-communities

Description This command configures BGP to disable sending standard, extended, or large communities to specific peers.

By default, all communities that are attached to a BGP route (any address family) are not stripped from the route when it is advertised to any type of peer: IBGP, EBGP, or confed-EBGP.

Default no disable-communities

Parameters **standard** — Advertise the Communities attribute to peers.

extended — Advertise the Extended Communities attribute to peers.

large — Advertise the Large Communities attribute to peers.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.190 disable-cookies

disable-cookies

Syntax [**no**] **disable-cookies**

Context **[Tree]** (config>subscr-mgmt>ppp-policy disable-cookies)

Full Context configure subscriber-mgmt ppp-policy disable-cookies

Description This command disables the use of cookies.

The **no** form of this command enables cookies.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.191 disable-explicit-null

disable-explicit-null

Syntax [**no**] **disable-explicit-null**

Context **[Tree]** (config>router>bgp>label-allocation>label-ipv6 disable-explicit-null)

Full Context configure router bgp label-allocation label-ipv6 disable-explicit-null

Description This command controls the allocation and use of explicit null MPLS labels with labeled-unicast ipv6 routes.

When this command is enabled (**no disable-explicit-null**), the following behaviors apply:

- during the times when the router is required to act as the BGP next-hop of a label-unicast IPv6 route that it is advertising, it sets the BGP label value to IPv6 explicit null (value 2), forcing a POP behavior for received packets.
- received label-unicast IPv6 routes never create tunnels in TTM that can be used to resolve other BGP routes (with an IPv6 next-hop).
- a received label-unicast IPv6 route can be resolved by a label-ipv4 BGP tunnel that is transported over a stacked tunnel (SR-TE LSP or LDPoRSVP LSP)

When this command is disabled (**disable-explicit-null**), the following behaviors apply:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- during those times when the router is required to act as the BGP next-hop of a label-unicast IPv6 route that it is advertising, it sets the BGP label value to a proper value in the dynamic label range and programs a POP or SWAP operation for that label, depending on the origin of the route and various import policy actions that could apply to the route
- received label-unicast IPv6 routes that have a prefix length of 128 bits are automatically installed in TTM so that they can be used to resolve other (non-labeled-unicast) BGP routes (with an IPv6 next-hop)
- a received label-unicast ipv6 route cannot be resolved by a label-ipv4 BGP tunnel that is transported over a stacked tunnel (SR-TE LSP or LDPoRSVP LSP)
- the label-ipv6 routes used for ECMP towards an IPv6 destination cannot be a mix of routes with regular label values and routes with special (IPv6 explicit null) label values

Changes in the operational status do not cause the BGP sessions of the base router to reset.

Platforms All

8.192 disable-fast-external-failover

disable-fast-external-failover

Syntax [**no**] **disable-fast-external-failover**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy disable-fast-external-failover)

Full Context configure subscriber-mgmt bgp-peering-policy disable-fast-external-failover

Description This command configures BGP fast external failover.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

disable-fast-external-failover

Syntax [**no**] **disable-fast-external-failover**

Context **[Tree]** (config>service>vprn>bgp disable-fast-external-failover)
[Tree] (config>service>vprn>bgp>group disable-fast-external-failover)
[Tree] (config>service>vprn>bgp>group>neighbor disable-fast-external-failover)

Full Context configure service vprn bgp disable-fast-external-failover
configure service vprn bgp group disable-fast-external-failover
configure service vprn bgp group neighbor disable-fast-external-failover

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures BGP fast external failover.

Platforms All

disable-fast-external-failover

Syntax [**no**] **disable-fast-external-failover**

Context **[Tree]** (config>router>bgp disable-fast-external-failover)
[Tree] (config>router>bgp>group disable-fast-external-failover)
[Tree] (config>router>bgp>group>neighbor disable-fast-external-failover)

Full Context configure router bgp disable-fast-external-failover
configure router bgp group disable-fast-external-failover
configure router bgp group neighbor disable-fast-external-failover

Description This command configures BGP fast external failover.

Default no disable-fast-external-failover

Platforms All

8.193 disable-graceful-shutdown

disable-graceful-shutdown

Syntax [**no**] **disable-graceful-shutdown**

Context **[Tree]** (config>system>login-control>ssh disable-graceful-shutdown)

Full Context configure system login-control ssh disable-graceful-shutdown

Description This command enables graceful shutdown of SSH sessions.

The **no** form of this command disables graceful shutdown of SSH sessions.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.194 disable-ldp-sync

disable-ldp-sync

Syntax [**no**] **disable-ldp-sync**

Context **[Tree]** (config>router>isis disable-ldp-sync)

Full Context configure router isis disable-ldp-sync

Description This command disables the IGP-LDP synchronization feature on all interfaces participating in the OSPF or IS-IS routing protocol. When this command is executed, IGP immediately advertises the actual value of the link cost for all interfaces which have the IGP-LDP synchronization enabled if the currently advertised cost is different. It will then disable IGP-LDP synchronization for all interfaces. This command does not delete the interface configuration. The **no** form of this command has to be entered to re-enable IGP-LDP synchronization for this routing protocol.

The **no** form of this command restores the default settings and re-enables IGP-LDP synchronization on all interfaces participating in the OSPF or IS-IS routing protocol and for which the ldp-sync-timer is configured.

Default no disable-ldp-sync

Platforms All

disable-ldp-sync

Syntax [**no**] **disable-ldp-sync**

Context **[Tree]** (config>router>ospf disable-ldp-sync)
[Tree] (config>router>ospf3 disable-ldp-sync)

Full Context configure router ospf disable-ldp-sync
configure router ospf3 disable-ldp-sync

Description This command disables the IGP-LDP synchronization feature on all interfaces participating in the OSPF routing protocol. When this command is executed, IGP immediately advertises the actual value of the link cost for all interfaces which have the IGP-LDP synchronization enabled if the currently advertised cost is different. It will then disable IGP-LDP synchronization for all interfaces. This command does not delete the interface configuration. The **no** form of this command has to be entered to re-enable IGP-LDP synchronization for this routing protocol.

The **no** form of this command restores the default settings and re-enables IGP-LDP synchronization on all interfaces participating in the OSPF or IS-IS routing protocol and for which the ldp-sync-timer is configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no disable-ldp-sync

Platforms All

8.195 disable-learning

disable-learning

Syntax [**no**] **disable-learning**

Context **[Tree]** (config>service>vpls disable-learning)
[Tree] (config>service>vpls>sap disable-learning)
[Tree] (config>service>vpls>spoke-sdp disable-learning)
[Tree] (config>service>template>vpls-template disable-learning)
[Tree] (config>service>vpls>vxlan disable-learning)

Full Context configure service template vpls-template disable-learning
configure service vpls disable-learning
configure service vpls sap disable-learning
configure service vpls spoke-sdp disable-learning
configure service vpls vxlan disable-learning

Description This command disables learning of new MAC addresses in the VPLS forwarding database (FDB) for the service instance, SAP instance, spoke-SDP instance, or VXLAN instance.

When **disable-learning** is enabled, new source MAC addresses are not entered in the VPLS service forwarding database. This applies for both local and remote MAC addresses.

When **no disable-learning** is specified for a VPLS on a 7450 ESS, it is possible to disable learning for specific SAPs and/or spoke SDPs by entering the **disable-learning command at the appropriate level.**

When **disable-learning** is disabled, new source MAC addresses are learned and entered into the VPLS forwarding database.

This parameter is mainly used in conjunction with the **discard-unknown** command.

The **no** form of this command enables learning of MAC addresses.

Default no disable-learning

Normal MAC learning is enabled. The default mode for VXLAN instances is **disable-learning**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls vxlan disable-learning

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service vpls sap disable-learning
- configure service template vpls-template disable-learning
- configure service vpls disable-learning
- configure service vpls spoke-sdp disable-learning

disable-learning

Syntax [**no**] **disable-learning**

Context **[Tree]** (config>service>pw-template disable-learning)

Full Context configure service pw-template disable-learning

Description This command enables learning of new MAC addresses.

This parameter is mainly used in conjunction with the **discard-unknown** command.

The **no** form of this command enables learning of MAC addresses.

Default no disable-learning (Normal MAC learning is enabled)

Platforms All

8.196 disable-route-table-install

disable-route-table-install

Syntax [**no**] **disable-route-table-install**

Context **[Tree]** (config>router>bgp disable-route-table-install)

Full Context configure router bgp disable-route-table-install

Description This command disables the installation of all IPv4, label-ipv4, IPv6 and label-ipv6 routes into the route table and tunnel table associated with the BGP instance.

Configuring this command prevents the advertisement of all IPv4, label-ipv4, IPv6 and label-ipv6 routes if there is a change of the BGP next-hop to one of the router's own addresses. Typically, this is only useful on a router that is a control-plane route reflector (not in the datapath).

The **no** form of the command enables the installation of all IPv4, label-ipv4, IPv6 and label-ipv6 routes into the route table and tunnel table associated with the BGP instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no disable-route-table-install

Platforms All

disable-route-table-install

Syntax [**no**] **disable-route-table-install**

Context **[Tree]** (config>router>policy-options>policy-statement>default-action disable-route-table-install)
[Tree] (config>router>policy-options>policy-statement>entry>action disable-route-table-install)

Full Context configure router policy-options policy-statement default-action disable-route-table-install
configure router policy-options policy-statement entry action disable-route-table-install

Description This command specifies that BGP routes (IPv4, IPv6, label-ipv4, label-ipv6) matching the policy entry (or, depending on the context, the policy's default-action) should not be installed in the route table, tunnel table (in the case of label-ipv4 routes), or IP FIB table.

This policy action has an effect only in BGP peer import policies. This policy action does not prevent the matched routes from contributing toward aggregate routes and does not prevent the matched routes from being advertised, even if next-hop-self has been applied. This means that incorrect use of this feature can blackhole traffic.

Marking label-ipv4 routes with this action does not prevent label-swap (ILM) entries from being programmed when such routes are re-advertised with a new BGP next-hop and label.

The **no** form of this command provides the default behavior of installing routes that are selected as the best path, ECMP path or backup path, depending on the circumstances.

Default no disable-route-table-install

Platforms All

8.197 disable-router-alert-check

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>router>igmp>group-interface disable-router-alert-check)
[Tree] (config>router>igmp>if disable-router-alert-check)
[Tree] (config>router>mld>group-interface disable-router-alert-check)
[Tree] (config>service>vprn>igmp>group-interface disable-router-alert-check)
[Tree] (config>service>vprn>mld>group-interface disable-router-alert-check)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router igmp group-interface disable-router-alert-check
configure router igmp interface disable-router-alert-check
configure router mld group-interface disable-router-alert-check
configure service vprn igmp group-interface disable-router-alert-check
configure service vprn mld group-interface disable-router-alert-check

Description This command disables router alert checking for IGMP/MLD messages received on this interface.

The **no** form of this command enables router alert checking.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface disable-router-alert-check
- configure service vprn mld group-interface disable-router-alert-check
- configure router mld group-interface disable-router-alert-check
- configure router igmp group-interface disable-router-alert-check

All

- configure router igmp interface disable-router-alert-check

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>router>mld>if disable-router-alert-check)

Full Context configure router mld interface disable-router-alert-check

Description This command enables router alert checking for MLD messages received on this interface.

The **no** form of this command disables router alert checking.

Platforms All

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>subscr-mgmt>igmp-policy disable-router-alert-check)

Full Context configure subscriber-mgmt igmp-policy disable-router-alert-check

Description This command disables router alert checking for IGMP messages received on this interface.

The **no** form of this command reverts to the default value.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-host-tracking disable-router-alert-check)

Full Context configure service vprn subscriber-interface group-interface sap igmp-host-tracking disable-router-alert-check

Description This command disables the IGMP router alert check option.

The **no** form of this command enables the router alert check.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>subscr-mgmt>mld-policy disable-router-alert-check)

Full Context configure subscriber-mgmt mld-policy disable-router-alert-check

Description This command disables router alert checking for MLD messages received on this interface.

The **no** form of this command enables router alert checking.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping disable-router-alert-check)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping disable-router-alert-check)
[Tree] (config>service>vpls>sap>igmp-snooping disable-router-alert-check)
[Tree] (config>service>vpls>sap>igmp-host-tracking disable-router-alert-check)
[Tree] (config>service>vpls>sap>mld-snooping disable-router-alert-check)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping disable-router-alert-check)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping disable-router-alert-check)

Full Context configure service vpls mesh-sdp igmp-snooping disable-router-alert-check
configure service vpls mesh-sdp mld-snooping disable-router-alert-check
configure service vpls sap igmp-host-tracking disable-router-alert-check
configure service vpls sap igmp-snooping disable-router-alert-check
configure service vpls sap mld-snooping disable-router-alert-check
configure service vpls spoke-sdp igmp-snooping disable-router-alert-check
configure service vpls spoke-sdp mld-snooping disable-router-alert-check

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command disables the IGMP or MLD router alert check option.

The **no** form of this command enables the router alert check.

Default no disable-router-alert-check

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vpls sap igmp-host-tracking disable-router-alert-check

All

- configure service vpls sap mld-snooping disable-router-alert-check
- configure service vpls spoke-sdp igmp-snooping disable-router-alert-check
- configure service vpls spoke-sdp mld-snooping disable-router-alert-check
- configure service vpls mesh-sdp igmp-snooping disable-router-alert-check
- configure service vpls sap igmp-snooping disable-router-alert-check
- configure service vpls mesh-sdp mld-snooping disable-router-alert-check

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>igmp-host-tracking disable-router-alert-check)
[Tree] (config>service>vprn>igmp>if disable-router-alert-check)

Full Context configure service ies subscriber-interface group-interface sap igmp-host-tracking disable-router-alert-check
configure service vprn igmp interface disable-router-alert-check

Description This command disables the IGMP router alert check option.

The **no** form of this command enables the router alert check.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap igmp-host-tracking disable-router-alert-check

All

- configure service vprn igmp interface disable-router-alert-check

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context **[Tree]** (config>service>vprn>mld>if disable-router-alert-check)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn mld interface disable-router-alert-check

Description This command disables router alert checking for MLD messages received on this interface.

The no form of this command enables the router alert checking.

Platforms All

8.198 disable-selective-fib

disable-selective-fib

Syntax [**no**] **disable-selective-fib**

Context **[Tree]** (config>service>vprn disable-selective-fib)

Full Context configure service vprn disable-selective-fib

Description This command specifies whether the system level selective FIB setting is overridden on this instance.

The **no** form of this command enables the selective FIB.

Default no disable-selective-fib

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

disable-selective-fib

Syntax [**no**] **disable-selective-fib**

Context **[Tree]** (config>router disable-selective-fib)

Full Context configure router disable-selective-fib

Description This command disables the selective FIB.

The **no** form of this command enables the selective FIB.

Default no disable-selective-fib

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.199 disable-send-bvpls-evpn-flush

disable-send-bvpls-evpn-flush

Syntax [**no**] **disable-send-bvpls-evpn-flush**

Context **[Tree]** (config>service>vpls>sap disable-send-bvpls-evpn-flush)
[Tree] (config>service>vpls>spoke-sdp disable-send-bvpls-evpn-flush)

Full Context configure service vpls sap disable-send-bvpls-evpn-flush
configure service vpls spoke-sdp disable-send-bvpls-evpn-flush

Description This command disables the ISID-based C-MAC flush indication when the corresponding SAP or spoke-SDP enters the operationally down state.

If the **send-bvpls-evpn-flush** is properly enabled, the **no** version of the command enables B-MAC/ISID route updates to be sent when the SAP or spoke-SDP is operationally down.

Default no disable-send-bvpls-evpn-flush

Platforms All

8.200 disable-shcv

disable-shcv

Syntax [**no**] **disable-shcv** [**alarm**] [**hold-time** *seconds*]

Context **[Tree]** (config>subscr-mgmt>ancp>policy>port-dwn disable-shcv)

Full Context configure subscriber-mgmt ancp ancp-policy port-down disable-shcv

Description When this command is configured, the node suspends SHCV for the hosts defined with this ANCP policy until the access node sends a port-up message. When the **hold-time** parameter is used, the node suspends SHCV for the period of time defined. If the **hold-time** parameter is not defined the node will suspend SHCV until a port-up message is received.

If the optional alarm flag is used, the node sends a SHCV alarm before suspending.

The **no** form of this command reverts to the default.

Parameters **alarm** — Specifies that the node sends an alarm before suspending SHCV.

seconds — Specifies the time that the node suspends SHCV.

Values 0 to 7200

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.201 disable-soft-reset-extension

disable-soft-reset-extension

Syntax [**no**] **disable-soft-reset-extension**

Context **[Tree]** (config>lag>bfd disable-soft-reset-extension)

Full Context configure lag bfd disable-soft-reset-extension

Description This command enables the BFD context and enables BFD over LAG links. Additional parameter configuration is required to make BFD over LAG links operational. Normally, BFD session timers are automatically extended during soft-reset operation on the IOMs and IMMs to avoid BFD sessions timing out and causing protocol events. However, in some cases this behavior is not desired as it could delay fast re-route transitions if they are in place. The optional disable-soft-reset-extension keyword allows this behavior to be disabled so that the BFD timers are not automatically extended.

Default no disable-soft-reset-extension

Parameters **disable-soft-reset-extension** — Disables the automatic extension of BFD timers during an IOM/IMM soft-reset.

Platforms All

8.202 disable-stickiness

disable-stickiness

Syntax [**no**] **disable-stickiness**

Context **[Tree]** (config>aaa>radius-srv-plcy>servers disable-stickiness)

Full Context configure aaa radius-server-policy servers disable-stickiness

Description This command disables a subscriber RADIUS accounting session from sticking with a single server under normal working conditions. If a direct algorithm is used, all subscriber RADIUS sessions will go directly to the server with the lowest configured index. If a failure occurs, a new in-service server with the next lowest index is used. When the original server recovers, if stickiness is not disabled, all existing sessions will continue to use the new server. This command disables stickiness, and as a result, the recovered original RADIUS server will

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

again service every subscriber. If a round-robin algorithm is used and stickiness is not disabled, an accounting session for a particular subscriber (or host, depending on the accounting mode) will stay with the same server. This command removes the stickiness and all subscriber accounting messages will go through the list of servers in a round-robin manner.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.203 disable-targeted-session

disable-targeted-session

Syntax [**no**] **disable-targeted-session**

Context **[Tree]** (config>router>ldp>targ-session disable-targeted-session)

Full Context configure router ldp targeted-session disable-targeted-session

Description This command disables support for SDP triggered automatic generated targeted sessions. Targeted sessions are LDP sessions between non-directly connected peers. The discovery messages for an indirect LDP session are addressed to the specified peer and not to the multicast address.

The **no** form of this command enables the set up of any targeted sessions.

Default no disable-targeted-session

Platforms All

8.204 disallow-igp

disallow-igp

Syntax [**no**] **disallow-igp**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop disallow-igp)

Full Context configure router static-route-entry indirect tunnel-next-hop disallow-igp

Description This optional command determines if the associated static route can be resolved via an IGP next-hop in the RTM if no tunnel next-hops are found in TTM.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When configured, the associated static route will not be resolved to an available IGP route in the RTM.

The **no** form of this command returns the behavior to the default, which allows the static route to be resolved via an IGP route in the RTM if no tunnel next-hop can be found in the TTM.

Default no disallow-igp

Platforms All

8.205 discard

discard

Syntax **discard** [**now**]

Context **[Tree]** (candidate discard)

Full Context candidate discard

Description This command deletes the entire contents of the candidate configuration and exits the edit-cfg mode. Undo cannot be used to recover a candidate that has been discarded with **candidate discard**.

Parameters **now** — Avoids a confirmation prompt for the discard.

8.206 discard-changes

discard-changes

Syntax [**no**] **discard-changes**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization discard-changes)

Full Context configure system security profile netconf base-op-authorization discard-changes

Description This command enables the NETCONF discard-changes operation.

The **no** form of this command disables the operation.

Default no discard-changes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

8.207 discard-rx-pause-frames

discard-rx-pause-frames

Syntax [**no**] **discard-rx-pause-frames**

Context **[Tree]** (config>port>ethernet discard-rx-pause-frames)

Full Context configure port ethernet discard-rx-pause-frames

Description This command discards received pause frames. Pause frames are used for local link flow control.

The **no** form of this command processes pause frames upon reception and the transmit side of the receiving port pauses in its transmissions.

Default no discard-rx-pause-frames

Platforms All

8.208 discard-unknown

discard-unknown

Syntax [**no**] **discard-unknown**

Context **[Tree]** (config>service>vpls discard-unknown)
[Tree] (config>service>template>vpls-template discard-unknown)

Full Context configure service template vpls-template discard-unknown
configure service vpls discard-unknown

Description By default, packets with unknown destination MAC addresses are flooded. If **discard-unknown** is enabled at the VPLS level, packets with unknown destination MAC address will be dropped instead (even when configured FDB size limits for VPLS or SAP are not yet reached).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command allows flooding of packets with unknown destination MAC addresses in the VPLS.

Default no discard-unknown — Packets with unknown destination MAC addresses are flooded.

Platforms All

8.209 discard-unknown-source

discard-unknown-source

Syntax [**no**] **discard-unknown-source**

Context **[Tree]** (config>service>template>vpls-sap-template discard-unknown-source)
[Tree] (config>service>template>vpls-template discard-unknown-source)
[Tree] (config>service>vpls>sap discard-unknown-source)
[Tree] (config>service>vpls>spoke-sdp discard-unknown-source)
[Tree] (config>service>vpls>vxlan discard-unknown-source)

Full Context configure service template vpls-sap-template discard-unknown-source
configure service template vpls-template discard-unknown-source
configure service vpls sap discard-unknown-source
configure service vpls spoke-sdp discard-unknown-source
configure service vpls vxlan discard-unknown-source

Description When this command is enabled, packets received on a SAP, a spoke-SDP, or a static VXLAN instance with an unknown source MAC address will be dropped only if the maximum number of MAC addresses for that SAP or spoke-SDP (see **max-nbr-mac-addr** [**config>service>vpls>sap max-nbr-mac-addr**, **config>service>vpls>spoke-sdp max-nbr-mac-addr**]) has been reached. If **max-nbr-mac-addr** has not been set for the SAP or spoke-SDP, enabling **discard-unknown-source** has no effect.

When disabled, the packets are forwarded based on the destination MAC addresses.

The **no** form of this command causes packets with an unknown source MAC addresses to be forwarded by destination MAC addresses in VPLS.

Default no discard-unknown-source

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls vxlan discard-unknown-source

All

- configure service vpls spoke-sdp discard-unknown-source
- configure service vpls sap discard-unknown-source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service template vpls-sap-template discard-unknown-source

discard-unknown-source

Syntax [**no**] **discard-unknown-source**

Context **[Tree]** (config>service>pw-template discard-unknown-source)

Full Context configure service pw-template discard-unknown-source

Description When this command is enabled, packets received with an unknown source MAC address will be dropped only if the maximum number of MAC addresses have been reached.

When disabled, the packets are forwarded based on the destination MAC addresses.

The **no** form of this command causes packets with an unknown source MAC addresses to be forwarded by destination MAC addresses.

Default no discard-unknown-source

Platforms All

8.210 disconnect

disconnect

Syntax **disconnect** [**address** *ip-address* | **session-id** *session-id* | **username** *user-name* | {**console** | **bluetooth** | **telnet** | **ftp** | **ssh** | **netconf** | **grpc**}]

Context **[Tree]** (admin disconnect)

Full Context admin disconnect

Description This command disconnects a user from a session.

Issuing the **disconnect** command without any parameters will disconnect the session in which the command was executed.

If any of the session type options (for example, **console, bluetooth, telnet, FTP, SSH**) are specified, then only the respective sessions are affected.

If no session type options are specified, then all sessions from the IP address or from the specified user are disconnected.

Any task that the user is executing is terminated. FTP files accessed by the user will not be removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A major severity security log event is created specifying what was terminated and by whom.

Parameters *ip-address* — Specifies the IP address to disconnect, specified in dotted decimal notation.

Note: IPv6 is supported on the 7750 SR and 7950 XRS.

Values

ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x* (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

session-id — The model-driven session ID. Can be obtained using the **show system management-interface datastore-locks** [**detail**] command.

user-name — Specifies the name of the user. The name can be up to 32 characters.

console — Disconnects the console session.

bluetooth — Disconnects the bluetooth session.

telnet — Disconnects the Telnet session.

ftp — Disconnects the FTP session.

ssh — Disconnects the SSH session.

netconf — Disconnects the NETCONF session.

grpc — Disconnects the GRPC session.

Platforms All

8.211 discover-delay

discover-delay

Syntax **discover-delay** *delay*
no discover-delay

Context [Tree] (config>service>ies>sub-if>grp-if>dhcp>osel discover-delay)
[Tree] (config>service>vprn>sub-if>dhcp>osel discover-delay)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>dhcp>osel discover-delay)

Full Context configure service ies subscriber-interface group-interface dhcp offer-selection discover-delay
configure service vprn subscriber-interface dhcp offer-selection discover-delay
configure service vprn subscriber-interface group-interface dhcp offer-selection discover-delay

Description This command configures the default time to delay DHCP Discover messages. The delay is applied to all DHCP Discover messages for which no per DHCP server or per client MAC delay is configured.

The **no** form of this command removes the delay.

Parameters *delay* — Specifies the default time to delay DHCP Discover messages, in deciseconds.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

discover-delay

Syntax **discover-delay** *delay*
no discover-delay

Context [Tree] (config>service>ies>sub-if>grp-if>dhcp>osel>clnt-mac discover-delay)
[Tree] (config>service>vprn>sub-if>dhcp>osel>clnt-mac discover-delay)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>osel>clnt-mac discover-delay)

Full Context configure service ies subscriber-interface group-interface dhcp offer-selection client-mac discover-delay
configure service vprn subscriber-interface dhcp offer-selection client-mac discover-delay
configure service vprn subscriber-interface group-interface dhcp offer-selection client-mac discover-delay

Description This command configures the amount of time to delay DHCP Discover messages from odd or even source MAC addresses.

The **no** form of this command removes the delay.

Parameters *delay* — Specifies the amount of time to delay DHCP Discover messages from odd or even source MAC addresses, in deciseconds.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

discover-delay

Syntax **discover-delay** *delay*
no discover-delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>dhcp>osel>srvr discover-delay)
[Tree] (config>service>vprn>sub-if>dhcp>osel>srvr discover-delay)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>osel>srvr discover-delay)

Full Context configure service ies subscriber-interface group-interface dhcp offer-selection server discover-delay
configure service vprn subscriber-interface dhcp offer-selection server discover-delay
configure service vprn subscriber-interface group-interface dhcp offer-selection server discover-delay

Description This command configures the amount of time to delay DHCP Discover messages relayed to the server.

The **no** form of this command removes the delay.

Parameters *delay* — Specifies the amount of time to delay DHCP Discover messages relayed to the server, in deciseconds.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.212 discovery

discovery

Syntax **discovery** [**padi**] [**pado**] [**padr**] [**pads**] [**padt**]
no discovery

Context [Tree] (debug>service>id>ppp>packet discovery)

Full Context debug service id ppp packet discovery

Description This command enables debugging for specific PPP discovery packets.

Parameters **padi** — Enables debugging for PADI PPP discovery packets.

pado — Enables debugging for PADO PPP discovery packets.

padr — Enables debugging for PADR PPP discovery packets.

pads — Enables debugging for PADS PPP discovery packets.

padt — Enables debugging for PADT PPP discovery packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

discovery

Syntax **discovery** [**padi**] [**pado**] [**padr**] [**pads**] [**padt**]

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg>pppoe-client>brg-id discovery)

Full Context debug subscriber-mgmt vrgw brg pppoe-client brg-id discovery

Description This command, limits debugging only to the specified messages in the discovery phase.

Parameters **padi** — Limits debugging only to padi messages.

pado — Limits debugging only to pado messages.

padr — Limits debugging only to padr messages.

pads — Limits debugging only to pads messages.

padt — Limits debugging only to padt messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

discovery

Syntax **discovery**

Context **[Tree]** (config>port>ethernet>efm-oam discovery)

Full Context configure port ethernet efm-oam discovery

Description This is the top level of the hierarchy containing various discovery parameters that allow the operator to control certain aspects of the negotiation process as well as what action to take when there is a mismatch in peer capabilities.

Platforms All

8.213 discovery-interval

discovery-interval

Syntax **discovery-interval** *interval-secs* [**boot** *interval-secs*]
no discovery-interval

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ipsec discovery-interval)

Full Context configure redundancy multi-chassis peer mc-ipsec discovery-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the time interval of tunnel-group stays in the Discovery state. Interval-1 is used as discovery-interval when a new tunnel-group is added to multi-chassis redundancy (mp-ipsec); interval-2 is used as discovery-interval when the system boots up, it is optional, when it is not specified, the interval-1 will be used.

Default discovery-interval 300 boot 300

Parameters *interval-secs* — Specifies the maximum duration, in seconds, of the discovery interval during which a newly activated multi- chassis IPsec tunnel-group will remain dormant while trying to contact its redundant peer. Groups held dormant in this manner will neither pass traffic nor negotiate security keys. This interval ends when either the redundant peer is contacted and a master election occurs, or when the maximum duration expires.

Values 1 to 1800

interval-secs — Specifies the maximum duration of an interval immediately following system startup. When the normal discovery interval for a group would expire while the post-boot discovery interval is still active, then the group's discovery interval is extended until the post-boot discovery interval expires. This allows an extension to the normal discovery stage of groups following a chassis reboot, to account for the larger variance in routing.

Values 1 to 1800

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.214 discriminator

discriminator

Syntax **discriminator** *discriminator*
no discriminator

Context **[Tree]** (config>bfd>seamless-bfd>reflector discriminator)

Full Context configure bfd seamless-bfd reflector discriminator

Description This command specifies the S-BFD discriminator.

The **no** form of this command removes the discriminator.

Parameters *discriminator* — Specifies the discriminator value.

Values 524288 to 526335

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

discriminator

Syntax **discriminator** *discriminator*
no discriminator

Context **[Tree]** (config>router>bfd>seamless-bfd>peer discriminator)

Full Context configure router bfd seamless-bfd peer discriminator

Description This command specifies the seamless BFD reflector discriminator for the remote peer node in the mapping table used by seamless BFD sessions initiated on the router.

The **no** form of this command removes the discriminator.

Parameters *discriminator* — Specifies the discriminator of the remote node.

Values 1 to 4294967295

Platforms All

8.215 dispersion

dispersion

Syntax **dispersion** *dispersion*

Context **[Tree]** (config>port>dwdm>coherent dispersion)

Full Context configure port dwdm coherent dispersion

Description This command configures the residual chromatic dispersion to be compensated when the coherent receiver is operating in manual dispersion control mode.

Default 0

Parameters *dispersion* — Specifies the dispersion compensation.

Values -50000 to 50000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.216 display

display

Syntax **display type** {*type*} *url-string* **format** {*format*} [**password** [*32 chars max*]]

Context **[Tree]** (admin>certificate display)

Full Context admin certificate display

Description This command displays the content of an input file in plain text.

Note: When displaying the key file content, only the key size and type are displayed.

The following list summarizes the formats supported by this command:

- System
  - system format
  - PKCS #12
  - PKCS #7 PEM encoded
  - PKCS #7 DER encoded
  - RFC4945
- Certificate Request
  - PKCS #10
- Key
  - system format
  - PKCS #12
- CRL
  - system format
  - PKCS #7 PEM encoded
  - PKCS #7 DER encoded
  - RFC4945

Parameters *url-string* — Specifies the local CF card url of the input file.

Values

url-string	<local-url> [up to 99 characters]
local-url	<cflash-id>/<file-path>
cflash-id	cf1: | cf2: | cf3:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type — Specifies the type of input file.

Values cert, key, crl, cert-request

format — Specifies the format of input file.

Values pkcs10, pkcs12, pkcs7-der, pkcs7-pem, pem, der

password — Specifies the password to decrypt the input file in case that it is an encrypted PKCS#12 file, up to 99 characters.

Platforms All

8.217 display-config

display-config

Syntax **display-config** [**detail** | **index**]

Context **[Tree]** (admin display-config)

Full Context admin display-config

Description This command displays the system's running configuration.

By default, only non-default settings are displayed.

Specifying the **detail** option displays all default and non-default configuration parameters.

Parameters **detail** — Displays default and non-default configuration parameters.

index — Displays only persistent-indices.

Platforms All

8.218 display-key

display-key

Syntax **display-key type** {**ike** | **esp**} **gateway name** *name* **dynamic-tunnel** *ip-address*:*port*
display-key type {**ike** | **esp**} **tunnel** *ipsec-tunnel-name*

Context **[Tree]** (admin>ipsec display-key)

Full Context admin ipsec display-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command displays existing IKE-SA or CHILD-SA keys..

Note: This command does not work if **config>ipsec>no show-ipsec-keys** or **no max-history-{esp|ike}-key-records** is configured under corresponding **ipsec-gw** or **ipsec-tunnel**.

Parameters *name* — The name, up to 32 characters.

ip-address — The IP address of the remote client.

Values

<ip-address>	ip-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D

port — The port of the remote client.

Values 0 to 65535

ipsec-tunnel-name — The IPsec tunnel name, up to 32 characters.

Output The following outputs are examples of the **admin ipsec display-key** command.

Sample Output

```
admin ipsec display-key type ike gateway name "rw" dynamic-tunnel 11.1.1.100:500
===============================================================================
IKE-SA history: max-num-records 3 current-num-saved-records 1
                local: 172.16.100.1 remote: 11.1.1.100
record [0]: established time: 01/25/2018 20:51:55
  Initiator-SPI: d67ac71d73656496 Responder-SPI: d67ac71d73656496  Ike Version: 2
  SK_er: aes128, len: 16, val: a5da1c57f09a7eb7dbe9526cd52e2189
  SK_ar: sha1, len: 20, val: c11797bb8ebe5a1fadf46363bf5e763552bb45d0
  SK_ei: aes128, len: 16, val: 467124009cc577a8b23882a81ab9df70
  SK_ai: sha1, len: 20, val: 7dfef89bad31cb72d1ca8da2c04a9521993c7f9
```

Sample Output

```
admin ipsec display-key type esp gateway name "rw" dynamic-tunnel 11.1.1.100:500

ESP-SA history: max-num-records 48 current-num-saved-records 2ynamic-tunnel 11.1.1.1
00:500
                local: 172.16.100.1 remote: 11.1.1.100
record [0]: established time: 01/25/2018 20:54:56
  InSpi:  154532(0x00025ba4)
          encr-alg: aes128 len: 16 val: 0xd26aa32d8bd328b1e8332fa5c7b5eeaa
          auth-alg: sha1 len: 20 val: 0x0b37ddb824a43921d3b0ee81a6910eed065a9845
  OutSpi: 3286259439(0xc3e056ef)
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
          encr-alg: aes128 len: 16 val: 0x3acd95376ce04fcded2e0c80cc4289cf
          alg: sha1 len: 20 val: 0x9f5a46b5cdc572972b44cdbd36b5f824ab060634
record [1]: established time: 01/25/2018 20:51:55
  InSpi:  261186(0x0003fc42)
          encr-alg: aes128 len: 16 val: 0x8bf97675d37de3e3f6e634e3e11fc3aa
          auth-alg: sha1 len: 20 val: 0xf10c0f0821488cc14f8715cc323441fc967a79dd
  OutSpi: 3246917342(0xc18806de)
          encr-alg: aes128 len: 16 val: 0xf36aaaa7a3a09734fe4fc6cd0ac9043e
          alg: sha1 len: 20 val: 0x40c13a444e4fb1d42a13812f70b17041ed0f56ee
```

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.219 dist-cpu-protection

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>subscr-mgmt>msap-policy dist-cpu-protection)
[Tree] (config>service>vprn>sub-if>grp-if>sap dist-cpu-protection)

Full Context configure service vprn subscriber-interface group-interface sap dist-cpu-protection
configure subscriber-mgmt msap-policy dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to an MSAP policy. The DCP policy is automatically assigned to MSAPs created with this policy. A non-existent DCP policy can be assigned to an **msap-policy** because an MSAP policy is similar to a template that is applied in the MSAP creation. The DCP policy is validated at the time that the MSAP is created, and the MSAP creation is blocked (and an appropriate log event created) if the DCP policy does not exist.

Note: For other types of objects (for example, normal non-MSAP SAPs and network interfaces) the DCP policy must exist before it can be assigned to the SAP.

The **no** form of this command removes the policy name from the configuration.

If no dist-cpu-protection policy is assigned to an MSAP policy, then the default access DCP policy (_default-access-policy) is used.

If no DCP functionality is required on the MSAP policy, then an empty DCP policy can be created and explicitly assigned to the MSAP policy.

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>subscr-mgmt>sap-template dist-cpu-protection)

Full Context configure subscriber-mgmt sap-template dist-cpu-protection

Description This command assigns a DCP policy to a SAP template. The policy is automatically assigned to SAPs that are autocreated with this SAP template. The **dist-cpu-protection** policy must exit before it is assigned to a SAP template.

The **no** form of this command removes the policy name from the configuration.

If a DCP policy is not assigned to an SAP template, the default access DCP policy (_defaultaccess-policy) is used.

If no DCP functionality is required on the autocreated SAPs, an empty DCP policy can be created and explicitly assigned to the SAP template.

Default no dist-cpu-protection

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>service>apipe>sap dist-cpu-protection)
[Tree] (config>service>cpipe>sap dist-cpu-protection)
[Tree] (config>service>epipe>sap dist-cpu-protection)
[Tree] (config>service>fpipe>sap dist-cpu-protection)
[Tree] (config>service>ipipe>sap dist-cpu-protection)

Full Context configure service apipe sap dist-cpu-protection
configure service cpipe sap dist-cpu-protection
configure service epipe sap dist-cpu-protection
configure service fpipe sap dist-cpu-protection
configure service ipipe sap dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid existing DCP policy can be assigned to a SAP or a network interface (this rule does not apply to templates, such as an **msap-policy** template).

If no dist-cpu-protection policy is assigned to a SAP, then the default access DCP policy (_default-access-policy) is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If no DCP functionality is required on the SAP, then an empty DCP policy can be created and explicitly assigned to the SAP.

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters in length

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap dist-cpu-protection
- configure service cpipe sap dist-cpu-protection

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap dist-cpu-protection

All

- configure service epipe sap dist-cpu-protection
- configure service ipipe sap dist-cpu-protection

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>service>vpls>sap dist-cpu-protection)

Full Context configure service vpls sap dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid existing DCP policy can be assigned to a SAP or a network interface (this rule does not apply to templates, such as an msap-policy template).

Default If no dist-cpu-protection policy is assigned to a SAP, then the default access DCP policy (_default-access-policy) is used. If no DCP functionality is required on the SAP, then an empty DCP policy can be created and explicitly assigned to the SAP.

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters in length

Platforms All

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap dist-cpu-protection)
[Tree] (config>service>ies>if>sap dist-cpu-protection)

Full Context configure service ies interface sap dist-cpu-protection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface sap dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid DCP policy can be assigned to a SAP or a network interface. This rule does not apply to templates such as an msap-policy.

Default If no dist-cpu-protection policy is assigned to an SAP, then the default access DCP policy (default-access-policy) is used. If no DCP functionality is required on the SAP, then an empty DCP policy can be created and explicitly assigned to the SAP policy.

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters in length

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap dist-cpu-protection

All

- configure service ies interface sap dist-cpu-protection

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>service>vprn>nw-if dist-cpu-protection)

Full Context configure service vprn network-interface dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to the network interface. Only a valid created DCP policy can be assigned to a network interface (this rule does not apply to templates such as an msap-policy).

Default If no dist-cpu-protection policy is assigned to the VPRN network interface, then the default network DCP policy (_default-network-policy) is used.

If no DCP functionality is required on the VPRN network interface then an empty DCP policy can be created and explicitly assigned to the VPRN network interface.

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters in length

Platforms All

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>service>vprn>if>sap dist-cpu-protection)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid created DCP policy can be assigned to a SAP or a network interface (This rule does not apply to templates such as an msap-policy).

Default If no dist-cpu-protection policy is assigned to an SAP policy, then the default access DCP policy (default-access-policy) is used. If no DCP functionality is required on the SAP policy, then an empty DCP policy can be created and explicitly assigned to the SAP policy.

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters in length

Platforms All

dist-cpu-protection

Syntax **dist-cpu-protection** *policy-name*
no dist-cpu-protection

Context **[Tree]** (config>router>if dist-cpu-protection)

Full Context configure router interface dist-cpu-protection

Description This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid created DCP policy can be assigned to a SAP or a network interface (note that this rule does not apply to templates such as an msap-policy).

Default no dist-cpu-protection

Parameters *policy-name* — Specifies the name of the DCP policy, up to 32 characters in length

Platforms All

dist-cpu-protection

Syntax **dist-cpu-protection**

Context **[Tree]** (config>system>security dist-cpu-protection)

Full Context configure system security dist-cpu-protection

Description Commands in this context configure the Distributed CPU Protection (DCP) feature.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.220 dist-lag-rate-shared

dist-lag-rate-shared

Syntax [**no**] **dist-lag-rate-shared**

Context **[Tree]** (config>qos>port-scheduler-policy dist-lag-rate-shared)

Full Context configure qos port-scheduler-policy dist-lag-rate-shared

Description This command enables sharing of rates when the port on which this port-scheduler-policy is configured is part of a LAG configured in **distribute** mode.

When enabled, the absolute rate values configured as part of the max-rate, PIR/CIR group rates and PIR/CIR level rates are shared across the member ports of the LAG when configured in **distribute** mode.

This command does not have any effect when the port on which this **port-scheduler-policy** is configured is part of a LAG in **link** or **port-fair** mode. Similarly, when rates are configured as a **percent-rate**, this parameter is ignored.

Platforms All

8.221 distinguisher

distinguisher

Syntax **distinguisher** *id*
no distinguisher

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy distinguisher)

Full Context configure router segment-routing sr-policies static-policy distinguisher

Description This command associates a distinguisher value with a statically defined segment routing policy. This is a mandatory parameter and configuration command for non-local segment routing policies (for which the **head-end** parameter is set to a value other than “local”). Every non-local segment routing policy must have a unique distinguisher value. When a non-local static segment routing policy is imported into BGP and originated as a BGP route, the configured distinguisher value is copied into the NLRI of the route.

The **no** form of this command removes the distinguisher association.

Default no distinguisher

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *id* — Specifies the distinguisher ID.

Values 1 to 4294967295

Platforms All

distinguisher

Syntax **distinguisher** *distinguisher-id*
no distinguisher

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from distinguisher)

Full Context configure router policy-options policy-statement entry from distinguisher

Description This command configures an SR Policy distinguisher as a route policy match criterion. This match criterion is only used in import policies.

The **no** form of this command removes the distinguisher ID match criterion from the configuration.

Parameters *distinguisher-id* — Specifies the SR policy distinguisher ID.

Values 0 to 4294967295

Platforms All

8.222 distributed-sub-mgmt

distributed-sub-mgmt

Syntax **distributed-sub-mgmt**

Context **[Tree]** (config>service>vprn>wlan-gw distributed-sub-mgmt)

Full Context configure service vprn wlan-gw distributed-sub-mgmt

Description Commands in this context configure Distributed Subscriber Management (DSM) for soft GRE group interface and for ranges of IEEE 802.1q VLAN tags in soft GRE group interfaces.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

distributed-sub-mgmt

Syntax **distributed-sub-mgmt**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>wlan-gw distributed-sub-mgmt)
[Tree] (config>router>wlan-gw distributed-sub-mgmt)
[Tree] (config>service>vprn>wlan-gw distributed-sub-mgmt)

Full Context configure router wlan-gw distributed-sub-mgmt
configure service vprn wlan-gw distributed-sub-mgmt
configure subscriber-mgmt wlan-gw distributed-sub-mgmt

Description Commands in this context configure profiles, templates and policies that can be applied to DSM subscribers.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

distributed-sub-mgmt

Syntax [**no**] **distributed-sub-mgmt**

Context [Tree] (config>isa>wlan-gw-group distributed-sub-mgmt)

Full Context configure isa wlan-gw-group distributed-sub-mgmt

Description This command configures the WLAN gateway distributed subscriber management.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

distributed-sub-mgmt

Syntax **distributed-sub-mgmt**

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range distributed-sub-mgmt)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range distributed-sub-mgmt)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt

Description Commands in this context configure distributed-sub-mgmt configuration per vlan-range. This also includes vlan-range default, which makes this configuration applicable to the **wlan-gw group-interface**.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.223 divert

divert

Syntax [**no**] **divert**

Context **[Tree]** (config>app-assure>group>policy>app-profile divert)

Full Context configure application-assurance group policy app-profile divert

Description This command enables the redirection of traffic to AA ISA for the system-wide forwarding classes diverted to application assurance (**divert-fc**) for AA subscribers using this application profile.

The **no** form of this command stops redirect of traffic to AA ISAs for the AA subscribers using this application profile.

Default no divert

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.224 divert-fc

divert-fc

Syntax [**no**] **divert-fc** *fc-name*

Context **[Tree]** (config>isa>aa-grp divert-fc)

Full Context configure isa application-assurance-group divert-fc

Description This command selects a forwarding class in the system to be diverted to an application assurance engine for this application assurance group. Only traffic to/from subscribers with application assurance enabled is diverted.

To divert multiple forwarding classes, the command needs to be executed multiple times specifying each forwarding class to be diverted at a time.

The **no** form of this command stops diverting of the traffic to an application assurance engine for this application assurance group.

Parameters *fc-name* — Creates a class instance of the forwarding class fc-name.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.225 dm

dm

Syntax **dm** [**test-id** *test-id*] [**create**]
no dm

Context **[Tree]** (config>oam-pm>session>mpls dm)

Full Context configure oam-pm session mpls dm

Description This command assigns an identifier to the DM test and creates the individual test.

The **no** form of this command removes the DM test function from the OAM-PM session.

Parameters *test-id* — Specifies the value of the 26-bit test identifier sent as session identifier in the DM PDU.

Values 0 to 67108863

create — Creates the DM test. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.226 dmm

dmm

Syntax **dmm** [**test-id** *test-id*] [**create**]
no dmm

Context **[Tree]** (config>oam-pm>session>ethernet dmm)

Full Context configure oam-pm session ethernet dmm

Description This command defines the test ID to be assigned to the delay test and creates the container to allow the individual test parameters to be configured.

The **no** form of this command removes the DMM test function from the PM Session.

Parameters *test-id* — Specifies the value to be placed in the 4-byte test ID field of an ETH-DMM PDU.

Values 0 to 2147483647

create — Creates the test.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

8.227 dmr-prefix

dmr-prefix

Syntax **dmr-prefix** *dmr-prefix*
no dmr-prefix

Context **[Tree]** (config>service>nat>map-domain dmr-prefix)

Full Context configure service nat map-domain dmr-prefix

Description This command configures the IPv6 prefix of the BR (dmr-prefix), which is used as a default MAP rule (route) in the CEs. Each MAP domain in the VSR has a unique dmr-prefix.

Parameters *dmr-prefix* — Specifies the IPv6 prefix associated with a MAP domain in the BR. The prefix represents a dmr-rule in the CE.

Values <*ipv6-prefix/prefix-length*> :
ipv6-prefix —— *x:x:x:x:x:x:x:x* (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x—[0 to FFFF]H
d—[0 to 255]D
prefix-length—[0 to 96]

Platforms VSR

8.228 dnat

dnat

Syntax [no] **dnat**

Context **[Tree]** (config>service>nat>nat-policy dnat)

Full Context configure service nat nat-policy dnat

Description This command defines context for destination NAT (DNAT) specific configuration under the nat-policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.229 dnat-only

dnat-only

Syntax **dnat-only router** *router-instance* **nat-group** *nat-group-id*
no dnat-only

Context **[Tree]** (config>service>nat>nat-policy>dnat dnat-only)

Full Context configure service nat nat-policy dnat dnat-only

Description This command configures outside routing context and nat-group in which DNAT translation shout take place. This command is mutually exclusive with the pool command in nat-policy. When DNAT-only is enabled, no source and port NAT (SNAPT) is performed. In other words, only the destination IP address (going from inside to outside) is translated while the source IP address and port are not translated.

Default none

Parameters **router** *router-instance* — Specifies the routing context on the outside (public side).

nat-group *nat-group-id* — Specifies the NAT group IP.

Values 1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dnat-only

Syntax **dnat-only**

Context **[Tree]** (config>router>nat>inside dnat-only)
[Tree] (config>router>nat>outside dnat-only)
[Tree] (config>service>vprn>nat>inside dnat-only)
[Tree] (config>service>vprn>nat>outside dnat-only)

Full Context configure router nat inside dnat-only
configure router nat outside dnat-only
configure service vprn nat inside dnat-only
configure service vprn nat outside dnat-only

Description Commands in this context configure the dnat-only parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.230 dns

dns

Syntax **dns ip-address** [**secondary** *ip-address*]
dns secondary *ip-address*
no dns [*ip-address*] [**secondary** *ip-address*]

Context **[Tree]** (config>service>ies>if>ipcp dns)

Full Context configure service ies interface ipcp dns

Description This command defines the DNS address to be assigned to the far-end of the associated PPP or MLPPP link through IPCP extensions. This command is only applicable if the associated SAP or port is a PPP or MLPPP interface with an IPCP encapsulation.

The **no** form of this command deletes either the specified primary DNS address, secondary DNS address or both addresses from the IPCP extension peer-ip-address configuration.

Default no dns

Parameters *ip-address* — Specifies a unicast IPv4 address for the primary DNS server to be signaled to the far-end of the associate PPP or MLPPP link via IPCP extensions.

secondary *ip-address* — Specifies a unicast IPv4 address for the secondary DNS server to be signaled to the far-end of the associate PPP or MLPPP link using IPCP extensions.

Platforms All

dns

Syntax [**no**] **dns**

Context **[Tree]** (config>service>vprn dns)

Full Context configure service vprn dns

Description Commands in this context configure domain name servers.

The **no** form of this command disables DNS for this service.

Platforms All

dns

Syntax **dns ip-address** [**secondary** *ip-address*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dns secondary *ip-address*
no dns [*ip-address*] [**secondary** *ip-address*]

Context **[Tree]** (config>service>vprn>if>ipcp dns)

Full Context configure service vprn interface ipcp dns

Description This command defines the dns address(es) to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface with an IPCP encapsulation.

The **no** form of this command deletes either the specified primary DNS address, secondary DNS address or both addresses from the IPCP extension peer-ip-address configuration.

Default no dns

Parameters *ip-address* — Specifies a unicast IPv4 address for the primary DNS server to be signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions.

secondary *ip-address* — Specifies a unicast IPv4 address for the secondary DNS server to be signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions.

Platforms All

dns

Syntax **dns target-addr** *dns-name* **name-server** *ip-address* [**source** *ip-address*] [**count** *send-count*] [**timeout** *timeout*] [**interval** *interval*] [**record-type** {**ipv4-a-record** | **ipv6-aaaa-record**}] [**router-instance** *router-instance*]

Context **[Tree]** (oam dns)
[Tree] (config>saa>test>type dns)

Full Context configure saa test type dns
oam dns

Description This command performs DNS name resolution. If **ipv4-a-record** is specified, DNS target addresses are queried for A records only. If **ipv6-aaaa-record** is specified, AAAA records are queried first, and if a successful response is not received, the DNS server is queried for A records (applies to the 7750 SR and 7950 XRS).

Parameters *dns-name* — Specifies the DNS domain name, up to 255 characters.

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the **interval** is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message response corresponding to the outstanding message request.

Values 1 to 10

Default 1

ip-address — Specifies the IP address of the primary DNS server.

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: 0 to FFFF]H
d: [0 to 255]D

record-type — Specifies a record type (applies to the 7750 SR and 7950 XRS only).

Values **ipv4-a-record —** A record-specific mapping of a host name to an IPv4 address.

ipv6-aaaa-record — A record-specific mapping to the Internet class that stores a single IPv6 address.

send-count — Specifies the number of messages to send. The **send-count** parameter overrides the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must have expired before the next message request is sent.

Values 1 to 100

Default 1

timeout — Specifies the time, in seconds, to override the default *timeout* value and is the amount of time that the router waits for a message response after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded.

Values 1 to 120

Default 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-instance — Specifies the preferred method to enter a service name or routing instance from which to launch the DNS query. This value is stored as the service name. This is the only service-linking function allowed for both mixed-mode and model-driven configuration modes.

Values

router-name	Base	Specifies a base routing instance
	management	Specifies a management routing instance
	_Base_and_management	Specifies a base routing instance and a management routing instance: if no response is received from the base, a management routing instance is used.
vprn-svc-name		Specifies a service name, up to 64 characters

Default _Base_and_management

Platforms All

dns

Syntax **dns**

Context **[Tree]** (config>router dns)

Full Context configure router dns

Description This command configures the DNS.

Default dns

Platforms All

dns

Syntax **dns**

Context **[Tree]** (config>system dns)

Full Context configure system dns

Description This command configures DNS settings.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.231 dns-domain

dns-domain

Syntax **dns-domain** *dns-name*
no dns-domain

Context **[Tree]** (bof dns-domain)

Full Context bof dns-domain

Description This command configures the domain name used when performing DNS address resolution. This is a required parameter if DNS address resolution is required. Only a single domain name can be configured. If multiple domain statements are configured, the last one encountered is used.

The **no** form of this command removes the domain name from the configuration.

Default no dns-domain

Parameters *dns-name* — Specifies the DNS domain name, up to 178 characters.

Platforms All

8.232 dns-ip-cache

dns-ip-cache

Syntax **dns-ip-cache** *dns-ip-cache-name* [**create**]
no dns-ip-cache *dns-ip-cache-name*

Context **[Tree]** (config>app-assure>group dns-ip-cache)

Full Context configure application-assurance group dns-ip-cache

Description This command configures a DNS IP cache used to snoop DNS requests generated by subscribers to populate a cache of IP addresses matching a specified list of domain names. In the context of URL content charging strengthening, it is also mandatory to specify a list of trusted DNS servers to populate the DNS IP cache.

Parameters *dns-ip-cache-name* — Specifies the Application Assurance DNS IP cache name, up to 32 characters.

create — Specifies a keyword used to create the DNS IP cache.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dns-ip-cache

Syntax **dns-ip-cache** *dns-ip-cache-name*

Context **[Tree]** (config>app-assure>group>sess-fltr>entry>match dns-ip-cache)

Full Context configure application-assurance group session-filter entry match dns-ip-cache

Description This command configures a DNS IP cache using session filter DST IP match criteria. It is typically combine with an allow action in the context of captive-redirect.

Parameters *dns-ip-cache-name* — Specifies the name of the DNS IP cache name, up to 32 characters.

8.233 dns-match

dns-match

Syntax **dns-match**

Context **[Tree]** (config>app-assure>group>dns-ip-cache dns-match)

Full Context configure application-assurance group dns-ip-cache dns-match

Description Commands in this context configure match parameters in the DNS IP cache.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.234 dns-options

dns-options

Syntax [**no**] **dns-options**

Context **[Tree]** (config>subscr-mgmt>rtr-adv-plcy dns-options)

Full Context configure subscriber-mgmt router-advertisement-policy dns-options

Description Commands in this context configure IPv6 DNS options for SLAAC hosts.

The **no** form of this command returns the command to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dns-options

Syntax [**no**] **dns-options**

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv dns-options)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv dns-options)
[Tree] (config>service>vprn>router-advert dns-options)
[Tree] (config>service>vprn>router-advertisement dns-options)
[Tree] (config>service>vprn>router-advert>if dns-options)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv dns-options)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv dns-options)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements dns-options
configure service ies subscriber-interface ipv6 router-advertisements dns-options
configure service vprn router-advertisement dns-options
configure service vprn router-advertisement interface dns-options
configure service vprn router-advertisement dns-options
configure service vprn subscriber-interface group-interface ipv6 router-advertisements dns-options
configure service vprn subscriber-interface ipv6 router-advertisements dns-options

Description Commands in this context configure DNS information for Stateless Address Auto-Configuration (SLAAC) hosts.

When specified at the router-advertisement level in the routing context, this command allows configuration of service-wide parameters. These can then be inherited at the interface level by specifying the **config>service>vprn>router-advert>if>dns-options>include-dns** command.

The **no** form of this command disables configuration of DNS information for Stateless Address Auto-Configuration (SLAAC) hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface ipv6 router-advertisements dns-options
- configure service vprn subscriber-interface ipv6 router-advertisements dns-options
- configure service ies subscriber-interface ipv6 router-advertisements dns-options
- configure service ies subscriber-interface group-interface ipv6 router-advertisements dns-options

All

- configure service vprn router-advertisement dns-options
- configure service vprn router-advertisement interface dns-options

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dns-options

Syntax [**no**] **dns-options**

Context **[Tree]** (config>router>router-advert dns-options)
[Tree] (config>router>router-advert>if dns-options)

Full Context configure router router-advertisement dns-options
configure router router-advertisement interface dns-options

Description Commands in this context configure DNS information for Stateless Address Auto-Configuration (SLAAC) hosts. When specified at the router-advertisement level in the routing context, this command allows configuration of service-wide parameters. These can then be inherited at the interface level by specifying the **config>router>router-advert>if>dns-options>include-dns** command.

The **no** form of this command disables configuration of DNS information for Stateless Address Auto-Configuration (SLAAC) hosts.

Platforms All

8.235 dns-server

dns-server

Syntax **dns-server** *ip-address* [*ip-address*]
no dns-server

Context **[Tree]** (config>router>dhcp>server>pool>options dns-server)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options dns-server)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>options dns-server)
[Tree] (config>service>vprn>dhcp>server>pool>options dns-server)

Full Context configure router dhcp local-dhcp-server pool options dns-server
configure service vprn dhcp local-dhcp-server pool options dns-server
configure subscriber-mgmt local-user-db ipoe host options dns-server
configure subscriber-mgmt local-user-db ppp host options dns-server

Description This command configures the IPv4 address of the DNS server.

The **no** form of this command removes the IPv4 address of the DNS server from the configuration.

Parameters *ip-address* — Specifies up to four DNS server IP addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dns-server

Syntax **dns-server** *ipv6-address* [*ipv6-address*]
no dns-server

Context **[Tree]** (config>router>dhcp6>server>defaults>options dns-server)
[Tree] (config>router>dhcp6>server>pool>options dns-server)
[Tree] (config>router>dhcp6>server>pool>prefix>options dns-server)
[Tree] (config>service>vprn>dhcp6>server>defaults>options dns-server)
[Tree] (config>service>vprn>dhcp6>server>pool>options dns-server)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix>options dns-server)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>options6 dns-server)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options6 dns-server)

Full Context configure router dhcp6 local-dhcp-server defaults options dns-server
configure router dhcp6 local-dhcp-server pool options dns-server
configure router dhcp6 local-dhcp-server pool prefix options dns-server
configure service vprn dhcp6 local-dhcp-server defaults options dns-server
configure service vprn dhcp6 local-dhcp-server pool options dns-server
configure service vprn dhcp6 local-dhcp-server pool prefix options dns-server
configure subscriber-mgmt local-user-db ipoe host options6 dns-server
configure subscriber-mgmt local-user-db ppp host options6 dns-server

Description This command configures IPv6 DNS server addresses that can be used for name resolution.

The **no** form of this command removes the IPv6 address of the DNS server from the configuration.

Parameters *ipv6-address* — Specifies up to four IPv6 DNS server addresses.

Values ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt local-user-db ppp host options6 dns-server
- configure subscriber-mgmt local-user-db ipoe host options6 dns-server
- configure router dhcp6 local-dhcp-server pool prefix options dns-server
- configure service vprn dhcp6 local-dhcp-server pool prefix options dns-server
- configure service vprn dhcp6 local-dhcp-server pool options dns-server
- configure router dhcp6 local-dhcp-server pool options dns-server

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure router dhcp6 local-dhcp-server defaults options dns-server
- configure service vprn dhcp6 local-dhcp-server defaults options dns-server

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dns-server

Syntax **dns-server** *ip-address*
no dns-server

Context **[Tree]** (config>app-assure>group>url-filter>web-service dns-server)

Full Context configure application-assurance group url-filter web-service dns-server

Description This command configures the DNS server that is used to resolve the web service host name.

The **no** form of this command removes the DNS server configuration.

Default no dns-server

Parameters *ip-address* — Specifies the IP address of the DNS server to use.

Values a.b.c.d[/mask] (IPv4),
x:x:x:x:x:x:x:x/prefix-length (IPv6)
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF] H
d - [0..255] D
prefix-length [0..128]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.236 dnssec

dnssec

Syntax **dnssec**

Context **[Tree]** (config>system>dns dnssec)

Full Context configure system dns dnssec

Description This command configures system Domain Name System Security Extensions (DNSSEC) settings.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.237 do-not-fragment

do-not-fragment

Syntax [**no**] **do-not-fragment**

Context **[Tree]** (config>oam-pm>session>ip do-not-fragment)

Full Context configure oam-pm session ip do-not-fragment

Description This command configures the Do Not Fragment (DF) bit in the IPv4 header of the TWAMP Light test packet in order to prevent packet fragmentation. This is only applicable to IPv4. IPv6 does not include the bit as part of the specification. This parameter is ignored but not blocked when the address is IPv6.

The **no** form of this command allows packet fragmentation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.238 dod-label-distribution

dod-label-distribution

Syntax [**no**] **dod-label-distribution**

Context **[Tree]** (config>router>ldp>session-params>peer dod-label-distribution)

Full Context configure router ldp session-parameters peer dod-label-distribution

Description This command enables the use of the LDP Downstream-on-Demand (DoD) label distribution procedures.

When this option is enabled, LDP will set the A-bit in the Label Initialization message when the LDP session to the peer is established. When both peers set the A-bit, they will both use the DoD label distribution method over the LDP session (RFC 5036).

This feature can only be enabled on a link-level LDP session and therefore will apply to prefix labels only, not service labels.

As soon as the link LDP session comes up, the router will send a label request to its DoD peer for the FEC prefix corresponding to the peer's LSR-id. The DoD peer LSR-id is found in the basic Hello discovery messages the peer used to establish the Hello adjacency with the router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Similarly if the router and the directly attached DoD peer entered into extended discovery and established a targeted LDP session, the router will immediately send a label request for the FEC prefix corresponding to the peer's LSR-id found in the extended discovery messages.

However, the router will not advertise any <FEC, label> bindings, including the FEC of its own LSR-id, unless the DoD peer requested it using a Label Request Message.

When the DoD peer sends a label request for any FEC prefix, the router will reply with a <FEC, label> binding for that prefix if the FEC was already activated on the router. If not, the router replies with a notification message containing the status code of "no route." The router will not attempt in the latter case to send a label request to the next-hop for the FEC prefix when the LDP session to this next-hop uses the DoD label distribution mode. Hence the reference to single-hop LDP DoD procedures.

As soon as the link LDP session comes up, the router will send a label request to its DoD peer for the FEC prefix corresponding to the peer's LSR-id. The DoD peer LSR-id is found in the basic Hello discovery messages the peer used to establish the Hello adjacency with the router.

Similarly if the router and the directly attached DoD peer entered into extended discovery and established a targeted LDP session, the router immediately sends a label request for the FEC prefix corresponding to the peer's LSR-id found in the extended discovery messages. Peer address has to be the peer LSR-ID address.

The **no** form of this command disables the DoD label distribution with an LDP neighbor.

Default no dod-label-distribution

Platforms All

8.239 domain

domain

Syntax **domain** *name* [**type** {**l2-domain** | **vrf-gre** | **vrf-vxlan** | **l2-domain-irb**}] [**create**]
no domain *name*

Context **[Tree]** (config>service>vsd domain)

Full Context configure service vsd domain

Description This command configures a vsd-domain that can be associated to a VPLS or VPRN service.

Parameters *name* — Specifies the name of the vsd-domain. 32 characters maximum.

l2-domain — Assigns the l2-domain type to the domain. l2-domain-type domains must be associated to a VPLS service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vrf-gre — Assigns the vrf-gre type to the domain. vrf-gre-type domains must be associated to a VPRN service.

vrf-vxlan — Assigns the vrf-vxlan type to the domain. vrf-vxlan-type domains must be associated to a VPLS service.

l2-domain-irb — Assigns the l2-domain-irb type to the domain. l2-domain-irb-type domains must be associated to a VPLS service.

create — This keyword is mandatory when creating the vsd-domain.

Platforms All

domain

Syntax **domain** *domain-name* **expression** *expression*
no domain *domain-name*

Context **[Tree]** (config>app-assure>group>dns-ip-cache>dns-match domain)

Full Context configure application-assurance group dns-ip-cache dns-match domain

Description This command configures a domain expression to populate the DNS IP cache. Up to 32 domains can be configured.

Parameters *domain-name* — Specifies the name of the domain expression entry.

expression — Specifies a domain name expression string, up to 64 characters, used to define a pattern match. This domain expression uses the same syntax as the expressions used in app-filters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

domain

Syntax **domain** *domain-name* [**nat-group** *nat-group-id*] [**create**]
no domain *domain-name*

Context **[Tree]** (config>router>firewall domain)
[Tree] (config>service>vprn>firewall domain)

Full Context configure router firewall domain
configure service vprn firewall domain

Description This command configures a domain to contain firewall parameters. Each domain must be assigned to a NAT group where firewall functionality will be performed.

The **no** form of the command removes the domain.

Parameters **create** — Mandatory keyword used when creating the domain.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

domain-name — Specifies the name of the domain, up to 32 characters maximum.

nat-group-id — Specifies the ID of the NAT group where the firewall functionality will be performed.

Values 1 to 4

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

domain

Syntax **domain router** *router-name* **name** *domain-name*
no domain

Context **[Tree]** (config>service>nat>firewall-policy domain)

Full Context configure service nat firewall-policy domain

Description This command specifies a router and domain to which the firewall policy will be applied. All associated traffic must be part of the prefixes specified by this domain.

The **no** form of the command removes the domain association from the firewall policy.

Default no domain

Parameters *domain-name* — Specifies the name of the firewall domain in the specified router instance. 32 characters maximum.

router-name — Specifies the name of the router instance to use.

Values *router-name* | *vprn-svc-id*
router-name — “Base”, “management”
vprn-svc-id — 1 to 2147483647

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

domain

Syntax **domain** *md-index* [**format** {*format*}] [**name** *md-name*] **level** *level* [**admin-name** *admin-name*]
domain *md-index*
no domain *md-index*

Context **[Tree]** (config>eth-cfm domain)

Full Context configure eth-cfm domain

Description This command configures Connectivity Fault Management domain parameters.

The **no** form of the command removes the MD index parameters from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *md-index* — Specifies the Maintenance Domain (MD) index value.

Values 1 to 4294967295

format *format* — Specifies a value that represents the type (format).

Values dns, mac, none, string

dns: Specifies the DNS name format.

mac: X:X:X:X:X:X-u
X: [0..FF]h
u: [0..65535]d

none: Specifies a Y.1731 domain format and the only format allowed to execute Y.1731 specific functions.

string Specifies an ASCII string.

Default string

name *md-name* — Specifies a generic Maintenance Domain (MD) name.

Values 1 to 43 characters

level *level* — Specifies the integer identifying the maintenance domain level (MD Level). Higher numbers correspond to higher maintenance domains, those with the greatest physical reach, with the highest values for customers' CFM packets. Lower numbers correspond to lower maintenance domains, those with more limited physical reach, with the lowest values for single bridges or physical links.

Values 0 to 7

admin-name *admin-name* — Specifies a creation time required parameter that allows the operator to assign a name value to the domain container. This is used for information and migration purposes. This value cannot be modified without destroying the domain. If no **admin-name** exists, the configured *md-index* value will be converted into a character string to become the **admin-name** reference. When upgrading from a release that does not include the **admin-name** configuration option, the *md-index* will be converted into a character string. Once a value is assigned to this *admin-name* value it cannot be modified.

Values 1 to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

domain

Syntax **domain** *domain*
no domain

Context **[Tree]** (config>system>ptp domain)

Full Context configure system ptp domain

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the PTP domain.

Note: Some profiles may require a domain number in a restricted range. The operator must ensure that the value aligns with the expected range for the profile.

The domain cannot be changed unless PTP is shutdown. If the PTP profile setting is changed, the domain is changed to the default domain for the new PTP profile.

The **no** form of this command reverts to the default configuration. The default value is dependent upon the configured profile, as detailed below.

Default domain 0 — profile ieee1588-2008

domain 4 — profile g8265dot1-2010

domain 24 — profile g8275dot1-2014

Parameters *domain* — Specifies the PTP domain.

Values 0 to 255 for ieee1588-2008
0 to 255 for g8265dot1-2010
24 to 43 for g8275dot1-2014

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.240 domain-id

domain-id

Syntax **domain-id** *global-field*:*local-field*
no domain-id

Context **[Tree]** (config>service>vprn>bgp domain-id)
[Tree] (config>service>vprn>bgp-evpn>mpls domain-id)
[Tree] (config>service>vprn>bgp-evpn>srv6 domain-id)
[Tree] (config>service>vprn>bgp-ipvpn>mpls domain-id)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 domain-id)

Full Context configure service vprn bgp domain-id
configure service vprn bgp-evpn mpls domain-id
configure service vprn bgp-evpn segment-routing-v6 domain-id
configure service vprn bgp-ipvpn mpls domain-id
configure service vprn bgp-ipvpn segment-routing-v6 domain-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the domain ID that identifies the network from which a BGP route was received before that route is exported to a different neighbor. The domain ID is part of a domain, represented as *domain-id*:*isf_safi_type* in the D-PATH attribute, as described in *draft-ietf-bess-evpn-ipvpn-interworking*. The D-PATH attribute is modified by gateway routers, where a gateway is defined as a PE where a VPRN is instantiated, and that VPRN advertises or receives routes from multiple BGP owners (for example, EVPN-IFL and BGP-IPVPN) or multiple instances of the same owner (for example, VPRN with two BGP-IPVPN instances).

In the following example, consider that a gateway receives prefix P in an EVPN-IFL instance with the following D-PATH from neighbor N:

Seg Len=1 / 65000:1:128

If the router imports the route in VPRN-1, BGP-EVPN SRv6 instance with domain 65000:2, it readvertises it to its BGP-IPVPN MPLS instance as follows:

Seg Len=2 / 65000:2:70 / 65000:1:128

That is, the gateway prepends the local domain ID and family to the D-PATH before readvertising the route into a different instance.

The D-PATH attribute is used on gateways to detect loops (for received routes where the D-PATH contains a local domain ID) and to make BGP best-path selection decisions based on the D-PATH length (shorter D-PATH is preferred).

The **no** form of this command removes the configured domain ID.

Default no domain-id

Parameters *global-field:local-field* — Specifies the domain ID.

Values

4byte-GlobalAdminValue:2byte-LocalAdminValue

4byte-GlobalAdminValue:	0 to 4294967295
2byte-LocalAdminValue	0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service vprn bgp-ipvpn segment-routing-v6 domain-id

All

- configure service vprn bgp-evpn mpls domain-id
- configure service vprn bgp-ipvpn mpls domain-id
- configure service vprn bgp domain-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.241 domain-name

domain-name

Syntax **domain-name** *domain-name*
no domain-name

Context **[Tree]** (config>router>dhcp>server>pool>options domain-name)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options domain-name)
[Tree] (config>router>dhcp6>server>defaults>options domain-name)
[Tree] (config>router>dhcp6>server>pool>options domain-name)
[Tree] (config>router>dhcp6>server>pool>prefix>options domain-name)
[Tree] (config>service>vprn>dhcp>server>pool>options domain-name)
[Tree] (config>service>vprn>dhcp6>server>pool>options domain-name)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix>options domain-name)

Full Context configure router dhcp local-dhcp-server pool options domain-name
configure router dhcp6 local-dhcp-server defaults options domain-name
configure router dhcp6 local-dhcp-server pool options domain-name
configure router dhcp6 local-dhcp-server pool prefix options domain-name
configure service vprn dhcp local-dhcp-server pool options domain-name
configure service vprn dhcp6 local-dhcp-server pool options domain-name
configure service vprn dhcp6 local-dhcp-server pool prefix options domain-name
configure subscriber-mgmt local-user-db ipoe host options domain-name

Description This command configures the default domain for a DHCP client that the router uses to complete unqualified host names (without a dotted-decimal domain name).

The **no** form of this command removes the name from the configuration.

Parameters *domain-name* — Specifies the domain name for the client, up to 127 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn dhcp6 local-dhcp-server pool prefix options domain-name
- configure subscriber-mgmt local-user-db ipoe host options domain-name
- configure router dhcp local-dhcp-server pool options domain-name
- configure service vprn dhcp local-dhcp-server pool options domain-name
- configure service vprn dhcp6 local-dhcp-server pool options domain-name
- configure router dhcp6 local-dhcp-server pool options domain-name
- configure router dhcp6 local-dhcp-server pool prefix options domain-name

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure router dhcp6 local-dhcp-server defaults options domain-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.242 dot1p

dot1p

Syntax **dot1p** *dot1p-priority* [**fc** *fc-name*] [**priority** {**low** | **high**}]
no dot1p *dot1p-priority*

Context **[Tree]** (config>qos>sap-ingress dot1p)

Full Context configure qos sap-ingress dot1p

Description This command explicitly sets the forwarding class or subclass or enqueuing priority when a packet is marked with a *dot1p-priority* specified. Adding a dot1p rule on the policy forces packets that match the *dot1p-priority* specified to override the forwarding class and enqueuing priority based on the parameters included in the dot1p rule. When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueuing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueuing priority derived from earlier matches in the classification hierarchy.

The *dot1p-priority* is derived from the most significant three bits in the IEEE 802.1q or IEEE 802.1p header. The three dot1p bits define 8 Class-of-Service (CoS) values commonly used to map packets to per-hop QoS behavior.

The **no** form of this command removes the explicit dot1p classification rule from the SAP ingress policy. Removing the rule on the policy immediately removes the rule on all ingress SAPs using the policy.

Parameters *dot1p-priority* — This value is a required parameter that specifies the unique IEEE 802.1p value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 to 7

fc *fc-name* — Specifies the value given for the *fc-name* parameter must be one of the predefined forwarding classes in the system. Specifying the fc-name is optional. When a packet matches the rule, the forwarding class is only overridden when the **fc** *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority — This parameter overrides the default enqueuing priority for all packets received on an ingress SAP using this policy that match this rule. Specifying the priority is optional. When a packet matches the rule, the enqueuing priority is only overridden when the priority parameter is defined on the rule. If the packet matches and priority is not explicitly defined in the rule, the enqueuing priority is inherited based on previous rule matches.

Default Inherits the priority defined by the default-priority statement.

high — This parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **high** for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

low — This parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **low** for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Platforms All

dot1p

Syntax **dot1p** *dot1p-value* [*dot1p-mask*]
no dot1p

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match dot1p)

Full Context configure qos sap-ingress mac-criteria entry match dot1p

Description The IEEE 802.1p value to be used as the match criterion.

Use the **no** form of this command to remove the dot1p value as the match criterion.

Default no dot1p

Parameters *dot1p-value* — Specifies the IEEE 802.1p value in decimal.

Values 0 to 7

dot1pmask — This 3-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	D	4
Hexadecimal	0xH	0x4
Binary	0bBBB	0b100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To select a range from 4 up to 7, specify *p-value* of 4 and a *mask* of 0b100 for value and mask.

Values 0 to 7 (decimal hex or binary)

Default 7

Platforms All

dot1p

Syntax **dot1p** *dot1p-value* [**fc** *fc-name*] [**profile** {**in** | **out** | **use-de** | **exceed** | **inplus**}]
no dot1p *dot1p-value*

Context **[Tree]** (config>qos>sap-egress dot1p)

Full Context configure qos sap-egress dot1p

Description This command defines a specific dot1p value that must be matched to perform the associated reclassification actions. If an egress packet on the SAP matches the specified dot1p value, the forwarding class or profile may be overridden. By default, the forwarding class and profile of the packet is derived from ingress classification and profiling functions.

The dot1p priority is derived from the most significant three bits in the IEEE 802.1q or IEEE 802.1p header. The three dot1p bits define 8 Class-of-Service (CoS) values commonly used to map packets to per-hop QoS behavior.

The reclassification actions from a dot1p reclassification rule may be overridden by a DSCP, IP precedence, or IP flow matching event.

The **fc** keyword is optional. When specified, the egress classification rule will overwrite the forwarding class derived from ingress. The new forwarding class is used for egress remarking and queue mapping decisions. If a DSCP, IP precedence, IPv6 criteria, or IP criteria match occurs after the dot1p match, the new forwarding class may be overridden by the higher priority match actions. If the higher priority match actions do not specify a new FC, the FC from the dot1p match will be used.

The **profile** keyword is optional. When specified, the egress classification rule will overwrite the profile of the packet derived from ingress. The new profile value is used for egress remarking and queue congestion behavior. If a DSCP, IP precedence, IPv6 criteria, or IP criteria match occurs after the dot1p match, the new profile may be overridden by the higher priority match actions. If the higher priority match actions do not specify a new profile, the profile from the dot1p match will be used.

The **no** form of this command removes the reclassification rule from the SAP egress QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *dot1p-value* — This value is a required parameter that specifies the unique IEEE 802.1p value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 to 7

fc *fc-name* — Specifies the value given for the *fc-name* parameter must be one of the predefined forwarding classes in the system. Specifying the FC name is optional. When a packet matches the rule, the forwarding class is only overridden when the **fc** *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

Default None

profile {in | out | use-de | exceed | inplus} — Specifies the profile reclassification action is optional. When specified, packets matching the dot1p value will be explicitly reclassified to the profile specified regardless of the ingress profiling decision. The explicit profile reclassification may be overwritten by a DSCP, IP precedence, IPv6 criteria, or IP criteria reclassification match. To remove the profile reclassification action for the specified dotp1 value, the **dot1p** command must be re-executed without the profile reclassification action defined.

Values **in** — Specifies that any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out — Specifies that any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

use-de — Specifies that the DE bit is used to determine the profile of the packet (in-profile is used when DE = 0 and out-of-profile is used when DE = 1).

exceed — Specifies that any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

inplus — Specifies that any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

Platforms All

dot1p

Syntax **dot1p** {*dot1p-value* | **in-profile** *dot1p-value* **out-profile** *dot1p-value* [**exceed-profile** *dot1p-value*]}

no dot1p

Context **[Tree]** (config>qos>sap-egress>fc dot1p)

Full Context configure qos sap-egress fc dot1p

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command explicitly defines the egress IEEE 802.1p (dot1p) bits marking for *fc-name*. When the marking is set, all packets of *fc-name* that have either an IEEE 802.1q or IEEE 802.1p encapsulation use the explicitly defined *dot1p-value*. If the egress packets for *fc-name* are not IEEE 802.1q or IEEE 802.1p encapsulated, the dot1p command has no effect.

The optional **in-profile** *dot1p-value* **out-profile** *dot1p-value* [**exceed-profile** *dot1p-value*] parameters added to the existing **dot1p** command adds the capability to mark on an egress SAP the in, out, and exceed-profile status via a certain dot1p combination, similarly with the DE options. All inplus-profile traffic is marked with the same value as in-profile traffic.

When the **in-profile** keyword is added, the **out-profile** keyword must be specified; however, **exceed-profile** is optional. If the optional **exceed-profile** *dot1p-value* is not included, any exceed-profile traffic will be marked with the same dot1p value as configured for the out-of-profile traffic.

The command with the additional structure may be used on the SAP when the internal in, out, and exceed-profile status needs to be communicated to an access network or customer device that does not support the DE bit.

When these commands are used, the DE bit or the equivalent field is left unchanged by the egress processing if a tag exists. If a new tag is added, the related DE bit is set to 0.

When the previous command (**dot1p** *dot1p-value*) is used without the new structure, it means that the dot1p value is used for the entire forwarding class, as it did before. The two versions of the command are mutually exclusive.

The in-profile or out-of-profile/exceed-profile status may be indicated via the DE bit setting if the **de-mark** command is used. The DE value used for exceed-profile is the same as that used for out-of-profile.

In the PBB case, for a Backbone SAP (B-SAP) and for packets originated from a local I-VPLS/PBB-Epipe, the command dictates the marking of the dot1p bits for both the BVID and ITAG.

The commands **dot1p-inner** and **dot1p-outer** take precedence over the **dot1p** command if both are specified in the same policy.

The **no** form of this command sets the IEEE 802.1p or IEEE 802.1q priority bits to 0.

Default no dot1p

Parameters **in-profile** *dot1p-value* — Specifies the 802.1p value to set for in-profile frames in this forwarding class.

Values 0 to 7

out-profile *dot1p-value* — Specifies the 802.1p value to set for out-profile frames in this forwarding class.

Values 0 to 7

exceed-profile *dot1p-value* — Specifies the 802.1p value to set for exceed-profile frames in this forwarding class.

Values 0 to 7

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

dot1p

Syntax **dot1p** *dot1p-priority* **fc** *fc-name* **profile** {**in** | **out** | **use-de**}
no dot1p

Context **[Tree]** (config>qos>network>ingress dot1p)

Full Context configure qos network ingress dot1p

Description This command explicitly sets the forwarding class or enqueuing priority and profile of the packet when a packet is marked with a *dot1p-priority* specified. Adding a dot1p rule on the policy forces packets that match the *dot1p-priority* specified to override and be assigned to the forwarding class and enqueuing priority and profile of the packet, based on the parameters included in the dot1p rule. When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueuing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueuing priority derived from earlier matches in the classification hierarchy.

The *dot1p-priority* is derived from the most significant three bits in the IEEE 802.1q or IEEE 802.1p header. The three dot1p bits define 8 Class-of-Service (CoS) values commonly used to map packets to per-hop Quality of Service (QoS) behavior.

The **no** form of this command removes the explicit dot1p classification rule from the policy. Removing the rule on the policy immediately removes the rule on all ingress SAPs using the policy.

Parameters *dot1p-priority* — This value is a required parameter that specifies the unique IEEE 802.1p value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 to 7

fc-name — Specifies the value given for the *fc-name* parameter must be one of the predefined forwarding classes in the system. Specifying the *fc-name* is optional. When a packet matches the rule, the forwarding class is only overridden when the **fc** *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

Values be, l2, af, l1, h2, ef, h1, nc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

profile {in | out | use-de} — All packets that are assigned to this forwarding class will be considered in-profile or out-of-profile based on this command or will use the DE bit to determine the profile of the packets (in-profile is used when DE = 0 and out-of-profile is used when DE = 1). In case of congestion, the in-profile packets are preferentially queued over the out-of-profile packets.

Platforms All

dot1p

Syntax **dot1p** *dot1p-priority*
no dot1p

Context **[Tree]** (config>qos>network>egress>fc dot1p)

Full Context configure qos network egress fc dot1p

Description This command is used whenever the dot1p bits are set to a common value regardless of the internal profile of the packets. Although it is not mandatory, this command should be used in combination with the **de-mark** command to enable the marking of the DE bit according to the internal profile of the packet.

This command acts as a shortcut for configuring the two existing commands with the same dot1p priority.

The **dot1p** *dot1p-priority* command is saved in the configuration as **dot1p-in-profile** *dot1p-priority* and **dot1p-out-profile** *dot1p-priority*. The inplus-profile traffic is marked with the same value as in-profile traffic. The exceed-profile traffic is marked with the same value as out-of-profile traffic.

Platforms All

dot1p

Syntax **dot1p** *dot1p-value* [*dot1p-mask*]
no dot1p

Context **[Tree]** (config>filter>mac-filter>entry>match dot1p)

Full Context configure filter mac-filter entry match dot1p

Description Configures an IEEE 802.1p value or range to be used as a MAC filter match criterion.

When a frame is missing the 802.1p bits, specifying an dot1p match criterion will fail for the frame and result in a non-match for the MAC filter entry.

The **no** form of the command removes the criterion from the match entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Egress **dot1p** value matching will only match if the customer payload contains the 802.1p bits. For example, if a packet ingresses on a null encapsulated SAP and the customer packet is IEEE 802.1Q or 802.1p tagged, the 802.1p bits will be present for a match evaluation. On the other hand, if a customer tagged frame is received on a dot1p encapsulated SAP, the tag will be stripped on ingress and there will be no 802.1p bits for a MAC filter match evaluation; in this case, any filter entry with a dot1p match criterion specified will fail.

Default no dot1p

Parameters *dot1p-value* — Specifies the IEEE 802.1p value in decimal.

Values 0 to 7

dot1p-mask — Specifies a 3-bit mask that can be configured using the decimal integer, hexadecimal or binary format.

Table 43 **dot1p-mask Formats**

Format Style	Format Syntax	Example
Decimal	D	4
Hexadecimal	0xH	0x4
Binary	0bBBB	0b100

To select a range from 4 up to 7 specify *dot1p-value* of 4 and a *dot1p-mask* of 0b100 for value and mask.

Default **7 (decimal)**

Values 1 to 7 (decimal)

Platforms All

dot1p

Syntax **dot1p** *dot1p-value* [*dot1p-mask*]

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match dot1p)

Full Context configure system security management-access-filter mac-filter entry match dot1p

Description This command configures Dot1p match conditions.

Table 44 **Management Access Filter dot1p Mask Format**

Format Style	Format Syntax	Example
Decimal	D	4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 44 **Management Access Filter dot1p Mask Format**

Format Style	Format Syntax	Example
Hexadecimal	0xH	0x4
Binary	0bBBB	0b100

Parameters *dot1p-value* — Specifies the IEEE 802.1p value in decimal.

Values 0 to 7

mask — Specifies the 3-bit mask can be configured using the following formats.

Platforms All

dot1p

Syntax **dot1p** *dot1p-name*
no dot1p

Context **[Tree]** (config>test-oam>icmp>ping-template dot1p)

Full Context configure test-oam icmp ping-template dot1p

Description This command specifies values of the outer and inner dot1p bits for the VLAN when dot1q or qinq encapsulation is used. This field is not exposed to egress QoS policies.

The **no** form of this command reverts to the default value.

Default dot1p 7

Parameters *dot1p-name* — Specifies the IEEE 802.1p value in decimal format.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.243 dot1p-in-profile

dot1p-in-profile

Syntax **dot1p-in-profile** *dot1p-priority*
no dot1p-in-profile

Context **[Tree]** (config>qos>network>egress>fc dot1p-in-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos network egress fc dot1p-in-profile

Description This command specifies dot1p in-profile mappings. The inplus-profile traffic is marked with the same value as in-profile traffic.

The **no** form of this command resets the configuration to the default in-profile *dot1p-priority* setting for *policy-id* 1.

Parameters *dot1p-priority* — Specifies the unique IEEE 802.1p value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 to 7

Platforms All

8.244 dot1p-inner

dot1p-inner

Syntax **dot1p-inner** {*dot1p-value* | **in-profile** *dot1p-value* **out-profile** *dot1p-value*}
no dot1p-inner

Context **[Tree]** (config>qos>sap-egress>fc dot1p-inner)

Full Context configure qos sap-egress fc dot1p-inner

Description This command explicitly defines the egress inner VLAN tag IEEE 802.1p (dot1p) bits marking for *fc-name*. When the marking is set, all packets of *fc-name* that have either an inner IEEE 802.1q or IEEE 802.1p encapsulation on a qinq SAP will use the explicitly defined *dot1p-value*. If the egress packets for *fc-name* are not IEEE 802.1q or IEEE 802.1p qinq encapsulated, this command has no effect.

The optional **in-profile** | *dot1p-value* **out-profile** *dot1p-value* parameters on the **dot1p-inner** command add the capability to mark the in-profile and out-of-profile status on an egress qinq SAP. The command with the additional parameters may be used on the SAP when the internal in-profile and out-of-profile status needs to be communicated to an access network or customer device that does not support the DE bit. When the in-profile keyword is added, the rest of the structure must be specified. All inplus-profile traffic is marked with the same value as in-profile traffic and all exceed-profile traffic is marked with the same value as out-of-profile traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When these commands are used, the DE bit or the equivalent field is left unchanged by the egress processing if an inner tag exists. If a new inner tag is added, the related DE bit is set to 0. The inplus/in or out/exceed-profile status may be indicated via the setting of the DE bit setting if the **de-mark(-inner)** command is used.

The two versions of the command (with and without parameters) are mutually exclusive.

This command takes precedence over the **dot1p** command if both are specified in the same policy, and over the default action where the marking is taken from a packet received at ingress.

The configuration of **qinq-mark-top-only** under the SAP egress takes precedence over the use of the **dot1p-inner** in the policy; that is, the inner VLAN tag is not remarked when **qinq-mark-top-only** is configured (the marking used for the inner VLAN tag is based on the current default, which is governed by the marking of the packet received at the ingress to the system).

The **no** form of the command sets the inner IEEE 802.1p or IEEE 802.1q priority bits to 0.

Remarking the inner dot1p is not supported based on the profile result of egress policing.

Default no dot1p-inner

Parameters *dot1p-value* — Specifies the 802.1p value to set for in-profile frames in this forwarding class.

Values 0 to 7

in-profile *dot1p-value* — Specifies the 802.1p value to set for in-profile frames in this forwarding class.

Values 0 to 7

out-profile *dot1p-value* — Specifies the 802.1p value to set for out-of-profile frames in this forwarding class.

Values 0 to 7

Platforms All

8.245 dot1p-out-profile

dot1p-out-profile

Syntax **dot1p-out-profile** *dot1p-priority*
no dot1p-out-profile

Context **[Tree]** (config>qos>network>egress>fc dot1p-out-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos network egress fc dot1p-out-profile

Description This command specifies dot1p out-of-profile mappings.

The exceed-profile traffic is marked with the same value as out-of-profile traffic.

The **no** form of this command resets the configuration to the default out-profile *dot1p-priority* setting for *policy-id* 1.

Parameters *dot1p-priority* — Specifies the unique IEEE 802.1p value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 to 7

Platforms All

8.246 dot1p-outer

dot1p-outer

Syntax **dot1p-outer** {*dot1p-value* | **in-profile** *dot1p-value* **out-profile** *dot1p-value* [**exceed-profile** *dot1p-value*]}
no dot1p-outer

Context **[Tree]** (config>qos>sap-egress>fc dot1p-outer)

Full Context configure qos sap-egress fc dot1p-outer

Description This command explicitly defines the egress outer or single VLAN tag IEEE 802.1p (dot1p) bits marking for *fc-name*. When the marking is set, all packets of fc-name that have either an outer or single IEEE 802.1q or IEEE 802.1p encapsulation on a qinq or a dot1p SAP, respectively, will use the explicitly defined *dot1p-value*. If the egress packets for *fc-name* are not IEEE 802.1q or IEEE 802.1p encapsulated, this command has no effect.

The optional **in-profile** *dot1p-value* **out-profile** *dot1p-value* [**exceed-profile** *dot1p-value*] parameters on the dot1p-outer command add the capability to mark the in, out, and exceed-profile status on an egress qinq or dot1p SAP. The command with the additional parameters may be used on the SAP when the internal in, out, and exceed-profile status needs to be communicated to an access network or customer device that does not support the DE bit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **in-profile** keyword is added, the **out-profile** keyword must be specified; however, **exceed-profile** is optional. If the optional **exceed-profile** *dot1p-value* is not included, any exceed-profile traffic will be marked with the same dot1p value as configured for the out-of-profile traffic. All inplus-profile traffic is marked with the same value as in-profile traffic.

When these commands are used, the DE bit or the equivalent field is left unchanged by the egress processing if a single or outer tag exists. If a new tag is added, the related DE bit is set to 0. The in, out, or exceed-profile status may be indicated via the setting of the DE bit setting if the **de-mark(-outer)** command is used. The DE value used for inplus is the same as that used for in-profile and the one used for exceed-profile is the same as that used for out of profile.

In the PBB case, for a Backbone SAP (B-SAP) and for packets originated from a local I-VPLS/ PBB-Epipe, the command dictates the marking of the dot1p bits for both the BVID and ITAG.

The two versions of the command (with and without parameters) are mutually exclusive.

This command takes precedence over the **dot1p** command if both are specified in the same policy, and over the default action where the marking is taken from a packet received at ingress.

The **no** form of the command sets the IEEE 802.1p or IEEE 802.1q priority bits to 0.

Default no dot1p-outer

Parameters *dot1p-value* — Specifies the 802.1p value to set for in-profile frames in this forwarding class.

Values 0 to 7

in-profile *dot1p-value* — Specifies the 802.1p value to set for in-profile frames in this forwarding class.

Values 0 to 7

out-profile *dot1p-value* — Specifies the 802.1p value to set for out-of-profile frames in this forwarding class.

Values 0 to 7

exceed-profile *dot1p-value* — Specifies the 802.1p value to set for exceed-profile frames in this forwarding class.

Values 0 to 7

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.247 dot1q

dot1q

Syntax **dot1q**

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg dot1q)

Full Context configure service system bgp-evpn ethernet-segment dot1q

Description This command creates the dot1q context for q-tag additions to the port or LAG virtual ES.

Platforms All

dot1q

Syntax **dot1q**

Context **[Tree]** (config>test-oam>build-packet>header dot1q)
[Tree] (debug>oam>build-packet>packet>field-override>header dot1q)

Full Context configure test-oam build-packet header dot1q
debug oam build-packet packet field-override header dot1q

Description This command creates a Dot1Q header and enables the context to define the associated parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.248 dot1q-etype

dot1q-etype

Syntax **dot1q-etype** *value*
no dot1q-etype

Context **[Tree]** (config>port>ethernet dot1q-etype)

Full Context configure port ethernet dot1q-etype

Description This command specifies the Ethertype expected when the port's encapsulation type is dot1q. Dot1q encapsulation is supported only on Ethernet interfaces.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the Ethertype to expect, in either decimal or hex.

Values 1536 to 65535 (0x0600 to 0xffff)

Default If the encap-type is dot1p, then the default is 0x8100. If the encap-type is qinq, then the default is 0x8100.

Platforms All

dot1q-etype

Syntax **dot1q-etype** *dot1q-etype*
no dot1q-etype

Context **[Tree]** (config>pw-port dot1q-etype)

Full Context configure pw-port dot1q-etype

Description This command configures the Dot1q Ethertype on the PW port. The PW port is used to extract a customer's Ethernet traffic that is transported in a tunnel over an IP/MPLS network. The **Dot1q-etype** represents the first two bytes (TPID) in the 802.1Q header of a single-tagged Ethernet frame or the inner 802.1Q header of the double-tagged Ethernet frame inside the tunnel.

The **no** form of this command removes the configuration.

Parameters *dot1q-etype* — The value for the **dot1q-etype** field, in hexadecimal format.

Values 0x0600..0xFFFF

Default 0x8100

Platforms All

8.249 dot1x

dot1x

Syntax **dot1x**

Context **[Tree]** (config>port>ethernet dot1x)

Full Context configure port ethernet dot1x

Description This command enables access to the context to configure port-specific 802.1x authentication attributes. This context can only be used when configuring a Fast Ethernet, Gigabit or 10-Gb Ethernet LAN ports on an appropriate MDA.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

dot1x

Syntax [**no**] **dot1x**

Context **[Tree]** (config>system>security dot1x)

Full Context configure system security dot1x

Description This command creates the context to configure 802.1x network access control on the router.

The **no** form of this command removes the 802.1x configuration.

Platforms All

8.250 down

down

Syntax **down ip** *seconds* [**init-only**]
no down ip
down ipv6 *seconds* [**init-only**]
no down ipv6

Context **[Tree]** (config>router>if>hold-time down)
[Tree] (config>service>ies>if>hold-time down)
[Tree] (config>service>ies>sub-if>hold-time down)
[Tree] (config>service>ies>red-if>hold-time down)
[Tree] (config>service>vpls>if>hold-time down)
[Tree] (config>service>vprn>if>hold-time down)
[Tree] (config>service>vprn>nw-if>hold-time down)
[Tree] (config>service>vprn>red-if>hold-time down)
[Tree] (config>service>vprn>sub-if>hold-time down)

Full Context configure router interface hold-time down
configure service ies interface hold-time down
configure service ies redundant-interface hold-time down
configure service ies subscriber-interface hold-time down
configure service vpls interface hold-time down
configure service vprn interface hold-time down
configure service vprn network-interface hold-time down
configure service vprn redundant-interface hold-time down
configure service vprn subscriber-interface hold-time down

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command causes a delay in the activation of the associated IP interface by the specified number of seconds. The delay is invoked whenever the system attempts to bring the associated IP interface up, unless the **init-only** option is configured. If the **init-only** option is configured, the delay is only applied when the IP interface is first configured or after a system reboot.

The **no** form of this command removes the command from the active configuration and removes the delay in activating the associated IP interface. If the configuration is removed during a delay period, the currently running delay will continue until it completes.

Default no down ip

Parameters *seconds* — The time delay, in seconds, to make the interface operational.

Values 1 to 1200

init-only — Specifies that the **down** delay is only applied when the interface is configured or after a reboot.

Values 1 to 1200

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface hold-time down
- configure service ies redundant-interface hold-time down
- configure service vprn redundant-interface hold-time down
- configure service ies subscriber-interface hold-time down

All

- configure service vprn network-interface hold-time down
- configure router interface hold-time down
- configure service ies interface hold-time down
- configure service vpls interface hold-time down
- configure service vprn interface hold-time down

8.251 down-count

down-count

Syntax **down-count** *down-count*
no down-count

Context **[Tree]** (config>port>sonet-sdh>path>cisco-hdlc down-count)
[Tree] (config>port>tdm>ds1>channel-group>cisco-hdlc down-count)
[Tree] (config>port>tdm>ds3>cisco-hdlc down-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>port>tdm>e1>channel-group>cisco-hdlc down-count)
[Tree] (config>port>tdm>e3>cisco-hdlc down-count)

Full Context configure port sonet-sdh path cisco-hdlc down-count
configure port tdm ds1 channel-group cisco-hdlc down-count
configure port tdm ds3 cisco-hdlc down-count
configure port tdm e1 channel-group cisco-hdlc down-count
configure port tdm e3 cisco-hdlc down-count

Description This command configures the number of keepalive intervals that must pass without receiving a keepalive packet before the link is declared down. It is expected that the nodes at the two endpoints of the cHDLC link are provisioned with the same values.

Default down-count 3

Parameters *down-count* — Specifies the number of keep alive intervals that must pass without receiving a keep alive packet before the link is declared down.

Values 3 to 16

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path cisco-hdlc down-count

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 cisco-hdlc down-count
- configure port tdm ds3 cisco-hdlc down-count
- configure port tdm ds1 channel-group cisco-hdlc down-count
- configure port tdm e1 channel-group cisco-hdlc down-count

8.252 down-link

down-link

Syntax **down-link gbr** *rate* **mbr** *rate*
no down-link

Context [Tree] (config>subscr-mgmt>gtp>peer-profile>ggsn>qos down-link)
[Tree] (config>subscr-mgmt>gtp>peer-profile>pgw>qos down-link)
[Tree] (config>subscr-mgmt>gtp>peer-profile>mme>qos down-link)

Full Context configure subscriber-mgmt gtp peer-profile ggsn qos down-link
configure subscriber-mgmt gtp peer-profile mme qos down-link
configure subscriber-mgmt gtp peer-profile pgw qos down-link

Description This command configures the down-link bitrate in kb/s to be used in the GTP messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Default down-link gbr 2000 mbr 2000

down-link gbr 2000 mbr 2000 - for ggsn

down-link gbr 0 mbr 0 - for mme and pgw

Parameters **gbr** *rate* — Specifies the downlink Guaranteed Bit Rate (GBR) to be used in the GTP messages as QOS IE (GTPv1) or Bearer QOS (GTPv2).

mbr *rate* — Specifies the downlink Maximum Bit Rate (MBR) to be used in the GTP messages as QOS IE (GTPv1) or Bearer QOS (GTPv2).

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.253 down-on-internal-error

down-on-internal-error

Syntax **down-on-internal-error** [**tx-disable**]
no down-on-internal-error

Context **[Tree]** (config>port>ethernet down-on-internal-error)

Full Context configure port ethernet down-on-internal-error

Description This command configures the system to bring a port operationally down in the event the system has detected internal MAC transmit errors (Int MAC Tx Errs).

Default no down-on-internal-error

Parameters **tx-disable** — Specifies that the laser should be disabled if an internal MAC transmit error is encountered. When used, this option requires that the operator explicitly cycle the admin state of the port to clear the error and re-enable the laser.

Platforms All

8.254 down-on-peer-tldp-pw-status-faults

down-on-peer-tldp-pw-status-faults

Syntax **down-on-peer-tldp-pw-status-faults**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no down-on-peer-tldp-pw-status-faults

Context **[Tree]** (config>service>epipe>pw-port down-on-peer-tldp-pw-status-faults)

Full Context configure service epipe pw-port down-on-peer-tldp-pw-status-faults

Description This command enables the PW port configured on an Epipe to go locally operationally down if any of the following status bits are received on a mate spoke-SDP across an FPE:

- 0x00000001 - Pseudowire Not Forwarding
- 0x00000002 - Local Attachment Circuit (ingress) Receive Fault
- 0x00000004 - Local Attachment Circuit (egress) Transmit Fault
- 0x00000008 - Local PSN-facing PW (ingress) Receive Fault
- 0x00000010 - Local PSN-facing PW (egress) Transmit Fault

The **no** form of the command specifies that the mate PW status fault bits are not taken into account in the operational state of the PW port.

Default no down-on-peer-tldp-pw-status-faults

Platforms All

8.255 down-threshold

down-threshold

Syntax **down-threshold** *percent-change* [**bw** *absolute-change*]

Context **[Tree]** (config>router>rsvp>dbw-accounting down-threshold)

Full Context configure router rsvp dbw-accounting down-threshold

Description This command sets the minimum change (in percent of the latest advertised value) above which a decrease in Maximum Reservable Link Bandwidth (MRLB) (IS-IS TE sub-TLV 10) or Maximum Reservable Bandwidth (MRB) (OSPF TE sub-TLV 7) triggers an IGP-TE update. This configuration only applies to a change in MRLB or MRB caused by dark bandwidth. Other events affecting MRLB/MRB (such as the change of the subscription factor or the loss of link in a LAG over which the RSVP interface is defined) trigger an immediate TE update, regardless of the importance of the impact.

Optionally, the threshold can also be expressed as an absolute value. In this case, the evaluation of the change is made using the percent change and the absolute change. An IGP-TE update is sent if both of these thresholds are crossed. Changing this parameter in the course of dark bandwidth accounting does not affect the accounting cycle.

Default down-threshold 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent-change* — Specifies the minimum decrease in MRLB/MRB, expressed in percent.

Values 0 to 100

absolute-change — Specifies the minimum decrease in MRLB/MRB, expressed in Mb/s.

Values 0 to 1000000

8.256 down-timeout

down-timeout

Syntax [**no**] **down-timeout**

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>health-check down-timeout)

Full Context configure aaa radius-server-policy servers health-check down-timeout

Description This command determines the interval to wait for a RADIUS reply message from the RADIUS server before a RADIUS server is declared out-of-service. By default, the value of the down-timeout is the number of retries multiplied by the timeout interval. Each host will use the configured timeout and retry value under the AAA RADIUS server policy.

timeout refers to the waiting period before the next retry attempt.

retry refers the number of times the host will attempt to contact the RADIUS server.

If a RADIUS server is declared out-of-service, the host pending retry attempts will move on to the next RADIUS server.

The **no** form of this command reverts to the default.

Parameters *minutes* — Specifies the timer to wait, in minutes, before declaring the RADIUS server that is down.

Values 1 to 5

seconds — Specifies the timer to wait, in seconds, before declaring the RADIUS server that is down.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.257 down-when-looped

down-when-looped

Syntax **down-when-looped**

Context **[Tree]** (config>port>ethernet down-when-looped)

Full Context configure port ethernet down-when-looped

Description This command configures Ethernet loop detection attributes.

Platforms All

8.258 downlink

downlink

Syntax **downlink aggregate-rate**
downlink arbiter *arbiter-name*
downlink policer *policer-id*
downlink queue *queue-id*
downlink scheduler *scheduler-name*
no downlink

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn>ambr-qos-mapping downlink)

Full Context configure subscriber-mgmt gtp apn-policy apn ambr-qos-mapping downlink

Description When enabled, the downlink rate in the APN-AMBR IE in an incoming GTP message is interpreted as a rate override for the specified egress QoS object. For queues and policers, the PIR is overridden.

This override uses standard SR OS QoS overrides. Therefore, a subsequent Gx/ RADIUS-based override removes this override.

The **no** form of this command disables the override mechanism.

Default no downlink

Parameters **aggregate-rate** — Specifies the aggregate rate.

arbiter-name — Specifies the name of the arbiter to be overridden, up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer-id — Specifies the ID of the policer to be overridden.

Values 1 to 63

queue-id — Specifies the ID of the queue to be overridden.

Values 1 to 8

scheduler-name — Specifies the name of the scheduler to be overridden, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.259 downlink-mbr-gbr

downlink-mbr-gbr

Syntax **downlink-mbr-gbr aggregate-rate**
downlink-mbr-gbr arbiter *arbiter-name*
downlink-mbr-gbr policer *policer-id*
downlink-mbr-gbr queue *queue-id*
downlink-mbr-gbr scheduler *scheduler-name*
no downlink-mbr-gbr

Context **[Tree]** (config>subscr-mgmt>sla-prof>pfcp>seq downlink-mbr-gbr)

Full Context configure subscriber-mgmt sla-profile pfcp-mappings session-qer downlink-mbr-gbr

Description This command configures the downlink MBR/GBR to QoS override mapping.

The **no** form of the command disables the downlink MBR/GBR mapping.

Default no downlink-mbr-gbr

Parameters **aggregate-rate** — Maps the MBR/GBR to a rate override for the aggregate rate.

arbiter-name — Specifies the arbiter target of the MBR/GBR override. The arbiter name can be up to 32 characters.

policer-id — Specifies the policer ID target of the MBR/GBR override.

Values 1 to 63

queue-id — Specifies the queue ID target of the MBR/GBR override.

Values 1 to 8

scheduler-name — Specifies the scheduler name target of the MBR/GBR override. The scheduler name can be up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.260 download-interval

download-interval

Syntax **download-interval** *minutes*
no download-interval

Context **[Tree]** (config>aaa>route-downloader download-interval)

Full Context configure aaa route-downloader download-interval

Description This command sets the time interval, in minutes, that the system waits for between two consecutive runs of the route-download process. The time is counted from the start-time of the run, thus, if an route-download process is still ongoing by the time the timer expires, the process will restart from count=1.

The **no** form of this command reverts to the default value.

Default download-interval 720

Parameters *minutes* — Specifies the time interval, in minutes, between the start of the last route downloader run and the start of the next route downloader run.

Values 1 to 1440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.261 downstream-ip-filter

downstream-ip-filter

Syntax **downstream-ip-filter** *filter-id*
no downstream-ip-filter

Context **[Tree]** (config>service>vprn>nat>inside downstream-ip-filter)

Full Context configure service vprn nat inside downstream-ip-filter

Description This command assigns an IPv4 filter policy to the downstream NAT interface. This filter is applied to downstream traffic after the NAT function is applied but before it enters the inside VPRN instance.

The **no** form of the command removes the filter from the configuration.

Default no downstream-ip-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *filter-id* — Specifies an existing IPv4 filter policy. Values can be expressed either as a decimal integer or as an ASCII string of up to 64 characters.

Values 1 to 65535, or ASCII string of up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

downstream-ip-filter

Syntax **downstream-ip-filter** *filter-id*
no downstream-ip-filter

Context **[Tree]** (config>router>nat>outside downstream-ip-filter)
[Tree] (config>service>vprn>nat>outside downstream-ip-filter)

Full Context configure router nat outside downstream-ip-filter
configure service vprn nat outside downstream-ip-filter

Description This command specifies a filter to apply to the downstream traffic after routing in the outside virtual router instance and before the NAT function; it is useful for traffic that bypasses the egress filters applied in the inside virtual router instance, such as DS-Lite traffic.

The **no** form of the command removes the filter from the configuration.

Default no downstream-ip-filter

Parameters *filter-id* — Specifies a filter up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.262 downstream-ipv6-filter

downstream-ipv6-filter

Syntax **downstream-ipv6-filter** *filter-id*
no downstream-ipv6-filter

Context **[Tree]** (config>router>nat>outside downstream-ipv6-filter)
[Tree] (config>service>vprn>nat>outside downstream-ipv6-filter)

Full Context configure router nat outside downstream-ipv6-filter
configure service vprn nat outside downstream-ipv6-filter

Description This command configures the ipv6-filter for downstream traffic. This filter is applied to downstream traffic after it leaves the outside virtual router instance but before the NAT function is applied. This is useful for shared v6 filters that apply to all v6 DSM hosts.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the filter from the configuration.

Default no downstream-ipv6-filter

Parameters *filter-id* — Specifies an IPv6 filter up to 64 characters in length.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.263 downstream-map-tlv

downstream-map-tlv

Syntax **downstream-map-tlv** *downstream-map-tlv*
no downstream-map-tlv

Context **[Tree]** (config>saa>test>type-multi-line>lsp-trace>sr-policy downstream-map-tlv)

Full Context configure saa test type-multi-line lsp-trace sr-policy downstream-map-tlv

Description This command configures the downstream mapping TLV that provides a mechanism for the sender and responder nodes to exchange and validate interface and label stack information for each downstream hop in the path of the LDP FEC an RSVP LSP, or a BGP IPv4 or IPv6 label route.

The following downstream mapping TLVs are supported: the original Downstream Mapping (DSMAP) TLV defined in RFC 4379 (obsoleted by RFC 8029) and the Downstream Detailed Mapping (DDMAP) TLV defined in RFC 6424.

The **no** form of this command removes the configuration.

Parameters *downstream-map-tlv* — Specifies which format of the downstream mapping TLV to use in the LSP trace packet. The DSMAP TLV is the original format in RFC 4379 (obsoleted by RFC 8029). The DDMAP is the new enhanced format specified in RFC 6424. The user can also choose not to include the downstream mapping TLV by entering the value none. When **lsp-trace** is used on a MPLS-TP LSP (static option), it can only be executed if the control-channel is set to none. In addition, the DSMAP/DDMAP TLV is only included in the echo request message if the egress interface is either a numbered IP interface or an unnumbered IP interface. The TLV is not included if the egress interface is of type **unnumbered-mpls-tp**.

Values ddmap: Sends a detailed downstream mapping TLV.
dsmap: Sends a downstream mapping TLV.
none: No mapping TLV is sent.

Default Inherited from global configuration of downstream mapping TLV in option **mpls-echo-request-downstream-map {dsmap | ddmap}**.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.264 dpd

dpd

Syntax **dpd** [**interval** *interval*] [**max-retries** *max-retries*] [**reply-only**]
no dpd

Context **[Tree]** (config>ipsec>ike-policy dpd)

Full Context configure ipsec ike-policy dpd

Description This command controls the dead peer detection mechanism.

The **no** form of this command removes the parameters from the configuration.

Default no dpd

Parameters *interval* — Specifies the DPD interval, in seconds. Since more time is necessary to determine if there is incoming traffic, the actual time needed to bring down the tunnel is larger than the DPD interval multiplied by max-retries.

Values 10 to 300

Default 30

max-retries — Specifies the maximum number of retries before the tunnel is removed.

Values 2 to 5

Default 3

reply-only — Specifies whether to initiate a DPD request if there is an incoming ESP or IKE packet. Issuing the command without the reply-only keyword does not initiate a DPD request if there is an incoming ESP packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.265 dr-activation-timer

dr-activation-timer

Syntax **dr-activation-timer** *seconds*

Context **[Tree]** (config>service>vpls>bind>evpn-mcast-gateway dr-activation-timer)

Full Context configure service vpls allow-ip-int-bind evpn-mcast-gateway dr-activation-timer

Description This command configures the designated router (DR) activation timer for the EVPN gateway.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

After the DR activation timer expires, each provider edge router (PE) runs the MEG or PEG DR election. The timer allows the PE to collect Inclusive Multicast Ethernet Tag routes from other MEG/PEG gateways and avoid running the DR election multiple times. The DR triggers the MEG/PEG first-hop and last-hop router actions on the router.

Default dr-activation-timer 3

Parameters *seconds* — Specifies DR election wait time, in seconds.

Values 0 to 100

Platforms All

8.266 drain

drain

Syntax [**no**] **drain**

Context **[Tree]** (config>service>vprn>dhcp>server>pool>subnet drain)

Full Context configure service vprn dhcp local-dhcp-server pool subnet drain

Description This command means no new leases can be assigned from this subnet and existing leases are cleaned up upon renew/rebind.

The **no** form of this command means the subnet is active and new leases can be assigned from it.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

drain

Syntax [**no**] **drain**

Context **[Tree]** (config>service>vprn>nat>outside>pool>address-range drain)
[Tree] (config>router>nat>outside>pool>address-range drain)

Full Context configure router nat outside pool address-range drain
configure service vprn nat outside pool address-range drain

Description This command starts or stops draining this NAT address range. When an address-range is being drained, it will not be used to serve new hosts. Existing hosts, however, will still be able to use the address that was assigned to them even if it is being drained. An address-range can only be deleted if the parent pool is shut down or if the range itself is effectively drained (hosts are no longer using the addresses).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.267 drop

drop

Syntax [**no**] **drop**

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action drop)

Full Context configure application-assurance group policy app-qos-policy entry action drop

Description This command configures the drop action on flows matching this AQP entry. When enabled, all flow traffic matching this AQP entry will be dropped. When drop action is part of a set of multiple actions to be applied to a single flow as result of one or more AQP entry match, drop action will be performed first and no other action will be invoked on that flow.

The **no** form of this command disables the drop action on flows matching this AQP entry.

Default no drop

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

drop

Syntax **drop**
drop packet-length {**lt** | **gt** | **eq**} *packet-length-value*
drop packet-length range *packet-length-value packet-length-value*
drop pattern expression *expression* **mask** *mask* **offset-type** *offset-type* **offset-value** *offset-value*
drop ttl {**lt** | **gt** | **eq**} *ttl-value*
drop ttl range *ttl-value ttl-value*

Context **[Tree]** (config>filter>ip-filter>entry>action drop)

Full Context configure filter ip-filter entry action drop

Description This command configures the drop action for the traffic that matches this filter entry.

Traffic can, also, be dropped based on *pkt-length*, *packet-length range*, *ttl*, *ttl range*, or a pattern of conditional match criteria.

Packets that match the filter entry match criteria, and not the conditional match criteria value, are implicitly forwarded with no further match in the following filter entries.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For pattern match:

- the expression is left-aligned for odd number bytes, for example, the expression 0xABC is programmed 0x0ABC in the line card
- the 'data' offset requires protocol UDP or TCP to be selected in the filter entry match criteria.

Parameters **packet-length** — Specifies drop packets matching both the filter entry match criteria and the *packet-length value* defined in the **drop** action statement. Packets matching the filter entry match criteria and not matching the *packet-length* value, as defined in the **drop** action statement, are implicitly forwarded with no further match in the following filter entries.

Values lt — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

packet-length-value — Specifies the packet length value for the rate limit action.

Values 0 to 65535

range — Specifies an inclusive range. When **range** is used, the start of the range (the first value entered) must be smaller than the end of the range (the second value entered).

expression — Specifies the hexadecimal pattern to match; up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

mask — Specifies the mask for the pattern expression, up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

offset-type — Specifies the starting point reference for the offset-value of this pattern.

Values layer-3, layer-4, data, dns-qtype

offset-value — Specifies the offset value for the pattern expression. Dns-qtype supports offset value of 0.

Values 0 to 255

ttl-value — Specifies drop packets matching both the filter entry match criteria and the TTL value defined in the drop action statement. Packets matching the filter entry match criteria and not matching the TTL value, as defined in the drop action statement, are implicitly forwarded with no further match in the following filter entries.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

drop

Syntax **drop**
drop hop-limit {**lt** | **gt** | **eq**} *hop-limit-value*
drop hop-limit range hop-limit-value *hop-limit-value*
drop pattern expression *expression* **mask** *mask* **offset-type** *offset-type* **offset-value** *offset-value*
drop payload-length {**lt** | **gt** | **eq**} *payload-length-value*
drop payload-length range *payload-length-value payload-length-value*

Context **[Tree]** (config>filter>ipv6-filter>entry>action drop)

Full Context configure filter ipv6-filter entry action drop

Description This command configures the drop action for the traffic that matches this filter entry.

Traffic can, also, be dropped based on *payload-length*, *payload-length range*, *hop-limit*, *hop-limit range*, or a pattern of conditional match criteria.

Packets that match the filter entry match criteria, but do not match the conditional match criteria value, are implicitly forwarded with no further match in the following filter entries.

For pattern match:

- the expression is left-aligned for the odd number bytes, for example, the expression 0xABC is programmed 0x0ABC in the line card
- the 'data' offset requires protocol UDP or TCP to be selected in the filter entry match criteria

Parameters **hop-limit** — Specifies the hop-limit value for the drop action.

Values lt — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.
eq — Specifies “equal to”.
gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

hop-limit-value — Specifies the hop-limit value for the drop action.

Values 0 to 255

range — Specifies an inclusive range. When the **range** parameter is used, the start of the range (the first value entered) must be smaller than the end of the range (the second value entered).

expression — Specifies the hexadecimal pattern to match; up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

mask — Specifies the mask for the pattern expression, up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

offset-type — Specifies the starting point reference for the offset-value of this pattern.

Values layer-3, layer-4, data, dns-qtype

offset-value — Specifies the offset value for the pattern expression. Dns-qtype supports offset value of 0.

Values 0 to 255

payload-length — Specifies drop packets matching both the filter entry match criteria and the payload-length-value defined in the drop action statement. Packets matching the filter entry match criteria and not matching the payload-length-value, as defined in the drop action statement, are implicitly forwarded with no further match in the following filter entries.

Values lt — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

payload-length-value — Specifies the payload length value for the drop action.

Values 0 to 65535

Platforms All

drop

Syntax **drop**

Context **[Tree]** (config>filter>mac-filter>entry>action drop)

Full Context configure filter mac-filter entry action drop

Description This command sets the MAC filter entry action to drop.

Platforms All

8.268 drop-count

drop-count

Syntax **drop-count** *count*
no drop-count

Context **[Tree]** (config>service>vprn>static-route-entry>indirect>cpe-check drop-count)
[Tree] (config>service>vprn>static-route-entry>next-hop>cpe-check drop-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn static-route-entry indirect cpe-check drop-count
configure service vprn static-route-entry next-hop cpe-check drop-count

Description This optional parameter specifies the number of consecutive ping-replies that must be missed to declare the CPE down and to deactivate the associated static route.

Default drop-count 3

Parameters *count* — An integer count value.

Values 1 to 255

Platforms All

drop-count

Syntax **drop-count** *consecutive-failures* [**hold-down** *seconds*]
no drop-count

Context **[Tree]** (config>filter>redirect-policy>dest>ping-test drop-count)

Full Context configure filter redirect-policy destination ping-test drop-count

Description This command specifies the number of consecutive requests that must fail for the destination to be declared unreachable and the time to hold destination unreachable before repeating tests.

Default drop-count 3 hold-down 0

Parameters *consecutive-failures* — Specifies the number of consecutive ping test failures before declaring the destination down.

Values 1 to 60

hold-down *seconds* — Specifies the amount of time, in seconds, that the system should be held down if any of the test has marked it unreachable.

Values 0 to 86400

Platforms All

drop-count

Syntax **drop-count** *count*
no drop-count

Context **[Tree]** (config>router>static-route-entry>indirect>cpe-check drop-count)
[Tree] (config>router>static-route-entry>next-hop>cpe-check drop-count)

Full Context configure router static-route-entry indirect cpe-check drop-count
configure router static-route-entry next-hop cpe-check drop-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This optional parameter specifies the number of consecutive ping-replies that must be missed to declare the CPE down and to deactivate the associated static route.

Default drop-count 3

Parameters *count* — Specifies the integer count value.

Values 1 to 255

Platforms All

drop-count

Syntax **drop-count** *count*
no drop-count

Context **[Tree]** (config>vrrp>policy>priority-event>host-unreachable drop-count)

Full Context configure vrrp policy priority-event host-unreachable drop-count

Description This command configures the number of consecutively sent ICMP echo request messages that must fail before the host unreachable priority control event is set.

The **drop-count** command is used to define the number of consecutive message send attempts that must fail for the **host-unreachable** priority event to enter the set state. Each unsuccessful attempt increments the event's consecutive message drop counter. With each successful attempt, the event's consecutive message drop counter resets to zero.

If the event's consecutive message drop counter reaches the **drop-count** value, the **host-unreachable** priority event enters the set state.

The event's **hold-set** value defines how long the event must stay in the set state even when a successful message attempt clears the consecutive drop counter. The event is not cleared until the consecutive drop counter is less than the **drop-count** value and the **hold-set** timer has a value of zero (expired).

The **no** form of the command reverts to the default value.

Default drop-count 3 — 3 consecutive ICMP echo request failures are required before the host unreachable priority control event is set.

Parameters *count* — The number of ICMP echo request message attempts that must fail for the event to enter the set state. It also defines the threshold so a lower consecutive number of failures can clear the event state.

Values 1 to 60

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.269 drop-extracted-traffic

drop-extracted-traffic

Syntax **drop-extracted-traffic**

Context [Tree] (config>filter>ip-filter>entry>action drop-extracted-traffic)
[Tree] (config>filter>ipv6-filter>entry>action drop-extracted-traffic)

Full Context configure filter ip-filter entry action drop-extracted-traffic
configure filter ipv6-filter entry action drop-extracted-traffic

Description This command specifies that a packet matching this filter entry is dropped if extracted to the CPM. Packets matching the filter entry match criteria and not extracted to the CPM are forwarded with no further match in the following filter entries.

Platforms All

8.270 drop-routes-with-srv6-tlvs

drop-routes-with-srv6-tlvs

Syntax **[no] drop-routes-with-srv6-tlvs**

Context [Tree] (config>router>bgp>group>srv6>route drop-routes-with-srv6-tlvs)
[Tree] (config>router>bgp>group>neighbor>srv6>route drop-routes-with-srv6-tlvs)

Full Context configure router bgp group neighbor segment-routing-v6 route-advertisement drop-routes-with-srv6-tlvs
configure router bgp group segment-routing-v6 route-advertisement drop-routes-with-srv6-tlvs

Description This command configures the router to drop and not advertise BGP routes (that belong to any address family) with SRv6 TLVs.

The **no** form of this command configures the router to advertise BGP routes with SRv6 TLVs.

Default no drop-routes-with-srv6-tlvs

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.271 drop-tail

drop-tail

Syntax **drop-tail**

Context [Tree] (config>mcast-mgmt>bw-plcy>t2>prim-path>queue drop-tail)
[Tree] (config>mcast-mgmt>bw-plcy>t2>sec-path>queue drop-tail)

Full Context configure mcast-management bandwidth-policy t2-paths primary-path queue-parameters drop-tail
configure mcast-management bandwidth-policy t2-paths secondary-path queue-parameters drop-tail

Description Commands in this context configure queue drop-tail parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

drop-tail

Syntax **drop-tail**

Context [Tree] (config>service>ies>if>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue drop-tail)
[Tree] (config>service>vpls>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue drop-tail)

Full Context configure service ies interface sap egress queue-override queue drop-tail
configure service ies interface sap ingress queue-override queue drop-tail
configure service vpls sap egress queue-override queue drop-tail
configure service vpls sap ingress queue-override queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms All

drop-tail

Syntax **drop-tail**

Context [Tree] (config>port>eth>access>ing>qgrp>qover>q drop-tail)
[Tree] (config>port>eth>access>egr>qgrp>qover>q drop-tail)
[Tree] (config>port>ethernet>network>egr>qgrp>qover>q drop-tail)

Full Context configure port ethernet access egress queue-group queue-overrides queue drop-tail
configure port ethernet access ingress queue-group queue-overrides queue drop-tail

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet network egress queue-group queue-overrides queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms All

drop-tail

Syntax **drop-tail**

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue drop-tail)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue drop-tail)
[Tree] (config>service>epipe>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue drop-tail)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue drop-tail)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue drop-tail)

Full Context configure service apipe sap egress queue-override queue drop-tail
configure service apipe sap ingress queue-override queue drop-tail
configure service cpipe sap egress queue-override queue drop-tail
configure service cpipe sap ingress queue-override queue drop-tail
configure service epipe sap egress queue-override queue drop-tail
configure service epipe sap ingress queue-override queue drop-tail
configure service fpipe sap egress queue-override queue drop-tail
configure service fpipe sap ingress queue-override queue drop-tail
configure service ipipe sap egress queue-override queue drop-tail
configure service ipipe sap ingress queue-override queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress queue-override queue drop-tail
- configure service fpipe sap ingress queue-override queue drop-tail
- configure service fpipe sap egress queue-override queue drop-tail
- configure service cpipe sap egress queue-override queue drop-tail

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress queue-override queue drop-tail
- configure service apipe sap egress queue-override queue drop-tail

All

- configure service ipipe sap egress queue-override queue drop-tail

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ipipe sap ingress queue-override queue drop-tail
- configure service epipe sap ingress queue-override queue drop-tail
- configure service epipe sap egress queue-override queue drop-tail

drop-tail

Syntax **drop-tail**

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue drop-tail)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue drop-tail)

Full Context configure service vprn interface sap egress queue-override queue drop-tail
configure service vprn interface sap ingress queue-override queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms All

drop-tail

Syntax **drop-tail**

Context **[Tree]** (config>qos>sap-egress>queue drop-tail)
[Tree] (config>qos>sap-ingress>queue drop-tail)

Full Context configure qos sap-egress queue drop-tail
configure qos sap-ingress queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms All

drop-tail

Syntax **drop-tail**

Context **[Tree]** (config>qos>network-queue>queue drop-tail)

Full Context configure qos network-queue queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

drop-tail

Syntax **drop-tail**

Context **[Tree]** (config>qos>qgrps>ing>qgrp>queue drop-tail)
[Tree] (config>qos>qgrps>egr>qgrp>queue drop-tail)

Full Context configure qos queue-group-templates egress queue-group queue drop-tail
configure qos queue-group-templates ingress queue-group queue drop-tail

Description Commands in this context configure queue drop-tail parameters.

Platforms All

drop-tail

Syntax **drop-tail**

Context **[Tree]** (config>qos>shared-queue>queue drop-tail)

Full Context configure qos shared-queue queue drop-tail

Description Commands in this context configure queue drop tail parameters.

Platforms All

8.272 drop-unidentified-traffic

drop-unidentified-traffic

Syntax [**no**] **drop-unidentified-traffic**

Context **[Tree]** (config>router>nat>inside>subscriber-identification drop-unidentified-traffic)
[Tree] (config>service>vprn>nat>inside>subscriber-identification drop-unidentified-traffic)

Full Context configure router nat inside subscriber-identification drop-unidentified-traffic
configure service vprn nat inside subscriber-identification drop-unidentified-traffic

Description When this command denies address translation to subscribers that have not been identified via accounting messages sent by BNG and received by Radius accounting proxy. This command has effect only in Subscriber Aware Application.

Default no drop-unidentified-traffic

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.273 drop-zero-ipv4-checksum

drop-zero-ipv4-checksum

Syntax [**no**] **drop-zero-ipv4-checksum**

Context **[Tree]** (config>service>vprn>inside>nat64 drop-zero-ipv4-checksum)

Full Context configure service vprn inside nat64 drop-zero-ipv4-checksum

Description This command specifies if UDP datagrams with zero IPv4 checksum are dropped.

If this command is disabled, the system calculates the IPv6 checksum for each such datagram.

drop-zero-ipv4-checksum

Syntax [**no**] **drop-zero-ipv4-checksum**

Context **[Tree]** (config>service>vprn>nat>inside>nat64 drop-zero-ipv4-checksum)
[Tree] (config>router>nat>inside>nat64 drop-zero-ipv4-checksum)

Full Context configure router nat inside nat64 drop-zero-ipv4-checksum
configure service vprn nat inside nat64 drop-zero-ipv4-checksum

Description This command enables the NAT64 node to drop received UDP datagrams with zero IPv4 checksum. By default, checksum is re-calculated for non-fragmented datagrams.

The **no** form of the command disables the command.

Default disabled

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.274 dropped-only

dropped-only

Syntax [**no**] **dropped-only**

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg>pppoe-client>brg-id dropped-only)

Full Context debug subscriber-mgmt vrgw brg pppoe-client brg-id dropped-only

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies that only packets that are dropped by the vRGW will be shown in debugging.

Default dropped-only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

8.275 ds1

ds1

Syntax [**no**] **ds1** *ds1-id*

Context **[Tree]** (config>port>tdm ds1)

Full Context configure port tdm ds1

Description Commands in this context configure digital signal level 1 (DS-1) frame parameters. The T-Carrier system was the first successful system that supported digitized voice transmission. The original transmission rate (1.544 Mb/s) in the T-1 (DS-1) line is commonly used by Internet service providers (ISPs) to connect to the Internet.

North America uses the T-Carrier system while Europe uses the E-Carrier system of transmission, using multiples of the DS- system. Digital signals are carried inside the carrier systems.

T-1 transmits DS-1-formatted data at 1.544 Mb/s through the network. The corresponding European carrier is E-1 with a data rate of 2.048 Mb/s. E-1 and T-1 (DS-1) can be interconnected for international use.

The **no** form of this command disables DS-1 capabilities.

Parameters *ds1-id* — Identifies the DS-1 channel being created.

Values DS1: 1 to 28, ds1-sonet-sdh-index

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

8.276 ds3

ds3

Syntax [**no**] **ds3** [*sonet-sdh-index*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>tdm ds3)

Full Context configure port tdm ds3

Description Commands in this context configure DS-3 parameters. DS-3 lines provide a speed of 44.736 Mb/s and is also frequently used by service providers. DS-3 lines carry 28 DS-1 signals and a 44.736 Mb/s data rate.

A DS-3 connection typically supports data rates of about 43 Mb/s. A T-3 line actually consists of 672 individual channels, each supporting 64 kb/s. T-3 lines are used mainly by Service Providers to connect to the Internet backbone and for the backbone itself.

Depending on the MDA type, the DS-3 parameters must be disabled if clear channel is enabled by default (for example, on the m12-ds3 MDA). Clear channel is a channel that uses out-of-band signaling, not in-band signaling, so the channel's entire bit rate is available. Channelization must be explicitly specified. Note that if DS-3 nodes are provisioned on a channelized SONET/SDH MDA you must provision the parent STS-1 SONET/STM0 SDH path first.

North America uses the T-Carrier system while Europe uses the E-Carrier system of transmission, using multiples of the DS system. Digital signals are carried inside the carrier systems.

The **no** form of this command disables DS-3 capabilities.

Parameters *sonet-sdh-index* — Specifies the components making up the specified SONET/SDH Path. Depending on the type of SONET/SDH port the *sonet-sdh-index* must specify more path indexes to specify the payload location of the path. The *sonet-sdh-index* differs for SONET and SDH ports.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

8.277 dsap

dsap

Syntax **dsap** *dsap-value* [*dsap-mask*]
no dsap

Context [Tree] (config>qos>sap-ingress>mac-criteria>entry>match dsap)

Full Context configure qos sap-ingress mac-criteria entry match dsap

Description Configures an Ethernet 802.2 LLC DSAP value or range for an ingress SAP QoS policy match criterion.

This is a 1-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The snap-pid field, etype field, ssap, and dsap fields are mutually exclusive and cannot be part of the same match criteria.

Use the **no** form of this command to remove the dsap value as the match criterion.

Default no dsap

Parameters *dsap-value* — The 8-bit dsap match criteria value in hexadecimal.

Values 0x00 to 0xFF (hex)

dsap-mask — This is optional and can be used when specifying a range of dsap values to use as the match criteria.

This 8-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Values 0x00 to 0xFF (hex)

Default FF

Platforms All

dsap

Syntax **dsap** *dsap-value* [*dsap-mask*]
no dsap

Context **[Tree]** (config>filter>mac-filter>entry>match dsap)

Full Context configure filter mac-filter entry match dsap

Description Configures an Ethernet 802.2 LLC DSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria.

Use the **no** form of the command to remove the dsap value as the match criterion.

Default no dsap

Parameters *dsap-value* — Specifies the 8-bit dsap match criteria value which can be expressed in decimal integer, hexadecimal or binary format.

Values 0 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dsap-mask — Specifies an optional parameter that may be used when specifying a range of dsap values to use as the match criteria.

This 8 bit mask can be configured using the decimal integer, hexadecimal or binary formats described in Table 45.

Table 45 **dsap-mask Formats**

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Default **255 (exact match)**
0x00 to 0xFF

Values 0 to 255

Platforms All

dsap

Syntax **dsap** *dsap-value* [*dsap-mask*]

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match dsap)

Full Context configure system security management-access-filter mac-filter entry match dsap

Description This command configures DSAP match conditions.

Parameters *dsap-value* — Specifies the 8-bit DSAP match criteria value in hexadecimal.

Values 0x00 to 0xFF (hex)

mask — Specifies a range of DSAP values to use as the match criteria.

This 8 bit mask can be configured using the formats described in Table 46:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 46 **Format Styles**

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Default FF (hex) (exact match)

Values 0x00 to 0xFF

Platforms All

8.278 dscp

dscp

Syntax **dscp** *dscp-name*
no dscp

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match dscp)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match dscp)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match dscp)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match dscp)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match dscp
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match dscp
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match dscp
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match dscp

Description This command configures DSCP match conditions.

The **no** form of this command reverts to the default.

Parameters *dscp-name* — Specifies the DSCP name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>service>ies>if>sap>ip-tunnel dscp)

Full Context configure service ies interface sap ip-tunnel dscp

Description This command sets the DSCP code-point in the outer IP header of encapsulated packets associated with a particular tunnel.

The **no** form of this command copies the DSCP value from the inner IP header (after remarking by the private tunnel SAP egress qos policy) to the outer IP header.

Default no dscp

Parameters *dscp* — Specifies the DSCP code-point to be used.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dscp

Syntax **dscp** *dscp-name* **fc** *fc-name*
no dscp *dscp-name*

Context **[Tree]** (config>router>sgt-qos dscp)
[Tree] (config>service>vprn>sgt-qos dscp)

Full Context configure router sgt-qos dscp
configure service vprn sgt-qos dscp

Description This command creates a mapping between the DiffServ Code Point (DSCP) of the self-generated traffic and the forwarding class.

Self-generated traffic that matches the specified DSCP will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all 64 DSCPs to the forwarding class.

All DSCP names that define a DSCP value must be explicitly defined.

The **no** form of this command removes the DSCP-to-forwarding class association.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *dscp-name* — Specifies the name of the DSCP to be associated with the forwarding class. DiffServ code point can only be specified by its name and only an existing DiffServ code point can be specified. The software provides names for the well-known code points.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc *fc-name* — Specifies the forwarding class name. All packets with a DSCP value or MPLS EXP bit that are not defined will be placed in this forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>service>vprn>if>sap>ip-tunnel dscp)

Full Context configure service vprn interface sap ip-tunnel dscp

Description This command sets the DSCP code-point in the outer IP header of GRE encapsulated packets associated with a particular GRE tunnel. The default, set using the **no** form of this command, is to copy the DSCP value from the inner IP header (after remarking by the private tunnel SAP egress qos policy) to the outer IP header.

Default no dscp

Parameters *dscp* — Specifies the DSCP code-point to be used.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dscp

Syntax **dscp in-profile** *dscp-name* **out-profile** *dscp-name*
no dscp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>policy>aqp>entry>action>remark dscp)

Full Context configure application-assurance group policy app-qos-policy entry action remark dscp

Description Commands in this context configure DSCP remark action or actions on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured DSCP name.

DSCP remark can only be applied when the entry remarks forwarding class or forwarding class and priority. In-profile and out-of profile of a given packet for DSCP remark is assessed after all AQP policing and priority remarking actions took place.

The **no** form of this command stops DSCP remarking action on flows matching this AQP entry.

Default no dscp

Parameters **in-profile** *dscp-name* — Specifies the DSCP name to use to remark in-profile flows that match this policy.

out-profile *dscp-name* — Specifies the DSCP name to use to remark out-of-profile flows that match this policy.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dscp

Syntax **dscp** {**eq** | **neq**} *dscp-name*
no dscp

Context [Tree] (config>app-assure>group>policy>aqp>entry>match dscp)
[Tree] (config>app-assure>group>sess-fltr>entry>match dscp)

Full Context configure application-assurance group policy app-qos-policy entry match dscp
configure application-assurance group session-filter entry match dscp

Description This command adds a DSCP name to the match criteria used by this entry.

The no form of this command removes dscp from match criteria for this entry.

Default no dscp

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dscp-name — Specifies the DSCP name to be used in the match.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>test-oam>build-packet>header>ipv4 dscp)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv4 dscp)

Full Context configure test-oam build-packet header ipv4 dscp
debug oam build-packet packet field-override header ipv4 dscp

Description This command defines the DSCP value to be used in the IPv4 header.

The **no** form of this command reverts to the default.

Default dscp be

Parameters *dscp-name* — Specifies the DSCP value to be used in the IPv4 header.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>test-oam>build-packet>header>ipv6 dscp)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv6 dscp)

Full Context configure test-oam build-packet header ipv6 dscp
debug oam build-packet packet field-override header ipv6 dscp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the DSCP value to be used in the IPv6 header.

The **no** form of this command removes the DSCP name.

Parameters *dscp-name* — Specifies the DSCP value to be used in the IPv6 header.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dscp

Syntax **dscp** *dscp-name*
dscp resolve

Context **[Tree]** (config>oam-pm>session>ip dscp)

Full Context configure oam-pm session ip dscp

Description This command can be used to explicitly configure the DSCP value to the specified *dscp-name*, or to use the configured **fc** and **profile** values to derive the DSCP value from the egress network QoS policy 1.

Default dscp resolve

Parameters *dscp-name* — Specifies the Diffserv code point name.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

resolve — Specifies to use the configured **fc** and **profile** values to derive the DSCP value from the egress network QoS policy 1.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>oam-pm>session>mpls dscp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure oam-pm session mpls dscp

Description This command can be used to explicitly configure the DSCP value that is carried in the DM PDU. This value is not used on the launch point or the reflector to influence the QoS behavior on the network elements. The frame itself has no IP information because it uses the General Associated Channel Header (G-Ach). The fc and profile values are used to influence QoS behavior on the launch point and the responder.

The **no** form of this command reverts the dscp carried in the DM PDU to default.

Default dscp be

Parameters *dscp-name* — Specifies the Diffserv code point name.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5,nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41,af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Values be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dscp

Syntax **dscp** *dscp-name* [*dscp-name*] **fc** *fc-name* [**priority** {**low** | **high**}]
no dscp *dscp-name* [*dscp-name*]

Context **[Tree]** (config>qos>sap-ingress dscp)

Full Context configure qos sap-ingress dscp

Description This command explicitly sets the forwarding class or subclass or enqueuing priority when a packet is marked with the DiffServ Code Point (DSCP) value contained in the *dscp-name*. A list of up to eight dscp-names can be entered on a single command. The lists of dscp-names within the configuration are managed by the system to ensure that each list does not exceed eight names. Entering more than eight dscp-names with the same parameters (**fc**, **priority**) will result in multiple lists being created. Conversely, multiple lists with the same parameters (fc, priority) are merged and the lists repacked to a maximum of eight per list if DSCP names are removed or the parameters changed so the multiple lists use the same parameters. Also, if a subset of a list is entered with different parameters, then a new list will be created for the subset. When the list is stored in the configuration, the DSCP names are sorted by their DSCP value in ascending numerical order; consequently, the order in the configuration may not be exactly what the user entered.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Adding a DSCP rule on the policy forces packets that match the DSCP value specified to override the forwarding class and enqueuing priority based on the parameters included in the DSCP rule. When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueuing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueuing priority derived from earlier matches in the classification hierarchy.

The DSCP value (referred to here by *dscp-name*) is derived from the most significant six bits in the IPv4 header ToS byte field (DSCP bits) or the Traffic Class field from the IPv6 header. If the packet does not have an IP header, DSCP-based matching is not performed. The six DSCP bits define 64 DSCP values used to map packets to per-hop Quality of Service (QoS) behavior. The most significant three bits in the IP header ToS byte field are also commonly used in a more traditional manner to specify an IP precedence value, causing an overlap between the precedence space and the DSCP space. Both IP precedence and DSCP classification rules are supported.

DSCP rules have a higher match priority than IP precedence rules and where a *dscp-name* DSCP value overlaps an *ip-prec-value*, the DSCP rule takes precedence.

The **no** form of this command removes the specified the *dscp-names* from the explicit DSCP classification rule in the SAP ingress policy. As *dscp-names* are removed, the system repacks the lists of *dscp-names* with the same parameters (up to eight per list). As the **no** command does not have any additional parameters, it is possible to remove multiple *dscp-names* from multiple DSCP statements having different parameters with one command. If a *dscp-name* specified in a **no** command does not exist in any DSCP statement, then the command is aborted at that point with an error message displayed; any DSCP names in the list before the failed entry will be processed as normal but the processing will stop at the failed entry so that the remainder of the list is not processed.

Removing the *dscp-name* from the policy immediately removes the DSCP name on all ingress SAPs using the policy.

Parameters *dscp-name* — The DSCP name is a required parameter that specifies the unique IP header ToS byte DSCP bits value that will match the DSCP rule. If the command is executed multiple times with the same *dscp-name*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of 64 DSCP rules are allowed on a single policy and a maximum of eight *dscp-names* can be specified in a single statement.

The specified name must exist as a *dscp-name*. SR OS software provides names for the well-known code points; these can be shown using the following command:

```
A:PE# show qos dscp-table
============================================================
DSCP Mapping
============================================================
DSCP Name      DSCP Value     TOS (bin)      TOS (hex)
------------------------------------------------------------
be             0              0000 0000      00
cp1            1              0000 0100      04
cp2            2              0000 1000      08
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cp3	3	0000 1100	0C
cp4	4	0001 0000	10
cp5	5	0001 0100	14
cp6	6	0001 1000	18
cp7	7	0001 1100	1C
cs1	8	0010 0000	20
cp9	9	0010 0100	24
af11	10	0010 1000	28
cp11	11	0010 1100	2C
af12	12	0011 0000	30
cp13	13	0011 0100	34
af13	14	0011 1000	38
cp15	15	0011 1100	3C
cs2	16	0100 0000	40
cp17	17	0100 0100	44
af21	18	0100 1000	48
cp19	19	0100 1100	4C
af22	20	0101 0000	50
cp21	21	0101 0100	54
af23	22	0101 1000	58
cp23	23	0101 1100	5C
cs3	24	0110 0000	60
cp25	25	0110 0100	64
af31	26	0110 1000	68
cp27	27	0110 1100	6C
af32	28	0111 0000	70
cp29	29	0111 0100	74
af33	30	0111 1000	78
cp31	31	0111 1100	7C
cs4	32	1000 0000	80
cp33	33	1000 0100	84
af41	34	1000 1000	88
cp35	35	1000 1100	8C
af42	36	1001 0000	90
cp37	37	1001 0100	94
af43	38	1001 1000	98
cp39	39	1001 1100	9C
cs5	40	1010 0000	A0
cp41	41	1010 0100	A4
cp42	42	1010 1000	A8
cp43	43	1010 1100	AC
cp44	44	1011 0000	B0
cp45	45	1011 0100	B4
ef	46	1011 1000	B8
cp47	47	1011 1100	BC
nc1	48	1100 0000	C0
cp49	49	1100 0100	C4
cp50	50	1100 1000	C8
cp51	51	1100 1100	CC
cp52	52	1101 0000	D0
cp53	53	1101 0100	D4
cp54	54	1101 1000	D8
cp55	55	1101 1100	DC
nc2	56	1110 0000	E0
cp57	57	1110 0100	E4
cp58	58	1110 1000	E8
cp59	59	1110 1100	EC
cp60	60	1111 0000	F0
cp61	61	1111 0100	F4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
cp62            62              1111 1000       F8
cp63            63              1111 1100       FC
===========================================================
```

fc *fc-name* — The value given for *fc-name* must be one of the predefined forwarding classes in the system. Specifying the *fc-name* is optional. When a packet matches the rule, the forwarding class is only overridden when the **fc** *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

The *subclass-name* parameter is optional and used with the *fc-name* parameter to define a preexisting subclass. The *fc-name* and *subclass-name* parameters must be separated by a period (.). If *subclass-name* does not exist in the context of *fc-name*, an error will occur. If *subclass-name* is removed using the **no fc** *fc-name.subclass-name* **force** command, the **default-fc** command will automatically drop the *subclass-name* and only use *fc-name* (the parent forwarding class for the subclass) as the forwarding class.

Values

fc: *class*[.*subclass*]

class: be, l2, af, l1, h2, ef, h1, nc

subclass: 29 characters max

Default Inherit (when **fc** *fc-name* is not defined, the rule preserves the previous forwarding class of the packet).

priority — This parameter overrides the default enqueuing priority for all packets received on an ingress SAP using this policy that match this rule. Specifying the priority is optional. When a packet matches the rule, the enqueuing priority is only overridden when the priority parameter is defined on the rule. If the packet matches and priority is not explicitly defined in the rule, the enqueuing priority is inherited based on previous rule matches.

Default Inherits the priority defined by the default-priority statement.

high — This parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **high** for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

low — This parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **low** for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry>match dscp)
[Tree] (config>qos>sap-egress>ip-criteria>entry>match dscp)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry>match dscp)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry>match dscp)

Full Context configure qos sap-egress ip-criteria entry match dscp
configure qos sap-egress ipv6-criteria entry match dscp
configure qos sap-ingress ip-criteria entry match dscp
configure qos sap-ingress ipv6-criteria entry match dscp

Description This command configures a DSCP code point to be used as a SAP QoS policy match criterion.

The **no** form of this command removes the DSCP match criterion.

Default no dscp

Parameters *dscp-name* — Specifies a dscp name that has been previously mapped to a value using the **dscp-name** command. The DiffServ code point can only be specified by its name.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms All

dscp

Syntax **dscp** *dscp-name* [*dscp-name*] [**fc** *fc-name*] [**profile** {**in** | **out** | **exceed** | **inplus**}]
no dscp *dscp-name* [*dscp-name*]

Context **[Tree]** (config>qos>sap-egress dscp)

Full Context configure qos sap-egress dscp

Description This command defines IP Differentiated Services Code Point (DSCP) names that must be matched to perform the associated reclassification actions. The specified name must exist as a DSCP name. SR OS software provides names for the well-known code points. A list of up to eight DSCP names can be entered on a single command. The lists of DSCP names within the configuration are managed by the system to ensure that each list does not exceed eight names. Entering more than eight DSCP names with the same parameters (**fc** and **profile**)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

results in multiple lists being created. Conversely, multiple lists with the same parameters (**fc** and **profile**) are merged and the lists repacked to a maximum of eight per list if DSCP names are removed or the parameters changed so the multiple lists use the same parameters. Also, if a subset of a list is entered with different parameters, a new list is created for the subset. When the list is stored in the configuration, the DSCP names are sorted by their DSCP value in ascending numerical order; consequently, the order in the configuration may not be exactly what the user entered.

If an egress packet on the SAP matches an IP DSCP value corresponding to a specified DSCP name, the forwarding class, profile egress queue accounting behavior may be overridden. By default, the forwarding class and profile of the packet is derived from ingress classification and profiling functions. Matching a DSCP-based reclassification rule will override all IP precedence-based reclassification rule actions.

The IP DSCP bits used to match against DSCP reclassification rules come from the Type of Service (ToS) field within the IPv4 header or the traffic class field from the IPv6 header. If the packet does not have an IP header, DSCP-based matching is not performed.

The reclassification actions from a DSCP reclassification rule may be overridden by an IP flow match event.

The **fc** keyword is optional. When specified, the egress classification rule will overwrite the forwarding class derived from ingress. The new forwarding class is used for egress remarking and queue mapping decisions. If an IP criteria match occurs after the DSCP match, the new forwarding class may be overridden by the higher priority match actions. If the higher priority match actions do not specify a new fc, the fc from the dscp match will be used.

The **profile** keyword is optional. When specified, the egress classification rule will overwrite the profile of the packet derived from ingress. The new profile value is used for egress remarking and queue congestion behavior. If an IP criteria match occurs after the DSCP match, the new profile may be overridden by the higher priority match actions. If the higher priority match actions do not specify a new profile, the profile from the DSCP match will be used.

The **no** form of this command removes the specified the *dscp-names* from the reclassification rule in the SAP egress QoS policy. As *dscp-names* are removed, the system repacks the lists of *dscp-names* with the same parameters (up to 8 per list). As the **no** command does not have any additional parameters, it is possible to remove multiple *dscp-names* from multiple DSCP statements having different parameters with one command. If a *dscp-name* specified in a **no** command does not exist in any DSCP statement, the command is aborted at that point with an error message displayed. Any *dscp-names* in the list before the failed entry will be processed as normal but the processing will stop at the failed entry so that the remainder of the list is not processed.

Parameters *dscp-name* — The *dscp-name* parameter is required when defining a DSCP reclassification rule. The specified name must exist as a DSCP name. A maximum of eight DSCP names can be specified in a single statement. SR OS software provides names for the well-known code points. These can be shown using the following command:

```
A:PE# show qos dscp-table
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
===========================================================
DSCP Mapping
===========================================================
DSCP Name       DSCP Value     TOS (bin)       TOS (hex)
-----------------------------------------------------------
be              0              0000 0000       00
cp1             1              0000 0100       04
cp2             2              0000 1000       08
cp3             3              0000 1100       0C
cp4             4              0001 0000       10
cp5             5              0001 0100       14
cp6             6              0001 1000       18
cp7             7              0001 1100       1C
cs1             8              0010 0000       20
cp9             9              0010 0100       24
af11            10             0010 1000       28
cp11            11             0010 1100       2C
af12            12             0011 0000       30
cp13            13             0011 0100       34
af13            14             0011 1000       38
cp15            15             0011 1100       3C
cs2             16             0100 0000       40
cp17            17             0100 0100       44
af21            18             0100 1000       48
cp19            19             0100 1100       4C
af22            20             0101 0000       50
cp21            21             0101 0100       54
af23            22             0101 1000       58
cp23            23             0101 1100       5C
cs3             24             0110 0000       60
cp25            25             0110 0100       64
af31            26             0110 1000       68
cp27            27             0110 1100       6C
af32            28             0111 0000       70
cp29            29             0111 0100       74
af33            30             0111 1000       78
cp31            31             0111 1100       7C
cs4             32             1000 0000       80
cp33            33             1000 0100       84
af41            34             1000 1000       88
cp35            35             1000 1100       8C
af42            36             1001 0000       90
cp37            37             1001 0100       94
af43            38             1001 1000       98
cp39            39             1001 1100       9C
cs5             40             1010 0000       A0
cp41            41             1010 0100       A4
cp42            42             1010 1000       A8
cp43            43             1010 1100       AC
cp44            44             1011 0000       B0
cp45            45             1011 0100       B4
ef              46             1011 1000       B8
cp47            47             1011 1100       BC
nc1             48             1100 0000       C0
cp49            49             1100 0100       C4
cp50            50             1100 1000       C8
cp51            51             1100 1100       CC
cp52            52             1101 0000       D0
cp53            53             1101 0100       D4
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
cp54            54              1101 1000       D8
cp55            55              1101 1100       DC
nc2             56              1110 0000       E0
cp57            57              1110 0100       E4
cp58            58              1110 1000       E8
cp59            59              1110 1100       EC
cp60            60              1111 0000       F0
cp61            61              1111 0100       F4
cp62            62              1111 1000       F8
cp63            63              1111 1100       FC
===============================================================
```

fc-name: — The **fc** reclassification action is optional. When specified, packets matching the IP DSCP value corresponding to a specified *dscp-name* will be explicitly reclassified to the forwarding class specified as *fc-name* regardless of the ingress classification decision. The explicit forwarding class reclassification may be overwritten by an IP criteria reclassification match. The **fc** name defined must be one of the eight forwarding classes supported by the system. To remove the forwarding class reclassification action for the specified DSCP value, the **dscp** command must be re-executed without the **fc** reclassification action defined.

Values be, l1, af, l2, h1, ef, h2 or nc

counter-id — Specifies the counter ID.

profile — The profile reclassification action is optional. When specified, packets matching the IP DSCP value corresponding to a specified *dscp-name* will be explicitly reclassified to the specified profile regardless of the ingress profiling decision. The explicit profile reclassification may be overwritten by an IPv6 criteria or IP criteria reclassification match. To remove the profile reclassification action for the specified *dscp-name*, the **dscp** command must be re-executed without the profile reclassification action defined.

in — Specifies that any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out — Specifies that any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

exceed — Specifies that when **exceed** is specified, any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

inplus — Specifies that any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

Platforms All

dscp

Syntax **dscp** {*dscp-name* | **in-profile** *dscp-name* **out-profile** *dscp-name* [**exceed-profile** *dscp-name*]}
no dscp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>sap-egress>fc dscp)

Full Context configure qos sap-egress fc dscp

Description This command configures a DSCP to be used for remarking packets from the specified FC. If the optional **exceed-profile**, **in-profile**, or **out-profile** keyword is specified, the command will remark different DSCP depending on whether the packet was classified to be exceed, in-profile, or out-of-profile ingress to the node. All inplus-profile traffic is marked with the same value as in-profile traffic.

Default no dscp

Parameters *dscp-name* — Specifies a DSCP name that has been previously mapped to a value using the **dscp-name** command. The DSCP can only be specified by its name.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

exceed-profile *dscp-name* — This optional parameter specifies the DSCP name to be used to remark the traffic that is exceed-profile. If not specified, this defaults to the same value configured for **out-profile** parameter.

in-profile *dscp-name* — Specifies the DSCP name to be used to remark the traffic that is in-profile.

out-profile *dscp-name* — Specifies the DSCP name to be used to remark the traffic that is out-of-profile.

Platforms All

dscp

Syntax **dscp** *dscp-name* **fc** *fc-name* **profile** {**in** | **out**}
no dscp

Context [Tree] (config>qos>network>ingress dscp)

Full Context configure qos network ingress dscp

Description This command creates a mapping between the DiffServ Code Point (DSCP) of the network ingress traffic and the forwarding class.

Ingress traffic that matches the specified DSCP will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all 64 DiffServ code points to the forwarding class. For undefined code points, packets are assigned to the forwarding class specified under the **default-action** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the DiffServ code point-to-forwarding class association. The **default-action** then applies to that code point value.

Parameters *dscp-name* — The name of the DiffServ code point to be associated with the forwarding class. DiffServ code point can only be specified by its name and only an existing DiffServ code point can be specified. The software provides names for the well-known code points.

The system-defined names available are as follows. The system-defined names must be referenced as all lowercase, exactly as shown in the first column in Table 47 and Table 48.

Additional names-to-code point value associations can be added using the '**dscp-name** *dscp-name dscp-value*' command.

The actual mapping is being done on the *dscp-value*, not the *dscp-name* that references the *dscp-value*. If a second *dscp-name* that references the same *dscp-value* is mapped within the policy, an error will occur. The second name will not be accepted until the first name is removed.

Table 47 **Default DSCP Names to DSCP Value Mapping**

DSCP Name	DSCP Value Decimal	DSCP Value Hexadecimal	DSCP Value Binary
nc1	48	0x30	0b110000
nc2	56	0x38	0b111000
ef	46	0x2e	0b101110
af41	34	0x22	0b100010
af42	36	0x24	0b100100
af43	38	0x26	0b100110
af31	26	0x1a	0b011010
af32	28	0x1c	0b011100
af33	30	0x1d	0b011110
af21	18	0x12	0b010010
af22	20	0x14	0b010100
af23	22	0x16	0b010110
af11	10	0x0a	0b001010
af12	12	0x0c	0b001100
af13	14	0x0e	0b001110
default	0	0x00	0b000000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 48 **Default Class Selector Code Points to DSCP Value Mapping**

DSCP Name	DSCP Value Decimal	DSCP Value Hexadecimal	DSCP Value Binary
cs7	56	0x38	0b111000
cs6	48	0X30	0b110000
cs5	40	0x28	0b101000
cs4	32	0x20	0b100000
cs3	24	0x18	0b011000
cs2	16	0x10	0b010000
cs1	08	0x8	0b001000

fc-name — Enter this required parameter to specify the *fc-name* with which the code point will be associated.

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out} — Enter this required parameter to indicate whether the DiffServ code point value is the in-profile or out-of-profile value. For every DSCP value defined, the profile must be indicated. If a DSCP value is not mapped, the default-action forwarding class and profile state will be used for that value.

DSCP values mapping to forwarding classes Expedited (ef), High-1 (h1) and Network-Control (nc) can only be set to in-profile.

DSCP values mapping to forwarding class “be” can only be set to out-of-profile.

Values in, out

Platforms All

dscp

Syntax **dscp** *dscp-name* **fc** *fc-name* **profile** {**in** | **out** | **exceed** | **inplus**}
no dscp *dscp-name*

Context **[Tree]** (config>qos>network>egress dscp)

Full Context configure qos network egress dscp

Description This command configures an IP Differentiated Services Code Point (DSCP) value that must be matched to perform the associated reclassification actions. If an egress packet on an IES/VPRN interface spoke SDP, on a CSC network interface in a VPRN, or on a network interface that the network QoS policy is applied to, matches the specified IP DSCP value, the forwarding class and profile may be overridden.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, the forwarding class and profile of the packet are derived from ingress classification and profiling functions. Matching a DHCP-based reclassification rule will override all IP precedence-based reclassification rule actions.

The IP DSCP bits used to match against DSCP reclassification rules come from the Type of Service (ToS) field within the IPv4 header or the Traffic Class field from the IPv6 header. If the packet does not have an IP header, DSCP-based matching is not performed.

The configuration of egress DSCP classification and the configuration of an egress IP criteria or IPv6 criteria entry statement within a network QoS policy are mutually exclusive.

The IP precedence- and DSCP-based reclassification are supported on a network interface, on a CSC network interface in a VPRN, and on a PW used in an IES or VPRN spoke interface. The CLI will block the application of a network QoS policy with the egress reclassification commands to the spoke SDP part of a Layer 2 service.

Conversely, the CLI will not allow the user to add the egress reclassification commands to a network QoS policy if the policy is being used by a Layer 2 spoke SDP.

The egress reclassification commands will only take effect if the redirection of the spoke SDP or CSC interface to use an egress port queue group succeeds. For example, the following CLI command would be successful:

config>**service**>**vprn**>**if**>**spoke-sdp**>**egress**>**qos** *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

config>**service**>**ies**>**if**>**spoke-sdp>egress**>**qos** *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

config>service>vprn>nw-if>qos *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

If the redirection command fails, the PW will use the network QoS policy assigned to the network IP interface, however any reclassification in the network QoS policy applied to the network interface will be ignored.

The **no** form of this command removes the egress reclassification rule.

Parameters *dscp-name* — be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc *fc-name* — be, l2, af, l1, h2, ef, h1, nc

profile {**in** | **out | exceed | inplus**} — The profile reclassification action is mandatory. When specified, packets matching the DSCP value will be explicitly reclassified to the profile specified regardless of the ingress profiling decision. To remove the profile reclassification action for the specified DSCP value, the **no dscp** command must be executed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

in - Specifies that any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out - Specifies that any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

exceed - Specifies that any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

inplus - Specifies that any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

Platforms All

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry>match dscp)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry>match dscp)
[Tree] (config>qos>network>egress>ip-criteria>entry>match dscp)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match dscp)

Full Context configure qos network egress ip-criteria entry match dscp
configure qos network egress ipv6-criteria entry match dscp
configure qos network ingress ip-criteria entry match dscp
configure qos network ingress ipv6-criteria entry match dscp

Description This command configures a DSCP to be used as a network QoS policy match criterion.

The **no** form of this command removes the DSCP match criterion.

Parameters *dscp-name* — Specifies a DSCP name that has been previously mapped to a value using the **dscp-name** command. The DSCP can only be specified by its name.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms All

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>filter>ip-filter>entry>match dscp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>filter>ipv6-filter>entry>match dscp)

Full Context configure filter ip-filter entry match dscp
configure filter ipv6-filter entry match dscp

Description This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.

The **no** form of the command removes the DSCP match criterion.

Default no dscp

Parameters *dscp-name* — Configures a DSCP name. The DiffServ code point may only be specified by its name.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms All

dscp

Syntax **dscp** *dscp-name*
no dscp

Context [Tree] (cfg>sys>sec>cpm>ip-filter>entry>match dscp)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match dscp)

Full Context configure system security cpm-filter ip-filter entry match dscp
configure system security cpm-filter ipv6-filter entry match dscp

Description This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.

The **no** form of this command removes the DSCP match criterion.

Default no dscp

Parameters *dscp-name* — Configures a dscp name that has been previously mapped to a value using the **dscp-name** command. The DiffServ code point may only be specified by its name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dscp

Syntax **dscp** {*dscp-value* | *dscp-name*}

Context **[Tree]** (config>router>sgt-qos>application>grpc dscp)

Full Context configure router sgt-qos application grpc dscp

Description This command configures a DiffServ Code Point (DSCP) name to be used for gRPC.

Parameters *dscp-value* — Represents the gRPC traffic class.

Values 0 to 63

dscp-name — Represents the gRPC traffic class.

Values none, be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dscp

Syntax **dscp** *dscp-name*
no dscp

Context **[Tree]** (config>test-oam>icmp>ping-template dscp)

Full Context configure test-oam icmp ping-template dscp

Description This command specifies the DSCP to be carried in the IP header. This value is not exposed to egress QoS policies. This command uses well-known DSCP names.

The **no** form of this command reverts to the default value.

Default dscp nc1

Parameters *dscp-name* — Specifies the DSCP name, up to 32 characters.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dscp

Syntax **dscp** *dscp-name*

Context **[Tree]** (config>test-oam>link-meas>template>twl dscp)

Full Context configure test-oam link-measurement measurement-template twamp-light dscp

Description This command configures the DSCP to be copied into the IP header of each TWAMP Light echo request packet launched for the test.

Default dscp nc1

Parameters *dscp-name* — Specifies the DSCP code point to be used.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.279 dscp-in-profile

dscp-in-profile

Syntax **dscp-in-profile** *dscp-name*
no dscp-in-profile

Context **[Tree]** (config>qos>network>egress>fc dscp-in-profile)

Full Context configure qos network egress fc dscp-in-profile

Description This command specifies the in-profile DSCP name for the forwarding class. The corresponding DSCP value will be used for all IP packets that require marking at egress on this forwarding class queue, and that are in-profile. The inplus-profile traffic is marked with the same value as in-profile traffic.

When multiple DSCP names are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command resets the configuration to the factory default in-profile DSCP name setting for *policy-id* 1.

Parameters *dscp-name* — Specifies the system- or user-defined, case-sensitive *dscp-name.*

Values Any defined system- or user-defined *dscp-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

8.280 dscp-out-profile

dscp-out-profile

Syntax **dscp-out-profile** *dscp-name*
no dscp-out-profile

Context **[Tree]** (config>qos>network>egress>fc dscp-out-profile)

Full Context configure qos network egress fc dscp-out-profile

Description This command specifies the out-of-profile DSCP name for the forwarding class. The corresponding DSCP value will be used for all IP packets requiring marking the egress on this forwarding class queue that are out-of-profile. The exceed-profile traffic is marked with the same value as out-of-profile traffic.

When multiple DSCP names are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command resets the configuration to the factory default out-of-profile DSCP name setting for *policy-id* 1.

Default

Policy-id 1:	Factory setting
Policy-id 2 to 65535:	Policy-id setting

Parameters *dscp-name* — Specifies the system- or user-defined, case-sensitive *dscp-name.*

Values Any defined system- or user-defined *dscp-name*

Platforms All

8.281 dslite-lsn-sub

dslite-lsn-sub

Syntax [**no**] **dslite-lsn-sub router** *router-instance* **b4** *ipv6-prefix*

Context **[Tree]** (config>li>li-source>nat dslite-lsn-sub)

Full Context configure li li-source nat dslite-lsn-sub

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Dual-Stack Lite LSN subscriber source.

The **no** form of this command removes the value from the configuration.

Parameters *router-instance* — Specifies the router instance the pool belongs to, either by router name or service ID.

Values *router-name*: “Base” or “management”

Default Base

ipv6-prefix — Specifies the IPv6 address.

Values

ipv6-prefix:	<prefix>/<length>
prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x to [0 to FFFF]H
	d to [0 to 255]D
<length>	[0 to 128]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.282 dslite-max-subscriber-limit

dslite-max-subscriber-limit

Syntax **dslite-max-subscriber-limit** *max*
no dslite-max-subscriber-limit

Context **[Tree]** (config>service>vprn>nat>inside dslite-max-subscriber-limit)
[Tree] (config>router>nat>inside>dslite dslite-max-subscriber-limit)

Full Context configure router nat inside dslite dslite-max-subscriber-limit
configure service vprn nat inside dslite-max-subscriber-limit

Description This command sets the value for the number of high order bits of the source IPv6 address that will be considered as DS-Lite subscriber. The remaining bits of the source IPv6 address will be masked off, effectively aggregation all IPv6 source addresses under the configured prefix length into a single DS-Lite subscriber. Source IPv4 addresses/ports of the traffic carried within the DS-Lite subscriber will be translated into a single outside IPv4 address and the corresponding deterministic port-block (port-blocks can be extended).

The range of values for subscriber-prefix-length in non-deterministic DS-Lite is limited from 32 to 64 (a prefix will be considered as a DS-Lite subscriber) or it can be set to a value of 128 (the source IPv6 address is considered as a DS-Lite subscriber).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In cases where deterministic DS-Lite is enabled in a giver inside routing context, the range of values of the subscriber-prefix-length depends on the value of dslite-max-subscriber-limit parameter as follows:

subscriber-prefix-length – n = [32..64,128]

where n = log2(dslite-max-subscriber-limit)

[or in an alternate form: dslite-max-subscriber-limit = 2^n.]

In other words the largest prefix length for the deterministic DS-Lite subscriber will be 32+n, where n = log2(dslite-max-subscriber-limit). The subscriber prefix length can extend up to 64 bits. Beyond 64 bits for the subscriber prefix length, there only one value is allowed: 128. In the case n must be 0, which means that the mapping between B4 elements (or IPv6 address) and the IPv4 outside addresses is in 1:1 ratio (no sharing of outside IPv4 addresses).

This parameter can be changed only when there are no deterministic prefixes configured in the same routing context.

Default 128

Parameters *max* — In non-deterministic DS-Lite this value can be 32 to 64,128, assuming that the deterministic DS-Lite is not concurrently enabled in the same inside routing context.

In case that deterministic DS-Lite is enabled, this value can be within the range [(32+n)..64,128] where n = log2(dslite-max-subscriber-limit). The value of 128 is allowed only when n=0 (each subscriber is mapped to a single outside IPv4 IP address).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.283 dsm

dsm

Syntax [**no**] **dsm**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>ue-state dsm)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ue-state dsm

Description This command enables matching on DSM UEs.

The **no** form of this command disables matching on DSM UEs, unless UE state matching is disabled altogether.

Default no dsm

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dsm

Syntax [**no**] **dsm**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state dsm)

Full Context configure subscriber-mgmt wlan-gw ue-query state dsm

Description This command enables matching on UEs in a DSM state.

The **no** form of this command disables matching on UEs in a DSM state, unless all state matching is disabled.

Default no dsm

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.284 dsm-ip-filter

dsm-ip-filter

Syntax **dsm-ip-filter** *dsm-ip-filter-name*
no dsm-ip-filter

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm dsm-ip-filter)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm dsm-ip-filter)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt dsm-ip-filter
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt dsm-ip-filter

Description This command configures an IP filter that is distributed on ISA cards.

This command specifies the IP filter applied to all UEs corresponding to default vlan-range (such as a group-interface) or the specified vlan-range. The IP filter can be created in the **config>subscr-mgmt>isa-filter** context, and can contain up to 1024 match entries. The IP filter can be overridden per UE from RADIUS via access-accept or COA.

The **no** form of this command reverts to the default.

Parameters *dsm-ip-filter-name* — Specifies the identifier of the distributed-sub-mgmt IP filter.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.285 dsm-subscriber

dsm-subscriber

Syntax [**no**] **dsm-subscriber mac** *mac-address*

Context **[Tree]** (config>li>li-source>wlan-gw dsm-subscriber)

Full Context configure li li-source wlan-gw dsm-subscriber

Description This command configures the DSM UE source.

Parameters *mac-address* — Specifies the MAC address.

Values mac-addr: xx:xx:xx:xx:xx:xx **example:** 00:0c:f1:99:85:b8
or XX:XX:XX:XX:XX:XX **example:** 00-0C-F1-99-85-B8

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.286 dsmap

dsmap

Syntax **dsmap** *if-num*
no dsmap

Context **[Tree]** (config>router>mpls>lsp>working-tp-path>mep dsmap)
[Tree] (config>router>mpls>lsp>protect-tp-path>mep dsmap)
[Tree] (config>router>mpls>lsp>transit-path>forward-path>mip dsmap)
[Tree] (config>router>mpls>lsp>transit-path>reverse-path>mip dsmap)

Full Context configure router mpls lsp protect-tp-path mep dsmap
configure router mpls lsp transit-path forward-path mip dsmap
configure router mpls lsp transit-path reverse-path mip dsmap
configure router mpls lsp working-tp-path mep dsmap

Description This command is used to configure the values to use in the DSMAP TLV sent by a node in an LSP Trace echo request for a static MPLS-TP LSP. A node sending a DSMAP TLV will include the in-if-num and out-if-num values. Additionally, it will include the out-label for the LSP in the Label TLV for the DSMAP in the echo request message.

The **no** form of this command equals to a value 0 (this means no interface validation will be performed).

Default no dsmap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *if-num* — This is a 32-bit value corresponding to the expected ingress interface if-num used by an MPLS-TP LSP for the next hop downstream.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.287 dst-ip

dst-ip

Syntax **dst-ip** {*ipv6-address* | *prefix-length*}
dst-ip {*ip-address/mask* | *ip-address netmask*
no dst-ip

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match dst-ip)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match dst-ip)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match dst-ip
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match dst-ip

Description This command configures the destination IP match condition.

The **no** form of this command reverts to the default.

Parameters *ip-address/mask* — Specifies the IPv4 address and mask.

Values

ip-address	a.b.c.d
mask	0 to 32

netmask — Specifies the mask, expressed as a dotted quad.

Values a.b.c.d

ipv6-address — Specifies the IPv6 address (applies only to the 7750 SR).

Values

ipv6-address	x:x:x:x:x:x:x:x (where x is [0 to FFFF]H)
	:x:x:x:x:x:d.d.d.d (where d is [0 to 255]D)

prefix-length — Specifies the prefix length (applies only to the 7750 SR).

Values 1 to 128

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dst-ip

Syntax **dst-ip** *ip-address*
no dst-ip

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring>in-band-control-path dst-ip)
[Tree] (config>redundancy>mc>peer>mcr>node>cv dst-ip)
[Tree] (config>redundancy>mc>peer>mc>l3-ring>in-band-control-path dst-ip)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring in-band-control-path dst-ip
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify dst-ip
configure redundancy multi-chassis peer mc-ring ring in-band-control-path dst-ip

Description This command specifies the destination IP address used in the inband control connection. If the address is not configured, the ring cannot become operational.

Default no dst-ip

Parameters *ip-address* — Specifies the destination IP address.

Values a.b.c.d (no multicast address)

Platforms All

dst-ip

Syntax **dst-ip** *ip-prefix/length*
no dst-ip

Context **[Tree]** (config>subscr-mgmt>isa-filter>entry>match dst-ip)
[Tree] (config>subscr-mgmt>isa-filter>ipv6>entry>match dst-ip)

Full Context configure subscriber-mgmt isa-filter entry match dst-ip
configure subscriber-mgmt isa-filter ipv6 entry match dst-ip

Description This command specifies that the packet's destination IP address must match the specified IP prefix and mask.

The **no** form of this command disables the match on the destination IP.

Parameters *ip-prefix/length* — Specifies the IP prefix to match.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dst-ip

Syntax **dst-ip** *ip-address* **protocol** *ip-protocol* **dst-port** *port-number*
dst-ip *ip-address* **protocol** *ip-protocol* **dst-port** *port-number* **prefix-length** *prefix-length*
no dst-ip *ip-address* **protocol** *ip-protocol* **dst-port** *port-number*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>http-rdr-plcy>fwd-entries dst-ip)

Full Context configure subscriber-mgmt http-redirect-policy forward-entries dst-ip

Description This command configures traffic flow to be forwarded via match in the redirect policy.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address to match the destination address in the IP header of the traffic received from the subscriber.

prefix-length — Specifies the length of the prefix specified by the ip-address.

Values 1 to 128 for IPv6
1 to 32 for IPv4

ip-protocol — Specifies the protocol to match the IP protocol in the IP header of the traffic received from the subscriber.

Values tcp, udp

port-number — Specifies the port to match the destination port in the HTTP request.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-ip

Syntax **dst-ip** {**eq** | **neq**} *ip-address*
dst-ip {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
no dst-ip

Context [Tree] (config>app-assure>group>policy>aqp>entry>match dst-ip)

Full Context configure application-assurance group policy app-qos-policy entry match dst-ip

Description This command specifies a destination IP address to use as match criteria.

Default no dst-ip

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified address or prefix.

neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

d - [0..255]D
prefix-length [1..128]

ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-ip

Syntax **dst-ip** *ip-address*
dst-ip dns-ip-cache *dns-ip-cache-name*
dst-ip ip-prefix-list *ip-prefix-list-name*
no dst-ip

Context **[Tree]** (config>app-assure>group>sess-fltr>entry>match dst-ip)

Full Context configure application-assurance group session-filter entry match dst-ip

Description This command configures the destination IP address to match.

Default no dst-ip

Parameters *ip-address* — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D
	prefix-length [1..128]

dns-ip-cache-name — Specifies the name of the dns-ip-cache policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-ip

Syntax **dst-ip** {**eq** | **neq**} *ip-address*
no dst-ip

Context **[Tree]** (debug>app-assure>group>traffic-capture>match dst-ip)

Full Context debug application-assurance group traffic-capture match dst-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures debugging on a destination IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-ip

Syntax **dst-ip** {ip-address/mask | *ip-address ipv4-address-mask*}

Context **[Tree]** (config>li>li-filter>li-ip-filter>entry>match dst-ip)

Full Context configure li li-filter li-ip-filter entry match dst-ip

Description This command configures destination IP address LI filter match criterion.

The **no** form of this command removes any configured destination IP address. The match criterion is ignored.

Parameters *ip-address* — Specifies any address specified as dotted quad.

Values a.b.c.d

mask — Specifies eight 16-bit hexadecimal pieces representing bit match criteria.

Values 1 to 32

ipv4-address-mask — Specifies a mask expressed in dotted quad notation.

Values 0.0.0.0 to 255.255.255.255

Platforms All

dst-ip

Syntax **dst-ip** {*ipv6-address*/*prefix-length* | *ipv6-address ipv6-address-mask*}
no dst-ip

Context **[Tree]** (config>li>li-filter>li-ipv6-filter>entry>match dst-ip)

Full Context configure li li-filter li-ipv6-filter entry match dst-ip

Description This command configures destination IPv6 address LI filter match criterion.

The **no** form of this command removes any configured destination IPv6 address. The match criterion is ignored.

Parameters *ipv6-address* — Specifies any IPv6 address entered as:.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix-length — Specifies the prefix length.

Values 1 to 128

ipv6-address-mask — Specifies any IPv6 address mask expressed as:

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

dst-ip

Syntax **dst-ip** {*ip-address/mask* | *ip-address* [*ipv4-address-mask*] | **ip-prefix-list** *prefix-list-name*}
no dst-ip

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry>match dst-ip)
[Tree] (config>qos>sap-egress>ip-criteria>entry>match dst-ip)

Full Context configure qos sap-egress ip-criteria entry match dst-ip
configure qos sap-ingress ip-criteria entry match dst-ip

Description This command configures a destination address range to be used as a SAP QoS policy match criterion.

To match on the IPv4 destination address, specify the address and its associated mask, e.g., 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used for IPv4.

The **no** form of this command removes the destination IPv4 address match criterion.

Default no dst-ip

Parameters *ip-address* — Specifies the destination IPv4 address specified in dotted decimal notation.

Values ip-address: a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

prefix-list-name — Specifies the IPv4 prefix list name, a string of up to 32 printable ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dst-ip

Syntax **dst-ip** {*ipv6-address/prefix-length* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *ipv6-prefix-list-name*}
no dst-ip

Context **[Tree]** (config>qos>sap-ingress>ipv6-criteria>entry>match dst-ip)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry>match dst-ip)

Full Context configure qos sap-egress ipv6-criteria entry match dst-ip
configure qos sap-ingress ipv6-criteria entry match dst-ip

Description This command configures a destination address range to be used as a SAP QoS policy match criterion.

To match on the IPv6 destination address, specify the address and its associated mask, e.g. 2001:db8:1000::/64.

The **no** form of this command removes the destination IPv6 address match criterion.

Default no dst-ip

Parameters *ipv6-address* — Specifies the IPv6 address for the IP match criterion in hexadecimal digits (applies to the 7750 SR and 7950 XRS).

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

prefix-length — Specifies the IPv6 prefix length for the IPv6 address expressed as a decimal integer (applies to the 7750 SR and 7950 XRS).

Values 1 to 128

ipv6-address-mask — Specifies the IPv6 address mask.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

ipv6-prefix-list-name — Specifies the IPv6 prefix list name, a string of up to 32 printable ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

dst-ip

Syntax **dst-ip** {*ip-address/mask* | *ip-address ipv4-address-mask*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dst-ip {*ipv6-address/mask* | *ipv6-address ipv6-address-mask*}
no dst-ip

Context **[Tree]** (config>qos>network>egress>ip-criteria>entry>match dst-ip)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match dst-ip)

Full Context configure qos network egress ip-criteria entry match dst-ip
configure qos network egress ipv6-criteria entry match dst-ip

Description This command configures a destination address range to be used as a network QoS policy match criterion.

To match on the destination address, specify the address and its associated mask, for example, when specifying an IPv4 address, 10.1.0.0/16 or 10.1.0.0 255.255.0.0 can be used.

The **no** form of this command removes the destination IP address match criterion.

Parameters *ip-address* — Specifies the source IPv4 address specified in dotted decimal notation.

Values ip-address: a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

ipv6-address — Specifies the IPv6 prefix for the IP match criterion in hex digits.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

mask — Specifies the length of the IPv6 address expressed as a decimal integer.

Values 1 to 128

ipv6-address-mask — Specifies the eight 16-bit hexadecimal pieces representing bit match criteria.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

Platforms All

dst-ip

Syntax **dst-ip** {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *ip-prefix-list-name*}
dst-ip {*ipv6-address/mask* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *ipv6-prefix-list-name*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no dst-ip

Context [Tree] (config>qos>network>ingress>ip-criteria>entry>match dst-ip)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry>match dst-ip)

Full Context configure qos network ingress ip-criteria entry match dst-ip
configure qos network ingress ipv6-criteria entry match dst-ip

Description This command configures a destination address range to be used as a network QoS policy match criterion.

To match on the destination address, specify the address and its associated mask, for example, when specifying an IPv4 address, 10.1.0.0/16 or 10.1.0.0 255.255.0.0 can be used.

The **no** form of this command removes the destination IP address match criterion.

Parameters *ip-address* — Specifies the source IPv4 address specified in dotted decimal notation.

Values ip-address: a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

ip-prefix-list-name — Specifies an IPv4 prefix list which contains IPv4 address prefixes to be matched. IP prefix lists are only supported at a network ingress.

Values A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

ipv6-address — Specifies the IPv6 prefix for the IP match criterion in hex digits.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

mask — Specifies the length of the IPv6 address expressed as a decimal integer.

Values 1 to 128

ipv6-address-mask — Specifies the eight 16-bit hexadecimal pieces representing bit match criteria.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-prefix-list-name — Specifies an IPv6 prefix list which contains IPv6 address prefixes to be matched. IPv6 prefix lists are only supported at a network ingress.

Values A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

dst-ip

Syntax **IPv4:**
dst-ip {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}
IPv6:
dst-ip {*ipv6-address/prefix-length* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *prefix-list-name*}
no dst-ip

Context **[Tree]** (config>filter>ip-exception>entry>match dst-ip)
[Tree] (config>filter>ip-filter>entry>match dst-ip)
[Tree] (config>filter>ipv6-exception>entry>match dst-ip)
[Tree] (config>filter>ipv6-filter>entry>match dst-ip)

Full Context configure filter ip-exception entry match dst-ip
configure filter ip-filter entry match dst-ip
configure filter ipv6-exception entry match dst-ip
configure filter ipv6-filter entry match dst-ip

Description This command configures a destination address range to be used as a filter policy match criterion.

To match on the destination address, specify the address and its associated mask, e.g., 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used for IPv4.

The **no** form of this command removes the destination IPv4 or IPv6 address match criterion.

Default no dst-ip

Parameters *ip-address* — Specifies the destination IPv4 address in dotted decimal notation.

Values a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-prefix-list or **ipv6-prefix-list** *prefix-list-name* — Specifies to use a list of IP prefixes referred to by *prefix-list-name*, which is a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

ipv6-address — Specifies the IPv6 prefix for the IP match criterion in hex digits.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

prefix-length — Specifies the IPv6 prefix length for the *ipv6-address* as a decimal integer.

Values 1 to 128

ipv6-address-mask — Specifies the eight 16-bit hexadecimal pieces representing bit match criteria.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

Platforms All

- configure filter ip-filter entry match dst-ip
- configure filter ipv6-filter entry match dst-ip

VSR

- configure filter ip-exception entry match dst-ip
- configure filter ipv6-exception entry match dst-ip

dst-ip

Syntax **dst-ip** *ip-address/mask*
dst-ip *ip-address netmask*
dst-ip ip-prefix-list *ip-prefix-list-name*
no dst-ip

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match dst-ip)

Full Context configure system security cpm-filter ip-filter entry match dst-ip

Description This command configures a destination IP address range to be used as an IP filter match criterion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To match on the destination IP address, specify the address and its associated mask, for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

The **no** form of this command removes the destination IP address match criterion.

Default no dst-ip

Parameters *ip-address* — Specifies the IP address for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 **to** 255.255.255.255

ip-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 to 32

netmask — Specifies the dotted quad equivalent of the mask length.

Values 0.0.0.0 to 255.255.255.255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dst-ip

Syntax **dst-ip** [*ipv6-address /prefix-length*] [**ipv6-prefix-list** *ipv6-prefix-list-name*]
no dst-ip

Context **[Tree]** (cfg>sys>sec>cpm>ipv6-filter>entry>match dst-ip)

Full Context configure system security cpm-filter ipv6-filter entry match dst-ip

Description This command configures a destination IPv6 address range to be used as an IPv6 filter match criterion.

To match on the destination IPv6 address, specify the address.

The **no** form of this command removes the destination IP address match criterion.

This command only applies to the 7750 SR and 7950 XRS.

Default no dst-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address for the IPv6 match criterion in dotted decimal notation. An IPv6 IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:0:217A.

Values

x:x:x:x:x:x:x:x	(eight 16-bit pieces)	
x:x:x:x:x:x:d.d.d.d		
	x:	[0 to .FFFF]H
	d:	[0 to 255]D
prefix-length:	1 to 128	

ipv6-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ipv6-prefix-list-name — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.288 dst-ipv4-address

dst-ipv4-address

Syntax **dst-ipv4-address** *a.b.c.d*
no dst-ipv4-address

Context **[Tree]** (config>test-oam>build-packet>header>ipv4 dst-ipv4-address)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv4 dst-ipv4-address)

Full Context configure test-oam build-packet header ipv4 dst-ipv4-address
debug oam build-packet packet field-override header ipv4 dst-ipv4-address

Description This command defines the destination IPv4 address to be used in the IPv4 header.

The **no** form of this command removes the destination IPv4 address value.

Default dst-ipv4-address 0.0.0.0

Parameters *a.b.c.d* — Specifies the IPv4 destination address to be used in the IPv4 header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.289 dst-ipv6-address

dst-ipv6-address

Syntax **dst-ipv6-address** *ipv6-address*
no dst-ipv6-address

Context **[Tree]** (config>test-oam>build-packet>header>ipv6 dst-ipv6-address)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv6 dst-ipv6-address)

Full Context configure test-oam build-packet header ipv6 dst-ipv6-address
debug oam build-packet packet field-override header ipv6 dst-ipv6-address

Description This command defines the destination IPv6 address to be used in the IPv6 header.

The **no** form of this command removes the IPv6 address.

Parameters *ipv6-address* — Specifies the IPv6 destination address to be used in the IPv6 header.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	0 to FFFF]H
	d:	[0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.290 dst-mac

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context **[Tree]** (config>li>li-filter>li-mac-filter>entry>match dst-mac)

Full Context configure li li-filter li-mac-filter entry match dst-mac

Description This command configures a destination MAC address or range to be used as a MAC filter match criterion.

The **no** form of this command removes the destination mac address as the match criterion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ieee-address* — Specifies the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — Specifies a 48-bit mask that can be configured using:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a destination MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default **0xFFFFFFFFFFFF** (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF

Platforms All

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match dst-mac)

Full Context configure qos sap-ingress mac-criteria entry match dst-mac

Description Configures a destination MAC address or range to be used as a Service Ingress QoS policy match criterion.

The **no** form of this command removes the destination MAC address as the match criterion.

Default no dst-mac

Parameters *ieee-address* — The MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — A 48-bit mask to match a range of MAC address values.
This 48-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0xFFFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All packets with a source MAC OUI value of 00-03-FA, subject to a match condition, should be specified as: 0003FA000000 0x0FFFFF000000

Values 0x00000000000000 to 0xFFFFFFFFFFFF (hex)

Default 0xFFFFFFFFFFFF

Platforms All

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context **[Tree]** (config>filter>mac-filter>entry>match dst-mac)

Full Context configure filter mac-filter entry match dst-mac

Description Configures a destination MAC address or range to be used as a MAC filter match criterion.

The **no** form of the command removes the destination mac address as the match criterion.

Default no dst-mac

Parameters *ieee-address* — Specifies the MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit. Note that both upper and lower case are supported.

ieee-address-mask — Specifies a 48-bit mask to match a range of MAC address values.

To configure so that all packets with a destination MAC OUI value of 00:03:FA are subject to a match condition then the entry should be specified as: 00:03:FA:00:00:00 FF:FF:FF:00:00:00.

Default ff:ff:ff:ff:ff:ff (exact match)

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH
where H is a hexadecimal digit. to 0xFFFFFFFFFFFF
Note that both upper and lower case are supported.

Platforms All

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match dst-mac)

Full Context configure system security management-access-filter mac-filter entry match dst-mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the destination MAC match condition.

Parameters *ieee-address* — Specifies the MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

mask — Specifies a 48-bit mask to match a range of MAC address values.

Platforms All

8.291 dst-mac-address

dst-mac-address

Syntax **dst-mac-address** *ieee-address*
no dst-mac-address

Context **[Tree]** (config>test-oam>build-packet>header>ethernet dst-mac-address)
[Tree] (debug>oam>build-packet>packet>field-override>header>ethernet dst-mac-address)

Full Context configure test-oam build-packet header ethernet dst-mac-address
debug oam build-packet packet field-override header ethernet dst-mac-address

Description This command defines the destination MAC address for the Ethernet header.

The **no** form of this command deletes the configured MAC address.

Default dst-mac-address 00:00:00:00:00:00

Parameters *ieee-address* — Specifies the destination Ethernet MAC address to be used in the Ethernet header. Specifies the 48-bit MAC address.

Values xx:xx:xx:xx:xx:xx

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.292 dst-port

dst-port

Syntax **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
dst-port range *start end*
no dst-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match dst-port)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match dst-port)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match dst-port)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match dst-port)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match dst-port
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match dst-port
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match dst-port
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match dst-port

Description This command configures the destination port match condition.

The **no** form of this command reverts to the default.

Parameters **lt** | **gt** | **eq** — Specifies the operator.

dst-port-number — Specifies the destination port number as a decimal hex or binary.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dst-port

Syntax **dst-port** *operator port-number*
no dst-port

Context [Tree] (config>subscr-mgmt>isa-filter>entry>match dst-port)
[Tree] (config>subscr-mgmt>isa-filter>ipv6>entry>match dst-port)

Full Context configure subscriber-mgmt isa-filter entry match dst-port
configure subscriber-mgmt isa-filter ipv6 entry match dst-port

Description This command specifies that the packet's UDP/TCP dst-port must match a specific value. This command is not valid in a match context that is not specific to UDP or TCP.

The **no** form of this command removes matching of the layer-4 port.

Parameters *operator* — Specifies that the only supported value is eq (equal to). The destination port value must be equal to the *port-number* value.

port-number — Specifies the number of the port to match.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dst-port

Syntax **dst-port** *tcp-port*
no dst-port

Context **[Tree]** (config>subscr-mgmt>http-rdr-plcy dst-port)

Full Context configure subscriber-mgmt http-redirect-policy dst-port

Description This command specifies the port to match the destination port in the HTTP request.

HTTP traffic that does not match this port, is not redirected.

The **no** form of this command reverts to the default.

Default dst-port 80

Parameters *tcp-port* — Specifies the TCP port.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-port

Syntax **dst-port** {**eq** | **neq**} *port-num*
dst-port {**eq** | **neq**} **port-list** *port-list-name*
dst-port {**eq** | **neq**} **range** *start-port-num end-port-num*
no dst-port

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match dst-port)

Full Context configure application-assurance group policy app-qos-policy entry match dst-port

Description This command specifies a destination TCP/UDP port, destination port list, or destination range to use as match criteria.

The **no** form of this command removes the parameters from the configuration.

Default no dst-port

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the destination port number.

Values 0 to 65535

start-port-num end-port-num — Specifies the start or end destination port number.

Values 0 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port-list-name — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-port

Syntax **dst-port** {**eq** | **gt** | **lt**} *port-num*
dst-port port-list *port-list-name*
dst-port range *start-port-num end-port-num*
no dst-port

Context **[Tree]** (config>app-assure>group>sess-fltr>entry>match dst-port)

Full Context configure application-assurance group session-filter entry match dst-port

Description This command specifies a destination TCP/UDP port, destination port list, or destination range to use as match criteria.

The **no** form of this command removes the parameters from the configuration.

Default no dst-port

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified port.

gt — Specifies all port numbers greater than the port-number match.

lt — Specifies all port numbers less than the port-number match.

port-num — Specifies the destination port number.

Values 0 to 65535

start-port-num end-port-num — Specifies the start or end destination port number.

Values 0 to 65535

port-list-name — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-port

Syntax **dst-port** {**eq** | **neq**} *port-num*
no dst-port

Context **[Tree]** (debug>app-assure>group>traffic-capture>match dst-port)

Full Context debug application-assurance group traffic-capture match dst-port

Description This command configures debugging on a destination port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

dst-port

Syntax **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
dst-port range *dst-port-number dst-port-number*
no dst-port

Context **[Tree]** (config>li>li-filter>li-ip-filter>entry>match dst-port)
[Tree] (config>li>li-filter>li-ipv6-filter>entry>match dst-port)

Full Context configure li li-filter li-ip-filter entry match dst-port
configure li li-filter li-ipv6-filter entry match dst-port

Description This command configures a destination TCP or UDP port number or port range for an IP LI filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (second, third, and so on) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of this command removes the destination port match criterion.

Parameters **lt** — Specifies all port numbers less than *dst-port-number* match.

gt — Specifies all port numbers greater than *dst-port-number* match.

eq — Specifies that *dst-port-number* must be an exact match.

dst-port-number — Specifies an inclusive range of port numbers to be used as a match criteria. The destination port numbers *start-port* and *end-port* are expressed as decimal integers.

Values [0..65535]D
[0x0..0xFFFF]H
[0b0..0b1111111111111111]B

Platforms All

dst-port

Syntax **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
dst-port range *start end*
no dst-port

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry>match dst-port)
[Tree] (config>qos>sap-egress>ip-criteria>entry>match dst-port)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry>match dst-port)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry>match dst-port)

Full Context configure qos sap-egress ip-criteria entry match dst-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos sap-egress ipv6-criteria entry match dst-port
configure qos sap-ingress ip-criteria entry match dst-port
configure qos sap-ingress ipv6-criteria entry match dst-port

Description This command configures a destination TCP or UDP port number or port range for a SAP QoS policy match criterion.

The **no** form of this command removes the destination port match criterion.

Default no dst-port

Parameters **{lt | gt | eq}** *dst-port-number* — The TCP or UDP port numbers to match, specified as less than (**lt**), greater than (**gt**), or equal to (**eq**) to the destination port value, specified as a decimal integer.

Values 1 to 65535 (decimal)

range *start end* — The range of TCP or UDP port values to match, specified as between the *start* and *end* destination port values inclusive.

Values 1 to 65535 (decimal)

Platforms All

dst-port

Syntax **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
dst-port port-list *port-list-name*
dst-port range *start end*
no dst-port

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry>match dst-port)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry>match dst-port)
[Tree] (config>qos>network>egress>ip-criteria>entry>match dst-port)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match dst-port)

Full Context configure qos network egress ip-criteria entry match dst-port
configure qos network egress ipv6-criteria entry match dst-port
configure qos network ingress ip-criteria entry match dst-port
configure qos network ingress ipv6-criteria entry match dst-port

Description This command configures a destination TCP or UDP port number, port range, or a port list for a network QoS policy match criterion.

The **no** form of this command removes the destination port match criterion.

Parameters **lt** — Keyword used to specify TCP or UDP port numbers to match that are less than the destination port value.

gt — Keyword used to specify TCP or UDP port numbers to match that are greater than the destination port value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

eq — Keyword used to specify TCP or UDP port numbers to match that are equal to the destination port value.

dst-port-number — Specifies the TCP or UDP port numbers to match, specified as less than (lt), greater than (gt), or equal to (eq) the destination port value, specified as a decimal integer.

Values 1 to 65535

port-list-name — Specifies a port list name, up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

start — Specifies the starting range of TCP or UDP port values to match.

Values 1 to 65535

end — Specifies the end range of TCP or UDP port values to match.

Values 1 to 65535

Platforms All

dst-port

Syntax **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
dst-port port-list *port-list-name*
dst-port range *dst-port-number dst-port-number*
no dst-port

Context **[Tree]** (config>filter>ip-exception>entry>match dst-port)
[Tree] (config>filter>ip-filter>entry>match dst-port)
[Tree] (config>filter>ipv6-exception>entry>match dst-port)
[Tree] (config>filter>ipv6-filter>entry>match dst-port)

Full Context configure filter ip-exception entry match dst-port
configure filter ip-filter entry match dst-port
configure filter ipv6-exception entry match dst-port
configure filter ipv6-filter entry match dst-port

Description This command configures a destination TCP, UDP, or SCTP port number or port range for an IP filter or IP exception match criterion. An entry containing Layer 4 non-zero match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information. Similarly an entry containing the "**dst-port eq** 0" match criterion, may match non-initial fragments when the destination port value is not present in a packet fragment and other match criteria are also met.

The **no** form of the command removes the destination port match criterion.

Default no dst-port

Parameters **lt** — Specifies that all port numbers less than the *dst-port-number* match.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gt — Specifies that all port numbers greater than the *dst-port-number* match.

eq — Specifies that the *dst-port-number* must be an exact match.

dst-port-number — Specifies the destination port number to be used as a match criteria expressed as a decimal integer, as well as in hexadecimal or binary format. The following value is for decimal integer format only.

Values 0 to 65535

port-list-name — Specifies to use a list of ports referred to by *port-list-name*, which is a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

dst-port-number dst-port-number — Specifies inclusive port range between two *dst-port-number* values.

Platforms All

- configure filter ip-filter entry match dst-port
- configure filter ipv6-filter entry match dst-port

VSR

- configure filter ip-exception entry match dst-port
- configure filter ipv6-exception entry match dst-port

dst-port

Syntax **dst-port** *value* [*mask*]
no dst-port

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry dst-port)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry dst-port)

Full Context configure system security management-access-filter ip-filter entry dst-port
configure system security management-access-filter ipv6-filter entry dst-port

Description This command configures a destination TCP or UDP port number or port range for a management access filter match criterion.

The **no** form of this command removes the destination port match criterion.

Parameters *value* — Specifies the destination TCP or UDP port number as match criteria.

Values 1 **to** 65535 (decimal)

mask — Specifies the mask used to specify a range of destination port numbers as the match criterion.

This 16 bit mask can be configured using the formats described in Table 49:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 49 **Format Styles to Configure Mask**

Format Style	Format Syntax	Example
Decimal	DDDDD	63488
Hexadecimal	0xHHHH	0xF800
Binary	0bBBBBBBBBBBBBBBB	0b1111100000000000

To select a range from 1024 up to 2047, specify 1024 0xFC00 for value and mask.

Default **65535** (exact match)

Values 1 to 65535 (decimal)

Platforms All

dst-port

Syntax **dst-port** [*tcp/udp port-number*] [*mask*]
dst-port port-list *port-list-name*
dst-port range *tcp/udp port-number tcp/udp port-number*
no dst-port

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match dst-port)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match dst-port)

Full Context configure system security cpm-filter ip-filter entry match dst-port
configure system security cpm-filter ipv6-filter entry match dst-port

Description This command specifies the TCP/UDP port or port name to match the destination-port of the packet.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of this command removes the destination port match criterion.

Default no dst-port

Parameters *tcp/udp port-number* — Specifies the destination port number to be used as a match criteria expressed as a decimal integer.

Values 0 to 65535 (accepted in decimal hex or binary)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port-list-name — Specifies the port list name to be used as a match criteria for the destination port.

mask — Specifies the 16 bit mask to be applied when matching the destination port.

Values [0x0000 to 0xFFFF] | [0 to 65535] | [0b0000000000000000 to 0b1111111111111111]

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.293 dst-port-range

dst-port-range

Syntax **dst-port-range start** *port-number* **end** *port-number*
no dst-port-range

Context **[Tree]** (config>service>nat>nat-classifier>entry>match dst-port-range)

Full Context configure service nat nat-classifier entry match dst-port-range

Description This command configures a destination TCP or UDP port number or port range.

Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd,etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of the command removes the destination port match criterion.

Default dst-port-range start 0 end 65535

Parameters **start** *port-number* — Specifies the start of the port range expressed as a decimal integer.

Values 0 to 65535

end *port-number* — Specifies the end of the port range expressed as a decimal integer.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.294 dst-tcp-port

dst-tcp-port

Syntax **dst-tcp-port** *tcp-port*
no dst-tcp-port

Context **[Tree]** (config>test-oam>build-packet>header>tcp dst-tcp-port)

Full Context configure test-oam build-packet header tcp dst-tcp-port

Description This command defines the destination TCP port to be used in the test TCP header.

The **no** form of this command reverts to the default.

Default dst-tcp-port 0

Parameters *tcp-port* — Specifies the destination TCP port to be used in the test TCP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dst-tcp-port

Syntax **dst-tcp-port** *tcp-port*
no dst-tcp-port

Context **[Tree]** (debug>oam>build-packet>packet>field-override>header>tcp dst-tcp-port)

Full Context debug oam build-packet packet field-override header tcp dst-tcp-port

Description This command defines the destination TCP port to be used in the TCP header.

The **no** form of this command reverts to the default.

Default no override

Parameters *tcp-port* — Specifies the destination TCP port to be used in the TCP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.295 dst-udp-port

dst-udp-port

Syntax **dst-udp-port** *udp-port*
no dst-udp-port

Context **[Tree]** (config>test-oam>build-packet>header>udp dst-udp-port)

Full Context configure test-oam build-packet header udp dst-udp-port

Description This command defines the destination TCP port to be used in the test TCP header.

The **no** form of this command reverts to the default.

Default dst-udp-port 0

Parameters *udp-port* — Specifies the destination UDP port to be used in the test UDP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

dst-udp-port

Syntax **dst-udp-port** *udp-port*
no dst-udp-port

Context **[Tree]** (debug>oam>build-packet>packet>field-override>header>udp dst-udp-port)

Full Context debug oam build-packet packet field-override header udp dst-udp-port

Description This command defines the destination TCP port to be used in the TCP header.

The **no** form of this command reverts to the default.

Default no override

Parameters *udp-port* — Specifies the destination UDP port to be used in the UDP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.296 dst-zone

dst-zone

Syntax [**no**] **dst-zone** {*std-zone-name* | *non-std-zone-name*}

Context **[Tree]** (config>system>time dst-zone)

Full Context configure system time dst-zone

Description This command configures the start and end dates and offset for summer time or daylight savings time to override system defaults or for user defined time zones.

When configured, the time is adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends.

If the time zone configured is listed in the Time Zones section, then the starting and ending parameters and offset do not need to be configured with this command unless it is necessary to override the system defaults. The command returns an error if the start and ending dates and times are not available either the Time Zones section on or entered as optional parameters in this command.

Up to five summer time zones may be configured, for example, for five successive years or for five different time zones. Configuring a sixth entry will return an error message. If no summer (daylight savings) time is supplied, it is assumed no summer time adjustment is required.

The **no** form of the command removes a configured summer (daylight savings) time entry.

Parameters *std-zone-name* — Specifies the standard time zone name. The standard name must be a system-defined zone in the Time Zones section. For zone names in the table that have an implicit summer time setting, for example MDT for Mountain Daylight Saving Time, the remaining **start-date**, **end-date** and **offset** parameters need to be provided unless it is necessary to override the system defaults for the time zone.

Values ADT, NDT, AKDT, CDT, CEST, EDT, EEST, MDT, NZDT, PDT, WEST

non-std-zone-name — Specifies the non-standard time zone name. Create a user-defined name created using the zone. The name can be a maximum of 5 characters in length.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.297 dual-stack-lite

dual-stack-lite

Syntax **dual-stack-lite**

Context **[Tree]** (config>service>vprn>nat dual-stack-lite)
[Tree] (config>router>nat>inside dual-stack-lite)

Full Context configure router nat inside dual-stack-lite
configure service vprn nat dual-stack-lite

Description Commands in this context configure Dual-Stack Lite (DS-Lite) NAT parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.298 dual-stack-lite-address

dual-stack-lite-address

Syntax **dual-stack-lite-address** *ipv6-address*
no dual-stack-lite-address

Context **[Tree]** (config>router>pcp-server>server dual-stack-lite-address)

Full Context configure router pcp-server server dual-stack-lite-address

Description This command configures the inside dual stack lite AFTR address.

The **no** form of this command reverts to the default value.

Default no dual-stack-lite-address

Parameters *ipv6-address* — Specifies the IPv6 address.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.299 duid

duid

Syntax **duid** *duid* [**iaid** *iaid*]
no duid

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6>pfx-delegate>prefix duid)

Full Context configure service ies interface ipv6 dhcp6-server prefix-delegation prefix duid

Description This command configures the DHCP Unique Identifier (DUID) of the DHCP client.

The **no** form of this command reverts to the default.

Default duid 2

Parameters *duid* — Specifies the ID of the requesting router, up to a maximum of 128 hex values. If set to a non-zero value the prefix defined will only be delegated to this router. If set to zero, the prefix is delegated to any requesting router.

iaid — Specifies the identity association identification (IAID) from the requesting router that needs to match to delegate the prefix defined in this row. If set to 0 no match on the received IAID is done.

Values 1 to 4294967295

Platforms All

8.300 dup-detect

dup-detect

Syntax **dup-detect** [**anti-spoof-mac** *mac-address*] **window** *minutes* **num-moves** *count* **hold-down** [*minutes* | **max**]
dup-detect anti-spoof-mac *mac-address* **window** *minutes* **num-moves** *count* **hold-down** [*minutes* | **max**] [**static-black-hole**]

Context **[Tree]** (config>service>vpls>proxy-arp dup-detect)
[Tree] (config>service>vpls>proxy-nd dup-detect)

Full Context configure service vpls proxy-arp dup-detect
configure service vpls proxy-nd dup-detect

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables a mechanism that detects duplicate IPs and ARP/ND spoofing attacks. Attempts (relevant to dynamic and EVPN entry types) to add the same IP (different MAC) are monitored for **window** <*minutes*>. When <*count*> is reached within that **window**, the proxy-ARP/ND entry for the suspected IP is marked as duplicate. An alarm is also triggered. This condition is cleared when **hold-down** time expires (max does not expire) or a **clear** command is issued.

If the **anti-spoof-mac** is configured, the proxy-ARP/ND offending entry's MAC is replaced with this <*mac-address*> and advertised in an unsolicited GARP/NA for local SAP/SDP-bindings, and in EVPN to remote PEs. This mechanism assumes that the same **anti-spoof-mac** is configured in all the PEs for the same service and that traffic with destination **anti-spoof-mac** received on SAPs/SDP-bindings will be dropped. An ingress **mac-filter** may be configured to drop traffic to the **anti-spoof-mac**.

The **anti-spoof-mac** can also be combined with the **static-black-hole** option. To use a black-hole MAC entry for the **anti-spoof-mac** function in a proxy-ARP/ND service, the following must be configured:

- **static-black-hole** option for the **anti-spoof-mac**
- a static black-hole MAC using the same MAC address used for the **anti-spoof-mac: static-mac mac** <*mac-address*> **create black-hole** command.

When both **anti-spoof-mac** and **static-black-hole** commands are configured, the MAC is advertised in EVPN as Static. Locally, the MAC will be shown in the FDB as CStatic and associated with a black-hole.

The combination of the **anti-spoof-mac** and the **static-black-hole** options ensures that any frame arriving in the system with MAC DA=**anti-spoof-mac** will be discarded, regardless of the ingress endpoint type (SAP/SDP-binding or EVPN) and without the need for a filter.

If the user wants to redirect the traffic with MAC DA=**anti-spoof-mac** instead of discarding it, redirect filters should be configured on SAPs/SDP-bindings instead of the **static-black-hole** option.

If the **static-black-hole** option is not configured for the **anti-spoof-mac**, the behavior is as follows:

- The **anti-spoof-mac** is not programmed in the FDB.
- Any attempt to add a Static MAC (or any other MAC) with the **anti-spoof-mac** value will be rejected by the system.
- A mac-filter is needed to discard traffic with MAC DA=**anti-spoof-mac**.

Any changes to the configuration of **anti-spoof-mac** require proxy-arp or proxy-nd to first be shut down. Refer to “ARP/ND Snooping and Proxy Support” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide: VLL, VPLS, PBB, and EVPN* for more information.

Default dup-detect window 3 num-moves 5 hold-down 9

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **window** *minutes* — Specifies the window size in minutes.

Values 1 to 15

Default 3

count — Specifies the number of moves required so that an entry is declared duplicate.

Values 3 to 10

Default 5

hold-down *minutes* — Specifies the hold-down time for a duplicate entry.

Values 2 to 60

Default 9

hold-down max — Specifies permanent hold-down time for a duplicate entry.

mac-address — Specifies the optional anti-spoof-mac to use.

Platforms All

8.301 duplex

duplex

Syntax **duplex** {**full** | **half**}

Context **[Tree]** (config>port>ethernet duplex)

Full Context configure port ethernet duplex

Description This command configures the duplex of a Fast Ethernet port when autonegotiation is disabled.

This configuration command allows for the configuration of the duplex mode of a Fast Ethernet port. If the port is configured to autonegotiate this parameter is ignored.

Default duplex full

Parameters **full** — Sets the link to full duplex mode.

half — Sets the link to half duplex mode.

Platforms All

duplex

Syntax **duplex** {**full** | **half**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (bof duplex)

Full Context bof duplex

Description This command configures the duplex mode of the CPM management Ethernet port when autonegotiation is disabled in the running configuration and the Boot Option File (BOF). If the port is configured to autonegotiate this parameter will be ignored.

Parameters **full** — Sets the link to full duplex mode.

half — Sets the link to half duplex mode.

Platforms All

8.302 dwdm

dwdm

Syntax **dwdm**

Context [Tree] (config>port dwdm)

Full Context configure port dwdm

Description This command configures the Dense Wavelength Division Multiplexing (DWDM) parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

8.303 dying-gasp

dying-gasp

Syntax [**no**] **dying-gasp**

Context [Tree] (config>port>ethernet>efm-oam>link-mon>local-sf-action>info-notification dying-gasp)

Full Context configure port ethernet efm-oam link-monitoring local-sf-action info-notification dying-gasp

Description This command sets the dying gasp Flag field in the Information OAM PDU when the local signal failure (sf-threshold) threshold is reached. This will be maintained in all subsequent Information OAM PDUs until the situation is cleared.

Interactions: The signal failure threshold will trigger these actions.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no dying-gasp

Platforms All

dying-gasp

Syntax **dying-gasp local-port-action** {**log-only** | **out-of-service**}

Context **[Tree]** (config>port>ethernet>efm-oam>peer-rdi-rx dying-gasp)

Full Context configure port ethernet efm-oam peer-rdi-rx dying-gasp

Description This command defines how to react to the reception of a dying gasp Flag field set in the informational OAMPDU.

Default dying-gasp local-port-action out-of-service

Parameters **local-port-action** — Defines whether or not the local port will be affected when a dying gasp event is received from a peer.

log-only — Keyword that prevents the port from being affected when the local peer receives a dying gasp. The dying gasp will be logged but the port will remain operational.

out-of-service — Keyword that causes the port to enter a non-operation down state with a port state of link up. The error will be logged upon reception of dying gasp. The port will not be available to service data but will continue to carry Link OAM traffic to ensure the link is monitored.

Platforms All

8.304 dying-gasp-tx-on-reset

dying-gasp-tx-on-reset

Syntax [**no**] **dying-gasp-tx-on-reset**

Context **[Tree]** (config>system>ethernet>efm-oam dying-gasp-tx-on-reset)
[Tree] (config>port>ethernet>efm-oam dying-gasp-tx-on-reset)

Full Context configure port ethernet efm-oam dying-gasp-tx-on-reset
configure system ethernet efm-oam dying-gasp-tx-on-reset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables generation of the Information OAM PDU off-cycle when the soft reset notification is received by the EFM application. The local port state remains under the control of the Soft Reset application and does not change based on this EFM function. If the port is operationally up then the local node will continue to consider the port as available for service data and forwarding. If the upstream node requires notification to route around the local node undergoing the soft reset, notification must be sent to those nodes. This is a disruptive function.

This command is disabled by default at the system level and enabled by default at the port level. The combination of the system-level and port-level configuration determines if the dying gasp on soft reset function is active on individual ports. Both the system-level and port-level commands must be enabled in order to support generation of the Information OAM PDU for soft reset. If either is disabled, dying gasp is not active on those ports. This functionality must be enabled prior to the soft reset.

When both **grace-tx-enable** and **dying-gasp-tx-on-reset** are active on the same port, **grace-tx-enable** takes precedence when a soft reset is invoked if the Peer Vendor OUI being received is 00:16:4d (ALU) or the configured **config>port>ethernet>efm-oam grace-vendor-oui** value. The **grace-tx-enable** command should not be configured if the Nokia Vendor Specific Grace TLV is not supported on the remote peer, including Nokia 7750 SR equipment prior to release 11.0 R4.

Default config>system>ethernet>efm-oam>no dying-gasp-tx-on-reset

config>port>ethernet>efm-oam>dying-gasp-tx-on-reset

Platforms All

8.305 dynamic

dynamic

Syntax **dynamic** *ip-address* [**create**]
no dynamic *ip-address*

Context **[Tree]** (config>service>vpls>proxy-arp dynamic)
[Tree] (config>service>vpls>proxy-nd dynamic)

Full Context configure service vpls proxy-arp dynamic
configure service vpls proxy-nd dynamic

Description This command creates a dynamic IP that can be associated to a MAC list. The configured dynamic IP is only converted to a dynamic entry when the resolve process for the IP has passed successfully.

A summary of the IP resolution process is as follows:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- A resolve message is sent for the configured IP as soon as the dynamic IP is configured. The message is sent with a configurable frequency of 1 to 60 minutes (using the **resolve** command); the default value is 5 minutes. The actual resolve interval is a “tittered” value of the configured interval.
- The resolve message is an ARP-request or NS message flooded to all the non-EVPN endpoints in the service, irrespective of the status of the **unknown-arp-request-flood-evpn** or **unknown-ns-flood-evpn** commands. The router sends resolve messages at the configured frequency until a dynamic entry for the IP is created in the proxy-ARP or proxy-ND table. The IP entry is created only if all of the following conditions are true.
  - An ARP, GARP, or NA message is received for the configured IP.
  - The associated MAC exists in the configured MAC list for the IP.

    If the MAC list is empty or not configured, the router does not create an entry for the IP.
- After a dynamic entry is created in the proxy-ARP or proxy-ND table, the IP->MAC entry is advertised in the EVPN.

The **no** form of the command deletes the dynamic IP and the associated proxy-ARP or proxy-ND entry, if it exists.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address.

Values ip-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
where:
x: [0 to FFFF]H
d: [0 to 255]D

Platforms All

dynamic

Syntax **dynamic**

Context **[Tree]** (config>router>if>if-attr>delay dynamic)

Full Context configure router interface if-attribute delay dynamic

Description Commands in this context configure dynamic link measurement delay options for the IP interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.306 dynamic-arp-populate

dynamic-arp-populate

Syntax [**no**] **dynamic-arp-populate**

Context **[Tree]** (config>service>vpls>proxy-arp dynamic-arp-populate)

Full Context configure service vpls proxy-arp dynamic-arp-populate

Description This command enables the addition of dynamic entries to the proxy-ARP table (disabled by default). When executed, the system will populate proxy-ARP entries from snooped GARP/ ARP messages on SAPs/SDP-bindings. These entries will be shown as dynamic.

When disabled, dynamic-arp entries will be flushed from the proxy-ARP table. Enabling dynamic-arp-populate is only recommended in networks with a consistent configuration of this command in all the PEs.

Default no dynamic-arp-populate

Platforms All

8.307 dynamic-bgp

dynamic-bgp

Syntax [**no**] **dynamic-bgp**

Context **[Tree]** (config>router>static-route-entry>black-hole dynamic-bgp)

Full Context configure router static-route-entry black-hole dynamic-bgp

Description This optional command controls the behavior of the associated static route so that if a matching BGP route to the same exact prefix is present in BGP, the static route's nexthop is set to the BGP’s nexthop value. If there is no matching active BGP route, the static route's nexthop is set to be a black-hole nexthop.

Default no dynamic-bgp

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.308 dynamic-bypass

dynamic-bypass

Syntax **dynamic-bypass** [**enable** | **disable**]
no dynamic-bypass

Context **[Tree]** (config>router>mpls dynamic-bypass)

Full Context configure router mpls dynamic-bypass

Description This command disables the creation of dynamic bypass LSPs in FRR. One or more manual bypass LSPs must be configured to protect the primary LSP path at the PLR nodes.

Default dynamic-bypass enable

Platforms All

8.309 dynamic-cost

dynamic-cost

Syntax [**no**] **dynamic-cost**

Context **[Tree]** (config>lag dynamic-cost)

Full Context configure lag dynamic-cost

Description This command enables OSPF or ISIS costing of a Link Aggregation Group (LAG) based on the available aggregated, operational bandwidth.

The path cost is dynamically calculated based on the interface bandwidth. OSPF path cost can be changed through the interface metric or the reference bandwidth.

If dynamic cost is configured, then costing is applied based on the total number of links configured and the cost advertised is inversely proportional to the number of links available at the time. This is provided that the number of links that are up exceeds the configured LAG threshold value at which time the configured threshold action determines if, and at what cost, this LAG will be advertised.

For example: Assume a physical link in OSPF has a cost associated with it of 100, and the LAG consists of four physical links. The cost associated with the logical link is 25. If one link fails then the cost would automatically be adjusted to 33.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If dynamic cost is not configured and OSPF autocost is configured, then costing is applied based on the total number of links configured. This cost will remain static provided the number of links that are up exceeds the configured LAG threshold value at which time the configured threshold action determines if and at what cost this LAG will be advertised.

If dynamic-cost is configured and OSPF autocost is not configured, the cost is determined by the cost configured on the OSPF metric provided the number of links available exceeds the configured LAG threshold value at which time the configured threshold action determines if this LAG will be advertised.

If neither dynamic-cost nor OSPF autocost are configured, the cost advertised is determined by the cost configured on the OSPF metric provided the number of links available exceeds the configured LAG threshold value at which time the configured threshold action determines if this LAG will be advertised.

The **no** form of this command removes dynamic costing from the LAG.

Default no dynamic-cost

Platforms All

8.310 dynamic-egress-label-limit

dynamic-egress-label-limit

Syntax [**no**] **dynamic-egress-label-limit**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls dynamic-egress-label-limit)
[Tree] (config>service>vpls>bgp-evpn>mpls dynamic-egress-label-limit)
[Tree] (config>service>vprn>bgp-evpn>mpls dynamic-egress-label-limit)
[Tree] (config>service>vprn>bgp-ipvpn>mpls dynamic-egress-label-limit)

Full Context configure service epipe bgp-evpn mpls dynamic-egress-label-limit
configure service vpls bgp-evpn mpls dynamic-egress-label-limit
configure service vprn bgp-evpn mpls dynamic-egress-label-limit
configure service vprn bgp-ipvpn mpls dynamic-egress-label-limit

Description This command relaxes the egress MPLS label limit check when resolving BGP next hops in the tunnel table.

For VPRN services, the OAM label is never computed and, therefore, one more egress label is allowed.

For EVPN (Epipe and VPLS) services, the system only computes the control word and ESI label if they are used. For the control word, the system reduces the egress label limit by one label if the control word is configured in the service. When configured, the ESI label is not counted for Epipes or VPLS services without an ES.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command, for EVPN, Epipe, and VPLS services, always accounts for the ESI label and control word.

Default no dynamic-egress-label-limit

Platforms All

8.311 dynamic-enforcement-policer-pool

dynamic-enforcement-policer-pool

Syntax [**no**] **dynamic-enforcement-policer-pool** *number-of-policers*

Context **[Tree]** (config>card>fp>ingress>dist-cpu-protection dynamic-enforcement-policer-pool)

Full Context configure card fp ingress dist-cpu-protection dynamic-enforcement-policer-pool

Description This command reserves a set of policers for use as dynamic enforcement policers for the Distributed CPU Protection (DCP) feature. Policers are allocated from this pool and instantiated as per-object-per-protocol dynamic enforcement policers after a local monitor is triggered for an object (such as a SAP or Network Interface). Any change to this configured value automatically clears the high water mark, timestamp, and failed allocation counts as seen under “show card x fp y dist-cpu-protection” and in the tmnxFpDcpDynEnfrcPlcrStatTable in the TIMETRA-CHASSIS-MIB. Decreasing this value to below the currently used/allocated number causes all dynamic policers to be returned to the free pool (and traffic returns to the local monitors).

Default no dynamic-enforcement-policer-pool

Parameters *number-of-policers* — specifies the number of policers to be reserved.

Values 1000 to 32000

Platforms All

8.312 dynamic-fields

dynamic-fields

Syntax [**no**] **dynamic-fields**

Context **[Tree]** (config>app-assure>group>cflowd>comp>template dynamic-fields)
[Tree] (config>app-assure>group>cflowd>rtp-perf>audio-template dynamic-fields)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>app-assure>group>cflowd>rtp-perf>video-template dynamic-fields)
[Tree] (config>app-assure>group>cflowd>rtp-perf>voice-template dynamic-fields)
[Tree] (config>app-assure>group>cflowd>tcp-perf>template dynamic-fields)
[Tree] (config>app-assure>group>cflowd>volume>template dynamic-fields)

Full Context configure application-assurance group cflowd comprehensive template dynamic-fields
configure application-assurance group cflowd rtp-performance audio-template dynamic-fields
configure application-assurance group cflowd rtp-performance video-template dynamic-fields
configure application-assurance group cflowd rtp-performance voice-template dynamic-fields
configure application-assurance group cflowd tcp-performance template dynamic-fields
configure application-assurance group cflowd volume template dynamic-fields

Description Commands in this context configure which fields are included in the exported cflowd template.

The **no** form of this command removes all configured dynamic fields from the template.

Note: This command is only supported if the **dynamic** option is configured in the **field-selection** command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

8.313 dynamic-keying

dynamic-keying

Syntax [**no**] **dynamic-keying**

Context [Tree] (config>service>ies>if>ipsec>ipsec-tunnel dynamic-keying)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel dynamic-keying)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel dynamic-keying)
[Tree] (config>router>if>ipsec>ipsec-tunnel dynamic-keying)
[Tree] (config>ipsec>trans-mode-prof dynamic-keying)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying
configure router interface ipsec ipsec-tunnel dynamic-keying
configure service ies interface ipsec ipsec-tunnel dynamic-keying
configure service vprn interface ipsec ipsec-tunnel dynamic-keying
configure service vprn interface sap ipsec-tunnel dynamic-keying

Description This command enables dynamic keying for the IPsec tunnel.

The **no** form of this command disables dynamic keying.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel dynamic-keying
- configure ipsec ipsec-transport-mode-profile dynamic-keying

VSR

- configure service ies interface ipsec ipsec-tunnel dynamic-keying
- configure router interface ipsec ipsec-tunnel dynamic-keying
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying

8.314 dynamic-mbs

dynamic-mbs

Syntax [**no**] **dynamic-mbs**

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue dynamic-mbs)

Full Context configure qos queue-group-templates egress queue-group queue dynamic-mbs

Description This command enables support for dynamically modifying the MBS size of a queue using HQoS in order to maintain the maximum latency for traffic in the queue based on the queue's configured MBS and the ratio of its operational PIR to its administrative PIR. As the HQoS algorithm updates the operational PIR, by reducing or increasing it, the MBS of the queue is adjusted accordingly.

The configuration of dynamic MBS and the configuration of queue depth monitoring (**monitor-queue-depth** command) are mutually exclusive. Queue depth monitoring is an override on the queue where the queue group is applied.

The **no** form of this command disables dynamic MBS resizing.

Default no dynamic-mbs

Platforms All

8.315 dynamic-nd-populate

dynamic-nd-populate

Syntax [**no**] **dynamic-nd-populate**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>proxy-nd dynamic-nd-populate)

Full Context configure service vpls proxy-nd dynamic-nd-populate

Description This command enables the addition of dynamic entries to the proxy-ND table. The command is disabled by default. When executed, the system will populate proxy-ND entries from snooped Neighbor Advertisement (NA) messages on SAPs/SDP-bindings, in addition to the entries coming from EVPN (if the EVPN is enabled). These entries will be shown as dynamic, as opposed to EVPN entries or static entries.

When disabled, dynamic-ND entries will be flushed from the proxy-ND table. Enabling **dynamic-nd-populate** is only recommended in networks with a consistent configuration of this command in all the PEs.

Default no dynamic-nd-populate

Platforms All

8.316 dynamic-neighbor

dynamic-neighbor

Syntax **dynamic-neighbor**

Context [Tree] (config>service>vprn>bgp>group dynamic-neighbor)

Full Context configure service vprn bgp group dynamic-neighbor

Description Commands in this context configure dynamic BGP sessions for a peer group.

Platforms All

dynamic-neighbor

Syntax **dynamic-neighbor**

Context [Tree] (config>router>bgp>group dynamic-neighbor)

Full Context configure router bgp group dynamic-neighbor

Description Commands in this context configure dynamic BGP sessions for a peer group.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.317 dynamic-neighbor-limit

dynamic-neighbor-limit

Syntax **dynamic-neighbor-limit** *peers*
no dynamic-neighbor-limit

Context **[Tree]** (config>service>vprn>bgp dynamic-neighbor-limit)
[Tree] (config>service>vprn>bgp>group dynamic-neighbor-limit)

Full Context configure service vprn bgp dynamic-neighbor-limit
configure service vprn bgp group dynamic-neighbor-limit

Description This command configures the maximum number of dynamic BGP sessions that are accepted from remote peers associated with the entire BGP instance or a specific peer group. If accepting a new dynamic session would cause either the group limit or the instance limit to be exceeded, then the new session attempt is rejected and a Notification message is sent back to the remote peer.

The **no** form of this command removes the limit on the number of dynamic sessions.

Default no dynamic-neighbor-limit

Parameters *peers* — Specifies the maximum number of dynamic BGP sessions.

Values 1 to 8192

Platforms All

dynamic-neighbor-limit

Syntax **dynamic-neighbor-limit** *peers*
no dynamic-neighbor-limit

Context **[Tree]** (config>router>bgp dynamic-neighbor-limit)
[Tree] (config>router>bgp>group dynamic-neighbor-limit)

Full Context configure router bgp dynamic-neighbor-limit
configure router bgp group dynamic-neighbor-limit

Description This command configures the maximum number of dynamic BGP sessions that will be accepted from remote peers associated with the entire BGP instance or a specific peer group. If accepting a new dynamic session would cause either the group limit or the instance limit to be exceeded, then the new session attempt is rejected and a Notification message is sent back to the remote peer.

The **no** form of this command removes the limit on the number of dynamic sessions.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no dynamic-neighbor-limit

Parameters *peers* — Specifies the maximum number of dynamic BGP sessions.

Values 1 to 8192

Platforms All

8.318 dynamic-parameters

dynamic-parameters

Syntax **dynamic-parameters**

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>protocol dynamic-parameters)

Full Context configure system security dist-cpu-protection policy protocol dynamic-parameters

Description The dynamic-parameters are used to instantiate a dynamic enforcement policer for the protocol when the associated **local-monitoring-policer** is considered as exceeding its rate parameters (at the end of a minimum monitoring time of 60 seconds).

Platforms All

8.319 dynamic-policer

dynamic-policer

Syntax **dynamic-policer**

Context **[Tree]** (config>qos>sap-egress dynamic-policer)
[Tree] (config>qos>sap-ingress dynamic-policer)

Full Context configure qos sap-egress dynamic-policer
configure qos sap-ingress dynamic-policer

Description Commands in this context configure common properties for dynamic-policers. Dynamic policers are instantiated and terminated on demand due to an action request submitted by the policy server (for example, using a Gx interface). The actions types behind dynamic policers are typically related to rate-limiting or volume monitoring. The dynamic-policers can be instantiated on demand at any time during the lifetime of the sla-profile instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.320 dynamic-services

dynamic-services

Syntax **dynamic-services**

Context **[Tree]** (config>service>vpls>sap dynamic-services)

Full Context configure service vpls sap dynamic-services

Description Commands in this context configure dynamic services parameters on a capture SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dynamic-services

Syntax **dynamic-services**

Context **[Tree]** (config>service dynamic-services)

Full Context configure service dynamic-services

Description Commands in this context configure dynamic data services. Only available on systems with multi-core CPM (CPM3 or up).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dynamic-services

Syntax [**no**] **dynamic-services**

Context **[Tree]** (debug dynamic-services)

Full Context debug dynamic-services

Description Commands in this context configure dynamic services debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.321 dynamic-services-policy

dynamic-services-policy

Syntax **dynamic-services-policy** *dynsrv-policy-name* [**create**]
no dynamic-services-policy *dynsrv-policy-name*

Context **[Tree]** (config>service>dynsvc dynamic-services-policy)

Full Context configure service dynamic-services dynamic-services-policy

Description This command creates a new dynamic services policy that can be used to create dynamic data services.

The **no** form of this command removes the dynamic services policy from the configuration. This is only allowed when there are no active dynamic data services referencing this policy.

Parameters *dynsrv-policy-name* — Specifies a unique name of a dynamic services policy up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

dynamic-services-policy

Syntax **dynamic-services-policy** *name*
no dynamic-services-policy

Context **[Tree]** (config>service>dynsvc>ladb>user>idx dynamic-services-policy)
[Tree] (config>service>vpls>sap>dyn-svc dynamic-services-policy)

Full Context configure service dynamic-services local-auth-db user-name index dynamic-services-policy
configure service vpls sap dynamic-services dynamic-services-policy

Description This command specifies the local configured dynamic data service policy to use for provisioning (local authentication database context) or authentication (**capture-sap** context) of this dynamic service. If not specified, the dynamic services policy with the name **default** is used. If the default policy does not exist, then the dynamic data service setup or authentication fails.

The **no** form of this command removes the dynamic services policy from the configuration.

Parameters *name* — Specifies a dynamic services policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.322 dynamic-topology-discover

dynamic-topology-discover

Syntax [**no**] **dynamic-topology-discover**

Context **[Tree]** (config>service>vpls>gsmp>group>ancp dynamic-topology-discover)
[Tree] (config>service>vprn>gsmp>group>ancp dynamic-topology-discover)

Full Context configure service vpls gsmp group ancp dynamic-topology-discover
configure service vprn gsmp group ancp dynamic-topology-discover

Description This command enables the ANCP dynamic topology discovery capability.

The **no** form of this command disables the feature.

Platforms All

8.323 dynamic-tunnel-redundant-next-hop

dynamic-tunnel-redundant-next-hop

Syntax **dynamic-tunnel-redundant-next-hop** *ip-address*
no dynamic-tunnel-redundant-next-hop

Context **[Tree]** (config>service>ies>if dynamic-tunnel-redundant-next-hop)
[Tree] (config>service>vprn>if dynamic-tunnel-redundant-next-hop)

Full Context configure service ies interface dynamic-tunnel-redundant-next-hop
configure service vprn interface dynamic-tunnel-redundant-next-hop

Description This command specifies redundant next-hop address on a public or private IPsec interface (with public or private tunnel-sap) for dynamic IPsec tunnel. The specified next-hop address is used by a standby node to shunt traffic to master in case it receives the address.

The next-hop address is resolved in the routing table of a corresponding service.

Default no dynamic-tunnel-redundant-next-hop

Parameters *ip-address* — Specifies the dynamic ISA tunnel redundant next-hop address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

8.324 dynmldp

dynmldp

Syntax **dynmldp** [**detail**]
no dynmldp

Context **[Tree]** (debug>router>pim dynmldp)

Full Context debug router pim dynmldp

Description This command enables debugging for dynamic MLDP.

The **no** form of this command disables dynamic MLDP debugging.

Parameters **detail** — Debugs detailed dynamic MLDP information.

Platforms All

8.325 dynsvc-password

dynsvc-password

Syntax **dynsvc-password** *password* [**hash** | **hash2**]
no dynsvc-password

Context **[Tree]** (config>system>security>password dynsvc-password)

Full Context configure system security password dynsvc-password

Description

Note: See also the description for the **enable-dynamic-services-config** command.

This command allows a user with admin permissions to configure a system wide password which enables a user to enter a special dynamic services configuration mode.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password are determined by the **complexity** command.

The **no** form of this command removes the dynsvc password from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *password* — Configures the password which enables a user to enter a special dynamic services configuration mode. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the **hash2** keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9 e Commands

9.1 e-counters

e-counters

Syntax **e-counters** [**all**]
no e-counters

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue e-counters)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue e-counters)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters

Description Commands in this context configure egress counter parameters for this custom record.

The **no** form of this command reverts to the default.

Parameters **all** — Includes all counters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

e-counters

Syntax **e-counters** [**all**]
no e-counters

Context **[Tree]** (config>log>acct-policy>cr>policer e-counters)
[Tree] (config>log>acct-policy>cr>queue e-counters)
[Tree] (config>log>acct-policy>cr>ref-policer e-counters)
[Tree] (config>log>acct-policy>cr>ref-queue e-counters)

Full Context configure log accounting-policy custom-record policer e-counters
configure log accounting-policy custom-record queue e-counters
configure log accounting-policy custom-record ref-policer e-counters
configure log accounting-policy custom-record ref-queue e-counters

Description This command configures egress counter parameters for this custom record.

The **no** form of this command reverts all egress counters to their default value.

Default e-counters

Parameters **all** — Specifies that all egress counters should be included.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

9.2 e1

e1

Syntax **e1** [*e1-id*]

Context **[Tree]** (config>port>tdm e1)

Full Context configure port tdm e1

Description Commands in this context configure E-1 parameters. E-1 is a basic time division multiplexing scheme used to carry digital circuits. It is also a standard WAN digital communication format designed to operate over copper facilities at a rate of 2.048 Mb/s.

North America uses the T-Carrier system while Europe uses the E-Carrier system of transmission, using multiples of the DS system. Digital signals are carried inside the carrier systems.

The **no** form of this command disables E-1 capabilities.

Parameters *e1-id* — Specifies the E-1 channel being created.

Values E1: 1 to 21, e1-sonet-sdh-index

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

9.3 e2e-protection-type

e2e-protection-type

Syntax **e2e-protection-type** *protection-type*
no e2e-protection-type

Context **[Tree]** (config>router>gmpls>lsp e2e-protection-type)

Full Context configure router gmpls lsp e2e-protection-type

Description This command defines the end-to-end recovery type for the gLSP. This is the recovery model between the source and terminating UNI-C nodes of the GMPLS LSP.

The **no** form of this command removes any configured end-to-end recovery, and the GMPLS LSP becomes unprotected.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default e2e-protection-type unprotected

Parameters *protection-type* — Specifies the end-to-end GMPLS recovery type.

Values unprotected | one-to-N | sbr

Default unprotected

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.4 e3

e3

Syntax [**no**] **e3** [*sonet-sdh-index*]

Context **[Tree]** (config>port>tdm e3)

Full Context configure port tdm e3

Description Commands in this context configure E-3 parameters. E-3 lines provide a speed of 44.736 Mb/s and is also frequently used by service providers. E-3 lines carry 16 E-1 signals with a data rate of 34.368 Mb/s.

An E-3 connection typically supports data rates of about 43 Mb/s. An E-3 line actually consists of 672 individual channels, each supporting 64 kb/s. E-3 lines are used mainly by Service Providers to connect to the Internet backbone and for the backbone itself.

Depending on the MDA type, the E-3 parameters must be disabled if clear channel is enabled by default (for example, on the m12-ds3e3 MDA). Clear channel is a channel that uses out-of-band signaling, not in-band signaling, so the channel's entire bit rate is available. Channelization must be explicitly specified. Note that if E-3 nodes are provisioned on the channelized SONET/SDH MDA you must provision the parent STS-1 SONET/STM0 SDH path first.

North America uses the T-Carrier system while Europe uses the E-Carrier system of transmission, using multiples of the DS system. Digital signals are carried inside the carrier systems.

The **no** form of this command disables E-3 capabilities.

Parameters *sonet-sdh-index* — Specifies the components making up the specified SONET/SDH Path. Depending on the type of SONET/SDH port the *sonet-sdh-index* must specify more path indexes to specify the payload location of the path. The *sonet-sdh-index* differs for SONET and SDH ports.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.5 ea-length

ea-length

Syntax **ea-length** *ea-bits-length*
no ea-length

Context **[Tree]** (config>service>nat>map-domain>mapping-rule ea-length)

Full Context configure service nat map-domain mapping-rule ea-length

Description This command configures the length of EA bits in the MAP rule. The **no ea-length** statement sets the **ea-length** to 0.

Default no ea-length

Parameters *ea-bits-length* — Specifies the length of the EA bits.

Values 1 to 48

Platforms VSR

9.6 eapol-destination-address

eapol-destination-address

Syntax **eapol-destination-address** *mac*
no eapol-destination-address

Context **[Tree]** (config>port>ethernet>dot1x>macsec>sub-port eapol-destination-address)

Full Context configure port ethernet dot1x macsec sub-port eapol-destination-address

Description The EAPoL destination MAC address uses a destination multicast MAC address of 01:80:C2:00:00:03. Some networks cannot tunnel this packet over the network and consume these packets, causing the MKA session to fail. This command can change the destination MAC of the EAPoL to the unicast address of the MACsec peer, and as such, the EAPoL and MKA signaling will be unicasted between two peers.

The **no** form of this command returns the value to the default.

Default no eapol-destination-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac* — Specifies the desired destination MAC address to be used by the EAPOL MKA packets of this sub-port.

Values aa:bb:cc:dd:ee:ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.

Platforms All

9.7 ebgp-default-reject-policy

ebgp-default-reject-policy

Syntax **ebgp-default-reject-policy** [**import**] [**export**]
no ebgp-default-reject-policy

Context **[Tree]** (config>service>vprn>bgp ebgp-default-reject-policy)
[Tree] (config>service>vprn>bgp>group ebgp-default-reject-policy)
[Tree] (config>service>vprn>bgp>group>neighbor ebgp-default-reject-policy)

Full Context configure service vprn bgp ebgp-default-reject-policy
configure service vprn bgp group ebgp-default-reject-policy
configure service vprn bgp group neighbor ebgp-default-reject-policy

Description This command configures the default import and export policy behavior for EBGP neighbors.

The **no** form of this command removes the default import and export policy behavior.

Default no ebgp-default-reject-policy

Parameters **import** — Specifies the default reject import policy for EBGP neighbors.

export — Specifies the default reject export policy for EBGP neighbors.

Platforms All

ebgp-default-reject-policy

Syntax **ebgp-default-reject-policy** [**import**] [**export**]
no ebgp-default-reject-policy

Context **[Tree]** (config>router>bgp ebgp-default-reject-policy)
[Tree] (config>router>bgp>group ebgp-default-reject-policy)
[Tree] (config>router>bgp>group>neighbor ebgp-default-reject-policy)

Full Context configure router bgp ebgp-default-reject-policy
configure router bgp group ebgp-default-reject-policy
configure router bgp group neighbor ebgp-default-reject-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the default import and export policy behavior for EBGP neighbors.

The **no** form of this command removes the default import and export policy behavior.

Default no ebgp-default-reject-policy

Parameters **import** — Specifies the default reject import policy for EBGP neighbors.

export — Specifies the default reject export policy for EBGP neighbors.

Platforms All

9.8 ebgp-ibgp-equal

ebgp-ibgp-equal

Syntax **ebgp-ibgp-equal** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**]
no ebgp-ibgp-equal

Context **[Tree]** (config>service>vprn>bgp>best-path-selection ebgp-ibgp-equal)

Full Context configure service vprn bgp best-path-selection ebgp-ibgp-equal

Description This command instructs the BGP decision process to ignore the difference between EBGP and IBGP routes in selecting the best path and eligible multipaths (if multipath and ECMP are enabled). The result is a form of EIBGP load-balancing in a multipath scenario.

The operator can apply the behavior selectively to only certain types of routes by specifying one or more address family names in the command.

The **no** form of this command configures the router in the BGP decision process to prefer an EBGP learned route over an IBGP learned route.

Default no ebgp-ibgp-equal

Parameters **ipv4** — Specifies that the command should be applied to unlabeled unicast IPv4 routes.

ipv6 — Specifies that the command should be applied to unlabeled unicast IPv6 routes.

label-ipv4 — Specifies that the command should be applied to labeled IPv4 routes.

label-ipv6 — Specifies that the command should be applied to labeled IPv6 routes.

Platforms All

ebgp-ibgp-equal

Syntax **ebgp-ibgp-equal** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**] [**vpn-ipv4**] [**vpn-ipv6**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ebgp-ibgp-equal

Context [Tree] (config>router>bgp>best-path-selection ebgp-ibgp-equal)

Full Context configure router bgp best-path-selection ebgp-ibgp-equal

Description This command instructs the BGP decision process to ignore the difference between EBGP and IBGP routes in selecting the best path and eligible multipaths (if multipath and ECMP are enabled). The result is a form of EIBGP load-balancing in a multipath scenario.

By default (with the **no** form of this command), the BGP decision process prefers an EBGP learned route over an IBGP learned route.

The behavior can be applied selectively to only certain types of routes by specifying one or more address family names in the command. If no families are specified, the command applies to IPv4, IPv6, label-IPv4, label-IPv6, VPN-IPv4, and VPN-IPv6 routes.

Default no ebgp-ibgp-equal

Parameters **ipv4** — Specifies that the command should be applied to unlabeled unicast IPv4 routes.

ipv6 — Specifies that the command should be applied to unlabeled unicast IPv6 routes.

label-ipv4 — Specifies that the command should be applied to labeled unicast IPv4 routes.

label-ipv6 — Specifies that the command should be applied to labeled unicast IPv6 routes.

vpn-ipv4 — Specifies that the command should be applied to IPv4 VPN routes.

vpn-ipv6 — Specifies that the command should be applied to IPv6 VPN routes.

Platforms All

9.9 ecdsa

ecdsa

Syntax **ecdsa**

Context [Tree] (config>system>security>user>public-keys ecdsa)

Full Context configure system security user public-keys ecdsa

Description This command allows the user to enter the context to configure ECDSA public keys.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.10 ecdsa-key

ecdsa-key

Syntax **ecdsa-key** *key-id* [**create**]
no ecdsa-key *key-id*

Context **[Tree]** (config>system>security>user>public-keys>ecdsa ecdsa-key)

Full Context configure system security user public-keys ecdsa ecdsa-key

Description This command creates an ECDSA public key and associates it with the username. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.

Parameters **create** — Keyword used to create an ECDSA key. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

key-id — Specifies the key identifier.

Values 1 to 32

Platforms All

9.11 echo

echo

Syntax **echo** [*text-to-echo*] [*extra-text-to-echo*] [*more-text*]

Context **[Tree]** (global echo)

Full Context global echo

Description This command echoes arguments on the command line. The primary use of this command is to allow messages to be displayed to the screen in files executed with the **exec** command.

Parameters *text-to-echo* — Specifies a text string to be echoed, up to 256 characters.

extra-text-to-echo — Specifies more text to be echoed, up to 256 characters.

more-text — Specifies more text to be echoed, up to 256 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.12 echo-interval

echo-interval

Syntax **echo-interval** *seconds*
no echo-interval

Context **[Tree]** (config>open-flow>of-switch echo-interval)

Full Context configure open-flow of-switch echo-interval

Description This command configures the Echo Request interval for monitoring the OpenFlow control channels to the controllers for this OpenFlow switch instance.

The **no** form of this command restores default value.

Default echo-interval 10

Parameters *seconds* — Specifies an interval, in seconds.

Values 1 to 3600

Platforms All

9.13 echo-multiple

echo-multiple

Syntax **echo-multiple** *value*
no echo-multiple

Context **[Tree]** (config>open-flow>of-switch echo-multiple)

Full Context configure open-flow of-switch echo-multiple

Description This command configures the number of consecutive Echo Reply messages that must be lost to declare OF control channel down.

The **no** form of this command restores default value.

Default echo-multiple 3

Parameters *value* — Specifies the threshold value for the number of consecutive Echo Rely messages lost.

Values 3 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

9.14 echo-receive

echo-receive

Syntax **echo-receive** *echo-interval*
no echo-receive

Context **[Tree]** (config>router>bfd>bfd-template echo-receive)

Full Context configure router bfd bfd-template echo-receive

Description This command sets the minimum echo receive interval, in milliseconds, for a session. This is not used by a BFD session for MPLS-TP.

The **no** form of this command reverts to the default value.

Default echo-receive 100

Parameters *echo-interval* — Specifies the echo receive interval.

Values 100 ms to 100,000 ms in 1 ms increments

Default 100

Platforms All

9.15 ecmp

ecmp

Syntax **ecmp** *max-ecmp-routes*

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls ecmp)
[Tree] (config>service>epipe>bgp-evpn>srv6 ecmp)
[Tree] (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel ecmp)
[Tree] (config>service>epipe>bgp-evpn>vxlan ecmp)
[Tree] (config>service>vpls>bgp-evpn>mpls ecmp)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel ecmp)
[Tree] (config>service>vpls>bgp-evpn>vxlan ecmp)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel ecmp
configure service epipe bgp-evpn mpls ecmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe bgp-evpn segment-routing-v6 ecmp
configure service epipe bgp-evpn vxlan ecmp
configure service vpls bgp-evpn mpls auto-bind-tunnel ecmp
configure service vpls bgp-evpn mpls ecmp
configure service vpls bgp-evpn vxlan ecmp

Description When configured in a VPLS service, this command controls the number of paths that are allowed to reach a specified MAC address when that MAC in the FDB is associated to a remote all-active multi-homed ES.

The configuration of two or more ECMP paths to a specified MAC enables the aliasing function described in RFC 7432.

When used in an Epipe service, this command controls the number of paths that are allowed to reach a specified remote Ethernet tag that is associated to an ES destination.

Default ecmp 1

Parameters *max-ecmp-routes* — Specifies the number of paths allowed to the same multi-homed MAC address or Ethernet tag.

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service epipe bgp-evpn segment-routing-v6 ecmp

All

- configure service vpls bgp-evpn mpls ecmp
- configure service epipe bgp-evpn mpls ecmp
- configure service epipe bgp-evpn vxlan ecmp
- configure service vpls bgp-evpn vxlan ecmp
- configure service epipe bgp-evpn mpls auto-bind-tunnel ecmp
- configure service vpls bgp-evpn mpls auto-bind-tunnel ecmp

ecmp

Syntax **ecmp** *max-ecmp-routes*
no ecmp

Context **[Tree]** (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel ecmp)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel ecmp)

Full Context configure service vprn bgp-evpn mpls auto-bind-tunnel ecmp
configure service vprn bgp-ipvpn mpls auto-bind-tunnel ecmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of tunnels that may be used as ECMP next-hops for the VPRN. This value overrides any values that are configured using the **config**>**service**>**vprn**>**ecmp** command.

The **no** form of this command removes the configured overriding value, and the value configured using the **config**>**service**>**vprn**>**ecmp** command is used.

Default ecmp 1

Parameters *max-ecmp-routes* — Specifies the maximum number of tunnels that may be used as ECMP next-hops for the VPRN.

Values 1 to 32

Default 1

Platforms All

ecmp

Syntax **ecmp** *max-ecmp-routes*
no ecmp

Context **[Tree]** (config>router ecmp)

Full Context configure router ecmp

Description This command enables ECMP and configures the number of routes for path sharing; for example, the value 2 means two equal cost routes will be used for cost sharing.

ECMP can only be used for routes learned with the same preference and same protocol.

When more ECMP routes are available at the best preference than configured in *max-ecmp-routes,* then the lowest next-hop IP address algorithm is used to select the number of routes configured in *max-ecmp-routes*.

The **no** form of this command disables ECMP path sharing. If ECMP is disabled and multiple routes are available at the best preference and equal cost, then the route with the lowest next-hop IP address is used.

Default no ecmp

Parameters *max-ecmp-routes* — Specifies the maximum number of equal cost routes allowed on this routing table instance, expressed as a decimal integer. Setting ECMP *max-ecmp-routes* to 1 yields the same result as entering **no ecmp**.

Values 1 to 64

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ecmp

Syntax **ecmp** *max-ecmp-routes*
no ecmp

Context **[Tree]** (config>service>vprn ecmp)

Full Context configure service vprn ecmp

Description This command enables equal-cost multipath (ECMP) and configures the number of routes for path sharing. For example, the value of 2 means that 2 equal cost routes are used for cost sharing.

ECMP groups form when the system routes to the same destination with equal cost values. Routing table entries can be entered manually (as static routes), or they can be formed when neighbors are discovered and routing table information is exchanged by routing protocols. The system can balance traffic across the groups with equal costs.

ECMP can only be used for routes learned with the same preference and same protocol. See the discussion on preferences in the **application6** command.

When more ECMP routes are available at the best preference than configured by the *max-ecmp-routes* parameter, then the lowest next-hop IP address algorithm is used to select the number of routes configured.

The **no** form of this command disables ECMP path sharing. If ECMP is disabled and multiple routes are available at the best preference and equal cost, the newly updated route is used.

Default no ecmp

Parameters *max-ecmp-routes* — Specifies the maximum number of routes for path sharing.

Values 1 to 64

Platforms All

9.16 ecmp-opt-threshold

ecmp-opt-threshold

Syntax **ecmp-opt-threshold** *preference-level*
no ecmp-opt-threshold

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle ecmp-opt-threshold)

Full Context configure mcast-management multicast-info-policy bundle ecmp-opt-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the preference level threshold where multicast ECMP path management can dynamically optimize channels based on topology or bandwidth events. If the channels preference is equal to or less than the ecmp-opt-threshold, ECMP can move the channel between ECMP paths when bandwidth distribution events happen. Channels with a preference level higher than the threshold are moved during these events.

The default ECMP optimization limit threshold is 7. This means that multicast channels with a preference level of 0 to 7 (all channels) are allowed to move between ECMP paths. The ecmp-opt-threshold command can be used to change the default threshold.

Changing the threshold causes all channels ECMP optimization eligibility to be reevaluated.

The **no** form of this command restores the default ECMP optimization preference threshold value.

Default ecmp-opt-threshold 7

Parameters *preference-level* — The preference-level parameter is required when specifying the ecmp-opt-threshold. An integer value from 0 to 7 must be specified.

Values 0 to 7

Platforms All

9.17 ecmp-unequal-cost

ecmp-unequal-cost

Syntax [**no**] **ecmp-unequal-cost**

Context **[Tree]** (config>service>vprn ecmp-unequal-cost)

Full Context configure service vprn ecmp-unequal-cost

Description This command relaxes the constraint that ECMP multipaths must have the same IGP cost to reach the BGP next-hop. When VPN routes for the same IP prefix are imported into a VPRN service, they are eligible to be used as multipaths. The resulting route is programmed as an ECMP IP route.

The BGP best path selection algorithm is the basis for choosing the set of imported VPN routes that can be combined to form an ECMP route. Normally (unless an **ignore-nh-metric** command is configured), the BGP decision process gives higher preference to VPN routes with a lower next-hop cost if other, more significant criteria, are tied. In these circumstances, a VPN route cannot be an eligible multipath if it does not have the same next-hop cost as the best VPN route. Configuring this command removes this restriction and allows the multipaths to have different (meaning lower) next-hop costs than the best route. This broadens the applicability of multipath and can result in better load balancing in the network.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command applies only to the following types of routes imported by a VPRN.

- vpn-ipv4
- vpn-ipv6
- mcast-vpn-ipv4
- mcast-vpn-ipv6

The **no** form of this command restores the default behavior that requires next-hop costs of multipaths to be equal, unless the next-hop cost is completely removed from the BGP decision process.

Default ecmp-unequal-cost

Platforms All

9.18 ect-algorithm

ect-algorithm

Syntax **ect-algorithm fid-range** *fid-range* {**low-path-id**| **high-path-id**}

Context **[Tree]** (config>service>vpls>spb>level ect-algorithm)

Full Context configure service vpls spb level ect-algorithm

Description This command configures the ect-algorithm associated with a FID. Names are:

- low-path-id
- high-path-id

The algorithm for low-path-id chooses the path with the lowest metric and uses the sum of each Bridge-ID to break-ties (in this case preferring the lowest bridge identifiers).

The algorithm for high-path-id choose the path with the lowest metric and the sum of each Bridge-ID (after each one is modified by the algorithm mask) to break-ties (in this case preferring the highest bridge identifiers).

A Forwarding Identifier (FID) is an abstraction of the IEEE 802.1 SPB Base VID and represents the VLAN (B-VPLS) in IS-IS LSPs. B-VPLS services with the same FID share B-MACs and I-SIDs. (the SAP encapsulation VLAN tag may be set to the same value as the FID or to any other valid VLAN tag). One or more FIDs can be associated with an ECT-algorithm by using the FID range. User B-VPLS services may share the same FID as the control B-VPLS or use independent FIDs where each FID has an assigned ect-algorithm. B-VPLS services with i-vpls services must have an independent FID. B-VPLS services with only PBB Epipes may share FIDs with other B-VPLS services including the control B-VPLS service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The ect-algorithm is associated with the FID and can only be changed only when there are no VPLS, SAPs or SDP bindings associated with the FID. The FID must be independent from the FID assigned to other services.

Default ect-algorithm fid-range 1-4095 low-path-id

Parameters *name* — low-path-id, high-path-id.

fid-range — Range of Forwarding Identifier values.

Values 1 to 4095

Platforms All

9.19 edge-port

edge-port

Syntax [**no**] **edge-port**

Context **[Tree]** (config>service>vpls>sap>stp edge-port)
[Tree] (config>service>template>vpls-sap-template>stp edge-port)
[Tree] (config>service>vpls>spoke-sdp>stp edge-port)

Full Context configure service template vpls-sap-template stp edge-port
configure service vpls sap stp edge-port
configure service vpls spoke-sdp stp edge-port

Description This command configures the SAP or SDP as an edge or non-edge port. If **auto-edge** is enabled for the SAP, this value will be used only as the initial value.

Note: The function of the **edge-port** command is similar to the **rapid-start** command. It tells RSTP that it is on the edge of the network (for example, there are no other bridges connected to that port) and, as a consequence, it can immediately transition to a forwarding state if the port becomes available.

RSTP, however, can detect that the actual situation is different from what **edge-port** may indicate.

Initially, the value of the SAP or spoke-SDP parameter is set to edge-port. This value will change if:

- A BPDU is received on that port. This means that after all there is another bridge connected to this port. Then the edge-port becomes disabled.
- If auto-edge is configured and no BPDU is received within a certain period of time, RSTP concludes that it is on an edge and enables the edge-port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the edge port setting to the default value.

Default no edge-port

Platforms All

edge-port

Syntax [**no**] **edge-port**

Context **[Tree]** (config>service>pw-template>stp edge-port)

Full Context configure service pw-template stp edge-port

Description This command configures the SAP or SDP as an edge or non-edge port. If **auto-edge** is enabled for the SAP, this value will be used only as the initial value.

Note: On the 7750 SR and the 7950 XRS, the function of the **edge-port** command is similar to the **rapid-start** command. It tells RSTP that it is on the edge of the network (for example, there are no other bridges connected to that port) and, as a consequence, it can immediately transition to a forwarding state if the port becomes available.

RSTP, however, can detect that the actual situation is different from what **edge-port** may indicate.

Initially, the value of the SAP or spoke SDP parameter is set to edge-port. This value will change if:

- A BPDU is received on that port. This means that after all there is another bridge connected to this port. Then the edge-port becomes disabled.
- If auto-edge is configured and no BPDU is received within a certain period of time, RSTP concludes that it is on an edge and enables the edge-port.

The **no** form of this command returns the edge port setting to the default value.

Default no edge-port

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.20 edit

edit

Syntax **edit** [**exclusive**]

Context **[Tree]** (candidate edit)

Full Context candidate edit

Description This command enables the edit-cfg mode where changes can be made to the candidate configuration and sets the edit-point to the end of the candidate. In edit-cfg mode the CLI prompt contains **edit-cfg** near the root of the prompt. Commands in the **candidate** CLI branch, except **candidate edit**, are available only when in edit-cfg mode.

Parameters **exclusive** — Allows a user to exclusively create a candidate configuration by blocking other users (and other sessions of the same user) from entering edit-cfg mode. Exclusive edit-cfg mode can only be entered if the candidate configuration is empty and no user is in edit-cfg mode. Once a user is in exclusive edit-cfg mode no other users/sessions are allowed in edit-cfg mode. The user must either commit or discard the exclusive candidate before leaving exclusive edit-cfg mode. If the CLI session times out while a user is in exclusive edit-cfg mode then the contents of the candidate are discarded. The **admin disconnect** command can be used to force a user to disconnect (and to clear the contents of the candidate) if they have the candidate locked.

Platforms All

9.21 edit-config

edit-config

Syntax [**no**] **edit-config**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization edit-config)

Full Context configure system security profile netconf base-op-authorization edit-config

Description This command enables the NETCONF edit-config operation.

The **no** form of this command disables the operation.

Default no edit-config

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

9.22 efm

efm

Syntax **efm** *port-id* **local-loopback** {**start** | **stop**}
efm *port-id* **remote-loopback** {**start** | **stop**}

Context **[Tree]** (oam efm)

Full Context oam efm

Description This command enables Ethernet in the First Mile (EFM) OAM tests loopback tests on the specified port. The EFM OAM remote loopback OAMPDU is sent to the peering device to trigger remote loopback.

When EFM OAM is disabled or shutdown on a port, the dying gasp flag for the OAMPDU is set for the OAMPDUs sent to the peer. This speeds up the peer loss detection time.

Parameters *port-id* — Specifies the port ID.

Note: On the 7950 XRS, The XMA ID takes the place of the MDA.

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

local-loopback {**start** | **stop**} — Specifies whether to start or stop local loopback tests on the specified port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-loopback {**start** | **stop**} — Specifies whether to start or stop remote Ethernet in the First Mile (EFM) OAM loopback tests on the specified port. The EFM OAM remote loopback OAMPDU is sent to the peering device to trigger remote loopback.

For EFM OAM tunneling to function properly, EFM OAM tunneling should be configured for VLL services or a VPLS service with two SAPs only.

Platforms All

9.23 efm-oam

efm-oam

Syntax **efm-oam**

Context **[Tree]** (config>port>ethernet efm-oam)

Full Context configure port ethernet efm-oam

Description This command configures EFM-OAM attributes.

Platforms All

9.24 egr-ip-load-balancing

egr-ip-load-balancing

Syntax **egr-ip-load-balancing** {**source** | **destination** | **inner-ip**}
no egr-ip-load-balancing

Context **[Tree]** (config>service>ies>if>load-balancing egr-ip-load-balancing)

Full Context configure service ies interface load-balancing egr-ip-load-balancing

Description This command specifies whether to include the source address or destination address or both in the LAG/ECMP hash on IP interfaces. Additionally, when l4-load-balancing is enabled, the command also applies to the inclusion of source/destination port in the hash inputs.

The **no** form of this command includes both source and destination parameters.

Default no egr-ip-load-balancing

Parameters *source* — Specifies using the source address and, if l4-load balancing is enabled, the source port in the hash, ignore destination address/port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

destination — Specifies using the destination address and, if l4-load balancing is enabled, the destination port in the hash, ignore source address/port.

inner-ip — Specifies using the inner IP header parameters instead of the outer IP header parameters in the LAG/ECMP hash for IPv4 encapsulated traffic.

Platforms All

egr-ip-load-balancing

Syntax **egr-ip-load-balancing** {**source** | **destination** | **inner-ip**}
no egr-ip-load-balancing

Context **[Tree]** (config>service>vprn>if>load-balancing egr-ip-load-balancing)
[Tree] (config>service>vprn>if>nw-if>load-balancing egr-ip-load-balancing)

Full Context configure service vprn interface load-balancing egr-ip-load-balancing
configure service vprn interface nw-if load-balancing egr-ip-load-balancing

Description This command specifies whether to include the source address or destination address or both in the LAG/ECMP hash on IP interfaces. Additionally, when l4-load-balancing is enabled, the command also applies to the inclusion of source/destination port in the hash inputs.

The **no** form of this command includes both source and destination parameters.

Default no egr-ip-load-balancing

Parameters **source** — Specifies using the source address and (if l4-load balancing is enabled) source port in the hash, ignore destination address/port.

destination — Specifies using the destination address and (if l4-load balancing is enabled) destination port in the hash, ignore source address/port.

inner-ip — Specifies use of the inner IP header parameters instead of outer IP header parameters in LAG/ECMP hash for IPv4 encapsulated traffic.

Platforms All

egr-ip-load-balancing

Syntax **egr-ip-load-balancing** {**source** | **destination** | **inner-ip**}
no egr-ip-load-balancing

Context **[Tree]** (config>router>if>load-balancing egr-ip-load-balancing)

Full Context configure router interface load-balancing egr-ip-load-balancing

Description This command specifies whether to include source address or destination address or both in LAG/ECMP hash on IP interfaces. Additionally, when l4-load-balancing is enabled the command applies also to inclusion of source/destination port in the hash inputs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command includes both source and destination parameters.

Default no egr-ip-load-balancing

Parameters **source** — Specifies using source address and (if l4-load balancing is enabled) source port in the hash, ignore destination address/port

destination — Specifies using destination address and (if l4-load balancing is enabled) destination port in the hash, ignore source address/port.

inner-ip — Specifies use of the inner IP header parameters instead of outer IP header parameters in LAG/ECMP hash for IPv4 encapsulated traffic.

Platforms All

9.25 egr-percentage-of-rate

egr-percentage-of-rate

Syntax **egr-percentage-of-rate** *egr-rate-percentage*
no egr-percentage-of-rate

Context **[Tree]** (config>port>modify-buffer-allocation-rate egr-percentage-of-rate)

Full Context configure port modify-buffer-allocation-rate egr-percentage-of-rate

Description The **egr-percentage-of-rate** command increases or decreases the active bandwidth associated with the egress port that affects the amount of egress buffer space managed by the port. Changing a ports active bandwidth using the **egr-percentage-of-rate** command is an effective means of artificially lowering the buffers managed by one egress port and giving them to other egress ports on the same MDA.

The **egr-percentage-of-rate** command accepts a percentage value that increases or decreases the active bandwidth based on the defined percentage. A value of 50% causes the active bandwidth to be reduced by 50%. A value of 150% causes the active bandwidth to be increased by 50%. Values from 1 to 1000 percent are supported.

A value of 100 (the default value) is equivalent to executing the **no egr-percentage-of-rate** command and restores the egress active rate to the normal value.

The **no** form of this command removes any artificial increase or decrease of the egress active bandwidth used for egress buffer space allocation to the port. The **no egr-percentage-of-rate** command sets the egress rate percentage to 100%.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *egr-rate-percentage* — The *egr-rate-percentage* parameter is required and specifies the percentage value used to modify the current egress active bandwidth of the port. This does not actually change the bandwidth available on the port in any way. The defined *egr-rate-percentage* parameter is multiplied by the egress active bandwidth of the port. A value of 150 results in an increase of 50% (1.5 x Rate).

Values 1 to 1000

Default 100 (no change to active rate)

Platforms All

9.26 egr-vtep

egr-vtep

Syntax **egr-vtep** {*ip-address* | *ipv6-address*}
no egr-vtep

Context **[Tree]** (config>service>epipe>vxlan egr-vtep)
[Tree] (config>service>vpls>vxlan egr-vtep)

Full Context configure service epipe vxlan egr-vtep
configure service vpls vxlan egr-vtep

Description This command configures the static destination VTEP IP used when originating VXLAN packets for the service.

Parameters *ip-address* — Specifies the IPv4 address used as the destination VTEP when originating VXLAN packets for the service.

ipv6-address — Specifies the IPv6 address used as the destination VTEP when originating VXLAN packets for the service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls vxlan egr-vtep

All

- configure service epipe vxlan egr-vtep

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.27 egr-weight

egr-weight

Syntax **egr-weight access** *access-weight* **network** *network-weight*
no egr-weight

Context **[Tree]** (config>port>hybrid-buffer-allocation egr-weight)

Full Context configure port hybrid-buffer-allocation egr-weight

Description This command configures the sharing of the egress buffers allocated to a hybrid port among the access and network contexts. By default, it is split equally between network and access.

The **no** form of this command reverts to the default values for the egress access and network weights.

Parameters *access-weight* — Specifies the access weight as an integer.

Values 0 to 100

Default 50

network-weight — Specifies the network weight as an integer.

Values 0 to 100

Default 50

Platforms All

9.28 egress

egress

Syntax **egress**

Context **[Tree]** (config>subscr-mgmt>ancp>ancp-policy egress)

Full Context configure subscriber-mgmt ancp ancp-policy egress

Description Commands in this context configure egress ANCP policy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>subscr-mgmt>msap-policy>ies-vprn egress)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only egress)

Full Context configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters egress
configure subscriber-mgmt msap-policy vpls-only-sap-parameters egress

Description Commands in this context configure egress policies for Managed SAPs (MSAPs).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

egress

Syntax **egress**

Context **[Tree]** (config>service>vprn>if>spoke-sdp egress)
[Tree] (config>service>vprn>red-if>spoke-sdp egress)

Full Context configure service vprn interface spoke-sdp egress
configure service vprn redundant-interface spoke-sdp egress

Description This command configures egress SDP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp egress

All

- configure service vprn interface spoke-sdp egress

egress

Syntax **egress**

Context **[Tree]** (config>subscr-mgmt>sla-profile egress)

Full Context configure subscriber-mgmt sla-profile egress

Description Commands in this context configure egress parameters for the SLA profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>if>sap egress)
[Tree] (config>service>ies>sub-if>grp-if>sap egress)
[Tree] (config>service>vpls>sap egress)
[Tree] (config>service>vprn>sub-if>grp-if>sap egress)

Full Context configure service ies interface sap egress
configure service ies subscriber-interface group-interface sap egress
configure service vpls sap egress
configure service vprn subscriber-interface group-interface sap egress

Description Commands in this context configure egress Quality of Service (QoS) policies and filter policies.

If no QoS policy is defined, the system default QoS policy is used for egress processing. If no egress filter is defined, no filtering is performed.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap egress
- configure service ies subscriber-interface group-interface sap egress

All

- configure service ies interface sap egress
- configure service vpls sap egress

egress

Syntax **egress**

Context **[Tree]** (config>service>vpls>sap egress)

Full Context configure service vpls sap egress

Description Commands in this context configure egress filter policies.

If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If **no** egress filter is defined, no filtering is performed.

Platforms All

egress

Syntax **egress**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>spoke-sdp egress)
[Tree] (config>service>ies>red-if>spoke-sdp egress)
[Tree] (config>service>vpls>mesh-sdp egress)
[Tree] (config>service>vpls>spoke-sdp egress)

Full Context configure service ies interface spoke-sdp egress
configure service ies redundant-interface spoke-sdp egress
configure service vpls mesh-sdp egress
configure service vpls spoke-sdp egress

Description Commands in this context configure egress SDP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies redundant-interface spoke-sdp egress

All

- configure service vpls spoke-sdp egress
- configure service vpls mesh-sdp egress
- configure service ies interface spoke-sdp egress

egress

Syntax **egress**

Context [Tree] (config>service>ies>sub-if>grp-if>sap>atm egress)
[Tree] (config>service>vpls>sap>atm egress)
[Tree] (config>service>vprn>if>sap>atm egress)
[Tree] (config>service>vprn>sub-if>grp-if>sap>atm egress)

Full Context configure service ies subscriber-interface group-interface sap atm egress
configure service vpls sap atm egress
configure service vprn interface sap atm egress
configure service vprn subscriber-interface group-interface sap atm egress

Description Commands in this context configure egress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service ies subscriber-interface group-interface sap atm egress
- configure service vprn subscriber-interface group-interface sap atm egress

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service vpls sap atm egress
- configure service vprn interface sap atm egress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>port>ethernet>access egress)
[Tree] (config>port>ethernet>network egress)

Full Context configure port ethernet access egress
configure port ethernet network egress

Description This command configures Ethernet access egress port parameters.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw egress)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress

Description Commands in this context configure egress QoS parameters for wlan-gw tunnels.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

egress

Syntax **egress**

Context **[Tree]** (config>card>mda>access egress)
[Tree] (config>card>mda>network egress)
[Tree] (config>port>access egress)
[Tree] (config>port>network egress)

Full Context configure card mda access egress
configure card mda network egress
configure port access egress
configure port network egress

Description Commands in this context configure egress buffer pool parameters which define the percentage of the pool buffers that are used for CBS calculations and specify the slope policy that is configured in the **config>qos>slope-policy** context.

On the MDA level, network and access egress pools are only allocated on channelized MDAs.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>card>fp egress)

Full Context configure card fp egress

Description This command enables access to the egress **fp** CLI context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

egress

Syntax **egress**

Context **[Tree]** (config>port>ethernet egress)

Full Context configure port ethernet egress

Description This command configures Ethernet egress port parameters.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>port>ml-bundle>mlfr egress)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay>frf-12 egress)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay egress)
[Tree] (config>port>tdm>e1>channel-group>frame-relay>frf-12 egress)
[Tree] (config>port>tdm>ds3>frame-relay>frf-12 egress)
[Tree] (config>port>tdm>e3>frame-relay>frf-12 egress)
[Tree] (config>port>sonet-sdh>path>frame-relay>frf-12 egress)

Full Context configure port multilink-bundle mlfr egress
configure port sonet-sdh path frame-relay frf-12 egress
configure port tdm ds1 channel-group frame-relay egress
configure port tdm ds1 channel-group frame-relay frf-12 egress
configure port tdm ds3 frame-relay frf-12 egress
configure port tdm e1 channel-group frame-relay frf-12 egress
configure port tdm e3 frame-relay frf-12 egress

Description Commands in this context configure the egress QoS profile for an MLFR bundle or a Frame Relay port with FRF.12 UNI/NNI fragmentation enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port sonet-sdh path frame-relay frf-12 egress

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlfr egress

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 frame-relay frf-12 egress
- configure port tdm ds1 channel-group frame-relay frf-12 egress
- configure port tdm ds3 frame-relay frf-12 egress
- configure port tdm e1 channel-group frame-relay frf-12 egress

egress

Syntax **egress**

Context **[Tree]** (config>port>ml-bundle>mlppp egress)

Full Context configure port multilink-bundle mlppp egress

Description Commands in this context configure egress MLPPP QoS profile parameters for the multilink bundle.

Platforms 7450 ESS, 7750 SR-7/12/12e

egress

Syntax **egress**

Context **[Tree]** (config>port>sonet-sdh>path>atm>ilmi egress)

Full Context configure port sonet-sdh path atm ilmi egress

Description Commands in this context configure egress traffic attributes for the ILMI link.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

egress

Syntax **egress**

Context **[Tree]** (config>service>sdp>binding>pw-port egress)

Full Context configure service sdp binding pw-port egress

Description Commands in this context configure PW port egress side parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>apipe>sap>atm egress)
[Tree] (config>service>epipe>sap>atm egress)

Full Context configure service apipe sap atm egress
configure service epipe sap atm egress

Description This command configures egress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

egress

Syntax **egress**

Context **[Tree]** (config>service>apipe>sap egress)
[Tree] (config>service>cpipe>sap egress)
[Tree] (config>service>epipe>sap egress)
[Tree] (config>service>fpipe>sap egress)
[Tree] (config>service>ipipe>sap egress)

Full Context configure service apipe sap egress
configure service cpipe sap egress
configure service epipe sap egress
configure service fpipe sap egress
configure service ipipe sap egress

Description Commands in this context configure egress SAP parameters.

If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress
- configure service cpipe sap egress

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress

All

- configure service ipipe sap egress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap egress

egress

Syntax **egress**

Context **[Tree]** (config>service>apipe>spoke-sdp egress)
[Tree] (config>service>cpipe>spoke-sdp egress)
[Tree] (config>service>epipe>spoke-sdp egress)
[Tree] (config>service>fpipe>spoke-sdp egress)
[Tree] (config>service>ipipe>spoke-sdp egress)

Full Context configure service apipe spoke-sdp egress
configure service cpipe spoke-sdp egress
configure service epipe spoke-sdp egress
configure service fpipe spoke-sdp egress
configure service ipipe spoke-sdp egress

Description This command configures the egress SDP context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp egress
- configure service cpipe spoke-sdp egress

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp egress

All

- configure service ipipe spoke-sdp egress
- configure service epipe spoke-sdp egress

egress

Syntax **egress**

Context **[Tree]** (config>service>epipe>pw-port egress)

Full Context configure service epipe pw-port egress

Description Commands in this context configure PW-port egress-side parameters

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>service>template>epipe-sap-template egress)

Full Context configure service template epipe-sap-template egress

Description Commands in this context configure egress filter policies.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>aarp-interface>spoke-sdp egress)

Full Context configure service ies aarp-interface spoke-sdp egress

Description Commands in this context configure the egress for a spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>if>vpls egress)

Full Context configure service ies interface vpls egress

Description The egress node under the vpls binding is used to define the optional sap-egress QoS policy that will be used for reclassifying the egress forwarding class or profile for routed packets associated with the IP interface on the attached VPLS or I-VPLS service context.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>if>sap>atm egress)

Full Context configure service ies interface sap atm egress

Description Commands in this context configure egress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>service>vprn>aarp-interface>spoke-sdp egress)

Full Context configure service vprn aarp-interface spoke-sdp egress

Description Commands in this context configure the egress for a spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

egress

Syntax **egress**

Context **[Tree]** (config>service>vprn>nw-if egress)

Full Context configure service vprn network-interface egress

Description Commands in this context configure egress network filter policies for the interface.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>vprn>if>sap egress)

Full Context configure service vprn interface sap egress

Description Commands in this context configure egress SAP Quality of Service (QoS) policies and filter policies.

If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter is defined, no filtering is performed.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>vprn>if>vpls egress)

Full Context configure service vprn interface vpls egress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The egress node under the vpls binding is used to define the optional sap-egress QoS policy that will be used for reclassifying the egress forwarding class or profile for routed packets associated with the IP interface on the attached VPLS service context.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>vprn>network-interface egress)

Full Context configure service vprn network-interface egress

Description Commands in this context configure egress network filter policies for the interface.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>aa-interface>sap egress)
[Tree] (config>service>vprn>aa-interface>sap egress)

Full Context configure service ies aa-interface sap egress
configure service vprn aa-interface sap egress

Description Commands in this context configure egress parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

egress

Syntax **egress**

Context **[Tree]** (config>isa>aa-grp>qos egress)

Full Context configure isa application-assurance-group qos egress

Description Commands in this context configure IOM port-level Quality of Service for this application assurance group in the egress direction (traffic entering an application assurance engine).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>service>ies>video-interface>video-sap egress)
[Tree] (config>service>vpls>video-interface>video-sap egress)
[Tree] (config>service>vprn>video-interface>video-sap egress)

Full Context configure service ies video-interface video-sap egress
configure service vpls video-interface video-sap egress
configure service vprn video-interface video-sap egress

Description Commands in this context configure egress parameters for the service's video SAP.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

egress

Syntax **egress**

Context **[Tree]** (config>mirror>mirror-dest>spoke-sdp egress)
[Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp egress)

Full Context configure mirror mirror-dest remote-source spoke-sdp egress
configure mirror mirror-dest spoke-sdp egress

Description Commands in this context configure spoke SDP egress parameters.

Platforms All

egress

Syntax [**no**] **egress**

Context **[Tree]** (config>mirror>mirror-dest>sap egress)

Full Context configure mirror mirror-dest sap egress

Description This command enables access to the context to associate an egress SAP Quality of Service (QoS) policy with a mirror destination SAP.

If no QoS policy is defined, the system default SAP egress QoS policy is used for egress processing.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>qos>network egress)

Full Context configure qos network egress

Description This command is used to enter the CLI node that creates or edits egress policy entries that specify the forwarding class queues to be instantiated when this policy is applied to the network port.

The forwarding class and profile state mapping to in- and out-of-profile DiffServ Code Points (DSCPs), dot1p, and MPLS EXP bits mapping for all labeled packets are also defined in this context.

All service packets are aggregated into DiffServ-based egress queues on the network interface. The service packets are transported either with IP GRE encapsulation or over a MPLS LSP. The exception is with the IES service. In this case, the actual customer IP header has the DSCP field mapped.

All out-of-profile service packets are marked with the corresponding out-of-profile DSCP, dot1p, or the EXP bit value at network egress. All the in-profile service ingress packets are marked with the corresponding in-profile DSCP, dot1p, or EXP bit value based on the forwarding class to which they belong. The exceed-profile traffic is marked with the same value as out-of-profile traffic and the inplus-profile traffic is marked with the same value as in-profile traffic.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>qos>queue-group-templates egress)

Full Context configure qos queue-group-templates egress

Description Commands in this context configure QoS egress queue groups. Egress queue group templates can be applied to egress Ethernet ports to create an egress queue group.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>router>if egress)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface egress

Description This command enables access to the context to configure egress network filter policies for the IP interface. If an egress filter is not defined, no filtering is performed.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>cust>multi-service-site egress)

Full Context configure service customer multi-service-site egress

Description Commands in this context configure the egress node associate an existing scheduler policy name with the customer site. The egress node is an entity to associate commands that complement the association.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>service>pw-template egress)

Full Context configure service pw-template egress

Description Commands in this context configure spoke SDP binding egress filter parameters.

Platforms All

egress

Syntax **egress**

Context **[Tree]** (config>subscr-mgmt>msap-policy>atm egress)

Full Context configure subscriber-mgmt msap-policy atm egress

Description Commands in this context configure MSAP ATM egress parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

egress

Syntax **egress**

Context **[Tree]** (config>subscr-mgmt>sub-prof egress)

Full Context configure subscriber-mgmt sub-profile egress

Description Commands in this context configure subscriber profile egress setting parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.29 egress-counter-map

egress-counter-map

Syntax **egress-counter-map policer** *policer-id* **traffic-type** {**unicast** | **multicast** | **broadcast**} [**create**]
egress-counter-map queue *queue-id* **traffic-type** {**unicast** | **multicast** | **broadcast**} [**create**]
no egress-counter-map policer *policer-id*
no egress-counter-map queue *queue-id*

Context **[Tree]** (config>sflow egress-counter-map)

Full Context configure sflow egress-counter-map

Description This command configures the egress counter map for sFlow. The map must be configured so sFlow agent understands how to interpret data collected against SAP queues and policers. Multiple queues and policers can be mapped to the same **traffic-type** using separate line entries.

The **no** form of this command deletes a SAP policy queue/policer from the map.

Parameters *policer-id* — Specifies the policer ID in a SAP egress QoS policy. If the SAP policy does not have a policer with the specified ID, the map entry will be ignored for this SAP.

Values 1 to 8

queue-id — Specifies the queue ID in a SAP egress QoS policy. If the SAP policy does not have a queue with the specified ID, the map entry will be ignored for this SAP.

Values 1 to 8

Platforms 7750 SR, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.30 egress-engineering

egress-engineering

Syntax **egress-engineering**
no egress-engineering

Context **[Tree]** (config>router>bgp>group egress-engineering)
[Tree] (config>router>bgp>group>neighbor egress-engineering)

Full Context configure router bgp group egress-engineering
configure router bgp group neighbor egress-engineering

Description Commands in this context configure egress engineering on a specific neighbor or all neighbors in a BGP group.

If egress engineering is not configured in the neighbor context, the configuration is inherited from the group context.

The **no** form of this command removes the egress engineering configuration.

Default no egress-engineering

Platforms All

9.31 egress-fc

egress-fc

Syntax **egress-fc** *fc-name*
no egress-fc

Context **[Tree]** (config>qos>sap-ingress>fc egress-fc)

Full Context configure qos sap-ingress fc egress-fc

Description This command configures the forwarding class to be used by the egress QoS processing. It overrides the forwarding class determined by ingress classification but not the QoS Policy Propagation via BGP.

The forwarding class or forwarding subclass can be overridden.

The new egress forwarding class is applicable to both SAP egress and network egress.

Default no egress-fc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *fc-name* — Specifies the forwarding class name to be used by the egress QoS processing.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

9.32 egress-ip-filter-entries

egress-ip-filter-entries

Syntax [**no**] **egress-ip-filter-entries**

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl egress-ip-filter-entries)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries

Description Commands in this context configure the egress IP filter parameters.

The **no** form of this command reverts to the default.

Default egress-ip-filter-entries

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.33 egress-ipv6-filter-entries

egress-ipv6-filter-entries

Syntax [**no**] **egress-ipv6-filter-entries**

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl egress-ipv6-filter-entries)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries

Description Commands in this context configure the egress IPv6 filter parameters.

The **no** form of this command reverts to the default.

Default egress-ipv6-filter-entries

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.34 egress-pbr

egress-pbr

Syntax **egress-pbr** {**default-load-balancing** | **l4-load-balancing**}
no egress-pbr

Context **[Tree]** (config>filter>ip-filter>entry egress-pbr)
[Tree] (config>filter>ipv6-filter>entry egress-pbr)

Full Context configure filter ip-filter entry egress-pbr
configure filter ipv6-filter entry egress-pbr

Description This command specifies that the configured PBR action is applicable to egress processing. The command should only be enabled in ACL policies used by residential subscribers. Enabling **egress-pbr** on filters not deployed for residential subscribers is not blocked but may lead to unexpected behavior and should be avoided.

The **no** form of this command removes the **egress-pbr** designation of the filter entry's action.

Default no egress-pbr

Parameters **default-load-balancing** — Sets load-balancing to the default (hash based on SA/DA of the packet).

l4-load-balancing — Includes TCP/UDP port (if available) in the hash.

Platforms All

9.35 egress-peer-engineering

egress-peer-engineering

Syntax **egress-peer-engineering**
no egress-peer-engineering

Context **[Tree]** (config>router>bgp egress-peer-engineering)

Full Context configure router bgp egress-peer-engineering

Description Commands in this context configure EPE parameters in BGP.

The **no** form of this command removes the EPE parameters from the BGP context.

Default no egress-peer-engineering

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

9.36 egress-peer-engineering-label-unicast

egress-peer-engineering-label-unicast

Syntax [**no**] **egress-peer-engineering-label-unicast**

Context **[Tree]** (config>router>bgp>group egress-peer-engineering-label-unicast)
[Tree] (config>router>bgp>group>neighbor egress-peer-engineering-label-unicast)

Full Context configure router bgp group egress-peer-engineering-label-unicast
configure router bgp group neighbor egress-peer-engineering-label-unicast

Description This command enables the generation of a label-unicast route for each /32 or /128 prefix that corresponds to the BGP neighbor or group address in the scope of the command. These routes can be advertised to other routers to recursively resolve unlabeled BGP routes for AS external destinations. They support the Egress Peer Engineering (EPE) use case.

The **no** form of this command disables the generation of EPE label-unicast routes.

Default no egress-peer-engineering-label-unicast

Platforms All

9.37 egress-policer

egress-policer

Syntax **egress-policer** [*policer-name*]
no egress-policer

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm egress-policer)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm egress-policer)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt egress-policer
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt egress-policer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the egress policer applied to all UEs corresponding to default vlan-range (such as, group-interface) or the specified vlan-range. The policer can be created in the **config>subscr-mgmt>isa-policer** context. The egress policer can be overridden per UE from RADIUS via access-accept or COA.

The **no** form of this command reverts to the default.

Parameters *policer-name* — Specifies the identifier of the distributed-sub-mgmt policer for egress traffic up to 256 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.38 egress-port-queue-overrides

egress-port-queue-overrides

Syntax **egress-port-queue-overrides**

Context **[Tree]** (config>port>ethernet>network egress-port-queue-overrides)

Full Context configure port ethernet network egress-port-queue-overrides

Description Commands in this context configure Ethernet network egress port queue override parameters.

Platforms All

9.39 egress-rate

egress-rate

Syntax **egress-rate** *sub-rate*
no egress-rate

Context **[Tree]** (config>port>ethernet egress-rate)

Full Context configure port ethernet egress-rate

Description This command configures the rate of traffic leaving the network. The configured *sub-rate* uses packet-based accounting. An event log is generated each time the egress rate is modified unless the port is part of a LAG.

The **no** form of this command returns the value to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no egress-rate

Parameters *sub-rate* — Specifies the egress rate in kb/s.

Values 1 to 100000000

Platforms All

9.40 egress-rate-modify

egress-rate-modify

Syntax **egress-rate-modify agg-rate-limit**
egress-rate-modify scheduler *scheduler-name*
no egress-rate-modify

Context **[Tree]** (config>subscr-mgmt>trk-plcy egress-rate-modify)

Full Context configure subscriber-mgmt host-tracking-policy egress-rate-modify

Description This command specifies the egress-rate modification that is to be applied.

The **no** form of this command reverts to the default value.

Parameters **agg-rate-limit** — Specifies to use the egress rate limit.

scheduler-name — Specifies the scheduler name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

egress-rate-modify

Syntax **egress-rate-modify** [**agg-rate-limit** | **scheduler** *scheduler-name*]
no egress-rate-modify

Context **[Tree]** (config>subscr-mgmt>igmp-policy egress-rate-modify)

Full Context configure subscriber-mgmt igmp-policy egress-rate-modify

Description This command is used to apply HQoS Adjustment to a subscriber. HQoS Adjustment is needed when multicast traffic flow for the subscriber is dissociated from subscriber host queues. Multicast redirection is typical such case although it can be applied in direct IPoE subscriber per-sap replication mode.

The channel bandwidth definition policy is defined in the mcac policy under the **config>router>mcac>policy** context. The policy is applied under the redirected interface or under the group-interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In order for HQoS Adjustment to take effect, sub-mcac-policy must be in a no shutdown mode and applied under the sub-profile even if mcac is not deployed.

The **no** form of this command reverts to the default value.

Parameters **agg-rate-limit** — Specifies the aggregate14 rate modification to be applied. The subscriber's bandwidth is capped via the **agg-rate-limit** command in the sub-profile or with a Change of Authorization (CoA) request. This bandwidth cap is dynamically adjusted according to the multicast channel definition and channel association with the host via IGMP.

scheduler-name — Specifies the schedule name. The subscriber's bandwidth is capped via the scheduling-policy in the sub-profile or with a Change of Authorization (CoA) request. HQoS Adjustment will modify the rate of the scheduler defined in the scheduling policy or configured via CoA.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

egress-rate-modify

Syntax **egress-rate-modify agg-rate-limit**
egress-rate-modify scheduler *scheduler-name*
no egress-rate-modify

Context **[Tree]** (config>subscr-mgmt>mld-policy egress-rate-modify)

Full Context configure subscriber-mgmt mld-policy egress-rate-modify

Description This command configures the egress rate modification.

The **no** form of this command removes the values from the configuration.

Parameters **agg-rate-limit** — Specifies that the maximum total rate for all subscriber egress queues for each subscriber associated with the policy.

scheduler-name — Specifies the scheduler to be applied for egress rate modification.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

egress-rate-modify

Syntax [**no**] **egress-rate-modify**

Context **[Tree]** (config>port>ethernet>access>egress>vport egress-rate-modify)
[Tree] (config>port>sonet-sdh>path>access>egress>vport egress-rate-modify)

Full Context configure port ethernet access egress vport egress-rate-modify
configure port sonet-sdh path access egress vport egress-rate-modify

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command applies HQoS Adjustment to a Vport. HQoS Adjustment refers to the dynamic adjustment of the rate limit at an QoS enforcement point within a Nokia router when the multicast traffic stream is disjointed from the unicast traffic stream. This QoS enforcement point within the router represents the physical point further down in the access part of the network where the two streams join each other and potentially can cause congestion.

An example would be a PON port which is shared amongst subscriber's multicast traffic (single copy of each channel) and subscriber's unicast traffic. The bandwidth control point for this PON port resides in the upstream Nokia BNG node in the form of a Vport. In the case where the multicast delivery method of the BNG utilizes redirection, the multicast traffic in the BNG will flow outside of the subscriber or the Vport context and thus will bypass any bandwidth enforcement in the Nokia router. To correct this, a Vport bandwidth adjustment is necessary in the router that will account for the multicast bandwidth consumption that is bypassing Vport in the router but is present in the PON port whose bandwidth is controlled by Vport.

An estimate of the multicast bandwidth consumption on the PON port can be made at the Vport level based on the IGMP messages sourced from the subscribers behind the PON port. This process is called HQoS Adjustment.

A multicast channel bandwidth is subtracted from or added to the Vport rate limit according to the received IGMP Join/Leave messages and the channel bandwidth definition policy associated with the Vport (indirectly through a group-interface). Since the multicast traffic on the PON port is shared amongst subscribers behind this PON port, only the first IGMP Join or the last IGMP Leave per multicast channel is tracked for the purpose of the Vport bandwidth modification.

The Vport rate that will be affected by this functionality depends on the configuration:

- In case the **agg-rate** within the Vport is configured, its value will be modified based on the IGMP activity associated with the subscriber under this Vport.
- In case the port-scheduler-policy within the Vport is referenced, the max-rate defined in the corresponding port-scheduler-policy will be modified based on the IGMP activity associated with the subscriber under this Vport.

The channel bandwidth definition policy is defined in the mcac policy in the **config>router>mcac>policy** context. The policy is applied under the group-interface or in case of redirection under the redirected-interface.

The rates in effect can be displayed with the following two commands:

show port 1/1/5 vport *name*

qos scheduler-hierarchy port *port-id* **vport** *vport-name*

The configuration of a scheduler policy under a Vport, which is only applicable to Ethernet interfaces, is mutually exclusive with the configuration of the **egress-rate-modify** parameter.

Context: HQoS Adjustment for Vport is disabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port sonet-sdh path access egress vport egress-rate-modify

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure port ethernet access egress vport egress-rate-modify

9.41 egress-scheduler-override

egress-scheduler-override

Syntax **egress-scheduler-override** [**create**]
no egress-scheduler-override

Context **[Tree]** (config>port>sonet-sdh>path egress-scheduler-override)
[Tree] (config>port>ethernet egress-scheduler-override)
[Tree] (config>port>tdm>ds1>channel-group egress-scheduler-override)
[Tree] (config>port>tdm>ds3 egress-scheduler-override)
[Tree] (config>port>tdm>e1>channel-group egress-scheduler-override)
[Tree] (config>port>tdm>e3 egress-scheduler-override)

Full Context configure port ethernet egress-scheduler-override
configure port sonet-sdh path egress-scheduler-override
configure port tdm ds1 channel-group egress-scheduler-override
configure port tdm ds3 egress-scheduler-override
configure port tdm e1 channel-group egress-scheduler-override
configure port tdm e3 egress-scheduler-override

Description This command applies egress scheduler overrides. When a port scheduler is associated with an egress port, it is possible to override the following parameters:

- The **max-rate** allowed for the scheduler.
- The maximum **rate** for each priority level 8 through 1.
- The CIR associated with each priority level 8 through 1.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for command syntax and usage for the **port-scheduler-policy** command.

The **no** form of this command removes all override parameters from the egress port or channel scheduler context. Once removed, the port scheduler reverts all rate parameters back to the parameters defined on the port-scheduler-policy associated with the port.

Parameters **create** — Mandatory while creating an entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path egress-scheduler-override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 egress-scheduler-override
- configure port tdm e3 egress-scheduler-override
- configure port tdm ds1 channel-group egress-scheduler-override
- configure port tdm e1 channel-group egress-scheduler-override

All

- configure port ethernet egress-scheduler-override

9.42 egress-scheduler-policy

egress-scheduler-policy

Syntax **egress-scheduler-policy** *port-sched-plcy*
no egress-scheduler-policy

Context **[Tree]** (config>port-policy egress-scheduler-policy)

Full Context configure port-policy egress-scheduler-policy

Description This command references a port scheduler policy that is defined under the **config>qos>port-scheduler-policy>** hierarchy. Port schedulers are instantiated on carrier IOMs towards all ISAs that are part of the lns-group.

The no form of the command removes the port scheduler policy from the configuration.

Default no egress-scheduler-policy

Parameters *port-sched-plcy* — Specifies the egress scheduler policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

egress-scheduler-policy

Syntax **egress-scheduler-policy** *port-scheduler-policy-name*
no egress-scheduler-policy

Context **[Tree]** (config>port>ethernet egress-scheduler-policy)
[Tree] (config>port>sonet-sdh>path egress-scheduler-policy)
[Tree] (config>port>tdm>ds1>channel-group egress-scheduler-policy)
[Tree] (config>port>tdm>ds3 egress-scheduler-policy)
[Tree] (config>port>tdm>e1>channel-group egress-scheduler-policy)
[Tree] (config>port>tdm>e3 egress-scheduler-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context
configure port ethernet egress-scheduler-policy
configure port sonet-sdh path egress-scheduler-policy
configure port tdm ds1 channel-group egress-scheduler-policy
configure port tdm ds3 egress-scheduler-policy
configure port tdm e1 channel-group egress-scheduler-policy
configure port tdm e3 egress-scheduler-policy

Description
This command enables the provisioning of an existing port-scheduler-policy to a port or channel.

The egress-scheduler-override node allows for the definition of the scheduler overrides for a specific port or channel.

When a port scheduler is active on a port or channel, all queues and intermediate service schedulers on the port are subject to receiving bandwidth from the scheduler. Any policers, queues, or schedulers with port-parent associations are mapped to the appropriate port priority levels based on the port-parent command parameters. Any policers, queues, or schedulers that do not have a port-parent or valid intermediate scheduler parent defined are treated as orphaned and are handled based on the port scheduler policies default or explicit orphan behavior.

The port scheduler maximum rate and priority level rate parameters may be overridden to allow unique values separate from the port-scheduler-policy-name attached to the port or channel. Use the **egress-scheduler-override** command to specify the port or channel specific scheduling parameters.

The **no** form of this command removes a port scheduler policy from an egress port or channel. Once the scheduler policy is removed, all orphaned policers, queues, and schedulers revert to a free running state governed only by the local queue or scheduler parameters. This includes any queues or schedulers with a port-parent association.

Parameters
port-scheduler-policy-name — Specifies an existing port-scheduler-policy configured in the **config>qos** context. The name can be up to 32 characters.

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path egress-scheduler-policy

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group egress-scheduler-policy
- configure port tdm ds1 channel-group egress-scheduler-policy
- configure port tdm ds3 egress-scheduler-policy
- configure port tdm e3 egress-scheduler-policy

All

- configure port ethernet egress-scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.43 egress-statistics

egress-statistics

Syntax **egress-statistics**

Context **[Tree]** (config>router>ldp egress-statistics)

Full Context configure router ldp egress-statistics

Description Commands in this context enter the LDP FEC prefix for the purpose of enabling egress data path statistics at the ingress LER for this FEC.

Platforms All

egress-statistics

Syntax [**no**] **egress-statistics**

Context **[Tree]** (config>router>mpls>lsp egress-statistics)
[Tree] (config>router>mpls>lsp-template egress-statistics)

Full Context configure router mpls lsp egress-statistics
configure router mpls lsp-template egress-statistics

Description This command configures statistics in the egress data path of an originating LSP at a head-end node. The user must execute the no shutdown for this command to effectively enable statistics.

Note: SR-TE LSP egress statistics are not supported on VSR.

The same set of counters is updated for packets forwarded over any path of the RSVP-TE LSP and over the lifetime of the LSP. In steady state, the counters are updated for packets forwarded over the active path of the LSP. The active path can be the primary path, one of the secondary paths, the FRR detour path, or the FRR bypass path when the head-end node is also the PLR.

For SR-TE LSPs, egress statistics are collected independently for each path (primary, backup standby or not), and are preserved on switchover (except for non-standby).

LSP egress statistics are collected if the head-end node is also the Penultimate-Popping Hop (PHP) node for a single-hop LSP using an implicit null egress label.

RSVP-TE LSP statistics are not collected on a dynamic or a static bypass tunnel itself.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Statistics collection on two labels of the stack is possible. Please refer to **config>system>ip>mpls>label-stack-statistics-count**.

The **no** form of this command disables the statistics in the egress data path and removes the accounting policy association from the LSP.

Default no egress-statistics

Platforms All

egress-statistics

Syntax [**no**] **egress-statistics**

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy egress-statistics)

Full Context configure router mpls forwarding-policies forwarding-policy egress-statistics

Description This command configures egress statistics in an MPLS forwarding policy.

The **no** form of this command removes any egress statistics in a forwarding policy.

Default no egress-statistics

Platforms All

egress-statistics

Syntax **egress-statistics**

Context **[Tree]** (config>router>isis>segm-rtng egress-statistics)
[Tree] (config>router>ospf>segm-rtng egress-statistics)
[Tree] (config>router>ospf3>segm-rtng egress-statistics)

Full Context configure router isis segment-routing egress-statistics
configure router ospf segment-routing egress-statistics
configure router ospf3 segment-routing egress-statistics

Description Commands in this context configure the egress statistics for IGP SIDs.

Platforms All

egress-statistics

Syntax [**no**] **egress-statistics**

Context **[Tree]** (config>router>segment-routing>sr-policies egress-statistics)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router segment-routing sr-policies egress-statistics

Description This command administratively enables the collection of egress traffic statistics for all segment routing policies.

The **no** form of this command disables egress traffic statistics collection for all segment routing policies.

Default no egress-statistics

Platforms All

egress-statistics

Syntax [**no**] **egress-statistics**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action egress-statistics)
[Tree] (config>router>policy-options>policy-statement>default-action egress-statistics)

Full Context configure router policy-options policy-statement default-action egress-statistics
configure router policy-options policy-statement entry action egress-statistics

Description This command enables the allocation of statistical indexes to BGP-LU route entries that are programmed on an egress data path.

The **no** form of this command disables the allocation of statistical indexes to BGP-LU entries.

Default no egress-statistics

Platforms All

9.44 egress-xpl

egress-xpl

Syntax **egress-xpl**

Context **[Tree]** (config>card>mda egress-xpl)

Full Context configure card mda egress-xpl

Description Commands in this context configure **egress-xpl** settings used by the **fail-on-error** feature.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.45 eibgp-loadbalance

eibgp-loadbalance

Syntax [**no**] **eibgp-loadbalance**

Context **[Tree]** (config>service>vprn>bgp eibgp-loadbalance)

Full Context configure service vprn bgp eibgp-loadbalance

Description This command enables eiBGP load sharing so routes with both MP-BGP and IPv4 next-hops can be used simultaneously.

In order for this command to be effective, the **ecmp** and **multipath** commands for the associated VPRN instance must also be configured to allow for multiple routes to the same destination.

The **no** form of this command used at the global level reverts to default values.

Default no eibgp-loadbalance

Platforms All

9.46 elmi

elmi

Syntax **elmi**

Context **[Tree]** (config>port>ethernet elmi)

Full Context configure port ethernet elmi

Description This command configures Ethernet Local Management Interface (E-LMI) parameters for the Ethernet port. E-LMI is only supported on Ethernet access ports with Dot1q encapsulation type.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.47 embed-filter

embed-filter

Syntax **IPv4:**
embed-filter *ip-filter-id* [**offset** *offset*] [{**active** | **inactive**}]
no embed-filter *ip-filter-id*
IPv6:
embed-filter *ipv6-filter-id* [**offset** *offset*] [{**active** | **inactive**}]
no embed-filter *ipv6-filter-id*
IPv4:
embed-filter flowspec [**group** *group-id*] [**router** {*router-instance* | **service-name** *vprn-service-name*}] [**offset** *offset*] [{**active** | **inactive**}]
no embed-filter flowspec [**group** *group-id*]
embed-filter open-flow *ofs-name* [{**system** | **service** {*service-id* | *service-name*} | **sap** *sap-id*}] [**offset** *offset*] [{**active** | **inactive**}]
no embed-filter open-flow *ofs-name* [{**system** | **service** {*service-id* | *service-name*} | **sap** *sap-id*}]
embed-filter vsd *vsd-filter-id* [**offset** *offset*] [{**active** | **inactive**}]
no embed-filter vsd *vsd-filter-id*

Context **[Tree]** (config>filter>ip-filter embed-filter)
[Tree] (config>filter>ipv6-filter embed-filter)
[Tree] (config>filter>mac-filter embed-filter)

Full Context configure filter ip-filter embed-filter
configure filter ipv6-filter embed-filter
configure filter mac-filter embed-filter

Description This command embeds a previously defined IPv4, IPv6, or MAC embedded filter policy or Hybrid OpenFlow switch instance into this exclusive, template, or system filter policy at the specified offset value. Rules derived from the BGP FlowSpec can also be embedded into template filter policies only.

Note: For MAC filters, embedding is supported for VSD filters or filter entries only.

The **embed-filter open-flow** *ofs-name* form of this command enables OpenFlow (OF) in GRT either by embedding the specified OpenFlow switch (OFS) instance with **switch-defined-cookie** disabled, or by embedding rules with sros-cookie:type “grt-cookie”, value 0, from the specified OFS instance with **switch-defined-cookie** enabled. The embedding filter can only be deployed in GRT context or be unassigned.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **embed-filter open-flow** *ofs-name* **system** form of this command enables OF in system filters by embedding rules with sros-cookie:type “system-cookie”, value 0, from the specified OFS instance with **switch-defined-cookie** enabled. The embedding filter can only be of scope **system**.

The **embed-filter open-flow** *ofs-name* **service** {*service-id* | *service-name*} form of this command enables OF in VPRN/VPLS filters by embedding rules with sros-cookie:type “service-cookie”, value **service-id**, from the specified OFS instance with **switch-defined-cookie** enabled—per service rules. The embedding filter can only be deployed in the specified VPRN/VPLS service. A single VPLS service can only support OF rules per SAP or per service.

The **embed-filter open-flow** *ofs-name* **sap** *sap-id* form of this command enables OF in VPLS SAP filters by embedding rules with sros-cookie:type “service-cookie”, value *service-id* and flow match conditions specifying the sap-id from the specified OFS instance with **switch-defined-cookie** enabled—per SAP OF rules. The embedding filter must be of type exclusive and can only be deployed on the specified SAP in the context of the specified VPLS service. A single VPLS service can only support OF rules per SAP or per service.

The **no embed-filter open-flow** *ofs-name* form of this command removes the OF embedding for the GRT context.

The **embed-filter flowspec** form of this command enables the embedding of rules derived from BGP FlowSpec routes into the filter policy that is being configured. The optional **group** parameter specifies that only FlowSpec routes tagged with an interface-set extended community containing this group ID should be selected for embedding. The optional **router** parameter specifies the routing instance source of the BGP FlowSpec routes; if the parameter is not specified, the routing instance is derived automatically from the context in which the filter policy is applied.

The **no embed-filter flowspec** form of this command removes the FlowSpec filter embedding from this filter policy.

The **embed-filter vsd** *vsd-filter-id* command refers to the VSD filter ID encoded _tmnx_vsd_filter-id. The filter is created dynamically and managed exclusively using the Python script, so rules can be inserted and removed in the correct VSD filters. The command is supported with IP, IPv6, and MAC filters. For more information about VSD filter provisioning, automation, and the Python script, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide: VLL, VPLS, PBB, and EVPN*.

The **no embed-filter vsd** *vsd-filter-id* form of this command removes the VSD filter embedding from this filter policy.

The **no embed-filter** *filter-id* form of this command removes the embedding from this filter policy.

See the description of embedded filter policies in this guide for further operational details.

Parameters **IPv4:** *ip-filter-id* — Specifies a previously defined IPv4 policy for embedding in this filter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IPv6: *ipv6-filter-id* — Specifies a previously defined IPv6 policy for embedding in this filter.

offset — Specifies that an embedded filter entry X will have an entry X + offset in the embedding filter.

Values 0 to 2097151

Default 0

active — Specifies that embedded filter entries are to be included in this embedding filter policy and activated on applicable line cards—default if no keyword is specified and omitted from **info** command output (but not **info detail**), or when saving the configuration.

inactive — Specifies that no embedded filter policy entries are to be included in this embedding filter policy. The embedding is configured but will not do anything.

flowspec — This keyword indicates that rules derived from BGP FlowSpec routes should be embedded into (or removed from, in case of the **no** form) the filter.

group-id — Specifies that only FlowSpec routes with an interface-set extended community with this value of *group-id* should be selected for embedding.

Values 0 to 16383

router-instance — Specifies a router instance.

vprn-service-name — Specifies the VPRN service name used for embedding FlowSpec rules.

open-flow — Indicates that rules derived from OpenFlow should be embedded into (or removed from, in case of the **no** form) the filter.

ofs-name — Specifies the name of the currently configured Hybrid OpenFlow Switch (OFS) instance.

Not including the **system**, **service** or **sap** parameters will specify OF in a GRT instance context by default. This allows embedding of OF rules into filters deployed in GRT instances from OFS with **switch-defined-cookie** disabled, or embedding rules from OFS with **switch-defined-cookie** enabled, when the FlowTable cookie encodes sros-cookie:type “grt-cookie”.

system — Used for OF control of system filters. Allows embedding of OF rules into system filters from OFS with **switch-defined-cookie** enabled. Only the rules with cookie value encoding “system-cookie” are embedded.

service-id — Specifies an existing VPRN or VPLS service ID that the embedding filter can be used for.

service-name — Specifies an existing VPRN or VPLS service name that the embedding filter can be used for.

Values 1 to 2147483647

service-name — Specifies an existing VPRN or VPLS service name up to 64 characters that the embedding filter can be used for.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap-id — Used for OF control of VPLS services when a PortID and VLAN ID match is required. Allows embedding of OF rules with a PortID and VLAN ID match into exclusive VPLS SAP filters. Only the rules with cookie value encoding the VPLS service, and flow table match encoding the specified SAP, are embedded into the filter. The embedding filter can only be deployed in the context of the specified SAP.

sap-id — Specifies an existing SAP that the embedding filter can be used for.

vsd-filter-id — Creates an embedded filter (filter ID: _tmnx_vsd_*filter-id*) for population by Nuage VSD.

Platforms All

9.48 embedded-rp

embedded-rp

Syntax **embedded-rp**

Context **[Tree]** (config>service>vprn>pim>rp>ipv6 embedded-rp)

Full Context configure service vprn pim rp ipv6 embedded-rp

Description This command enables context to configure IPv6 embedded RP parameters.

Platforms All

embedded-rp

Syntax [**no**] **embedded-rp**

Context **[Tree]** (config>router>pim>rp>ipv6 embedded-rp)

Full Context configure router pim rp ipv6 embedded-rp

Description Commands in this context configure embedded RP parameters.

Embedded RP is required to support IPv6 inter-domain multicast because there is no MSDP equivalent in IPv6.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The detailed protocol specification is defined in RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*. This RFC describes a multicast address allocation policy in which the address of the RP is encoded in the IPv6 multicast group address, and specifies a PIM-SM group-to-RP mapping to use the encoding, leveraging, and extending unicast-prefix-based addressing. This mechanism not only provides a simple solution for IPv6 inter-domain ASM but can be used as a simple solution for IPv6 intra-domain ASM with scoped multicast addresses as well. It can also be used as an automatic RP discovery mechanism in those deployment scenarios that would have previously used the Bootstrap Router protocol (BSR).

The **no** form of this command disables embedded RP.

Platforms All

9.49 emulated-server

emulated-server

Syntax **emulated-server** *ip-address*
no emulated-server

Context **[Tree]** (config>service>ies>if>dhcp>proxy-server emulated-server)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>proxy-server emulated-server)
[Tree] (config>service>vpls>sap>dhcp>proxy-server emulated-server)
[Tree] (config>service>vprn>if>dhcp>proxy-server emulated-server)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>proxy-server emulated-server)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>proxy-server emulated-server)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>proxy emulated-server)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server emulated-server)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>proxy emulated-server)

Full Context configure service ies interface dhcp proxy-server emulated-server
configure service ies subscriber-interface group-interface dhcp proxy-server emulated-server
configure service vpls sap dhcp proxy-server emulated-server
configure service vprn interface dhcp proxy-server emulated-server
configure service vprn subscriber-interface group-interface dhcp proxy-server emulated-server
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server emulated-server
configure service vprn subscriber-interface ipv6 dhcp6 proxy emulated-server
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp proxy-server emulated-server

Description This command configures the IP address which is used as the DHCP server address in the context of the SAP. Typically, the configured address should be in the context of the subnet represented by the service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default setting. The local proxy server will not become operational without the emulated-server address being specified.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the emulated server's IP address. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp proxy-server emulated-server
- configure service ies subscriber-interface group-interface dhcp proxy-server emulated-server
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp proxy-server emulated-server

All

- configure service vpls sap dhcp proxy-server emulated-server
- configure service vprn interface dhcp proxy-server emulated-server
- configure service ies interface dhcp proxy-server emulated-server

9.50 enable-admin

enable-admin

Syntax **enable-admin**

Context **[Tree]** (global enable-admin)

Full Context global enable-admin

Description See the description for the **admin-password** command. If the **admin-password** is configured in the **config>system>security>password** context, then any user can enter a special administrative mode by entering the **enable-admin** command.

enable-admin is in the default profile. By default, all users are given access to this command.

Once the **enable-admin** command is entered, the user is prompted for a password. If the password matches, the user is given unrestricted access to all the commands.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password are determined by the **complexity** command.

The following shows a password configuration example:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
A:ALA-1>config>system>security# info
----------------------------------------------
...
            password
                aging 365
                minimum-length 8
                attempts 5 time 5 lockout 20
                admin-password "rUYUz9XMo6I" hash
            exit
...
----------------------------------------------
A:ALA-1>config>system>security#
```

There are two ways to verify that a user is in the enable-admin mode:

- show users — administrator can know which users are in this mode
- Enter the **enable-admin** command again at the root prompt and an error message will be returned.

```
*A:node-1# show users
===============================================================================
User                            Type      Login time           Idle time
  Session ID   From
===============================================================================
                                Console         --             3d 10:16:12 --
  6            --
admin                           SSHv2     12OCT2018 20:44:15   0d 00:00:00 A-
 #83           192.168.0.10
admin                           SSHv2     12OCT2018 21:09:25   0d 00:05:10 --
  84           192.168.0.10
-------------------------------------------------------------------------------
Number of users: 2
'#' indicates the current active session
'A' indicates user is in admin mode
===============================================================================
*A:node-1# enable-admin
MINOR: CLI Already in admin mode.
*A:node-1#
```

9.51 enable-admin-control

enable-admin-control

Syntax **enable-admin-control**

Context **[Tree]** (config>system>security>password enable-admin-control)

Full Context configure system security password enable-admin-control

Description Enable the user to become a system administrator.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: This command applies to users on RADIUS, TACACS, and LDAP.

Platforms All

9.52 enable-asm-mdt

enable-asm-mdt

Syntax [**no**] **enable-asm-mdt**

Context **[Tree]** (config>service>vprn>mvpn>pt>selective enable-asm-mdt)

Full Context configure service vprn mvpn provider-tunnel selective enable-asm-mdt

Description This command enables Data MDT with PIM-ASM mode on the receiver PE node. PIM-ASM or PIM-SSM operation mode is derived based on the locally configured SSM range on the node.

If asm-mode is disabled using this command, then PIM-SSM mode is enabled for all groups, independent of the configured SSM range on the node.

Platforms All

9.53 enable-bfd-leaf

enable-bfd-leaf

Syntax [**no**] **enable-bfd-leaf**

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>rsvp enable-bfd-leaf)

Full Context configure service vprn mvpn provider-tunnel inclusive rsvp enable-bfd-leaf

Description This command enables unidirectional multi-point BFD session on a receiver (leaf) PE node for upstream fast failure detection over RSVP-TE P2MP LSP.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

enable-bfd-leaf

Syntax [**no**] **enable-bfd-leaf**

Context **[Tree]** (configure>service>vprn>mvpn>provider-tunnel>inclusive>p2mp-sr enable-bfd-leaf)

Full Context configure service vprn mvpn provider-tunnel inclusive p2mp-sr enable-bfd-leaf

Description This command enables unidirectional multipoint BFD sessions on a receiver (leaf) PE node for upstream fast failure detection over P2MP SR tree LSP.

The **no** form of this command disables unidirectional multipoint BFD sessions.

Default no enable-bfd-leaf

Platforms All

9.54 enable-bfd-root

enable-bfd-root

Syntax **enable-bfd-root** *transmit-interval* [**multiplier** *multiplier*]
no enable-bfd-root

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>rsvp enable-bfd-root)

Full Context configure service vprn mvpn provider-tunnel inclusive rsvp enable-bfd-root

Description This command enables unidirectional multi-point BFD session on a sender (Root) PE node for upstream fast failure detection over RSVP-TE P2MP LSP.

Parameters *transmit-interval* — Sets the transmit interval, in milliseconds.

Values 10 to 100000

Default 100

multiplier — Sets the multiplier for the BFD session.

Values 3 to 20

Default 3

Platforms All

enable-bfd-root

Syntax **enable-bfd-root** *transmit-interval* [**multiplier** *multiplier*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no enable-bfd-root

Context [Tree] (configure>service>vprn>mvpn>pt>inclusive>p2mp-sr enable-bfd-root)

Full Context configure service vprn mvpn provider-tunnel inclusive p2mp-sr enable-bfd-root

Description This command enables a unidirectional multi-point BFD session on a sender (Root) PE node for upstream fast failure detection over P2MP SR tree LSP. The node uses the multiplier and the transmit interval parameters to calculate the detection time, which is the period of time without receiving BFD packets after which the session failure is determined.

Default no enable-bfd-root

Parameters *transmit-interval* — Sets the transmit interval, in milliseconds.

Values 10 to 100000

Default 300

multiplier — Sets the multiplier for the transmit interval of the BFD session.

Values 3 to 20

Default 3

Platforms All

9.55 enable-bgp-vpn-backup

enable-bgp-vpn-backup

Syntax **enable-bgp-vpn-backup** [**ipv4**] [**ipv6**]
no enable-bgp-vpn-backup

Context [Tree] (config>service>vprn enable-bgp-vpn-backup)

Full Context configure service vprn enable-bgp-vpn-backup

Description This command allows BGP-VPN routes imported into the VPRN to be used as backup paths for IPv4 or IPv6 BGP-learned prefixes.

Parameters **ipv4** — Allows BGP-VPN routes to be used as backup paths for IPv4 prefixes.

ipv6 — Allows BGP-VPN routes to be used as backup paths for IPv6 prefixes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.56 enable-console-access

enable-console-access

Syntax [**no**] **enable-console-access**

Context **[Tree]** (config>system>satellite>eth-sat enable-console-access)

Full Context configure system satellite eth-sat enable-console-access

Description This command enables access to a satellite console interface for additional debugging purposes.

When configured through the 7750 SR, 7450 ESS, and 7950 XRS host CLI, the 7210 SAS console port is enabled to perform the debug function. Console commands are limited to specific show commands and no configuration or operational changes can be made using the 7210 console.

The **no** form of this command disables satellite console interface access.

Default no enable-console-access

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.57 enable-dscp-prec-remarking

enable-dscp-prec-remarking

Syntax [**no**] **enable-dscp-prec-remarking**

Context **[Tree]** (config>qos>sap-egress>policer enable-dscp-prec-remarking)

Full Context configure qos sap-egress policer enable-dscp-prec-remarking

Description This command enables DSCP/precedence remarking based on the profile state of a packet being forwarded by a SAP or subscriber egress policer. The DSCP/precedence can be remarked to a value independent of, or separately based on, the packet's profile, if the packet has an exceed, in-profile, or out-of-profile state.

Default no enable-dscp-prec-remarking

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.58 enable-dynamic-services-config

enable-dynamic-services-config

Syntax [**no**] **enable-dynamic-services-config**

Context **[Tree]** (global enable-dynamic-services-config)

Full Context global enable-dynamic-services-config

Description

Note: See also the description for the **dynsvc-password** command.

If the dynsvc-password is configured in the **config>system>security>password** context, then any user can enter a special dynamic services configuration mode by entering the **enable-dynamic-services-config** command.

The **enable-dynamic-services-config** command is not in the default profile. To give access to this command, the user must belong to the administrative profile or a new profile should be created.

Once the **enable-dynamic-services-config** command is entered, the user is prompted for a password. If the password matches, the user is given access to the dynamic services configuration. Access to static configuration is in this case prohibited.

To verify that a user is in the **enable-dynamic-services-config** mode, use the **show users** command. Users in the **enable-dynamic-services-config** mode lists the letter “D” next to the user’s CLI session.

The **no** form of this command disables the dynamic services configuration mode for this user.

9.59 enable-exceed-pir

enable-exceed-pir

Syntax [**no**] **enable-exceed-pir**

Context **[Tree]** (config>qos>sap-egress>policer enable-exceed-pir)

Full Context configure qos sap-egress policer enable-exceed-pir

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the forwarding of packets with an exceed-profile state and traffic exceeding the PIR for a SAP egress or a network egress queue group (configured in the egress queue group template) policer. This traffic is forwarded as exceed-profile instead of being dropped. This parameter is not supported when **policers-hqos-manageable** is configured in the SAP egress QoS policy.

Default no enable-exceed-pir

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

enable-exceed-pir

Syntax [**no**] **enable-exceed-pir**

Context **[Tree]** (cfg>qos>qgrps>egr>qgrp>policer enable-exceed-pir)

Full Context configure qos queue-group-templates egress queue-group policer enable-exceed-pir

Description This command enables the forwarding of traffic exceeding the PIR for a SAP egress or a network egress queue group (configured in the egress queue group template) policer. This traffic is forwarded as exceed-profile instead of being dropped.

Default no enable-exceed-pir

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

9.60 enable-fc-collection

enable-fc-collection

Syntax [**no**] **enable-fc-collection**

Context **[Tree]** (config>oam-pm>session>ethernet>lmm enable-fc-collection)

Full Context configure oam-pm session ethernet lmm enable-fc-collection

Description This command enables the ETH-LMM test within the OAM-PM session to collect per-FC counters. This command must be used in combination with the **collect-lmm-fc-stats** command for the entity over which the source MEP is defined. The **config**>**oam-pm**>**session**>**ethernet**>**priority** value must match the numerical value that represents the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The OAM-PM infrastructure does not validate that the proper counting mode has been configured on the entity that is linked to the source MEP, and does not validate that the FC and priority have been configured. The **show**>**eth-cfm**>**collect-lmm-fc-stats** command may be used to display the entities and the FCs on those entities that have established individual FC counters.

Sessions that launch from the same source MEP must use the same counting model; either **collect-lmm-fc-stats** for individual counters for the defined FCs, or **collect-lmm-stats** for a single all-encompassing counter.

Individual OAM-PM sessions must be configured if multiple Ethernet LMM tests are required for different FCs. Cross-session validation occurs to ensure that a source MEP does not include multiple tests that are using the same priority.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Platforms All

9.61 enable-graceful-shutdown

enable-graceful-shutdown

Syntax [**no**] **enable-graceful-shutdown**

Context **[Tree]** (config>system>login-control>telnet enable-graceful-shutdown)

Full Context configure system login-control telnet enable-graceful-shutdown

Description This command enables graceful shutdown of telnet sessions.

The **no** form of this command disables graceful shutdown of telnet sessions.

Platforms All

9.62 enable-grt

enable-grt

Syntax [**no**] **enable-grt**

Context **[Tree]** (config>service>vprn>grt-lookup enable-grt)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn grt-lookup enable-grt

Description This command enables the functions required for looking up routes in the Global Route Table (GRT) when the lookup in the local VRF fails. If this command is enabled without the use of a **static-route** option (as subcommand to this parent), a lookup in the local VRF is preferred over the GRT. When the local VRF returns no route table lookup matches, the result from the GRT is preferred.

The **no** form of this command disables the lookup in the GRT when the lookup in the local VRF fails.

Default no enable-grt

Platforms All

9.63 enable-icmp-vse

enable-icmp-vse

Syntax [**no**] **enable-icmp-vse**

Context **[Tree]** (config>system enable-icmp-vse)

Full Context configure system enable-icmp-vse

Description This command enables vendor specific extensions to ICMP.

Default no enable-icmp-vse

Platforms All

9.64 enable-ingress-stats

enable-ingress-stats

Syntax [**no**] **enable-ingress-stats**

Context **[Tree]** (config>router>if enable-ingress-stats)
[Tree] (config>service>ies>if enable-ingress-stats)
[Tree] (config>service>vprn>if enable-ingress-stats)
[Tree] (config>service>ies>sub-if>grp-if enable-ingress-stats)
[Tree] (config>service>vprn>sub-if>grp-if enable-ingress-stats)
[Tree] (config>service>vprn>nw-if enable-ingress-stats)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface enable-ingress-stats
configure service ies interface enable-ingress-stats
configure service ies subscriber-interface group-interface enable-ingress-stats
configure service vprn interface enable-ingress-stats
configure service vprn network-interface enable-ingress-stats
configure service vprn subscriber-interface group-interface enable-ingress-stats

Description This command enables the collection of ingress interface IP stats. This command is only applicable to IP statistics, and not to uRPF statistics.

If enabled, then the following statistics are collected:

- IPv4 offered packets
- IPv4 offered octets
- IPv6 offered packets
- IPv6 offered octets

Note: Octet statistics for IPv4 and IPv6 bytes at IP interfaces include the Layer 2 frame overhead.

Default no enable-ingress-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface enable-ingress-stats
- configure service vprn subscriber-interface group-interface enable-ingress-stats

All

- configure service ies interface enable-ingress-stats
- configure router interface enable-ingress-stats
- configure service vprn network-interface enable-ingress-stats
- configure service vprn interface enable-ingress-stats

9.65 enable-inter-as-vpn

enable-inter-as-vpn

Syntax [**no**] **enable-inter-as-vpn**

Context **[Tree]** (config>router>bgp enable-inter-as-vpn)

Full Context configure router bgp enable-inter-as-vpn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies whether VPNs can exchange routes across autonomous system boundaries, providing model B connectivity.

The **no** form of this command disallows ASBRs to advertise VPRN routes to their peers in other autonomous systems.

Default no enable-inter-as-vpn

Platforms All

9.66 enable-mac-accounting

enable-mac-accounting

Syntax [**no**] **enable-mac-accounting**

Context **[Tree]** (config>service>ies>if enable-mac-accounting)

Full Context configure service ies interface enable-mac-accounting

Description This command enables MAC accounting functionality on this interface.

The **no** form of this command disables MAC accounting functionality on this interface.

Platforms All

enable-mac-accounting

Syntax [**no**] **enable-mac-accounting**

Context **[Tree]** (config>service>vprn>if enable-mac-accounting)

Full Context configure service vprn interface enable-mac-accounting

Description This command enables MAC accounting functionality on this interface.

The **no** form of this command disables MAC accounting functionality on this interface.

Platforms All

enable-mac-accounting

Syntax [**no**] **enable-mac-accounting**

Context **[Tree]** (config>router>if enable-mac-accounting)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface enable-mac-accounting

Description This command enables MAC Accounting functionality for the interface.

Default no enable-mac-accounting

Platforms All

9.67 enable-mdt-spt

enable-mdt-spt

Syntax [**no**] **enable-mdt-spt**

Context **[Tree]** (config>router>pim enable-mdt-spt)

Full Context configure router pim enable-mdt-spt

Description This command enables SPT switchover for default MDT. On enable, PIM instance resets all MDTs and re-initiate setup.

The **no** form of this command disables SPT switchover for default MDT. On disable, PIM instance resets all MDTs and re-initiate setup.

Default no enable-mdt-spt

Platforms All

9.68 enable-notification

enable-notification

Syntax **enable-notification**
no enable-notification

Context **[Tree]** (config>service>vprn>bgp>graceful-restart enable-notification)
[Tree] (config>service>vprn>bgp>group>graceful-restart enable-notification)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart enable-notification)

Full Context configure service vprn bgp graceful-restart enable-notification
configure service vprn bgp group graceful-restart enable-notification
configure service vprn bgp group neighbor graceful-restart enable-notification

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When this command is present, the graceful restart capability sent by this router indicates support for NOTIFICATION messages. If the peer also supports this capability then the session can be restarted gracefully (while preserving forwarding) if either peer sends a NOTIFICATION message due to some type of event or error.

Default no enable-notification

Platforms All

enable-notification

Syntax **enable-notification**
no enable-notification

Context **[Tree]** (config>router>bgp>graceful-restart enable-notification)
[Tree] (config>router>bgp>group>graceful-restart enable-notification)
[Tree] (config>router>bgp>group>neighbor>graceful-restart enable-notification)

Full Context configure router bgp graceful-restart enable-notification
configure router bgp group graceful-restart enable-notification
configure router bgp group neighbor graceful-restart enable-notification

Description When this command is present, the graceful restart capability sent by this router indicates support for NOTIFICATION messages. If the peer also supports this capability, then the session can be restarted gracefully (while preserving forwarding) if either peer needs to send a NOTIFICATION message due to some type of event or error.

Default no enable-notification

Platforms All

9.69 enable-origin-validation

enable-origin-validation

Syntax **enable-origin-validation** [**ipv4**] [**ipv6**] [**label-ipv4**]
no enable-origin-validation

Context **[Tree]** (config>service>vprn>bgp>group enable-origin-validation)
[Tree] (config>service>vprn>bgp>group>neighbor enable-origin-validation)

Full Context configure service vprn bgp group enable-origin-validation
configure service vprn bgp group neighbor enable-origin-validation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When this command is added to the configuration of a group or neighbor, it causes every inbound IPv4, IPv6, and label-IPv4 route from that peer to be marked with one of the following origin validation states:

- Valid (0)
- Not-Found (1)
- Invalid (2)

By default (when no family parameter is present in the command) or when all the family options are specified, all unicast IPv4 (AFI1/SAFI1), label-IPv4 (AFI1/SAFI4), and unicast IPv6 (AFI2/SAFI1) routes are evaluated to determine their origin validation states. When only a subset of the family options are present, then only the corresponding address family routes are evaluated.

This command applies to all types of VPRN BGP peers, generally, it should only be applied to EBGP peers and groups that contain only EBGP peers.

The **no** form of this command disables the inspection of received routes from the peer to determine origin validation state.

Default no enable-origin-validation

Parameters **ipv4** — Enables origin validation processing for unlabeled unicast IPv4 routes.

ipv6 — Enables origin validation processing for unlabeled unicast IPv6 routes.

label-ipv4 — Enables origin validation processing for labeled IPv4 routes.

Platforms All

enable-origin-validation

Syntax **enable-origin-validation** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**]
no enable-origin-validation

Context **[Tree]** (config>router>bgp>group enable-origin-validation)
[Tree] (config>router>bgp>group>neighbor enable-origin-validation)

Full Context configure router bgp group enable-origin-validation
configure router bgp group neighbor enable-origin-validation

Description When the **enable-origin-validation** command is added to the configuration of a group or neighbor, it causes every inbound IPv4 or IPv6 route from that peer to be marked with one of the following origin validation states:

- Valid (0)
- Not-Found (1)
- Invalid (2)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default (when neither the ipv4 or ipv6 option is present in the command) or when both the ipv4 and ipv6 options are specified, all unicast IPv4 (AFI1/SAFI1), label-IPv4 (AFI1/SAFI4), unicast IPv6 (AFI2/SAFI1), and label-IPv6 (AFI2/SAFI4) routes are evaluated to determine their origin validation states. When only the ipv4 or ipv6 option is present, only the corresponding address family routes (unlabeled and labeled) are evaluated.

The **enable-origin-validation** command applies to all types of BGP peers, but as a general rule, it should only be applied to EBGP peers and groups that contain only EBGP peers.

Default no enable-origin-validation

Parameters **ipv4** — Enables origin validation processing for unlabeled unicast IPv4 routes.

ipv6 — Enables origin validation processing for unlabeled unicast IPv6 routes.

label-ipv4 — Enables origin validation processing for labeled IPv4 routes.

label-ipv6 — Enables origin validation processing for labeled IPv6 routes.

Platforms All

9.70 enable-peer-tracking

enable-peer-tracking

Syntax [**no**] **enable-peer-tracking**

Context **[Tree]** (config>service>vprn>bgp enable-peer-tracking)
[Tree] (config>service>vprn>bgp>group enable-peer-tracking)
[Tree] (config>service>vprn>bgp>group>neighbor enable-peer-tracking)

Full Context configure service vprn bgp enable-peer-tracking
configure service vprn bgp group enable-peer-tracking
configure service vprn bgp group neighbor enable-peer-tracking

Description This command enables BGP peer tracking.

Default no enable-peer-tracking

Platforms All

enable-peer-tracking

Syntax [**no**] **enable-peer-tracking**

Context **[Tree]** (config>router>bgp enable-peer-tracking)
[Tree] (config>router>bgp>group enable-peer-tracking)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>bgp>group>neighbor enable-peer-tracking)

Full Context configure router bgp enable-peer-tracking
configure router bgp group enable-peer-tracking
configure router bgp group neighbor enable-peer-tracking

Description This command enables BGP peer tracking. BGP peer tracking allows a BGP peer to be dropped immediately if the route used to resolve the BGP peer address is removed from the IP routing table and there is no alternative available. The BGP peer will not wait for the holdtimer to expire; therefore, the BGP re-convergence process is accelerated.

The **no** form of this command disables peer tracking.

Default no enable-peer-tracking

Platforms All

9.71 enable-port-id

enable-port-id

Syntax [**no**] **enable-port-id**

Context **[Tree]** (config>mirror>mirror-dest enable-port-id)

Full Context configure mirror mirror-dest enable-port-id

Description This command includes the mirrored packet system's port ID. The system port ID can be used to identify which port the packet was received or sent on. Inclusion of the port ID is only supported for **mirror-dest type ppp**.

The **no** form of this command disables the inclusion of the port ID of the system in the packet.

Platforms All

9.72 enable-rr-vpn-forwarding

enable-rr-vpn-forwarding

Syntax [**no**] **enable-rr-vpn-forwarding**

Context **[Tree]** (config>router>bgp enable-rr-vpn-forwarding)

Full Context configure router bgp enable-rr-vpn-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When this command is configured all received VPN-IP routes, regardless of route target, are imported into the dummy VRF, where the BGP next-hops are resolved. The **label-route-transport-tunnel** under **config>router>bgp>next-hop-resolution** determines what types of tunnels are eligible to resolve the next-hops. If a received VPN-IP route from IBGP peer X is resolved and selected as best so that it can be re-advertised to an IBGP peer Y, and the BGP next-hop is modified towards peer Y (by using the next-hop-self command in Y's group or neighbor context or by using a next-hop action in an export policy applied to Y) then BGP allocates a new VPRN service label value for the route, signals that new label value to Y and programs the IOM to do the corresponding label swap operation. The supported combinations of X and Y are outlined below:

- from X (client) to Y (client)
- from X (client) to Y (non-client)
- from X (non-client) to Y (client)

The **no** form of this command causes the re-advertisement of a VPN-IP route between one IBGP peer and another IBGP peer does not cause a new VPRN service label value to be signaled and programmed even if the BGP next-hop is changed through group/neighbor configuration or policy.

Nokia recommends leaving this command disabled for scaling and convergence reasons.

Default no enable-rr-vpn-forwarding

Platforms All

9.73 enable-rt-client

enable-rt-client

Syntax [**no**] **enable-rt-client**

Context **[Tree]** (config>isa>video-group enable-rt-client)

Full Context configure isa video-group enable-rt-client

Description By default, the video ISA has both client and server capability for RET (retransmission). The client capability can be disabled to enable higher performance

The **no** form of the command enables higher performance.

Default enable-rt-client

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.74 enable-subconfed-vpn-forwarding

enable-subconfed-vpn-forwarding

Syntax [**no**] **enable-subconfed-vpn-forwarding**

Context **[Tree]** (config>router>bgp enable-subconfed-vpn-forwarding)

Full Context configure router bgp enable-subconfed-vpn-forwarding

Description This command configures BGP to keep VPN-IPv4 and VPN-IPv6 routes within a subconfederation and allow a **next-hop-self** command to create label swap forwarding entries.

When this is enabled, the base router BGP instance retains all received VPN-IPv4 and VPN-IPv6 routes, even those with route targets not matching any VRF import policy of any locally configured VPRN. In addition, when this leaf is enabled and base router BGP is configured to apply a **next-hop-self** command to a peer of any type (EBGP, IBGP, or confed-EBGP), the VPN-IPv4 and VPN-IPv6 routes are advertised to the peer with a new BGP label and next-hop, and a label-swap forwarding entry is programmed.The preceding behaviors are applied when the **enable-inter-as-vpn** or the **enable-rr-vpn-forwarding** commands, both under the **configure router bgp** context, are also enabled in the same BGP instance and regardless of whether the base router has a confederation configuration.

The **no** form of this command disables subconfederation VPN forwarding.

Default no enable-subconfed-vpn-forwarding

Platforms All

9.75 enable-tech

enable-tech

Syntax [**no**] **enable-tech**

Context **[Tree]** (admin enable-tech)

Full Context admin enable-tech

Description This command enables the shell and kernel commands.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: This command should only be used with authorized direction of Nokia support.

Platforms All

9.76 enable-triggered-hosts

enable-triggered-hosts

Syntax [**no**] **enable-triggered-hosts**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wpp enable-triggered-hosts)
[Tree] (config>service>ies>sub-if>grp-if>wpp enable-triggered-hosts)

Full Context configure service ies subscriber-interface group-interface wpp enable-triggered-hosts
configure service vprn subscriber-interface group-interface wpp enable-triggered-hosts

Description This command enables system to auto creates ESM hosts upon successful WPP authentication. The default host must be configured under SAP on the subscriber SAP to redirect unauthenticated client traffic to the web portal.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.77 enable-vsd-config

enable-vsd-config

Syntax [**no**] **enable-vsd-config**

Context **[Tree]** (global enable-vsd-config)

Full Context global enable-vsd-config

Description This command allows editing of VSD services just like normal services. As this is an action that should only be executed by authorized personnel, the activation of this command is protected by the use of a password, defined under **configure system security password vsd-password**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.78 encap

encap

Syntax **encap**

Context **[Tree]** (config>mirror>mirror-dest encap)

Full Context configure mirror mirror-dest encap

Description Commands in this context configure encapsulation options for the mirrored traffic. Note that the use of **encap** is mutually exclusive with SAP or spoke SDP options in the same mirror destination. Only one type of encapsulation can be specified for a single mirror destination. Slicing and encap are mutually exclusive in the same **mirror-dest** context.

Platforms All

9.79 encap-defined-qos

encap-defined-qos

Syntax **encap-defined-qos**

Context **[Tree]** (config>service>vpls>sap>egress encap-defined-qos)

Full Context configure service vpls sap egress encap-defined-qos

Description This command creates a new QoS sub-context in B-VPLS SAP egress context. The user can define encapsulation groups, referred to as encap-group, based on the ISID value in the packet's encapsulation and assign a QoS policy and a scheduler policy or aggregate rate limit to the group.

Platforms All

9.80 encap-group

encap-group

Syntax **encap-group** *group-name* [**type** *group-type*] [**qos-per-member**] [**create**]
no encap-group *group-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap>egress>encap-defined-qos encap-group)

Full Context configure service vpls sap egress encap-defined-qos encap-group

Description This command defines an encapsulation group which consists of a group of ISID values. All packets forwarded on the egress of a B-VPLS SAP which payload header matches one of the ISID value in the encap-group will use the same QoS policy instance and scheduler policy or aggregate rate limit instance.

The user adds or removes members to the encap-group one at a time or as a range of contiguous values using the member command. However, when the qos-per-member option is enabled, members must be added or removed one at a time. These members are also referred to as ISID contexts.

The user can configure one or more encap-groups in the egress context of the same B-SAP, therefore defining different ISID values and applying each a different SAP egress QoS policy, and optionally a different scheduler policy/**agg-rate**. ISID values are unique within the context of a B-SAP. The same ISID value cannot be re-used in another encap-group under the same B-SAP but can be re-used in an encap-group under a different B-SAP. Finally, if the user adds to an encap-group an ISID value which is already a member of this encap-group, the command causes no effect. The same if the user attempts to remove an ISID value which is not a member of this encap-group.

Once a group is created, the user will assign a SAP egress QoS policy, and optionally a scheduler policy or aggregate rate limit, using the following commands:

config>service>vpls>sap>egress>encap-defined-qos>encap-group>qos *sap-egress-policy-id*

config>service>vpls>sap>egress>encap-defined-qos>encap-group>scheduler-policy *scheduler-policy-name*

config>service>vpls>sap>egress>encap-defined-qos>encap-group>agg-rate *kilobits-per-second*

A SAP egress QoS policy must first be assigned to the created encap group before the user can add members to this group. Conversely, the user cannot perform the **no qos** command until all members are deleted from the encap-group.

An explicit or the default SAP egress QoS policy continues to be applied to the entire B-SAP but this will serve to create the set of egress queues which are used to store and forward a packet which does not match any of the defined ISID values in any of the encap-groups for this SAP.

Only the queue definition and fc-to-queue mapping from the encap-group SAP egress QoS policy is applied to the ISID members. All other parameters configurable in a SAP egress QoS policy must be inherited from egress QoS policy applied to the B-SAP.

Furthermore, any other CLI option configured in the egress context of the B-SAP continues to apply to packets matching a member of any encap-group defined in this B-SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The keyword **qos-per-member** allows the user to specify that a separate queue set instance and scheduler/**agg-rate** instance will be created for each ISID value in the encap-group. By default, shared instances will be created for the entire encap-group.

When the B-SAP is configured on a LAG port, the ISID queue instances defined by all the encap-groups applied to the egress context of the SAP will be replicated on each member link of the LAG. The set of scheduler/**agg-rate** instances will be replicated per link or per IOM or XMA depending if the adapt-qos option is set to link/port-fair mode or distribute mode. This is the same behavior as that applied to the entire B-SAP in the current implementation.

The **no** form of this command deletes the encap-group.

Parameters *group-name* — Specifies the name of the encap-group and can be up to 32 ASCII characters in length

type — Specifies the type of the encapsulation ID used by this encap-group

Values isid

qos-per-member — Specifies that a separate queue set instance and scheduler/**agg-rate** instance will be created for each ISID value in the encap-group

Platforms All

9.81 encap-match

encap-match

Syntax **encap-match** {**all-encap** | **double-tag** *encap-value* | **single-tag** *encap-value* | **untagged**}
no encap-match

Context **[Tree]** (config>port>ethernet>dot1x>macsec>sub-port encap-match)

Full Context configure port ethernet dot1x macsec sub-port encap-match

Description This command defines the sub-set of traffic on this port affected by this MACsec sub-port.

In order to establish an end-to-end communication between the remote MACsec peers encrypting VLAN-tagged traffic, the MKA packets have to be able to travel over the network following the same path as the encrypted traffic. MKA packets are generated with specific tags depending on the traffic match criteria configured, as shown in Table 50.

The **no** form of this command removes all traffic sub-set definitions from the MACsec sub-port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 50 **MKA Packet Generation**

Configuration	Config Example (<s-tag>.<c-tag>)	MKA Packet Generation	Traffic pattern match/ behavior
PORT all-encap	Config>port>ethernet>dot1x>macsec Sub-port 10 encap-match all-encap ca-name 10	untagged MKA packet	Matches all traffic on the port, including untagged, single-tag, double-tag. This is the Release 15.0 default behavior.
Untagged	Config>port>ethernet>dot1x>macsec Sub-port 1 encap-match untagged ca-name 2	untagged MKA packet	Matches only untagged traffic on the port
802.1Q single S-TAG (specific S-TAG)	Config>port>ethernet>dot1x>macsec Sub-port 2 encap-match dot1q 1 ca-name 3	MKA packet generated with S-TAG=1	Matches only single-tag traffic on port with tag ID of 1
802.1Q single S-TAG (any S-TAG)	Config>port>ethernet>dot1x>macsec Sub-port 3 encap-match dot1q * ca-name 4	untagged MKA packet	Matches any single-tag traffic on port
802.1ad double tag (both tag have specific TAGs)	Config>port>ethernet>dot1x>macsec Sub-port 4 encap-match qinq 1.1 ca-name 5	MKA packet generated with S-tag=1 and C-TAG=1	Matches only double-tag traffic on port with service tag of 1 and customer tag of 1
802.1ad double tag (specific S-TAG, any C-TAG)	Config>port>ethernet>dot1x>macsec Sub-port 6 encap-match qinq 1.* ca-name 7	MKA packet generated with S-TAG=1	Matches only double-tag traffic on port with service tag of 1 and customer tag of any

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 50 **MKA Packet Generation**

Configuration	Config Example (<s-tag>.<c-tag>)	MKA Packet Generation	Traffic pattern match/ behavior
802.1ad double tag (any S-TAG, any C-TAG	Config>port>ethernet>dot1x>macsec Sub-port 7 encap-match double-tag *.* ca-name 8	untagged MKA packet	Matches any double-tag traffic on port

Default encap-match all-encap

Parameters **all-encap** — Specifies that all traffic patterns are matched including untagged, single-tag or double-tag, and all will be encrypted.

untagged — Specifies that only untagged traffic are matched and encrypted.

single-tag — Specifies that only dot1q traffic are matched. Either all single tag traffic can be matched, by using *, or a specific dot1q tag can be matched.

double-tag — Specifies that only qinq traffic are matched. The service tag can be specifically matched or a wild card match (*.*) can be used.

encap-value — Specifies the type and value of the packet encapsulation to match for this MACsec sub-port.

Type	Parameter
all-encap	—
untagged	—
dot1q	[*| s] (s = 0..4094)
qinq	[*.*| s.*| s.c] (s and c = 0..4094)

where:

- S = service tag
- C = customer tag

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.82 encap-offset

encap-offset

Syntax **encap-offset** [**type** *type*]
no encap-offset

Context **[Tree]** (config>subscr-mgmt>sub-profile>egress encap-offset)

Full Context configure subscriber-mgmt sub-profile egress encap-offset

Description This command enables the adjustment of the queue and subscriber aggregate rate based on the last mile Ethernet or ATM encapsulation.

The data path computes the adjusted frame size real-time for each serviced packet from a queue by adding the actual packet size to the fixed offset provided by CPM for this queue and variable AAL5 padding.

When this command is enabled, the fixed packet offset is derived from the encapsulation type value signaled in the Access-loop-encapsulation sub-TLV in the Vendor-Specific PPPoE Tags or DHCP Relay Options as per RFC 4679. If the user specifies an encapsulation type with the command, this value is used as the default value for all hosts of this subscriber until a host session signaled a valid value. The signaled value is applied to this host only and the remaining hosts of this subscriber continue to use the user entered default type value if configured, or no offset is applied. However, hosts of the same subscriber using the same SLA profile and which are on the same SAP will share the same instance of FC queues. In this case, the last valid encapsulation value signaled by a host of that same instance of the SAP egress QoS policy will override any previous signaled or configured value.

If the user manually applied a constant byte offset to each packet serviced by the queue by configuring the packet-byte-offset, it will have no effect on the net offset computed for the packet. This net offset is stored in the subscriber host table.

The procedures for handling signaling changes or configuration changes affecting the subscriber profile are as follows:

The avg-frame-size parameter in the subscriber profile is ignored.

If the user specifies an encapsulation type with the command, this value is used as the default value for all hosts of this subscriber until a host session signaled a valid value. The signaled value is applied to this host and other hosts of the same subscriber sharing the same SLA profile and which are on the same SAP. The remaining hosts of this subscriber continue to use the user entered default type value if configured, or no offset is applied.

If the user enables/disables the encap-offset option, or changes the parameter value of the encap-offset option, CPM immediately triggers a re-evaluation of subscribers hosts using the corresponding subscriber profile and an update the IOM with the new fixed offset value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a subscriber has a static host or an ARP host, the subscriber host continues to use the user-configured default encapsulation type value or the last valid encapsulation value signaled in the PPPoE tags or DHCP relay options by other hosts of the same subscriber which use the same SLA profile instance. If none was signaled or configured, then no rate adjustment is applied.

When the encap-offset option is configured in the subscriber profile, the subscriber host queue rates, that is, CLI and operational PIR and CIR as well as queue bucket updates, the queue statistics, that is, forwarded, dropped, and HQoS offered counters use the last-mile frame-over-the-wire format. The scheduler policy CLI and operational rates also use LM-FoW format. The port scheduler max-rate and the priority level rates and weights, if a Weighted Scheduler Group is used, are always entered in CLI and interpreted as local port frame-over-the-wire rates. The same is true for an agg-rate-limit applied to a Vport. Finally the subscriber agg-rate-limit is entered in CLI as last-mile frame-over-the-wire rate. The system maintains a running average frame expansion ratio for each queue to convert queue rates between these two formats.

The **no** form of this command reverts to the default.

Parameters *type* — The name of the default encapsulation used for all host queues of a subscriber in the absence of a valid value signaled in the PPPoE tags.

Values pppoa-llc, pppoa-null, pppoeoa-llc, pppoeoa-llc-fcs, pppoeoa-llc-tagged, pppoeoa-llc-tagged-fcs, pppoeoa-null, pppoeoa-null-fcs, pppoeoa-null-tagged, pppoeoa-null-tagged-fcs, ipoa-llc, ipoa-null, ipoeoa-llc, ipoeoa-llc-fcs, ipoeoa-llc-tagged, ipoeoa-llc-tagged-fcs, ipoeoa-null, ipoeoa-null-fcs, ipoeoa-null-tagged, ipoeoa-null-tagged-fcs, pppoe, pppoe-tagged, ipoe, ipoe-tagged

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

encap-offset

Syntax **encap-offset** [**type** *encap-type*]
no encap-offset

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>access-loop-encapsulation encap-offset)

Full Context configure subscriber-mgmt local-user-db ppp host access-loop-encapsulation encap-offset

Description This command is applicable within the LAC/LNS context. It provides the last mile link encapsulation information that is needed for proper (shaping) rate calculations and interleaving delay in the last mile.

The encapsulation value will be taken from the following sources in the order of priority:

- Statically provisioned value in local user database (LUDB).
- RADIUS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- PPPoE tags on LAC or ICRQ message (RFC 5515) on LNS

In case that the encapsulation information is not provided by any of the existing means (LUDB, RADIUS, AVP signaling, PPPoE Tags), then by default pppoea-null encapsulation will be in effect.

The following values are supported encapsulation values on LNS in the 7750 SR.

encap-type:

pppoa-llc	LLC (NLPID) PPPoA encapsulation.
pppoa-null	VC-MUX PPPoA encapsulation.
pppoeoa-llc	LLC/SNAP based bridged Ethernet PPPoEoA encapsulation without FCS.
pppoeoa-llc-fcs	LLC/SNAP based bridged Ethernet PPPoEoA encapsulation with FCS.
pppoeoa-null	VC-MUX PPPoEoA encapsulation without FCS.
pppoeoa-null-fcs	VC-MUX PPPoEoA encapsulation with FCS.
pppoe	PPPoE encapsulation.
pppoe-tagged	Tagged PPPoE Encapsulation.

The values are not supported encapsulation values on LNS in the 7750 SR.

pppoeoa-llc-tagged
pppoeoa-llc-tagged-fcs
pppoeoa-null-tagged
pppoeoa-null-tagged-fcs
ipoa-llc
ipoa-null
ipoeeoa-llc
ipoeoa-llc-fcs
ipoeoa-llc-tagged
ipoeoa-llc-tagged-fcs
ipoeoa-null
ipoeoa-null-fcs
ipoeoa-null-tagged
ipoeoa-null-tagged-fcs
ipoe
ipoe-tagged

Default no encap-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

9.83 encap-tag-range

encap-tag-range

Syntax **encap-tag-range start-tag** *start-tag* **end-tag** *end-tag*
no encap-tag-range

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident encap-tag-range)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-ident encap-tag-range)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification encap-tag-range
configure subscriber-mgmt local-user-db ppp host host-identification encap-tag-range

Description This command specifies a range of encapsulation tags as the host identifications. The encapsulation tag is dot1q or qinq on Ethernet port.

For dot1q, the start/end-tag is single number, range from 0-4094; for QinQ, the start/end-tag format is x.y, x or y could be “*”, which means ignore inner or outer tag.

Note: This command is only used when **encap-tag-range** is configured as one of the **match-list** parameters.

The **no** form of this command removes the encapsulation tag range from the configuration.

Parameters **start-tag** *start-tag* — Specifies the value of the start label in the range of SAPs allowed on this host.

Values

start-tag	dot1q	qtag1
	qinq	(qtag1.qtag2 | qtag1.* | *.qtag2)

end-tag *end-tag* — Specifies the value of the end label in the range of SAPs allowed on this host.

Values

end-tag	dot1q	qtag1
	qinq	(qtag1.qtag2 | qtag1.* | *.qtag2)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.84 encap-tag-separate-range

encap-tag-separate-range

Syntax **encap-tag-separate-range outer** *outer-encap-range* **inner** *inner-encap-range*
no encap-tag-separate-range

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident encap-tag-separate-range)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-ident encap-tag-separate-range)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification encap-tag-separate-range
configure subscriber-mgmt local-user-db ppp host host-identification encap-tag-separate-range

Description This command specifies a range of encapsulation tags as the host identifications.

Note: This command is only used when **encap-tag-separate-range** is configured as one of the **match-list** parameters.

The **no** form of this command removes the range of encapsulation tags from the configuration.

Default no encap-tag-separate-range

Parameters *outer-encap-range* — Specifies the value of the outer encapsulation tag range.

Values *start-qtag* - *end-qtag*
start-qtag: 0 to 4094
end-qtag: 0 to 4094

inner-encap-range — Specifies the value of the inner encapsulation tag range.

Values *start-qtag* - *end-qtag*
start-qtag: 0 to 4094
end-qtag: 0 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.85 encap-type

encap-type

Syntax **encap-type** {**default** | **null** | **dot1q** | **qinq**}
no encap-type

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>l2-access-points>l2-ap encap-type)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>l2-access-points>l2-ap encap-type)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-access-points l2-ap encap-type
configure service vprn subscriber-interface group-interface wlan-gw l2-access-points l2-ap encap-type

Description If different from default, this command overrides the value specified by **l2-ap-encap-type** on wlan-gw level. See the description of l2-ap-encap-type for more detail. This value can only be changed while the l2-ap is shut down.

The **no** form of this command sets the default value.

Default encap-type default

Parameters **default** — Specifies to use the value specified by l2-ap-encap-type.

null — Specifies to use both the SAP and the AP are not VLAN-tagged.

dot1q — Specifies to use either the AP or the SAP uses one VLAN tag.

qinq — Up to two VLAN tags are used by the AP or SAP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

encap-type

Syntax **encap-type** {**dot1q** | **null** | **qinq**}
no encap-type

Context [Tree] (config>port>ethernet encap-type)

Full Context configure port ethernet encap-type

Description This command configures the encapsulation method used to distinguish customer traffic on an Ethernet access port, or different VLANs on a network port.

The **no** form of this command restores the default.

Default encap-type null

Parameters **dot1q** — Ingress frames carry 802.1Q tags where each tag signifies a different service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

null — Ingress frames will not use any tags to delineate a service. As a result, only one service can be configured on a port with a null encapsulation type.

qinq — Specifies QinQ encapsulation.

Platforms All

encap-type

Syntax **encap-type** {**atm** | **bcp-null** | **bcp-dot1q** | **ipcp** | **ppp-auto** | **frame-relay** | **wan-mirror** | **cisco-hdlc**}

Context **[Tree]** (config>port>sonet-sdh>path encap-type)

Full Context configure port sonet-sdh path encap-type

Description This command configures the encapsulation method used to distinguish customer traffic on an access SONET/SDH channel sub-port.

When the **encap-type** is set to ATM the CRC default cannot be changed.

When the **encap-type** is ATM, ATM sub-layer verification (GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs)*) is automatically enabled. The result of the verification includes:

- Out of Cell Delineation (OCD) event count. The OCD event count is described in RFC 2515, *Definitions of Managed Objects for ATM Management*. Note that multiple events occurring within a second will be counted as 1 event for ATM and ASAP MDAs as a result of a hardware limit.
- Loss of Cell Delineation defect/alarm. The LCD defect/alarm is defined in RFC 2515, *Definitions of Managed Objects for ATM Management*. When a path is in an LCD defect state, the path's operational status will be down. When a path exits the LCD state, the path's operational status will change to up (assuming nothing else causes the path to stay down). A trap is raised to indicate the LCD status change. Also a P-RDI is sent to indicate the defect to the remote end.

The **encap-type** is only required when configuring a SONET/SDH path for access mode.

The **no** form of this command restores the default.

Default encap-type bcp-null

Parameters **atm** — Specifies that the encapsulation on the port is ATM.

bcp-null — Only a single service is configured on this channel and IEEE 802.1Q tags are not used as a service delimiter. Any IEEE 802.1Q tags encountered are regarded as part of the customer payload and transparently forwarded. When **bcp-null** encapsulation is specified, the PPP Bridge Control Protocol (BCP) is activated and all packets on this access port will be encapsulated in accordance with the BCP protocol.

Note that null ports will accept q-tagged frames.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bcp-dot1q — Ingress frames carry IEEE 802.1Q tags and the tags are used as service delimiter. Any untagged packets are silently discarded with exception of protocol specific packets. When **bcp-dot1q** encapsulation is specified, the PPP Bridge Control Protocol (BCP) is activated and all packets on this access port will be encapsulated in accordance with the BCP protocol.

ipcp — Ingress frames are encapsulated according to the IP Control Protocol. When **ipcp** encapsulation is specified, the PPP IP Control Protocol will be activated and only packets that comply with IPCP encapsulation are processed; others are silently discarded.

ppp-auto — Enables PPP on the associated port/channel. The activation of ipcp and mplscp is automatically enabled depending on the protocol configuration. This encap type is only valid on ports/channels in network mode.

frame-relay — Enables frame relay on the associated port/channel.

wan-mirror — The port is used for mirroring of frame-relay and POS ports. On these ports, no link management protocol would run.

cisco-hdlc — Monitors line status on a serial interface by exchanging keepalive request messages with peer network devices.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

encap-type

Syntax **encap-type** {**atm** | **bcp-null** | **bcp-dot1q** | **ipcp** | **ppp-auto** | **frame-relay** | **wan-mirror** | **cisco-hdlc** | **cem**}

Context **[Tree]** (config>port>tdm>ds1>channel-group encap-type)
[Tree] (config>port>tdm>ds3 encap-type)
[Tree] (config>port>tdm>e1>channel-group encap-type)
[Tree] (config>port>tdm>e3 encap-type)

Full Context configure port tdm ds1 channel-group encap-type
configure port tdm ds3 encap-type
configure port tdm e1 channel-group encap-type
configure port tdm e3 encap-type

Description This command configures the encapsulation method used to on the specified port, path, or channel. This parameter can be set on both access and network ports.

When the **encap-type** is set to ATM the CRC, timeslots, scrambling (if applicable), and idle-cycle-flags are set to ATM defaults respectively. When the encap-type is changed from ATM, those parameters are set to their non-ATM defaults.

When the **encap-type** is ATM, ATM sub-layer verification (GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs)*) is automatically enabled. When ATM PLCP cell mapping is used, the results of this verification include:

- PLCP Severely Errored Framing Seconds

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- PLCP Alarm State
- PLCP Unavailable Seconds Counter

When ATM direct cell mapping is used, the result of the verification includes:

- Out of Cell Delineation (OCD) event count. The OCD event count is described in RFC 2515, *Definitions of Managed Objects for ATM Management*. Note that multiple events occurring within a second will be counted as 1 event for ASAP MDAs as a result of a hardware limit.
- Loss of Cell Delineation defect/alarm. The LCD defect/alarm is defined in RFC 2515, *Definitions of Managed Objects for ATM Management*. When a path is in an LCD defect state, the path's operational status will be down. When a path exits the LCD state, the path's operational status will change to up (assuming nothing else causes the path to stay down). A trap is raised to indicate the LCD status change. Also, a P-RDI is sent to indicate the defect to the remote end.

The **no** form of this command restores the default.

Default encap-type bcp-null

Parameters **atm** — Specifies the encapsulation on the port is ATM.

bcp-null — When selected, this keyword specifies that only a single service is configured on this channel and IEEE 802.1Q tags are not used as a service delimiter. Any IEEE 802.1Q tags encountered are regarded as part of the customer payload and transparently forwarded. When bcp-null encapsulation is specified, the PPP Bridge Control Protocol (BCP) is activated and all packets on this access port will be encapsulated in accordance with the BCP protocol.

bcp-dot1q — When selected, this keyword specifies that ingress frames carry IEEE 802.1Q tags and the tags are used as service delimiter. Any untagged packets are silently discarded with exception of protocol specific packets. When bcp-dot1q encapsulation is specified, the PPP Bridge Control Protocol (BCP) is activated and all packets on this access port will be encapsulated in accordance with the BCP protocol.

ipcp — Ingress frames are encapsulated according to the IP Control Protocol. When ipcp encapsulation is specified, the PPP IP Control Protocol will be activated and only packets that comply with IPCP encapsulation are processed; others are silently discarded.

ppp-auto — (Network mode) Enables PPP on the associated port/channel. The activation of ipcp and mplscp is automatically enabled depending on the protocol configuration. This encap type is only valid on ports/channels in network mode.

frame-relay — Enables frame relay on the associated port/channel.

wan-mirror — The port is used for mirroring of frame-relay and POS ports. On these ports, no link management protocol will run.

cisco-hdlc — Monitors line status on a serial interface by exchanging keepalive request messages with peer network devices.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cem — Specifies that on circuit emulation MDAs, only the **cem** encap-type is supported. All other values are blocked with an appropriate warning. The **cem** encap-type is not supported on other MDAs and are blocked with an appropriate warning.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

encap-type

Syntax **encap-type** {**dot1q** | **null** | **qinq**}
no encap-type

Context **[Tree]** (config>lag encap-type)

Full Context configure lag encap-type

Description This command configures the encapsulation method used to distinguish customer traffic on a LAG. The encapsulation type is configurable on a LAG port. The LAG port and the port member encapsulation types must match when adding a port member.

If the encapsulation type of the LAG port is changed, the encapsulation type on all the port members will also change. The encapsulation type can be changed on the LAG port only if there is no interface associated with it. If the MTU is set to a non-default value, it will be reset to the default value when the encap type is changed.

The **no** form of this command restores the default.

Default encap-type null — All traffic on the port belongs to a single service or VLAN.

Parameters **dot1q** — Ingress frames carry 802.1Q tags where each tag signifies a different service.

null — Ingress frames will not use any tags to delineate a service. As a result, only one service can be configured on a port with a null encapsulation type.

qinq — Specifies QinQ encapsulation.

Platforms All

encap-type

Syntax **encap-type** {**dot1q**| **qinq**}
no encap-type

Context **[Tree]** (config>eth-tunnel>ethernet encap-type)

Full Context configure eth-tunnel ethernet encap-type

Description This command configures the encapsulation method used to distinguish customer traffic on a LAG. The encapsulation type is configurable on a LAG port. The LAG port and the port member encapsulation types must match when adding a port member.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the encapsulation type of the LAG port is changed, the encapsulation type on all the port members will also change. The encapsulation type can be changed on the LAG port only if there is no interface associated with it. If the MTU is set to a non-default value, it will be reset to the default value when the encap type is changed.

The **no** form of this command reverts to the default.

Default encap-type dot1q

Parameters **dot1q** — Specifies that frames carry 802.1Q tags where each tag signifies a different service.

qinq — Specifies the qinq encapsulation method.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

encap-type

Syntax **encap-type** {**dot1q** | **qinq**}
no encap-type

Context **[Tree]** (config>pw-port encap-type)

Full Context configure pw-port encap-type

Description This command configures the encapsulation type on a PW port. Customer Ethernet frames can be single-tagged or double-tagged, and this command determines the number of tags that the SR OS will check (and strip) on PW-SAP ingress and insert on PW-SAP egress.

The **no** form of this command removes the configuration.

Parameters **dot1q** — Specifies that the encapsulation type is dot1q; used when the customer's Ethernet frame is single-tagged.

qinq — Specifies that the encapsulation type is qinq; used when the customer's Ethernet frame is double-tagged.

Default dot1q

Platforms All

9.86 encapsulated-ip-mtu

encapsulated-ip-mtu

Syntax **encapsulated-ip-mtu** *bytes*
no encapsulated-ip-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>if>ipsec>ipsec-tunnel encapsulated-ip-mtu)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel encapsulated-ip-mtu)
[Tree] (config>service>ies>if>sap>ip-tunnel encapsulated-ip-mtu)
[Tree] (config>ipsec>tnl-temp encapsulated-ip-mtu)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel encapsulated-ip-mtu)
[Tree] (config>service>vprn>if>sap>ip-tunnel encapsulated-ip-mtu)
[Tree] (config>service>vprn>if>sap>ipsec-tun encapsulated-ip-mtu)

Full Context configure ipsec tunnel-template encapsulated-ip-mtu
configure router interface ipsec ipsec-tunnel encapsulated-ip-mtu
configure service ies interface ipsec ipsec-tunnel encapsulated-ip-mtu
configure service ies interface sap ip-tunnel encapsulated-ip-mtu
configure service vprn interface ipsec ipsec-tunnel encapsulated-ip-mtu
configure service vprn interface sap ip-tunnel encapsulated-ip-mtu
configure service vprn interface sap ipsec-tunnel encapsulated-ip-mtu

Description This command specifies the maximum size of encapsulated tunnel packet for the ipsec-tunnel, ip-tunnel, or the dynamic tunnels terminated on the ipsec-gw. If the encapsulated IPv4 or IPv6 tunnel packet exceeds the **encapsulated-ip-mtu**, then the system fragments the packet against the encapsulated-ip-mtu.

The **no** form of this command reverts to the default.

Default no encapsulated-ip-mtu

Parameters *bytes* — Specifies the maximum size in bytes.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ip-tunnel encapsulated-ip-mtu
- configure ipsec tunnel-template encapsulated-ip-mtu
- configure service vprn interface sap ipsec-tunnel encapsulated-ip-mtu
- configure service vprn interface sap ip-tunnel encapsulated-ip-mtu

VSR

- configure service vprn interface ipsec ipsec-tunnel encapsulated-ip-mtu
- configure service ies interface ipsec ipsec-tunnel encapsulated-ip-mtu
- configure router interface ipsec ipsec-tunnel encapsulated-ip-mtu

encapsulated-ip-mtu

Syntax **encapsulated-ip-mtu** *octets*
no encapsulated-ip-mtu

Context [Tree] (config>service>vprn>sap>ip-tunnel encapsulated-ip-mtu)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn sap ip-tunnel encapsulated-ip-mtu

Description This command configures the tunnel encapsulated IP MTU.

The **no** form of this command reverts to the default.

Parameters *octets* — Specifies the tunnel encapsulated IP MTU in octets.

9.87 encapsulation

encapsulation

Syntax **encapsulation** *atm-encap-type*

Context **[Tree]** (config>service>epipe>sap>atm encapsulation)
[Tree] (config>service>vpls>sap>atm encapsulation)

Full Context configure service epipe sap atm encapsulation
configure service vpls sap atm encapsulation

Description This command specifies the data encapsulation for an ATM PVCC delimited Epipe SAP. The definition references RFC 2684, *Multiprotocol Encapsulation over ATM AAL5,* and to the ATM Forum LAN Emulation specification.

Ingress traffic that does not match the configured encapsulation will be dropped.

Default encapsulation aal5snap-bridged

Parameters *atm-encap-type* — Specifies the encapsulation type.

Values **aal5snap-bridged** — Bridged encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.

aal5mux-bridged-eth-nofcs — Bridged IP encapsulation for VC multiplexed circuit as defined in RFC 2684.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

encapsulation

Syntax **encapsulation** *atm-encap-type*

Context **[Tree]** (config>service>ipipe>sap>atm encapsulation)

Full Context configure service ipipe sap atm encapsulation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the data encapsulation for an ATM PVCC delimited Ipipe SAP. The definition references RFC 2684, *Multiprotocol Encapsulation over ATM AAL5,* and to the ATM Forum LAN Emulation specification. Ingress traffic that does not match the configured encapsulation will be dropped.

Default encapsulation aal5snap-routed

Parameters *atm-encap-type* — Specifies the encapsulation type.

Values **aal5snap-routed** — Routed encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.

aal5mux-ip — Routed IP encapsulation for VC multiplexed circuit as defined in RFC 2684.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

encapsulation

Syntax **encapsulation** *atm-encap-type*

Context **[Tree]** (config>service>ies>if>sap>atm encapsulation)
[Tree] (config>service>vprn>if>sap>atm encapsulation)

Full Context configure service ies interface sap atm encapsulation
configure service vprn interface sap atm encapsulation

Description This command configures RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, encapsulation for an ATM PVCC delimited SAP. This command specifies the data encapsulation for an ATM PVCC delimited SAP. The definition also references the ATM Forum LAN Emulation specification. The encapsulation is driven by the services for which the SAP is configured.

Ingress traffic that does not match the configured encapsulation will be dropped.

Default encapsulation aal5snap-routed

Parameters *atm-encap-type* — Specifies the encapsulation type.

Values **aal5snap-routed** — Routed encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.

aal5mux-ip — Routed IP encapsulation for VC multiplexed circuit as defined in RFC 2684.

aal5snap-bridged — Bridged encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.

aal5mux-bridged-eth-nofcs — Bridged IP encapsulation for VC multiplexed circuit as defined in RFC 2684.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

9.88 encode

encode

Syntax **encode type** *type* **key** *key*
encode type *type* **key** *hash-key* **hash**
encode type *type* **key** *hash2-key* **hash2**
encode type *type* **key** *custom-key* **custom**
encode type *type* **cert-profile** *cert-profile-name*
no encode

Context **[Tree]** (config>app-assure>group>http-enrich>field encode)

Full Context configure application-assurance group http-enrich field encode

Description This command configures an HTTP header enrichment template field static string.

The **no** form of this command removes the template field static string.

Default no encode

Parameters *type* — Specifies whether the parameters are hashed with MD5 or encrypted with RC4 using the configured key, or if certificate-based encryption is used with RSA.

Values md5, rc4, certificate

key — Specifies the key string, 64 characters maximum.

hash-key — Specifies the first hashed key.

hash-key2 — Specifies the second hashed key.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

cert-profile-name — Specifies the name of the certificate profile to be used. This profile must have already been created using the **certificate-profile** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.89 encoding

encoding

Syntax **encoding** *encoding*
no encoding

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription encoding)

Full Context configure system telemetry persistent-subscriptions subscription encoding

Description This command configures the encoding type that is used for telemetry notifications in accordance with the definitions in the gNMI OpenConfig standard.

Default encoding json

Parameters *encoding* — Specifies the encoding type.

Values json, bytes, proto

Platforms All

9.90 encoding-type

encoding-type

Syntax **encoding-type** *encoding-type*
no encoding-type

Context **[Tree]** (config>router>gmpls>lsp encoding-type)

Full Context configure router gmpls lsp encoding-type

Description This command configures the encoding type of the payload carried by the GMPLS LSP; **line** is the only supported type.

Default encoding-type line

Parameters *encoding-type* — Specifies the encoding type.

Values line

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.91 encrypt

encrypt

Syntax **encrypt** {**on** | **off**}

Context **[Tree]** (bof encrypt)

Full Context bof encrypt

Description This command enables and disables encryption of the BOF using AES256 and SHA256.

When the BOF is encrypted on the compact flash, it is still reachable using the BOF interactive menu during node startup, and fields can be modified using the BOF interactive menu.

Default encrypt off

Parameters **on** — Enables BOF encryption

off — Disables BOF encryption

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.92 encryption-key

encryption-key

Syntax **encryption-key** *key* [**hash** | **hash2** | **custom**]
no encryption-key

Context **[Tree]** (bof encryption-key)

Full Context bof encryption-key

Description This command creates a key to be used by AES256 and SHA256 for configuration file encryption and hashing. This key is used for all configuration files (primary, secondary, and tertiary).

After creating or deleting a key, use the **admin save** command to save the configuration file with the current encryption key state.

The **no** form of this command deletes the encryption key.

Default no encryption-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *key* — Specifies the encryption key.

If the **hash**, **hash2**, or **custom** parameter is not configured, the key is entered in plaintext and the key length must be between 8 and 32 characters. A plaintext key cannot contain embedded nulls or end with " hash", " hash2", or " custom".

If the **hash**, **hash2**, or **custom** parameter is configured, the key is hashed and the key length must be between 1 and 64 characters.

hash — Keyword to specify that the key is entered in an encrypted form.

hash2 — Keyword to specify that the key is entered in a more complex encrypted form. The **hash2** encryption scheme is node-specific and the key cannot be transferred between nodes.

custom — Keyword to specify that the key uses custom encryption.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.93 encryption-keygroup

encryption-keygroup

Syntax **encryption-keygroup** *keygroup-id* **direction** *direction*
no encryption-keygroup direction *direction*

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>group-encryption encryption-keygroup)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>group-encryption encryption-keygroup)

Full Context configure service ies subscriber-interface group-interface wlan-gw group-encryption encryption-keygroup
configure service vprn subscriber-interface group-interface wlan-gw group-encryption encryption-keygroup

Description This command binds an encryption key-group to a WLAN-GW soft-GRE group interface. When configured in the inbound direction, received packets must be encrypted using one of the valid security-associations configured for the key-group. When configured in the outbound direction, L2oMPLSoGRE packets egressing the node use the "active-outbound-sa" associated with the key-group configured.

The **no** form of this command removes the encryption keygroup from the inbound or outbound group interface.

Parameters *keygroup-id* — Specifies the ID number or name of the keygroup.

Values 1 to 127, *keygroup-name* up to 64 characters

direction — Applies the keygroup to the inbound or outbound direction of a service.

Values inbound | outbound

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

encryption-keygroup

Syntax **encryption-keygroup** *keygroup-id* **direction** {**inbound** | **outbound**}
no encryption-keygroup direction {**inbound** | **outbound**}

Context **[Tree]** (config>router>if>group-encryption encryption-keygroup)

Full Context configure router interface group-encryption encryption-keygroup

Description This command is used to bind a key group to a router interface for inbound or outbound packet processing. When configured in the outbound direction, packets egressing the router use the **active-outbound-sa** associated with the configured key group. When configured in the inbound direction, received packets must be encrypted using one of the valid security associations configured for the key group.

The **no** form of this command removes the key group from the router interface in the specified direction.

Default no encryption-keygroup direction inbound
no encryption-keygroup direction outbound

Parameters *keygroup-id* — The ID number of the key group being configured.

Values 1 to 127, *keygroup-name* (64 characters maximum)

inbound — Binds the key group in the inbound direction.

outbound — Binds the key group in the outbound direction.

Platforms VSR

encryption-keygroup

Syntax **encryption-keygroup** *keygroup-id* [**create**]
no encryption-keygroup *keygroup-id*

Context **[Tree]** (config>grp-encryp encryption-keygroup)

Full Context configure group-encryption encryption-keygroup

Description This command is used to create a key group. Once the key group is created, use the command to enter the key group context or delete a key group.

The **no** form of the command removes the key group. Before using the **no** form, the key group association must be deleted from all services that are using this key group.

Parameters *keygroup-id* — The number or name of the key group being referenced.

Values 1 to 15, or *keygroup-name* (up to 64 characters)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Creates a key group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

encryption-keygroup

Syntax **encryption-keygroup** *keygroup-id* **direction** {**inbound** | **outbound**}
no encryption-keygroup direction {**inbound** | **outbound**}

Context **[Tree]** (config>service>pw-template encryption-keygroup)
[Tree] (config>service>sdp encryption-keygroup)
[Tree] (config>service>vprn encryption-keygroup)

Full Context configure service pw-template encryption-keygroup
configure service sdp encryption-keygroup
configure service vprn encryption-keygroup

Description This command is used to bind a key group to an SDP, VPRN service, or PW template for inbound or outbound packet processing. When configured in the outbound direction, packets egressing the node use the **active-outbound-sa** associated with the key group configured. When configured in the inbound direction, received packets must be encrypted using one of the valid security associations configured for the key group. Services using the SDP will be encrypted.

The encryption (enabled or disabled) configured on an SDP used to terminate a Layer 3 spoke SDP of a VPRN always overrides any VPRN-level configuration for encryption.

Encryption is enabled after the outbound direction is configured.

For PW template changes, the following **tools** command must be executed after the configuration changes are made: **tools**>**perform**>**service**>**eval-pw-template**>**allow-service-impact**. This command applies the changes to services that use the PW template.

The **no** form of the command removes the key group from the SDP or service in the specified direction (inbound or outbound).

Parameters *keygroup-id* — Specifies the number of the key group being configured.

Values 1 to 15 or *keygroup-name* (up to 64 characters)

direction {**inbound** | **outbound**} — Specifies the direction of the service that the key group will be bound to.

Platforms VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.94 encryption-offset

encryption-offset

Syntax **encryption-offset** *encryption-offset*
no encryption-offset

Context **[Tree]** (config>macsec>connectivity-association encryption-offset)

Full Context configure macsec connectivity-association encryption-offset

Description This command specifies the offset of the encryption in MACsec packet.

The encryption-offset is distributed by MKA (Key-server) to all parties.

It is signaled via MACsec capabilities. There are four basic settings for this. Table 51 breaks down the settings.

Table 51 **MACsec Basic Settings**

Setting	Description
0	MACsec is not implemented
1	Integrity without confidentiality
2	The following are supported: • Integrity without confidentiality • Integrity and confidentiality with a confidentiality offset of 0
3 [1]	The following are supported: • Integrity without confidentiality • Integrity and confidentiality with a confidentiality offset of 0, 30, or 50

Note:

1. SR OS supports setting (3) Integrity without confidentiality and Integrity and confidentiality with a confidentiality offset of 0, 30, or 50.

The **no** form of this command rejects all arriving traffic whether MACsec is secured or not.

Default encryption-offset 0

Parameters *encryption-offset* — Specifies the encryption.

Values 0 — encrypt the entire payload

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

30 — leave the IPv4 header in clear
50 — leave the IPv6 header in clear

Platforms All

9.95 end

end

Syntax **end** *end-week end-day end-month hours-minutes*

Context **[Tree]** (config>system>time>dst-zone end)

Full Context configure system time dst-zone end

Description This command configures start of summer time settings.

Default end first sunday january 00:00

Parameters *end-week* — Specifies the starting week of the month when the summer time ends.

Values first, second, third, fourth, last

Default first

end-day — Specifies the starting day of the week when the summer time ends.

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

Default sunday

end-month — Specifies the starting month of the year when the summer time takes effect.

Values january, february, march, april, may, june, july, august, september, october, november, december

Default january

hours-minutes — Specifies the time at which the summer time ends, in hh:mm format.

Values hours: 00 to 23
minutes: 00 to 59

Default 00:00

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

end

Syntax [**no**] **end** *function-value*

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc>func end)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end

Description Commands in this context configure the value and attributes of SRv6 End SID function of a locator. The End SID function encodes the basic behavior of a prefix or a node SID.

The End SID function for each SRH mode must be statically allocated. The value is not automatically allocated by default.

The **no** form of this command removes the specified End function.

Parameters *function-value* — Specifies an SRv6 End SID function value. Up to eight values can be configured per locator. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

9.96 end-dt4

end-dt4

Syntax **end-dt4** [*function-value*]
no end-dt4

Context **[Tree]** (config>service>vprn>srv6>locator>function end-dt4)

Full Context configure service vprn segment-routing-v6 locator function end-dt4

Description This command configures the SRv6 End.DT4 behavior and function value that is associated to the SRv6 instance in the service. This implies decapsulation and table lookup for IPv4 prefixes in the VPRN.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dt4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *function-value* — Specifies the optional static function value that is associated to the function behavior. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**. If not configured, the system allocates a value dynamically. Auto-allocated service function values have an upper range limited by the maximum service function length of 20 bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

end-dt4

Syntax **end-dt4** [*function-value*]
no end-dt4

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc>func end-dt4)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-dt4

Description This command configures the SRv6 End.DT4 behavior and function value associated with the base routing instance. This implies decapsulation and table lookup for IPv4 prefixes in the base routing table. These prefixes can be static routes or routes advertised in BGP.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dt4

Parameters *function-value* — Specifies the SRv6 End.DT4 function value. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**. Auto-allocated service function values have an upper range limited by the maximum service function length of 20-bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

9.97 end-dt46

end-dt46

Syntax **end-dt46** [*function-value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no end-dt46

Context [Tree] (config>service>vprn>srv6>locator>function end-dt46)

Full Context configure service vprn segment-routing-v6 locator function end-dt46

Description This command configures the SRv6 End.DT46 behavior and function value that is associated to the SRv6 instance in the service. This means that decapsulation and table lookup for IPv4 and IPv6 prefixes occurs in the VPRN service.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dt46

Parameters *function-value* — Specifies the optional static function value that is associated to the function behavior. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**. If not configured, the system allocates a value dynamically. Auto-allocated service function values have an upper range limited by the maximum service function length of 20-bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

end-dt46

Syntax **end-dt46** [*function-value*]
no end-dt46

Context [Tree] (config>router>segment-routing>srv6>inst>loc>func end-dt46)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-dt46

Description This command configured the SRv6 End.DT46 function behavior and value associated with the base routing instance. This implies decapsulation and table lookup for IPv4 and IPv6 prefixes in the base routing table. These prefixes can be static routes or routes advertised in BGP.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dt46

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *function-value* — Specifies the SRv6 End.DT46 function value. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**. Auto-allocated service function values have an upper range limited by the maximum service function length of 20-bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

9.98 end-dt6

end-dt6

Syntax **end-dt6** [*function-value*]
no end-dt6

Context **[Tree]** (config>service>vprn>srv6>locator>function end-dt6)

Full Context configure service vprn segment-routing-v6 locator function end-dt6

Description This command configures the SRv6 End.DT6 behavior and function value that is associated to the SRv6 instance in the service. This means that decapsulation and table lookup for IPv6 prefixes occurs in the VPRN service.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dt6

Parameters *function-value* — Specifies the optional static function value that is associated to the function behavior. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**. If not configured, the system allocates a value dynamically. Auto-allocated service function values have an upper range limited by the maximum service function length of 20-bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

end-dt6

Syntax [**no**] **end-dt6**
end-dt6 [*function-value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>segment-routing>srv6>inst>loc>func end-dt6)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-dt6

Description This command configures the SRv6 End.DT6 function behavior and value associated with the base routing instance. This means that decapsulation and table lookup for IPv6 prefixes occurs in the base routing table. These prefixes can be static routes or routes advertised in BGP.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dt6

Parameters *function-value* — Specifies the SRv6 End.DT6 function value. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**. Auto-allocated service function values have an upper range limited by the maximum service function length of 20-bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

9.99 end-dx2

end-dx2

Syntax **end-dx2** [*function-value*]
no end-dx2

Context [Tree] (config>service>epipe>srv6>locator>function end-dx2)

Full Context configure service epipe segment-routing-v6 locator function end-dx2

Description This command configures the SRv6 End.DX2 behavior and function value that is associated with the SRv6 instance in the service, which means that decapsulation and cross-connect to the egress SAP occurs in the Epipe service.

The **no** form of this command removes the function behavior and value from the configuration.

Default no end-dx2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *function-value* — Specifies the optional static function value that is associated with the function behavior. Statically allocated functions of all SID types in a locator have their upper range limited by the **config>router>segment-routing>srv6>loc>static-function max-entries**. If not configured, the system allocates a value dynamically. Auto-allocated service function values have an upper range limited by the maximum service function length of 20 bits that is used in the datapath lookup for service functions.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

9.100 end-marker-count

end-marker-count

Syntax **end-marker-count** *packets*
no end-marker-count

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile end-marker-count)

Full Context configure subscriber-mgmt gtp peer-profile end-marker-count

Description This command specifies the number of end marker packets that are sent when it is certain no more packets will be sent over the corresponding GTP-U tunnel, such as after a completed mobility event.

The **no** form of this command reverts the value to the default.

Default end-marker-count 1

Parameters *packets* — Specifies the number of end marker packets to send.

Values 0 to 5

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.101 end-of-data

end-of-data

Syntax [**no**] **end-of-data**

Context **[Tree]** (debug>router>rpki-session>packet end-of-data)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router rpki-session packet end-of-data

Description This command enables debugging for end of data RPKI packets.

The **no** form of this command disables debugging for end of data RPKI packets.

Platforms All

9.102 end-station-only

end-station-only

Syntax [**no**] **end-station-only**

Context **[Tree]** (config>service>vpls>mrp>mmrp end-station-only)

Full Context configure service vpls mrp mmrp end-station-only

Description This command configures the end-station-only. This option prevents MMRP messages from being generated or processed. It is useful in case all the MMRP entries for the B-VPLS are static.

Platforms All

9.103 end-time

end-time

Syntax **end-time** [*date* | *day-name*] *time*
no end-time

Context **[Tree]** (config>system>cron>sched end-time)

Full Context configure system cron schedule end-time

Description This command is used concurrently with type **periodic** or **calendar**. Using the type of **periodic**, end-time determines at which interval the schedule will end. Using the type of **calendar**, end-time determines on which date the schedule will end.

When **no end-time** is specified, the schedule runs forever.

Default no end-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *date* — Specifies the date to schedule a command.

Values YYYY:MM:DD in year:month:day number format

day-name — Specifies the day of the week to schedule a command.

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

time — Specifies the time of day to schedule a command.

Values hh:mm

Platforms All

end-time

Syntax **end-time** *date hours-minutes* [**UTC**]
end-time {**now** | **forever**}
no end-time

Context **[Tree]** (config>system>security>keychain>direction>uni>receive>entry end-time)

Full Context configure system security keychain direction uni receive entry end-time

Description This command specifies the calendar date and time after which the key specified by the authentication key is no longer eligible to sign or authenticate the protocol stream.

Default end-time forever

Parameters *date* — Specifies the calendar date after which the key specified by the authentication key is no longer eligible to sign or authenticate the protocol stream in the YYYY/MM/DD format. When no year is specified the system assumes the current year.

hours-minutes — Specifies the time after which the key specified by the authentication key is no longer eligible to sign or authenticate the protocol stream in the hh:mm[:ss] format. Seconds are optional, and if not included, assumed to be 0.

UTC — Indicates that time is given with reference to Coordinated Universal Time in the input.

now — Specifies a time equal to the current system time.

forever — Specifies that the key is always active.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.104 end-x

end-x

Syntax [**no**] **end-x** *function-value*

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc>func end-x)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-x

Description Commands in this context configure the attributes of the End.X SID function associated with a P2P interface. The End.X SID function encodes the behavior of an adjacency SID.

A static function value can be configured for each combination of SRH mode and protection type.

For a given interface, the static function value associated with the same combination of protection type and SRH mode overrides any corresponding automatically allocated function value (**end-x-auto-allocate** command configuration).

If more than one value is configured for an interface and combination of SRH mode and protection type, they are all advertised in IS-IS.

When used in remote TI-LFA repair tunnel programming, IS-IS uses rules to select one End.X value from the multiple values received in IS-IS link advertisements.

Values assigned to loopback and system interfaces are not advertised in IS-IS.

End.X SID functions for adjacencies over broadcast interfaces are always automatically allocated based on the configuration of the **end-x-auto-allocate** command.

The **no** form of this command removes the function value from the configuration.

Parameters *function-value* — Specifies the SRv6 End.X function. Statically allocated functions of all SID types in a locator have their value upper range limited by parameter **locator function-length static-function max-entries**.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.105 end-x-auto-allocate

end-x-auto-allocate

Syntax [**no**] **end-x-auto-allocate srh-mode** *srh-mode* **protection** *protection*

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc>func end-x-auto-allocate)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-x-auto-allocate

Description This command adds an list entry for the automatic allocation of the End.X SID function for all adjacencies over all network interfaces on the router (P2P and broadcast interfaces). Auto-allocated End.X SID function values have a range up to the maximum value of parameter **function-length** in a locator configuration.

A list entry is a combination of the protection type and the SRH mode. Any combinations in addition to the maximum number of entries supported by this command must be allocated statically for each P2P interface. The maximum number of entries in this list is two.

When no list entries are configured, no End.X function values are automatically allocated by default for a locator.

Note: Any change to this list causes a re-allocation of new function values to all interfaces on the router that results in flooding them to the network and triggers a new SPF in all routers.

The **no** form of this command removes a list entry.

Parameters *srh-mode* — Specifies the SRH mode for the SID.

Values psp — Penultimate Segment Pop of the SRH
usp — Ultimate Segment Pop of the SRH

protection — Specifies if the adjacency SID is protected.

Values protected, unprotected

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.106 endpoint

endpoint

Syntax **endpoint ip** *ip-address*
endpoint mac *ieee-address*
endpoint system-ip
endpoint system-mac
no endpoint

Context **[Tree]** (config>router>l2tp>group>mlppp endpoint)
[Tree] (config>router>l2tp>group>tunnel>mlppp endpoint)
[Tree] (config>service>vprn>l2tp>group>mlppp endpoint)
[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp endpoint)
[Tree] (config>subscr-mgmt>ppp-policy>mlppp endpoint)

Full Context configure router l2tp group mlppp endpoint
configure router l2tp group tunnel mlppp endpoint
configure service vprn l2tp group mlppp endpoint
configure service vprn l2tp group tunnel mlppp endpoint
configure subscriber-mgmt ppp-policy mlppp endpoint

Description When configured under the l2tp hierarchy, this command is applicable to LNS.

Within the ppp-policy, this command is applicable only to LAC.

The endpoint, according to RFC 1990, represents the system transmitting the packet. It is used during MLPPPoX negotiation phase to distinguish this peer from all others.

In the case that the client rejects the endpoint option during LCP negotiation, the LAC and the LNS must be able to negotiate the LCP session without the endpoint option.

The **no** form of this command disables sending endpoint option in LCP negotiation.

Parameters *ip-address* — Specifies the IPv4 address (class 2).

system-ip — Specifies to use the system IPv4 address (class 2).

ieee-address — Specifies the MAC address of the interface (class 3).

system-mac — Specifies to use the MAC address of the system (class 3).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

endpoint

Syntax **endpoint** *endpoint-name* [**create**]
no endpoint *endpoint-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>apipe endpoint)
[Tree] (config>service>cpipe endpoint)
[Tree] (config>service>epipe endpoint)
[Tree] (config>service>fpipe endpoint)
[Tree] (config>service>ipipe endpoint)

Full Context configure service apipe endpoint
configure service cpipe endpoint
configure service epipe endpoint
configure service fpipe endpoint
configure service ipipe endpoint

Description This command configures a service endpoint.

Parameters *endpoint-name* — Specifies an endpoint name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe endpoint
- configure service fpipe endpoint

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe endpoint

All

- configure service ipipe endpoint
- configure service epipe endpoint

endpoint

Syntax **endpoint** *endpoint-name* [**create**]
no endpoint

Context [Tree] (config>service>vpls endpoint)

Full Context configure service vpls endpoint

Description This command configures a service endpoint.

Parameters *endpoint-name* — Specifies an endpoint name up to 32 characters in length

create — This keyword is mandatory while creating a service endpoint

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

endpoint

Syntax **endpoint** *ip-address*
no endpoint

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy endpoint)

Full Context configure router mpls forwarding-policies forwarding-policy endpoint

Description This command configures the endpoint address for an MPLS forwarding policy.

The policy allows the user to forward unlabeled packets over a set of user-defined direct (with option to push a label stack) or indirect next hops. Routes are bound to an endpoint policy when their next hop matches the endpoint address of the policy.

The **no** form of the command removes the endpoint from the MPLS forwarding policy.

Parameters *ip-address* — Specifies the destination IPv4 or IPv6 address.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

Platforms All

endpoint

Syntax **endpoint** *endpoint-name* [**create**]
no endpoint *endpoint-name*

Context **[Tree]** (config>mirror>mirror-dest endpoint)
[Tree] (config>mirror>mirror-dest>sap endpoint)
[Tree] (config>mirror>mirror-dest>sdp endpoint)

Full Context configure mirror mirror-dest endpoint
configure mirror mirror-dest sap endpoint
configure mirror mirror-dest sdp endpoint

Description This command configures a service end point. A mirror service supports two implicit endpoints managed internally by the system. The following applies to endpoint configurations.

Up to two named endpoints may be created per service mirror or LI service. The endpoint name is locally significant to the service mirror or LI service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Objects (SAPs or SDPs) may be created on the service mirror or LI with the following limitations:
  - two implicit endpoint objects (without explicit endpoints defined)
  - one implicit and multiple explicit object with the same endpoint name
  - multiple explicit objects each with one of two explicit endpoint names
- All objects become associated implicitly or indirectly with the implicit endpoints 'x' and 'y'.
- Objects may be created without an explicit endpoint defined.
- Objects may be created with an explicit endpoint defined.
- Objects without an explicit endpoint may have an explicit endpoint defined without deleting the object.
- Objects with an explicit endpoint defined may be dynamically moved to another explicit endpoint or may have the explicit endpoint removed.

Creating an object without an explicit endpoint:

- If an object on a mirror or LI service has no explicit endpoint name associated, the system attempts to associate the object with implicit endpoint 'x' or 'y'.
- The implicit endpoint cannot have an existing object association.
- If both 'x' and 'y' are available, 'x' is selected.
- If an 'x' or 'y' association cannot be created, the object cannot be created.

Creating an object with an explicit endpoint name:

- The endpoint name must exist on the mirror or LI service.
- If this is the first object associated with the endpoint name:
  - the object is associated with either implicit endpoint 'x' or 'y'
  - the implicit endpoint cannot have an existing object associated
  - if both 'x' and 'y' are available, 'x' is selected
  - if 'x' or 'y' is not available, the object cannot be created
  - the implicit endpoint is now associated with the named endpoint
  - f this is not the first object associated with the endpoint name:
  - the object is associated with the named endpoint's implicit association

Changing an object’s implicit endpoint to an explicit endpoint name

- If the explicit endpoint name is associated with an implicit endpoint, the object is moved to that implicit endpoint
- If the object is the first to be associated with the explicit endpoint name:
  - the object is associated with either implicit endpoint 'x' or 'y'
  - the implicit endpoint cannot have an existing object associated (except this one)
  - if both 'x' and 'y' are available, 'x' is selected
  - if 'x' or 'y' is not available, the object cannot be moved to the explicit endpoint
  - if moved, the implicit endpoint is now associated with the named endpoint

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Changing an object's explicit endpoint to another explicit endpoint name

- If the new explicit endpoint name is associated with an implicit endpoint, the object is moved to that implicit endpoint
- If the object is the first to be associated with the new explicit endpoint name:
  - the object is associated with either implicit endpoint 'x' or 'y'
  - the implicit endpoint cannot have an existing object associated (except this one)
  - if both 'x' and 'y' are available, 'x' is selected
  - if 'x' or 'y' is not available, the object cannot be moved to the new endpoint
  - if moved, the implicit endpoint is now associated with the named endpoint

An explicitly named endpoint can have a maximum of one SAP and one ICB. Once a SAP is added to the endpoint, only one more object of type ICB sdp is allowed. The ICB sdp cannot be added to the endpoint if the SAP is not part of a MC-LAG instance. Conversely, a SAP which is not part of a MC-LAG instance cannot be added to an endpoint which already has an ICB sdp.

An explicitly named endpoint which does not have a SAP object can have a maximum of four SDPs which can include any of the following: a single primary SDP, one or many secondary SDPs with precedence, and a single ICB SDP.

The user can only add a SAP configured on a MC-LAG instance to this endpoint. Conversely, the user will not be able to change the mirror service type away from mirror service without first deleting the MC-LAG SAP.

The **no** form of this command removes the association of a SAP or an SDP with an explicit endpoint name. When removing an objects explicit endpoint association:

- The system attempts to associate the object with implicit endpoint 'x' or 'y'.
- The implicit endpoint cannot have an existing object association (except this one).
- If both 'x' and 'y' are available, 'x' is selected.
- If an 'x' or 'y' association cannot be created, the explicit endpoint cannot be removed.

Parameters *endpoint-name* — Specifies the endpoint name.

create — Mandatory keyword to create this entry.

Platforms All

endpoint

Syntax **endpoint** *ip-address*
no endpoint

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy endpoint)

Full Context configure router segment-routing sr-policies static-policy endpoint

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates an IPv4 or IPv6 endpoint address with a statically-defined segment routing policy. This association is mandatory when enabling an SR segment-routing policy.

The endpoint address 0.0.0.0 is a special value that matches all BGP next-hops. To use it, the BGP route must have a color-extended community with the color-only bits set to '01' or '10'.

The **no** form of this command removes the endpoint association.

Default no endpoint

Parameters *ip-address* — Specifies the endpoint IP address to be associated with the statically-defined segment-routing policy.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
x:	[0 to FFFF]H
d:	[0 to 255]D

Platforms All

endpoint

Syntax **endpoint** *ip-address*
no endpoint

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from endpoint)

Full Context configure router policy-options policy-statement entry from endpoint

Description This command configures an SR Policy endpoint address as a route policy match criterion. This match criterion is only used in import policies.

The **no** form of this command removes the endpoint IP match criterion from the configuration.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x [-interface]
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.107 endpoint-discriminator

endpoint-discriminator

Syntax **endpoint-discriminator class** {**ip-address** | **global-mac-address** | **null**} [**discriminator-id** *discriminator-id*]
no endpoint-discriminator

Context **[Tree]** (config>port>ml-bundle>mlppp endpoint-discriminator)

Full Context configure port multilink-bundle mlppp endpoint-discriminator

Description This command configures the endpoint-discriminator class and ID. The port must be shutdown to modify command parameters.

The **no** form of this command removes the parameters from the configuration.

Parameters **class** — Specifies the Link Control Protocol endpoint discriminator class field type.

Values ip-address, global-mac-address, null

Default Bundle type Default Physical MLPPP bundle ieee802dot1GlobalMacAddress MLPPP bundle protection group IP address

discriminator-id — Specifies the endpoint discriminator identifier value within the specified endpoint-discriminator class. The values below are only for the ip-address class. the string can be up to 20 characters.

Values Any valid IP address.

Platforms 7450 ESS, 7750 SR-7/12/12e

9.108 endstation-vid-group

endstation-vid-group

Syntax **endstation-vid-group** *id* **vlan-id** *startvid-endvid*
no endstation-vid-group *id*

Context **[Tree]** (config>service>vpls>mrp>mvrp endstation-vid-group)

Full Context configure service vpls mrp mvrp endstation-vid-group

Description This command specifies the range of VLAN IDs that are controlled by MVRP on the port associated with the parent SAP. When the command is present under a certain SAP, the MVRP will treat the associated virtual port as an end-station.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

MVRP endstation behavior means that configuration of a new data SAP with the outer tag in the configured endstation-vid-group will generate down that virtual port a MVRP declaration for the new [outer] VLAN attribute. Also registration received for the VLAN attribute in the range will be accepted but not propagated in the rest of MVRP context.

VPLS-groups are not allowed under the associated Management VPLS (M-VPLS) when the endstation is configured under one SAP. VPLS-groups can be supported in the chassis using a different M-VPLS.

The **no** form of this command removes the specified group id.

Default no endstation-vid-group

Parameters *id* — Specifies the range index

Values 1 to 4094

startvid-endvid — Specifies the range of VLANs to be controlled by MVRP

Values 1 to 4094

9.109 enforce-diffserv-lsp-fc

enforce-diffserv-lsp-fc

Syntax [**no**] **enforce-diffserv-lsp-fc**

Context **[Tree]** (config>service>sdp>class-forwarding enforce-diffserv-lsp-fc)

Full Context configure service sdp class-forwarding enforce-diffserv-lsp-fc

Description This command enables checking by RSVP that a Forwarding Class (FC) mapping to an LSP under the SDP configuration is compatible with the Diff-Serv Class Type (CT) configuration for this LSP.

When the user enables this option, the service manager inquires with RSVP if the FC is supported by the LSP. RSVP checks if the FC maps to the CT of the LSP, for example, the default class-type value or the class-type value entered at the LSP configuration level.

If RSVP did not validate the FC, then the service manager will return an error and the check has failed. In this case, packets matching this FC will be forwarded over the default LSP. Any addition of an LSP to an SDP that will not satisfy the FC check will also be rejected.

The service manager does not validate the default-lsp FC-to-CT mapping. Whether or not the FC is validated, the default-lsp will always end up being used in this case.

RSVP will not allow the user to change the CT of the LSP until no SDP with class-based forwarding enabled and the **enforce-diffserv-lsp-fc** option enabled is using this LSP. All other SDPs using this LSP are not concerned by this rule.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SDP will continue to enforce the mapping of a single LSP per FC. However, when **enforce-diffserv-lsp-fc** enabled, RSVP will also enforce the use of a single CT per FC as per the user configured mapping in RSVP.

If class-forwarding is enabled but **enforce-diffserv-lsp-fc** is disabled, forwarding of the service packets will continue to be based on the user entered mapping of FC to LSP name without further validation as per the existing implementation. The CT of the LSP does not matter in this case.

If class-forwarding is not enabled on the SDP, forwarding of the service packets will continue to be based on the ECMP/LAG hash routine. The CT of the LSP does not matter in this case.

The **no** form of this command reverts to the default value which is to use the user entered mapping of FC to LSP name.

Default no enforce-diffserv-lsp-fc

Platforms All

9.110 enforce-first-as

enforce-first-as

Syntax **enforce-first-as**

Context **[Tree]** (config>service>vprn>bgp enforce-first-as)
[Tree] (config>service>vprn>bgp>group enforce-first-as)
[Tree] (config>service>vprn>bgp>group>neighbor enforce-first-as)

Full Context configure service vprn bgp enforce-first-as
configure service vprn bgp group enforce-first-as
configure service vprn bgp group neighbor enforce-first-as

Description When this command is configured so that it applies to an EBGP session, all routes (belonging to all address families) that are received from the EBGP peer are checked to ensure that the most recent autonomous system number (ASN) in the AS_PATH attribute of each route matches the configured **peer-as** of the session; if it does not match, then either the session is reset (if **update-fault-tolerance** is not enabled) or the session is left up but the route is treated as withdrawn (if **update-fault-tolerance** is enabled).

Enabling or disabling this command on a session that is already up does not flap the session. When **enforce-first-as** is enabled, previously received routes are not checked for compliance with the rule. Enforcement applies only to routes received after the command is enabled and stops when the command is disabled.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

enforce-first-as

Syntax **enforce-first-as**

Context **[Tree]** (config>router>bgp enforce-first-as)
[Tree] (config>router>bgp>group enforce-first-as)
[Tree] (config>router>bgp>group>neighbor enforce-first-as)

Full Context configure router bgp enforce-first-as
configure router bgp group enforce-first-as
configure router bgp group neighbor enforce-first-as

Description When this command is configured so that it applies to an EBGP session, all routes (belonging to all address families) that are received from the EBGP peer are checked to ensure that the most recent autonomous system number (ASN) in the AS_PATH attribute of each route matches the configured **peer-as** of the session; if it does not match, then either the session is reset (if **update-fault-tolerance** is not enabled) or the session is left up but the route is treated as withdrawn (if **update-fault-tolerance** is enabled).

Enabling or disabling this command on a session that is already up does not flap the session. When **enforce-first-as** is enabled, previously received routes are not checked for compliance with the rule. Enforcement applies only to routes received after the command is enabled and stops when the command is disabled.

Platforms All

9.111 enforce-strict-tunnel-tagging

enforce-strict-tunnel-tagging

Syntax [**no**] **enforce-strict-tunnel-tagging**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel enforce-strict-tunnel-tagging)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel enforce-strict-tunnel-tagging)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel enforce-strict-tunnel-tagging)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel enforce-strict-tunnel-tagging
configure service vpls bgp-evpn mpls auto-bind-tunnel enforce-strict-tunnel-tagging
configure service vprn bgp-evpn mpls auto-bind-tunnel enforce-strict-tunnel-tagging

Description This command forces the system to only consider LSPs marked with an admin tag for next hop resolution. Untagged LSPs are not considered.

The **no** form of this command reverts to default value. While tagged RSVP and SR-TE LSPs are considered first, the system can fall back to using untagged LSPs of other types and does not exclude them depending on the **auto-bind-tunnel** configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no enforce-strict-tunnel-tagging

Platforms All

enforce-strict-tunnel-tagging

Syntax [**no**] **enforce-strict-tunnel-tagging**

Context **[Tree]** (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family enforce-strict-tunnel-tagging)
[Tree] (config>router>bgp>next-hop-resolution>shortcut-tunn>family enforce-strict-tunnel-tagging)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family enforce-strict-tunnel-tagging
configure router bgp next-hop-resolution shortcut-tunnel family enforce-strict-tunnel-tagging

Description This command forces the system to only consider LSPs marked with an **admin-tag** for next-hop resolution. Untagged LSPs are not be considered.

The **no** form of this command reverts to the default behavior. While tagged RSVP and SR-TE LSPs will be considered first, the system can fall back to using tagged LSPs that are not explicitly excluded by a route admin tag policy and untagged LSPs of other types and not exclude them.

Default no enforce-strict-tunnel-tagging

Platforms All

9.112 enforce-unique-if-index

enforce-unique-if-index

Syntax [**no**] **enforce-unique-if-index**

Context **[Tree]** (config>system>ip enforce-unique-if-index)

Full Context configure system ip enforce-unique-if-index

Description This command enables the options to force the creation of IP interface indexes so that they are globally unique across all routing contexts. In addition, the command ensures that any interface created using SNMP also has a system-wide unique IP interface index.

If this command is issued but the system has previously existing interface indexes that conflict, the command will be rejected until all the conflicts are removed. Pre-existing persistency tables should also be removed before enabling this system option.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command disables this option and returns the system to the default behavior.

Default no enforce-unique-if-index

Platforms All

9.113 enforcement

enforcement

Syntax **enforcement** {**static** *policer-name* | **dynamic** {*mon-policer-name* | **local-mon-bypass**}}

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>protocol enforcement)

Full Context configure system security dist-cpu-protection policy protocol enforcement

Description This command configures the enforcement method for the protocol.

Default enforcement dynamic local-mon-bypass

Parameters **static** — Specifies that the protocol is always enforced using a **static-policer**. Multiple protocols can reference the same **static-policer**. Packets of protocols that are statically enforced bypass any local monitors.

policer name — Specifies which **static-policer** to use.

dynamic — Specifies that a specific enforcement policer for this protocol for this SAP/object is instantiated when the associated **local-monitoring-policer** is determined to be in a nonconforming state (at the end of a minimum monitoring time of 60 seconds to reduce thrashing).

mon-policer-name — Specifies which **local-monitoring-policer** to use.

local-mon-bypass — This parameter is used to not include packets from this protocol in the local monitoring function, and when the local-monitor “trips”, do not instantiate a dynamic enforcement policer for this protocol.

Platforms All

9.114 engineID

engineID

Syntax [**no**] **engineID** *engine-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>snmp engineID)

Full Context configure system snmp engineID

Description This command sets the SNMP engineID to uniquely identify the SNMPv3 node. By default, the engineID is generated using information from the system backplane.

If SNMP engine ID is changed in the **config>system>snmp> engineID** *engine-id* context, the current configuration must be saved and a reboot must be executed. If not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.

Note: In conformance with IETF standard RFC 2274, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, hashing algorithms which generate SNMPv3 MD5 or SHA security digest keys use the engineID. Changing the SNMP engineID invalidates all SNMPv3 MD5 and SHA security digest keys and may render the node unmanageable.

When a chassis is replaced, use the engine ID of the first system and configure it in the new system to preserve SNMPv3 security keys. This allows management stations to use their existing authentication keys for the new system.

Ensure that the engine IDs are not used on multiple systems. A management domain can only have one instance of each engineID.

The **no** form of the command reverts to the default setting.

Parameters *engine-id* — Specifies an identifier from 10 to 64 hexadecimal digits (5 to 32 octet number), uniquely identifying this SNMPv3 node. This string is used to access this node from a remote host with SNMPv3.

Platforms All

9.115 enhanced-distribution

enhanced-distribution

Syntax [**no**] **enhanced-distribution**

Context [Tree] (config>cflowd enhanced-distribution)

Full Context configure cflowd enhanced-distribution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the inclusion of the ingress port ID into the hash algorithm used to distribute cflowd sample traffic to cflowd processes running on the 7950 XRS CPM. By including this new attribute, cflowd may see better distribution of flows across processing tasks if there is a limited number of IP interfaces on which sampling is performed, but those interfaces use LAGs with a large number of port members.

By enabling this option, the same flow may be captured multiple times if packets are received on multiple ingress ports.

This command is only applicable to cflowd running on a 7950 XRS platform.

The **no** form of this command removes the command from the configuration and disables the inclusion of the ingress port ID in the cflowd hash algorithm.

Default no enhanced-distribution

Platforms 7750 SR-14s, 7750 SR-7s, 7950 XRS

9.116 enqueue-on-pir-zero

enqueue-on-pir-zero

Syntax [**no**] **enqueue-on-pir-zero**

Context **[Tree]** (config>qos>adv-config-policy>child-control>bandwidth-distribution enqueue-on-pir-zero)

Full Context configure qos adv-config-policy child-control bandwidth-distribution enqueue-on-pir-zero

Description This command is used to enable queuing of new packets when H-QoS determines that a queue should stop forwarding (operational PIR set to zero). The default behavior is to allow the queue to continue to use the previously determined operational PIR and set the queue's MBS (Maximum Burst Size) to zero. This prevents new packets from being admitted to the queue until the PIR zero case terminates. The new behavior when **enqueue-on-pir-zero** is enabled is to set the operational PIR to zero and leave the queue's MBS set to the normal value.

This command overrides the **limit-pir-zero-drain** command.

The **no** form of this command reverts to default behavior.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.117 enroll

enroll

Syntax **enroll est-profile** *name* **key** *key-filename* **output** *output-cert-filename* [**hash-alg** *hash algorithm*] **subject-dn** *subject-dn* [**domain-name** *domain-names*] [**ip-addr** *ip-address* **|** *ipv6-address*] [**validate-cert-chain**] [**force**]

Context **[Tree]** (admin>certificate>est enroll)

Full Context admin certificate est enroll

Description This command enrolls a new certificate with Certificate Authority (CA) by the EST protocol specified with the **est-profile** *name* parameter with a imported private key specified by the **key** *key-filename* parameter.

The **est-profile** *name* specifies the authentication between the system and EST server.

The **hash-alg** *hash-algorithm*, **subject-dn** *subject-dn*, **domain-name** *domain-names*, and **ip-addr** *ip-address* parameters are used to generate the Certificate Signing Request (CSR) in the EST request message. The **domain-name** *domain-names* and **ip-addr** *ip-address* parameters are used as subject alternative names.

If **validate-cert-chain** is specified, the system validates the certificate's chain of result certificate before importing it. The "certificate chain" is the chain of all the certificates from the result certificate to the issuing CA. The "result certificate" is the new certificate returned by EST server.

The result certificate is imported and saved with the filename specified by the **output** *output-cert-filename*. If **force** is specified, the system overwrites the existing file with same name as the *output-cert-filename*.

Parameters *name* — Specifies EST profile name, up to 32 characters

key-filename — Specifies the filename of a key, up to 95 characters

output-cert-filename — Specifies the output certificate filename, up to 200 characters

hash-algorithm — Specifies the hash algorithm used in a certificate request.

Values sha1, sha224, sha256, sha384, sha512

subject-dn — Specifies the distinguish name, up to 256 characters, used as the subject in a certificate request, including:

- C-Country
- ST-State
- O-Organization name
- OU-Organization Unit name
- CN-common name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This parameter is formatted as a text string including any of the preceding attributes. The attribute and its value is linked by using “=”, and “,” is used to separate different attributes.

For example: C=US,ST=CA,O=ALU,CN=SR12

Values attr1=val1,attr2=val2

where: attrN={C | ST | O | OU | CN}, up to 256 characters

domain-names — Specifies domain names, up to 512 characters, separated by commas

ip-address — Specifies an IPv4 or IPv6 address string, up to 64 characters

validate-cert-chain — Specifies that the system validates the certificate’s chain of result certificate before importing it

force — Specifies that the system overwrites the existing file with same *output-cert-filename*

Platforms All

9.118 enter

enter

Syntax [**no**] **enter**

Context **[Tree]**
(config>system>management-interface>cli>md-cli>environment>command-completion enter)

Full Context configure system management-interface cli md-cli environment command-completion enter

Description This command enables completion on the enter character.

The **no** form of this command reverts to the default value.

Default enter

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.119 entropy-label

entropy-label

Syntax [**no**] **entropy-label**

Context **[Tree]** (config>service>epipe>spoke-sdp entropy-label)
[Tree] (config>service>ipipe>spoke-sdp entropy-label)
[Tree] (config>service>fpipe>spoke-sdp entropy-label)
[Tree] (config>service>vpls>spoke-sdp entropy-label)
[Tree] (config>service>vpls>mesh-sdp entropy-label)
[Tree] (config>service>pw-template entropy-label)
[Tree] (config>service>vpls>bgp-evpn>mpls entropy-label)
[Tree] (config>service>epipe>bgp-evpn>mpls entropy-label)

Full Context configure service epipe bgp-evpn mpls entropy-label
configure service epipe spoke-sdp entropy-label
configure service fpipe spoke-sdp entropy-label
configure service ipipe spoke-sdp entropy-label
configure service pw-template entropy-label
configure service vpls bgp-evpn mpls entropy-label
configure service vpls mesh-sdp entropy-label
configure service vpls spoke-sdp entropy-label

Description This command enables or disables the use of entropy labels for spoke SDPs.

If **entropy-label** is configured, the entropy label and ELI are inserted in packets for which at least one LSP in the stack for the far-end of the tunnel used by the service has advertised entropy-label-capability. If the tunnel is RSVP type, **entropy-label** can also be controlled under the **config>router>mpls** or **config>router>mpls>lsp** contexts.

The entropy label and hash label features are mutually exclusive. The entropy label cannot be configured on a spoke SDP or service where the hash label feature has already been configured.

Default no entropy-label

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp entropy-label

All

- configure service epipe bgp-evpn mpls entropy-label
- configure service epipe spoke-sdp entropy-label
- configure service vpls spoke-sdp entropy-label
- configure service pw-template entropy-label
- configure service vpls bgp-evpn mpls entropy-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ipipe spoke-sdp entropy-label
- configure service vpls mesh-sdp entropy-label

entropy-label

Syntax [**no**] **entropy-label**

Context **[Tree]** (config>service>ies>if>spoke-sdp entropy-label)

Full Context configure service ies interface spoke-sdp entropy-label

Description This command enables the use of entropy labels on a spoke-SDP bound to an IES interface.

If **entropy-label** is configured, the entropy label and ELI are inserted in packets for which at least one LSP in the stack for the far-end of the tunnel used by the service has advertised entropy-label-capability. If the tunnel is RSVP, **entropy-label** can also be controlled under the **config>router>mpls** or **config>router>mpls>lsp** contexts.

The entropy label and hash label features are mutually exclusive. The entropy label cannot be configured on a spoke-sdp or service where the hash label feature has already been configured.

Default no entropy-label

Platforms All

entropy-label

Syntax [**no**] **entropy-label**

Context **[Tree]** (config>service>vprn entropy-label)
[Tree] (config>service>vprn>if>spoke-sdp entropy-label)

Full Context configure service vprn entropy-label
configure service vprn interface spoke-sdp entropy-label

Description This command enables or disables the use of entropy labels for spoke SDPs on a VPRN.

If **entropy-label** is configured, the entropy label and ELI are inserted in packets for which at least one LSP in the stack for the far-end of the tunnel used by the service has advertised entropy-label-capability. If the tunnel is RSVP type, **entropy-label** can also be controlled under the **config>router>mpls** or **config>router>mpls>lsp** contexts.

The entropy label and the hash label features are mutually exclusive. The entropy label cannot be configured on a spoke SDP or service where the hash label feature has already been configured.

Default no entropy-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

entropy-label

Syntax **entropy-label**
[**no**] **entropy-label**

Context **[Tree]** (config>service>sdp>binding>pw-port entropy-label)

Full Context configure service sdp binding pw-port entropy-label

Description This command enables entropy label insertion on the PW port.

If this command is configured, the entropy label and ELI are inserted in packets for which at least one LSP in the stack for the far-end of the tunnel used by the service has advertised entropy label capability.

- If the tunnel is of type RSVP or SR-TE, the **entropy-label** must be enabled under the **config**>**router**>**mpls** or **config**>**router**>**mpls**>**lsp** contexts.
- If the tunnel is of type SR-ISIS, SR-OSPF or SR-TE, the **override-tunnel-elc** command must be configured under the **config**>**router**>**isis** or **config**>**router**>**ospf** contexts.
- If the tunnel is LDP, the entropy-level capability is configured under the **configure**>**router**>**ldp** context.

The entropy label is only applicable to PW ports bound to a static port, and not to ports using an FPE.

The **no** form of this command disables the entropy label insertion on the PW port.

Default no entropy-label

Platforms All

entropy-label

Syntax **entropy-label** {**rsvp-te** | **sr-te**} {**force-disable** | **enable**}

Context **[Tree]** (config>router>mpls entropy-label)

Full Context configure router mpls entropy-label

Description This command configures the use of entropy labels for MPLS.

The entropy label (EL) and entropy label indicator (ELI) require the insertion of two additional labels in the label stack. In some cases, this may result in an unsupported label stack depth or large changes in the label stack depth during the lifetime of an LSP (for example, due to switching from a primary path with ELC enabled to a secondary path for which the far end has not signaled ELC).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command provides control at the head end of an RSVP LSP or SR-TE LSP as to whether an EL is inserted on an LSP by ignoring the ELC signaled from the far-end LER, and to control how the additional label stack depth is accounted for.

By default, regardless of the value set for entropy label capability at the egress node, the ingress LER considers the EL and ELI in the label stack while sending the information to the TTM and NHLFE. The application using the LSP does not insert an EL and ELI in the label stack unless the far-end signals ELC and the application is configured to insert an entropy label.

When **entropy-label** is set to **force-disable**, the ingress LER does not consider EL and ELC in the label stack when sending the information to the TTM and NHLFE. Therefore, the system marks the TTM and NHLFE as ELC not supported, and applications do not insert an EL or ELI.

The **entropy-label** command value changes at either the MPLS level or the LSP level. The new operational value does not take effect until the LSP is re-signaled. A **shutdown** and **no shutdown** of the LSP is required to enable the new value.

The user can use the **clear** command or bounce MPLS itself (**shutdown**/**no shutdown**) to force the new value to take effect for a large numbers of LSPs.

Default entropy-label rsvp-te enable

Parameters **rsvp-te** — Applies the **entropy-label** command to RSVP LSPs.

sr-te — Applies the **entropy-label** command applies to SR-TE LSPs.

force-disable — Specifies that the ingress LER will not consider the EL and ELI in the label stack while sending the information to the TTM and NHLFE. The system marks the TTM and NHLFE as ELC not supported, and applications do not insert an EL or ELI in the label stack.

enable — Specifies that the ingress LER will consider what is signaled from the egress node for ELC for marking the NHLFE, while the TTM is always marked. Although applications only insert the entropy label if the far end signals ELC, the additional two labels of the EL and ELI are always accounted for.

Platforms All

entropy-label

Syntax **entropy-label** {**force-disable** | **enable** | **inherit**}

Context **[Tree]** (config>router>mpls>lsp entropy-label)
[Tree] (config>router>mpls>lsp-template entropy-label)

Full Context configure router mpls lsp entropy-label
configure router mpls lsp-template entropy-label

Description This command configures the use of entropy labels for an LSP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The entropy label (EL) and entropy label indicator (ELI) require the insertion of two additional labels in the label stack. In some cases, this may result in an unsupported label stack depth or large changes in the label stack depth during the lifetime of an LSP (for example, due to switching from a primary path with ELC enabled to a secondary path for which the far end has not signaled ELC).

This command provides control at the head end of an RSVP LSP or SR-TE LSP over whether an entropy label is inserted on an LSP by overriding the ELC signaled from the far-end LER, and control over how the additional label stack depth is accounted for.

By default, the value of **entropy-labe**l is inherited from the MPLS level. The command under the LSP context provides a means to override the default MPLS behavior on a per-LSP basis. For auto-LSPs, it can only be configured in LSP templates of type one-hope-p2p and mesh-p2p.

Under the LSP context, when the value of **entropy-label** is set to **enable**, the ingress LER will take into consideration what is signaled from the egress node for ELC when marking the NHLFE as entropy-label-capable. Since the value of **entropy-label** is set to **enable** at the LSP level, the system will always mark it in the TTM as entropy-label-capable regardless of the signaled value, in order to ensure that the potential additional label stack depth is accounted for. In this scenario, the TTM and NHLFE can be out of synchronization based on what is configured at the egress node. That is, the application will always account for the entropy label and ELI in the label stack without taking into consideration the signaled value of ELC.

When **entropy-labe**l is set to **force-disable**, the ingress LER will not consider EL and ELI in the label stack while sending the information to the TTM and NHLFE, regardless of what the far end signals. Therefore, the system will mark the TTM and NHLFE as ELC not supported, and applications will not insert an EL or ELI.

When the value of **entropy-label** changes at either the MPLS level or the LSP level, the new operational value will not take effect until the LSP is re-signaled. A **shutdown** and **no shutdown** of the LSP is required to enable the new value.

The user can use the **clear** command or bounce MPLS itself (**shutdown** and **no shutdown**) to force the new value to take effect for a large numbers of LSPs.

Default entropy-label inherit

Parameters **force-disable** — Indicates that the ingress LER will not consider the entropy label and ELI in the label stack while sending the information to the TTM and NHLFE. The system will mark the TTM and NHLFE as ELC not supported, and applications will not insert an EL or ELI in the label stack.

enable — Indicates that the ingress LER will take into consideration what is signaled from the egress node for ELC for marking the NHLFE, while the TTM is always marked. Therefore, although applications will only insert the entropy label if the far end signals ELC, the additional two labels of the entropy label EL and ELI are always accounted for.

inherit — Indicates that the value of **entropy-label** is inherited from the setting in the MPLS context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

entropy-label

Syntax [**no**] **entropy-label**

Context **[Tree]** (config>router entropy-label)

Full Context configure router entropy-label

Description If **entropy-label** is configured, the Entropy label and Entropy Label Indicator is inserted on packets for which at least one LSP in the stack for the far-end of the LDP or RSVP tunnel used by an IGP or BGP shortcut has advertised entropy-label-capability. If the tunnel is of type RSVP, then **entropy-label** must also have been enabled under **config>router>mpls** or **config>router>mpls>lsp**.

This configuration will result in other traffic that is forwarded over an LDP or RSVP LSP for which this router is the LER, and for which there is no explicit service endpoint on this router, to have the EL/ELI enabled, subject to the LSP far-end advertising entropy-label-capability. An example of such traffic includes packets arriving on a stitched LDP LSP forwarded over an RSVP LSP.

Default no entropy-label

Platforms All

entropy-label

Syntax **entropy-label**

Context **[Tree]** (config>router>isis entropy-label)
[Tree] (config>router>ospf entropy-label)

Full Context configure router isis entropy-label
configure router ospf entropy-label

Description Commands in this context configure entropy label capabilities for the routing protocol.

Platforms All

entropy-label

Syntax **entropy-label** {**force-disable** | **enable**}
no entropy-label

Context **[Tree]** (config>router>isis>segm-rtng entropy-label)
[Tree] (config>router>ospf>segm-rtng entropy-label)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router isis segment-routing entropy-label
configure router ospf segment-routing entropy-label

Description This command instructs the system to ignore any received IGP advertisements of entropy label capability relating to remote nodes in the network. It also prevents a user from configuring **override-tunnel-elc** for the IGP instance.

The **no** version of this command enables the processing of any received IGP advertisements of entropy label capability.

Default entropy-label enable

Parameters **force-disable** — Forces the system to ignore any received entropy label capability signaled in the IGP.

enable — Enables the system to process any received entropy label capability signaled in the IGP.

Platforms All

9.120 entropy-label-capability

entropy-label-capability

Syntax [**no**] **entropy-label-capability**

Context **[Tree]** (config>router>rsvp entropy-label-capability)
[Tree] (config>router>ldp entropy-label-capability)

Full Context configure router ldp entropy-label-capability
configure router rsvp entropy-label-capability

Description This command enables or disables ELC for RSV.

If **entropy-label-capability** is configured, then the system will signal (using the procedures specified in RFC 6790) that it is capable of receiving and processing the entropy label and ELI on incoming packets of RSVP and LDP LSPs.

If **no entropy-label-capability** is configured, then the system will not signal ELC. If an ELI is exposed on a packet where the tunnel label is popped at the termination of that LSP, and an entropy label is not configured, then the packet will be dropped.

Default no entropy-label-capability

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.121 entry

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>filter>dhcp-filter entry)
[Tree] (config>filter>dhcp6-filter entry)

Full Context configure filter dhcp-filter entry
configure filter dhcp6-filter entry

Description This command configures DHCP filter entries.

The **no** form of this command removes the entry from the configuration.

Parameters *entry-id* — Specifies the entry ID.

Values 1 to 65535

create — This keyword is required when first creating the DHCP filter entry. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms All

entry

Syntax **entry** *id* [**create**]
no entry *id*

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter entry)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry

Description This command configures an entry in the VAS filter.

The **no** form of this command removes the entry ID from the configuration.

Parameters *id* — Specified an entry in the VAS filter.

Values 0 to 4294967295

create — Keyword used to create the entry ID instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry key** *ancp-string* **customer** *customer-id* **multi-service-site** *customer-site-name* **ancp-policy** *policy-name*
entry key *ancp-string* **sap** *sap-id* **ancp-policy** *policy-name*
no entry key *ancp-string* **customer** *customer-id* **multi-service-site** *customer-site-name*
no entry key *ancp-string* **sap** *sap-id*

Context **[Tree]** (config>subscr-mgmt>ancp>static-map entry)

Full Context configure subscriber-mgmt ancp ancp-static-map entry

Description This command configures an ANCP name. When ANCP is configured to provide rate adaptation without the use of enhanced subscriber management, this command will define how to map an ANCP key (usually the circuit-id of the DSLAM port) to either a SAP and a scheduler name (when a Multi-Service Site (MSS) is not used) or a customer, site and scheduler name when MSS is used.

Different ANCP names may be used with the same SAPs or customer ID/MSS combinations to allow schedulers within the policy to be mapped to the ANCP names. An ANCP string and SAP combination may reference only one ancp-policy. An ANCP string and customer and site-name combination may reference a single ancp-policy.

The **no** form of this command reverts to the default.

Parameters *ancp-string* — Specifies the ASCII representation of the DSLAM circuit-id name, up to 63 characters.

customer-id — Specifies the associated existing customer ID.

Values 1 to 2147483647

customer-site-name — Specifies the associated customer's configured MSS name, up to 32 characters.

policy-name — Specifies an existing ANCP policy name, up to 32 characters.

sap-id — Specifies the physical port identifier portion of the SAP definition.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip entry)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6 entry)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip entry)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6 entry)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry

Description This command configures the IP filter entry.

The **no** form of this command reverts to the default.

Parameters *entry-id* — Specifies the entry ID.

Values 1 to 65535

create — Keyword used to create an entry. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry key** *sub-ident-string* [**sub-profile** *sub-profile-name*] [**alias** *sub-alias-string*] [**sla-profile** *sla-profile-name*] [**app-profile** *app-profile-name*]
no entry key *sub-ident-string*

Context **[Tree]** (config>subscr-mgmt>explicit-sub-map entry)

Full Context configure subscriber-mgmt explicit-subscriber-map entry

Description This command configures a subscriber identification string.

The **no** form of this command reverts to the default.

Parameters *sub-ident-string* — Specifies the profile string, up to 32 characters.

sub-profile-name — Specifies an existing subscriber profile name, up to 32 characters.

sub-alias-string — Specifies an alias for the subscriber identification string, up to 64 characters.

sla-profile-name — Specifies an existing SLA profile, up to 32 characters.

app-profile-name — Specifies an app profile name up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry key** *app-profile-string* **app-profile** *app-profile-name*
no entry key *app-profile-string*

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol>app-profile-map entry)

Full Context configure subscriber-mgmt sub-ident-policy app-profile-map entry

Description This command configures an application profile string.

The **no** form of this command removes the values from the configuration.

Parameters *app-profile-string* — Specifies the application profile string up to 16 characters.

app-profile-name — Specifies the application profile name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry key** *sla-profile-string* **sla-profile** *sla-profile-name*
no entry key *sla-profile-string*

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol>sla-profile-map entry)
[Tree] (config>subscr-mgmt>sub-prof>sla-profile-map entry)

Full Context configure subscriber-mgmt sub-ident-policy sla-profile-map entry
configure subscriber-mgmt sub-profile sla-profile-map entry

Description This command configures an SLA profile string. Each subscriber identification string can be provisioned into a subscriber mapping table providing an explicit mapping of the string to a specific subscriber profile. This allows certain subscribers to be directly mapped to the appropriate subscriber profile in the event that the default mappings are not desired for the subscriber.

An explicit mapping of a subscriber identification string to a subscriber profile cannot be defined with the subscriber profile name default. It is possible for the subscriber identification string to be entered in the mapping table without a defined subscriber profile which can result in the explicitly defined subscriber to be associated with the subscriber profile named default.

Explicitly mapping a subscriber identification string to a subscriber profile will cause an existing active subscriber associated with the string to be reassigned to the newly mapped subscriber profile. An explicit mapping overrides all default subscriber profile definitions.

Attempting to delete a subscriber profile that is currently defined as in an explicit subscriber identification string mapping will fail.

The system will fail the removal attempt of an explicit subscriber identification string mapping to a subscriber profile definition when an active subscriber is using the mapping and cannot be reassigned to a defined default non-provisioned subscriber profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *sla-profile-string* — Identifies the SLA profile string, up to 32 characters.

sla-profile-name — Identifies the SLA profile name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry key** *sub-profile-string* **sub-profile** *sub-profile-name*
no entry key *sub-profile-string*

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol>sub-profile-map entry)

Full Context configure subscriber-mgmt sub-ident-policy sub-profile-map entry

Description This command configures a subscriber profile string.

The **no** form of this command reverts to the default.

Parameters *sub-profile-string* — Specifies the subscriber profile string, up to 32 characters.

sub-profile-name — Specifies the subscriber profile name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax [**no**] **entry direction** *direction* **type** *type* **id** *id*

Context **[Tree]** (config>subscr-mgmt>accu-stats-policy entry)

Full Context configure subscriber-mgmt accu-stats-policy entry

Description This command defines the direction of the policer or queue to the stored and accumulated policy.

The **no** form of this command removes the entry.

Parameters *direction* — Specifies the direction of the queue or policer.

Values egress, ingress

type — Specifies whether the entry is for a queue or policer.

Values queue, policer

id — Specifies the queue or policer ID.

Values 1 to 63

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>subscr-mgmt>isa-filter entry)
[Tree] (config>subscr-mgmt>isa-filter>ipv6 entry)

Full Context configure subscriber-mgmt isa-filter entry
configure subscriber-mgmt isa-filter ipv6 entry

Description This command creates a new entry for this filter. When processing a packet, entries are matched in order, starting with the lowest entry-id. A maximum of 128 IPv4 and 128 IPv6 DSM filter entries are allowed.

The **no** form of this command removes the specified entry from the ISA filter.

Parameters *entry-id* — Specifies the numeric identifier for the filter entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** [*entry*] [**prefix-string** *prefix-string*] [**accounting-server-policy** *policy-name*] [**authentication-server-policy** *policy-name*] [**suffix-string** *suffix-string*]
no entry [*entry*]

Context **[Tree]** (config>router>radius-proxy>server>attribute-matching entry)
[Tree] (config>service>vprn>radius-proxy>server>attribute-matching entry)

Full Context configure router radius-proxy server attribute-matching entry
configure service vprn radius-proxy server attribute-matching entry

Description This command matches the specified prefix or suffix string with the selected accounting server policy or authentication server policy.

Parameters *entry* — Specifies an entry ID.

Values 1 to 32

prefix-string — Specifies the prefix string for matching up to 128 characters. If the suffix-string is also used, the combined length cannot exceed 126 characters.

suffix-string — Specifies the suffix string for matching up to 126 characters. If the prefix-string is also used, the combined length cannot exceed 126 characters.

policy-name — Specifies the RADIUS accounting or authentication policy up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>service>mrp>mrp-policy entry)

Full Context configure service mrp mrp-policy entry

Description This command creates or edits an mrp-policy entry. Multiple entries can be created using unique entry-id numbers within the policy. The implementation exits the policy on the first match found and executes the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit. An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and therefore will be rendered inactive.

The **no** form of this command removes the specified entry from the mrp-policy. Entries removed from the mrp-policy are immediately removed from all services where the policy is applied.

Parameters *entry-id* — An entry-id uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given entry-ids in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values 1 to 65535

create — Keyword; required when first creating the configuration context. When the context is created, one can navigate into the context without the create keyword.

Platforms All

entry

Syntax **entry** *range-entry-id* [**create**]
no entry *range-entry-id*

Context **[Tree]** (config>service>vpls>isid-policy entry)

Full Context configure service vpls isid-policy entry

Description This command creates or edits an ISID policy entry. Multiple entries can be created using unique entry-id numbers within the ISID policy.

entry-id — Specifies an entry-id uniquely identifies a ISID range and the corresponding actions. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

The following rules govern the usage of multiple entry statements:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- overlapping values are allowed:
  - isid from 301 to 310
  - isid from 305 to 315
  - isid 316
- the minimum and maximum values from overlapping ranges are considered and displayed. The above entries will be equivalent with “isid from 301 to 316” statement.
- there is no consistency check with the content of ISID statements from other entries. The entries will be evaluated in the order of their IDs and the first match will cause the implementation to execute the associated action for that entry.

no isid - removes all the previous statements under one entry.

no isid value | from value to higher-value - removes a specific ISID value or range. Must match a previously used positive statement: for example, if the command “isid 16 to 100” was used using “no isid 16 to 50”, it will not work but “no isid 16 to 100 will be successful.

Values 1 to 65535

Default no entry

Parameters *range-entry-id* — Specifies the ID of the ISID policy to be created or edited

Values 1 to 8191

create — Required when first creating the configuration context. Once the context is created, one can navigate into the context without the create keyword.

Platforms All

entry

Syntax **entry** *entry-id* [**name** *entry-name*]
no entry *entry-id*

Context **[Tree]** (config>service>vprn>log>filter entry)

Full Context configure service vprn log filter entry

Description This command is used to create or edit an event filter entry. Multiple entries may be created using unique *entry-id* values. The SR OS implementation exits the filter on the first match found and executes the action in accordance with the action command.

Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and are rendered inactive.

By default, no filter entries are defined. Entries must be explicitly configured.

The **no** form of this command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log-id's where the filter is applied.

Default No event filter entries are defined. An entry must be explicitly configured.

Parameters *entry-id* — The entry ID uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 to 999

name *entry-name* — Configures an optional entry name for the event filter, up to 64 characters, that can be used to refer to the entry after it is created.

Platforms All

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>policy>app-filter entry)

Full Context configure application-assurance group policy app-filter entry

Description This command creates an application filter entry.

App filter entries are an ordered list, the lowest numerical entry that matches the flow defines the application for that flow.

An application filter entry or entries configures match attributes of an application.

The **no** form of this command deletes the specified application filter entry.

Parameters *entry-id* — Specifies an integer that identifies an app-filter entry.

Values 1 to 65535

create — Keyword used to create the entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>policy>aqp entry)

Full Context configure application-assurance group policy app-qos-policy entry

Description This command creates an application QoS policy entry. A flow that matches multiple Application QoS policies (AQP) entries will have multiple AQP entries actions applied. When a conflict occurs for two or more actions, the action from the AQP entry with the lowest numerical value takes precedence.

The **no** form of this command deletes the specified application QoS policy entry.

Parameters *entry-id* — An integer identifying the AQP entry.

Values 1 to 65535

create — Mandatory keyword creates the entry. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>sess-fltr entry)

Full Context configure application-assurance group session-filter entry

Description This command configures a particular Application-Assurance session filter match entry. Every session filter can have zero or more session filter match entries. An application filter entry or entries configures match attributes of an application.

The **no** form of this command deletes the specified entry.

Parameters *entry-id* — Specifies an integer that identifies the entry.

Values 1 to 65535

create — Keyword used to create the entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* **direction** *direction* [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no entry *entry-id* **direction** *direction*

Context [Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg entry)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type entry

Description This command configures a TCA for the counter capturing hits for the specified GTP filter entry. A GTP filter entry TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Parameters *entry-id* — Specifies the GTP filter message-type entry identifier.

Values 1 to 255

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* **direction** *direction* [**create**]
no entry *entry-id* **direction** *direction*

Context [Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg-gtpv2 entry)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type-gtpv2 entry

Description This command configures a TCA for the counter capturing hits for the specified GTPv2 message type filter entry. A GTP filter entry TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating an entry TCA.

Parameters *entry-id* — Specifies the GTP filter message-type-gtpv2 entry identifier.

Values 516 to 770

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* **direction** *direction* [**create**]
no entry *entry-id* **direction** *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-fltr>imsi-apn entry)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter imsi-apn entry

Description This command configures a TCA for the counter capturing hits for the specified IMSI-APN filter entry. A GTP IMSI-APN filter entry TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating an entry TCA.

Parameters *entry-id* — Specifies the identifier for the IMSI-APN filter entry.

Values 1031 to 2030

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

entry

Syntax **entry** *entry-id* **direction** *direction* [**create**]
no entry *entry-id* **direction** *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>sctp-fltr>ppid entry)

Full Context configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid entry

Description This command configures a TCA for the counter capturing hits for the specified SCTP filter PPID entry. An SCTP filter entry TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Parameters *entry-id* — Specifies the SCTP filter PPID entry identifier.

Values 1 to 255

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* **direction** *direction* [**create**]
no entry *entry-id* **direction** *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>session-filter entry)

Full Context configure application-assurance group statistics threshold-crossing-alert session-filter entry

Description This command configures a TCA for the counter capturing hits for the specified session filter entry. A session filter entry TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Parameters *entry-id* — Specifies the SCTP filter PPID entry identifier.

Values 1 to 65535

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>imsi-apn-fltr entry)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter entry

Description This command configures an entry within the IMSI-APN filter to allow for IMSI-APN match and action configuration.

Parameters *entry-id* — Specifies the index into the IMSI-APN list that defines a custom filtering action.

Values 1031 to 2030

create — Keyword used to create the entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* **value** *gtp-message-value* **action** {**permit** | **deny**}
no entry *entry-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>gtp>gtp-fltr>msg entry)

Full Context configure application-assurance group gtp gtp-filter message-type entry

Description This command configures an entry for a specific GTPv1 message type value.

Parameters *entry-id* — Specifies the index into the GTP message value list that defines a custom message-type action.

Values 1 to 255

gtp-message-value — Specifies the GTPv1 message type, either as a numeric value or as a string.

Values 1 to 255 or 256 characters {echo-request, echo-response, error-indication, g-pdu, supported-extension-headers-notification}

permit | deny — Specifies the action to take for packets that match this GTP filter message entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* **value** *gtpv2-message-value* **action** {**permit** | **deny**}
no entry *entry-id*

Context [Tree] (config>app-assure>group>gtp>gtp-fltr>msg-gtpv2 entry)

Full Context configure application-assurance group gtp gtp-filter message-type-gtpv2 entry

Description This command configures an entry for a specific GTPv2 message type value.

Default entry permit

Parameters *entry-id* — Specifies the index into the GTP message value list that defines a custom message-type action.

Values 516 to 770

gtpv2-message-value — Specifies the GTPv2 message type, either as a numeric value or as a string.

Values 1 to 255 or 256 characters (such as: echo-request, echo-response, create-session-request, modify-bearer-request, change-notification-request, change-notification-response, modify-bearer-response, create-session-response, delete-session-request, delete-session-response, remote-ue-report-notification, remote-ue-report-acknowledge)

permit | deny — Specifies the action to take for packets that match this GTP filter message entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* **value** *ppid-value* **action** {**permit** | **deny**}
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>sctp-fltr>ppid entry)

Full Context configure application-assurance group sctp-filter ppid entry

Description This command specifies if an SCTP PPID value is allowed or not.

The **no** form of this command removes this PPID. In which case, the default action for the **sctp-filter>ppid** is applied.

Parameters *entry-id* — Specifies the SCTP filter PPID entry identifier.

ppid-value — Specifies the PPID value, either as numeric value or as a string.

Values 0 to 4294967295 D, 256 chars max

action {permit | deny} — Specifies to allow or deny the configured PPID.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
entry *entry-id*
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>transit-prefix-policy entry)

Full Context configure application-assurance group transit-prefix-policy entry

Description This command configures the index to a specific entry of a transit prefix policy.

The **no** form of this command removes the entry ID from the transit prefix policy configuration.

Parameters *entry-id* — Specifies a transit prefix policy entry.

Values 1 to 4294967295

create — Keyword used when creating an entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>cert-profile entry)

Full Context configure ipsec cert-profile entry

Description This command configures the certificate profile entry information

The **no** form of this command removes the *entry-id* value from the cert-profile configuration.

Parameters *entry-id* — Specifies the entry ID.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context [Tree] (config>ipsec>ts-list>local entry)
[Tree] (config>ipsec>ts-list>remote entry)

Full Context configure ipsec ts-list local entry
configure ipsec ts-list remote entry

Description This command creates a new TS-list entry or enables the context to configure an existing TS-list entry.

The **no** form of this command removes the entry from the local or remote configuration.

Parameters *entry-id* — Specifies the entry ID

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context [Tree] (config>router>ipsec>sec-plcy entry)
[Tree] (config>service>vprn>ipsec>sec-plcy entry)

Full Context configure router ipsec security-policy entry
configure service vprn ipsec security-policy entry

Description This command configures an IPsec security policy entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *entry-id* — Specifies the IPsec security policy entry.

Values 1 to 16

create — Keyword used to create the security policy entry instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec security-policy entry

VSR

- configure router ipsec security-policy entry

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>service>nat>nat-classifier entry)

Full Context configure service nat nat-classifier entry

Description This command creates or edits a nat-classifier entry. Multiple entries can be created using unique entry-id numbers within the nat-classifier. Entries must be sequenced from most to least explicit. An entry may not have any match criteria defined, in which case all UDP traffic will be matched. In case that the action is not explicitly configured, a default-action will be applied.

The **no** form of the command removes the specified entry from the filter. Entries removed from the nat-classifier are immediately removed from all entities to which the nat-classifier is applied.

Default none

Parameters *entry-id* — Specifies an entry-id that uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given entry-ids in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

entry

Syntax **entry** *li-entry-id* [**create**]
no entry *li-entry-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>li>li-filter>li-ip-filter entry)
[Tree] (config>li>li-filter>li-ipv6-filter entry)
[Tree] (config>li>li-filter>li-mac-filter entry)

Full Context configure li li-filter li-ip-filter entry
configure li li-filter li-ipv6-filter entry
configure li li-filter li-mac-filter entry

Description This command creates or edits a Lawful Interception filter entry. Multiple entries can be created using unique entry-id numbers within the filter.

An entry in an LI filter always has an implicit action of “forward”.

The **no** form of this command removes the specified entry from the filter. Entries removed from the filter are immediately removed from all services or network ports where the associated filter is applied.

LI filter entries can be used as li-source entries.

The entry numbers for LI filters serve purely as keys for managing the entries (deleting entries, and so on). The order of LI filter entries is not guaranteed to match the entry numbers and the software may reorder entries. Operators must use LI entries in a manner such that relative order of the LI entries amongst themselves is not important.

The **no** form of this command removes the LI entry ID from the configuration.

Parameters *li-entry-id* — Identifies the Lawful Interception filter entry.

Values 1 to 65536

Platforms All

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context [Tree] (config>qos>sap-egress>ip-criteria entry)
[Tree] (config>qos>sap-ingress>ip-criteria entry)
[Tree] (config>qos>sap-egress>ipv6-criteria entry)
[Tree] (config>qos>sap-ingress>ipv6-criteria entry)
[Tree] (config>qos>sap-ingress>mac-criteria entry)

Full Context configure qos sap-egress ip-criteria entry
configure qos sap-egress ipv6-criteria entry
configure qos sap-ingress ip-criteria entry
configure qos sap-ingress ipv6-criteria entry
configure qos sap-ingress mac-criteria entry

Description This command is used to create or edit an IP, IPv6, or MAC criteria entry for the policy. Multiple entries can be created using unique *entry-id* numbers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The list of flow criteria is evaluated in a top-down manner with the lowest entry ID at the top and the highest entry ID at the bottom. If the defined match criteria for an entry within the list matches the information in the egress packet, the system stops matching the packet against the list and performs the matching entries reclassification actions. If none of the entries match the packet, the IP flow reclassification list has no effect on the packet.

An entry is not populated in the list unless the action command is executed for the entry. An entry that is not populated in the list has no effect on egress packets. If the action command is executed without any explicit reclassification actions specified, the entry is populated in the list allowing packets matching the entry to exit the list, preventing them from matching entries lower in the list. Since this is the only flow reclassification entry that the packet matched and this entry explicitly states that no reclassification action is to be performed, the matching packet will not be reclassified.

The **no** form of this command removes the specified entry from the policy. Entries removed from the policy are immediately removed from all services where that policy is applied.

Parameters *entry-id* — The *entry-id,* expressed as an integer, uniquely identifies a match criterion and the corresponding action. It is recommended that multiple entries be given *entry-ids* in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

An entry cannot have any match criteria defined (in which case, everything matches) but must have at least the keyword **action fc** *fc-name* for it to be considered complete. Entries without the action keyword will be considered incomplete and, therefore, will be rendered inactive.

Values 1 to 65535

create — Required parameter when creating a flow entry when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the flow entry already exists.

Platforms All

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>qos>network>ingress>ip-criteria entry)
[Tree] (config>qos>network>ingress>ipv6-criteria entry)
[Tree] (config>qos>network>egress>ip-criteria entry)
[Tree] (config>qos>network>egress>ipv6-criteria entry)

Full Context configure qos network egress ip-criteria entry
configure qos network egress ipv6-criteria entry
configure qos network ingress ip-criteria entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure qos network ingress ipv6-criteria entry

Description This command is used to create or edit an IP or IPv6 criteria entry for the policy. Multiple entries can be created using unique entry numbers.

The list of flow criteria is evaluated in a top-down manner with the lowest entry ID at the top and the highest entry ID at the bottom. If the defined match criteria for an entry within the list matches the information in the packet, the system stops matching the packet against the list and performs the matching entries reclassification actions. If none of the entries match the packet, the IP flow reclassification list has no effect on the packet.

An entry is not populated in the list unless the action command is executed for the entry. An entry that is not populated in the list has no effect on ingress packets. If the **action** command is executed without any explicit reclassification actions specified, the entry is populated in the list allowing packets matching the entry to exit the list, preventing them from matching entries lower in the list. Since this is the only flow reclassification entry that the packet matched, and this entry explicitly states that no reclassification action is to be performed, the matching packet will not be reclassified.

The configuration of egress prec/DSCP classification and the configuration of an egress IP criteria or IPv6 criteria entry statement within a network QoS policy are mutually exclusive.

Network QoS policies containing egress **ip-criteria** or **ipv6-criteria entry** statements are only applicable to network interfaces. Configuration of **ip-criteria** or **ipv6-criteria entry** statements in a network egress QoS policy and the application of the policy on any object other than a GRT network interface are mutually exclusive.

The **no** form of this command removes the specified entry from the policy. Entries removed from the policy are immediately removed from all services to which that policy is applied.

Parameters *entry-id* — The entry identifier, expressed as an integer, uniquely identifies a match criterion and the corresponding action. It is recommended that multiple entries be given entry identifiers in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

An entry cannot have any match criteria defined (in which case, everything matches) but must have at least the keyword **action fc fc-name profile** *profile* for it to be considered complete. Entries without the action keyword will be considered incomplete and will be rendered inactive.

Values 1 to 65535

create — Required parameter when creating a flow entry when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled, and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the flow entry already exists.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>filter>ip-exception entry)
[Tree] (config>filter>ip-filter entry)
[Tree] (config>filter>ipv6-exception entry)
[Tree] (config>filter>ipv6-filter entry)
[Tree] (config>filter>mac-filter entry)

Full Context configure filter ip-exception entry
configure filter ip-filter entry
configure filter ipv6-exception entry
configure filter ipv6-filter entry
configure filter mac-filter entry

Description This command creates or edits an IPv4, IPv6, MAC, IP exception filter, or IPv6 exception filter entry. Multiple entries can be created using unique *entry-id* numbers within the filter. Entries must be sequenced from most to least explicit.

An entry may not have any match criteria defined (in which case everything matches) but must have at least the keyword **action** for it to be considered complete. Entries without the **action** keyword will be considered incomplete and hence will be rendered inactive.

The **no** form of the command removes the specified entry from the filter. Entries removed from the filter are immediately removed from all services or network ports where that filter is applied.

Parameters *entry-id* — Uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given *entry-id* in staggered increments. This allows users to insert a new entry in an existing policy without requiring to renumbering all the existing entries. The parameter is expressed as a decimal integer.

Values 1 to 2097151

create — This keyword is required to create the configuration context. Once the context is created, the user can enable the context with or without the **create** keyword.

Platforms All

- configure filter ip-filter entry
- configure filter mac-filter entry
- configure filter ipv6-filter entry

VSR

- configure filter ipv6-exception entry
- configure filter ip-exception entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax **entry** *entry-id* [**name** *entry-name*]
no entry *entry-id*

Context **[Tree]** (config>log>filter entry)

Full Context configure log filter entry

Description This command creates or edits an event filter entry. Multiple entries can be created using unique *entry-id* values. The SR OS implementation exits the filter on the first match found and executes the action in accordance with the **action** command.

Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and are rendered inactive.

By default, no filter entries are defined. Entries must be explicitly configured.

The **no** form of this command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log-id's where the filter is applied.

Parameters *entry-id* — The entry ID uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 to 999

name *entry-name* — Configures an optional entry name for the event filter, up to 64 characters, that can be used to refer to the entry after it is created.

Platforms All

entry

Syntax [**no**] **entry** *entry-id*

Context **[Tree]** (config>log>event-handling>handler>action-list entry)

Full Context configure log event-handling handler action-list entry

Description This command configures an EHS handler action-list entry. A handler can have multiple actions where each action, for example, could request the execution of a different script. When the handler is triggered it will walk through the list of configured actions.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the specified EHS handler action-list entry.

Parameters *entry-id* — Specifies the identifier of the EHS handler entry.

Values 1 to 1500

Platforms All

entry

Syntax [**no**] **entry** *entry-id*

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter entry)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter entry)
[Tree] (config>system>security>mgmt-access-filter>mac-filter entry)

Full Context configure system security management-access-filter ip-filter entry
configure system security management-access-filter ipv6-filter entry
configure system security management-access-filter mac-filter entry

Description This command is used to create or edit a management access IP(v4), IPv6, or MAC filter entry. Multiple entries can be created with unique *entry-id* numbers. The OS exits the filter upon the first match found and executes the actions according to the respective action command. For this reason, entries must be sequenced correctly from most to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** defined to be considered complete. Entries without the **action** keyword are considered incomplete and inactive.

The **no** form of this command removes the specified entry from the management access filter.

Parameters *entry-id* — Specifies an entry ID uniquely identifies a match criteria and the corresponding action. It is recommended that entries are numbered in staggered increments. This allows users to insert a new entry in an existing policy without having to renumber the existing entries.

Values 1 to 9999

Platforms All

entry

Syntax **entry** *entry-id*

Context **[Tree]** (config>sys>sec>cpm>ip-filter entry)
[Tree] (config>sys>sec>cpm>ipv6-filter entry)
[Tree] (config>sys>sec>cpm>mac-filter entry)

Full Context configure system security cpm-filter ip-filter entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security cpm-filter ipv6-filter entry
configure system security cpm-filter mac-filter entry

Description This command specifies a particular CPM filter match entry. Every CPM filter must have at least one filter match entry. Entries are created and deleted by user.

The default match criteria is match none.

Parameters *entry-id* — Identifies a CPM filter entry as configured on this system.

Values 1 to 131072

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

entry

Syntax **entry** *entry* **levels** *levels* **opcodes** *opcodes* **rate** *packet-rate-limit*
no entry

Context **[Tree]** (config>sys>security>cpu-protection>policy>eth-cfm entry)

Full Context configure system security cpu-protection policy eth-cfm entry

Description Builds the specific match and rate criteria. Up to ten entries may exist in up to four CPU protection policies.

The **no** form of this command reverses the match and rate criteria configured.

Default no entry

Parameters *rate* — Specifies a packet rate limit in frames per second, where a “0” means drop all.

Values 1 to 100

level — Specifies a domain level.

Values all: Wildcard entry level
range: 0 to 7: within specified range, multiple ranges allowed
number: 0 to 7: specific level number, may be combined with range

opcode — Specifies an operational code that identifies the application.

Values range: 0 to 255: within specified range, multiple ranges allowed
number: 0 to 255: specific level number, may be combined with range

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry

Syntax [**no**] **entry** *entry-id*

Context **[Tree]** (config>system>security>profile entry)

Full Context configure system security profile entry

Description This command is used to create a user profile entry.

More than one entry can be created with unique *entry-id* numbers. Exits when the first match is found and executes the actions according to the accompanying **action** command. Entries should be sequenced from most explicit to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** for it to be considered complete.

The **no** form of this command removes the specified entry from the user profile.

Parameters *entry-id* — Specifies an entry-id that uniquely identifies a user profile command match criteria and a corresponding action. If more than one entry is configured, the *entry-ids* should be numbered in staggered increments to allow users to insert a new entry without requiring renumbering of the existing entries.

Values 1 to 9999

Platforms All

entry

Syntax **entry** *entry-id* [**key** *authentication-key* | *hash-key* | *hash2-key* | *custom-key*] [**hash** | **hash2** | **custom**] **algorithm** *algorithm*]
no entry *entry-id*

Context **[Tree]** (config>system>security>keychain>direction>bi entry)
[Tree] (config>system>security>keychain>direction>uni>receive entry)
[Tree] (config>system>security>keychain>direction>uni>send entry)

Full Context configure system security keychain direction bi entry
configure system security keychain direction uni receive entry
configure system security keychain direction uni send entry

Description This command defines a particular key in the keychain. Entries are defined by an entry ID. A keychain must have valid entries for the TCP Enhanced Authentication mechanism to work.

If the entry is the active entry for sending, then this causes a new active key to be selected (if one is available using the youngest key rule). If it is the only possible key to send, then the system rejects the command with an error indicating the configured key is the only available send key.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the key is one of the eligible keys for receiving, it will be removed. If the key is the only possible eligible key, then the command is accepted, and an error indicating that this is the only eligible key will be generated.

The **no** form of this command removes the entry from the keychain.

Parameters *entry-id* — Specifies an entry that represents a key configuration to be applied to a keychain.

Values 0 to 63, null-key

key — Specifies a key ID which is used along with *keychain-name* and **direction** to uniquely identify this particular key entry.

authentication-key — Specifies the *authentication-key* that is used by the encryption algorithm. The key is used to sign and authenticate a protocol packet.

The *authentication-key* can be any combination of letters or numbers.

Values A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.

algorithm — Specifies an enumerated integer that indicates the encryption algorithm to be used by the key defined in the keychain.

Values aes-128-cmac-96 — Specifies an algorithm based on the AES standard for TCP authentication.

aes-128-gcm-16 — Specifies an algorithm used for MCS.

hmac-sha-1-96 — Specifies an algorithm based on SHA-1 for RSVP-TE and TCP authentication.

message-digest — MD5 hash used for TCP authentication.

hmac-md5 — MD5 hash used for IS-IS and RSVP-TE.

password – Specifies a simple password authentication for OSPF, IS-IS, and RSVP-TE.

hmac-sha-1 — Specifies the sha-1 algorithm for OSPF, IS-IS, and RSVP-TE.

hmac-sha-256 — Specifies the sha-256 algorithm for OSPF and IS-IS.

hash-key | *hash2-key* | *custom-key* — Specifies the hash key. The key can be any combination of ASCII characters up to 33 for the *hash-key* and 96 characters for the *hash2-key* (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies a custom hash version is used while saving the configuration files.

Platforms All

entry

Syntax **entry** *entry-id* [**create**]
no entry *entry-id*

Context **[Tree]** (config>system>security>tls>cert-profile entry)

Full Context configure system security tls cert-profile entry

Description This command configures an entry for the TLS certificate profile. A certificate profile may have up to eight entries. Currently, TLS uses the entry with the smallest ID number when responding to server requests.

The **no** form of the command deletes the specified entry.

Parameters *entry-id* — Specifies the identification number of the TLS certificate profile entry.

Values 1 to 8

create — Keyword used to create the TLS certificate profile entry.

Platforms All

entry

Syntax **entry** *entry-id expression reg-exp*
no entry

Context **[Tree]** (config>router>policy-options>as-path-group entry)

Full Context configure router policy-options as-path-group entry

Description This command creates the context to edit route policy entries within an autonomous system path group.

Multiple entries can be created using unique entries. The router exits the filter when the first match is found and executes the action specified. For this reason, entries must be sequenced correctly from most to least explicit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An entry does not require matching criteria defined (in which case, everything matches) but must have at least define an action in order to be considered complete. Entries without an action are considered incomplete and will be rendered inactive.

The **no** form of this command removes the specified entry from the autonomous system path group.

Parameters *entry-id* — Specifies the entry ID expressed as a decimal integer. An *entry-id* uniquely identifies match criteria and the corresponding action. It is recommended that multiple entries be given *entry-ids* in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values 1 to 4294967295

reg-exp — The AS path group regular expression. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

entry

Syntax **entry** *entry-id*
no entry

Context **[Tree]** (config>router>policy-options>policy-statement entry)

Full Context configure router policy-options policy-statement entry

Description This command creates the context to edit route policy entries within the route policy statement.

Multiple entries can be created using unique entries. The router exits the filter when the first match is found and executes the action specified. For this reason, entries must be sequenced correctly from most to least explicit.

An entry does not require matching criteria defined (in which case, everything matches) but must have at least define an action in order to be considered complete. Entries without an action are considered incomplete and will be rendered inactive.

The **no** form of this command removes the specified entry from the route policy statement.

Parameters *entry-id* — Specifies the entry ID expressed as a decimal integer. An *entry-id* uniquely identifies match criteria and the corresponding action. It is recommended that multiple entries be given *entry-ids* in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values 1 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

entry

Syntax **entry** *entry-id* **expression** *hostname* **category** *category*
no entry *entry-id*

Context **[Tree]** (config>app-assure>group>url-filter>web-service>classification-overrides entry)

Full Context configure application-assurance group url-filter web-service classification-overrides entry

Description This command creates a classification override, manually setting the category of a hostname.

The **no** form of this command removes the classification override entry.

Default no entry

Parameters *entry-id* — Specifies the classification of the override entry.

Values 1 to 65535

hostname — Specifies the hostname of the configured override category, up to 255 characters.

category — Specifies the override category, up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.122 entry-size

entry-size

Syntax **entry-size** *size*
no entry-size

Context **[Tree]** (config>python>py-policy>cache entry-size)

Full Context configure python python-policy cache entry-size

Description This command configures the maximum size of the data structure that can be stored in a single Python cache entry which includes both a value and key.

When requesting to store a data structure, the size of the serialized object is compared with the value specified. If larger, the object will not be stored and Python will return exception.

The **no** form of this command reverts to the default.

Default entry-size 256

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — Configures the maximum accepted size of a single cache entry.

Values 32 to 2048

Platforms All

9.123 environment

environment

Syntax **environment**

Context **[Tree]** (environment environment)

Full Context environment

Description Commands in this context set up the environment preferences.

Platforms All

environment

Syntax **environment**

Context **[Tree]** (config>system>management-interface>cli>md-cli environment)

Full Context configure system management-interface cli md-cli environment

Description Commands in this context configure MD-CLI session environment parameters.

Platforms All

9.124 epipe

epipe

Syntax **epipe** *service-id* **customer** *customer-id* [**vpn** *vpn-id*] [**vc-switching**] [**create**] **name** [*name*]
epipe *service-id* [**test**] [**create**] [**name** *name***]**
no epipe *service-id*

Context **[Tree]** (config>service epipe)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service epipe

Description This command configures an Epipe service instance. This command is used to configure a point-to-point epipe service. An Epipe connects two endpoints defined as Service Access Points (SAPs). Both SAPs may be defined in one 7450 ESS, 7750 SR, or 7950 XRS or they may be defined in separate devices connected over the service provider network. When the endpoint SAPs are separated by the service provider network, the far end SAP is generalized into a Service Distribution Point (SDP). This SDP describes a destination and the encapsulation method used to reach it.

No MAC learning or filtering is provided on an Epipe.

When creating a service, you must enter the **customer** keyword and specify a *customer-id* to associate the service with a customer. The *customer-id* must already exist, having been created using the **customer** command in the **service** context. After a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and re-created with a new customer association.

After a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified will result in an error.

By default, no epipe services exist until they are explicitly created with this command.

The **no** form of this command deletes the epipe service instance with the specified *service-id*. The service cannot be deleted until the service has been shut down.

Cpipe services are enabled on the 7450 ESS.

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7450 ESS, 7750 SR, or 7950 XRS on which this service is defined.

Values *service-id*: 1 to 2147483647
svc-name: up to 64 characters

customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN ID. If this parameter is not specified, the VPN ID uses the same service ID number.

Values 1 to 2147483647

Default null (0)

vc-switching — Specifies if the pseudowire switching signaling is used for the spoke SDPs configured in this service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

test — Specifies a unique test service type for the service context which will contain only a SAP configuration. The test service can be used to test the throughput and performance of a path for MPLS-TP PWs. This parameter applies to the 7450 ESS and 7750 SR only.

create — Keyword used to create the service instance. The **create** keyword requirement can be enabled/disabled in the **environment**>**create** context.

name *name* — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Values *name*: up to 64 characters

Platforms All

9.125 epipe-sap-template

epipe-sap-template

Syntax **epipe-sap-template** *name*
no epipe-sap-template

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>l2-access-points>l2-ap epipe-sap-template)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>l2-access-points>l2-ap epipe-sap-template)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-access-points l2-ap epipe-sap-template
configure service vprn subscriber-interface group-interface wlan-gw l2-access-points l2-ap epipe-sap-template

Description This command specifies which SAP parameter template should be applied to the l2-ap SAP. This can only be changed when the l2-ap is shut down.

The **no** form of this command removes the template, the SAP will use default parameters.

Parameters *name* — Specifies the name of the template to use

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

epipe-sap-template

Syntax **epipe-sap-template** *name* [**create**]
no epipe-sap-template *name*

Context **[Tree]** (config>service>template epipe-sap-template)

Full Context configure service template epipe-sap-template

Description This command specifies which SAP parameter template should be applied to the l2-ap SAP. This can only be changed when the l2-ap is shutdown.

The no form of this command removes the template, the SAP will use default parameters.

Parameters *name* — Specifies the SAP template name associated with this template.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.126 error

error

Syntax [**no**] **error** [**neighbor** *ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>rip error)

Full Context debug router rip error

Description This command enables debugging for RIP errors.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP errors sent on the neighbor IP address or interface.

Platforms All

error

Syntax [**no**] **error** [**neighbor** *ip-int-name* | *ipv6-address*]

Context **[Tree]** (debug>router>ripng error)

Full Context debug router ripng error

Description This command enables debugging for RIPng errors.

Parameters *ip-int-name* | *ipv6-address* — Debugs the RIPng errors sent on the neighbor IP address or interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

9.127 error-code

error-code

Syntax **error-code** *error-code* [**custom-msg-size** *custom-msg-size*]
no error-code *error-code*

Context **[Tree]** (config>app-assure>group>http-error-redirect error-code)

Full Context configure application-assurance group http-error-redirect error-code

Description This command refers to which HTTP status codes a redirect action is applied. Only messages with sizes less than that configured here (custom-msg-size) are eligible for redirect action.

The no form of this command removes the parameters from the configuration.

Parameters *error-code* — Specifies the error code for an HTTP error redirect.

Values 0 to 4294967295, of which 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 451, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 730, 731, and 735 are supported for redirect

custom-msg-size — Specifies the maximum message size above which redirect will not be done.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.128 error-drop

error-drop

Syntax **error-drop** [**event-log** *event-log-name*]
no error-drop

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action error-drop)

Full Context configure application-assurance group policy app-qos-policy entry action error-drop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a drop action for error flows (bad IP checksums, tcp/udp port 0, and so on).

Default no error-drop

Parameters *event-log-name* — Specifies the event log name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

error-drop

Syntax **error-drop direction** *direction* [**create**]
no error-drop direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca error-drop)

Full Context configure application-assurance group statistics threshold-crossing-alert error-drop

Description This command configures a TCA for the counter capturing error drops. An error drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating an error-drop TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the error drop TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.129 error-handling

error-handling

Syntax **error-handling**

Context **[Tree]** (config>service>vprn>bgp error-handling)
[Tree] (config>service>vprn>bgp>group error-handling)
[Tree] (config>service>vprn>bgp>group>neighbor error-handling)

Full Context configure service vprn bgp error-handling
configure service vprn bgp group error-handling
configure service vprn bgp group neighbor error-handling

Description This command specifies whether the error handling mechanism for optional transitive path attributes is enabled for this peer group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

error-handling

Syntax **error-handling**

Context **[Tree]** (config>router>bgp error-handling)
[Tree] (config>router>bgp>group error-handling)
[Tree] (config>router>bgp>group>neighbor error-handling)

Full Context configure router bgp error-handling
configure router bgp group error-handling
configure router bgp group neighbor error-handling

Description This command specifies whether updated BGP error handling procedures should be applied.

Platforms All

9.130 error-handling-action

error-handling-action

Syntax **error-handling-action** {**continue** | **block**}
no error-handling-action

Context **[Tree]** (config>subscr-mgmt>credit-control-policy error-handling-action)

Full Context configure subscriber-mgmt credit-control-policy error-handling-action

Description This command configures the error handling action for the policy.

The **no** form of this command reverts to the default.

Default error-handling-action continue

Parameters **continue** — Specifies to continue when an error occurs in the CC determination.

block — Specifies to block when an error occurs in the CC determination.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.131 error-report

error-report

Syntax [**no**] **error-report**

Context **[Tree]** (debug>router>rpki-session>packet error-report)

Full Context debug router rpki-session packet error-report

Description This command enables debugging for error report RPKI packets.

The **no** form of this command disables debugging for error report RPKI packets.

Platforms All

9.132 errored-frame

errored-frame

Syntax **errored-frame**

Context **[Tree]** (config>port>ethernet>efm-oam>link-monitoring errored-frame)

Full Context configure port ethernet efm-oam link-monitoring errored-frame

Description The context used to define errored frame parameters including thresholds, and windows of time to which the error count will be compared. An errored frame is counted when there is any frame error detected by the Ethernet physical layer. This excludes jumbo frames above 9192 bytes which are dropped prior to this function.

Platforms All

9.133 errored-frame-period

errored-frame-period

Syntax **errored-frame-period**

Context **[Tree]** (config>port>ethernet>efm-oam>link-monitoring errored-frame-period)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet efm-oam link-monitoring errored-frame-period

Description The context used to define errored frame parameters including thresholds, and windows of received packets to which the error count will be compared. An errored frame is counted when there is any frame error detected by the Ethernet physical layer. This excludes jumbo frames above 9192 bytes which are dropped prior to this function. The received packet count will be checked every one second to see if the window has been reached.

Platforms All

9.134 errored-frame-seconds

errored-frame-seconds

Syntax **errored-frame-seconds**

Context **[Tree]** (config>port>ethernet>efm-oam>link-monitoring errored-frame-seconds)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-seconds

Description This command defines the errored frame seconds parameters including thresholds, and windows of time to which the error count will be compared. An errored second is any second in which a single frame error occurred. An errored frame is counted when there is any frame error detected by the Ethernet physical layer. This excludes jumbo frames above 9192 bytes that are dropped prior to this function.

Platforms All

9.135 errored-symbols

errored-symbols

Syntax **errored-symbols**

Context **[Tree]** (config>port>ethernet>efm-oam>link-monitoring errored-symbols)

Full Context configure port ethernet efm-oam link-monitoring errored-symbols

Description This command defines the symbol error parameters including thresholds, and windows of time (converted to symbols in that time) to which the error count will be compared. A symbol error occurs when any encoded symbol is in error and independent of frame counters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.136 errors

errors

Syntax [**no**] **errors**

Context **[Tree]** (debug>dynsvc>scripts>event errors)
[Tree] (debug>dynsvc>scripts>inst>event errors)
[Tree] (debug>dynsvc>scripts>script>event errors)

Full Context debug dynamic-services scripts event errors
debug dynamic-services scripts instance event errors
debug dynamic-services scripts script event errors

Description This command enables/disables the generation of a specific dynamic data service script debugging event output: errors.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

errors

Syntax [**no**] **errors**

Context **[Tree]** (debug>vsd>scripts>event errors)
[Tree] (debug>vsd>scripts>instance errors)

Full Context debug vsd scripts event errors
debug vsd scripts instance errors

Description This command enables/disables the generation of a specific script debugging event output: **errors**.

Platforms All

9.137 es-activation-timer

es-activation-timer

Syntax **es-activation-timer** *seconds*
no es-activation-timer

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg es-activation-timer)

Full Context configure service system bgp-evpn ethernet-segment es-activation-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Ethernet Segment activation timer for a specified Ethernet Segment. The **es-activation-timer** delays the activation of a specified **ethernet-segment** on a specified PE that has been elected as DF (Designated Forwarder). Only when the **es-activation-timer** has expired, the SAP/SDP-binding associated to an **ethernet-segment** can be activated (in case of single-active multi-homing) or added to the default-multicast-list (in case of all-active multi-homing).

If **no es-activation-timer** is configured, the system uses the value configured in the **config>redundancy>bgp-evpn-multi-homing>es-activation-timer** context, if configured. Otherwise the system uses a default value of 3 seconds.

Default no es-activation-timer

Parameters *seconds* — Specifies the number of seconds for the **es-activation-timer**.

Values 0 to 100

Default 3

Platforms All

es-activation-timer

Syntax **es-activation-timer** *seconds*

Context **[Tree]** (config>redundancy>bgp-evpn-multi-homing es-activation-timer)

Full Context configure redundancy bgp-evpn-multi-homing es-activation-timer

Description This command configures the global Ethernet-Segment activation timer. The **es-activation-timer** delays the activation of a specified Ethernet-Segment on a specified PE that has been elected as DF (Designated Forwarder). Only when the **es-activation-timer** has expired, the SAP/SDP-binding associated to an Ethernet-Segment can be activated (in case of single-active multi-homing) or added to the default-multicast-list (in case of all-active multi-homing).

The **es-activation-timer** configured at the Ethernet-Segment level supersedes this global **es-activation-timer**.

Default es-activation-timer 3

Parameters *seconds* — Specifies the number of seconds for the **es-activation-timer**.

Values 0 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.138 es-orig-ip

es-orig-ip

Syntax **es-orig-ip** *ip-address*
no es-orig-ip

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg es-orig-ip)

Full Context configure service system bgp-evpn ethernet-segment es-orig-ip

Description This command modifies the Originating IP field advertised in the ES route for a given Ethernet Segment. By default, the Originating IP is the system-ip of the PE. However, this value can be changed to the IPv4 or IPv6 address configured with this command.

With the **es-orig-ip** configured, ES shutdown is required, for the following cases:

- When adding Local ES routes, the command changes how the ES routes are added to the candidate list; the configured IP address is added, instead of the system-ip.
- When advertising local ES routes, the configured IP address is used for the orig-ip of the route.

The **no** form of the command changes the originating IP address back to the system-ip.

Default no es-orig-ip

Parameters *ip-address* — Specifies an IPv4 or IPv6 address.

Values {*ip-address* | *ipv6-address*}

Platforms All

9.139 esa

esa

Syntax **esa** *esa-id* [**create**]
no esa *esa-id*

Context **[Tree]** (config esa)

Full Context configure esa

Description This command configures or creates an ESA instance with an identifier.

The **no** form of this command removes the ESA from the system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *esa-id* — Specifies the ESA identifier.

Values 1 to 16

create — Mandatory keyword used when creating an ESA instance in the config context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

9.140 esa-vm

esa-vm

Syntax [**no**] **esa-vm** [*esa-id*/*vm-id*]

Context **[Tree]** (config>isa>tunnel-group esa-vm)

Full Context configure isa tunnel-group esa-vm

Description This command specifies the tunnel ESA VM for the tunnel group. The ISA and ESA VM cannot co-exist in the same tunnel group.

Parameters *esa-id* — Specifies the ESA id

Values 1 to 16

vm-id — Specifies the VM id

Values 1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

esa-vm

Syntax **esa-vm** *vapp-id* [**drain**]
no esa-vm *vapp-id*

Context **[Tree]** (config>isa>lns-group esa-vm)

Full Context configure isa lns-group esa-vm

Description This command specifies the ISA and ESA VM to be used in the LNS group.

Parameters *vapp-id* — Displays the ID of the configured ESA and ESA VM.

Values

vapp-id:	*esa-id*/*vm-id*	
	esa-id	1 to 16
	vm-id	1 to 4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

drain — Specifies the draining of the ESA VM. The drain function gracefully redirects subscribers to other ESA VMs as it does not allow new subscribers to use the ESA VM. Eventually, the ESA VM will not service any subscriber and can be decommissioned gracefully.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

esa-vm

Syntax [**no**] **esa-vm** *vapp-id*

Context **[Tree]** (config>isa>wlan-group esa-vm)

Full Context configure isa wlan-group esa-vm

Description This command configures the ESA VM for the WLAN-GW group. It requires group redundancy to be configured in MDA mode.

Parameters *vapp-id* — Specifies the ID of the ESA and ESA VM to configure.

Values

vapp-id:	*esa-id*/*vm-id*	
	esa-id	1 to 16
	vm-id	1 to 4

esa-vm

Syntax [**no**] **esa-vm** *vapp-id*

Context **[Tree]** (config>isa>nat-group esa-vm)

Full Context configure isa nat-group esa-vm

Description This command assigns an ESA-VM to a NAT group.

Parameters *vapp-id* — Specifies the ESA and VM identifying a provisioned BB ISA.

Values

vapp-id:	*esa-id*/*vm-id*	
	esa-id	1 to 16
	vm-id	1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

esa-vm

Syntax [**no**] **esa-vm** *vapp-id*

Context **[Tree]** (config>isa>video-group esa-vm)

Full Context configure isa video-group esa-vm

Description This command assigns an ESA-VM to a video group.

The **no** form of this command removes the specified ESA-VM from the video group.

Default no esa-vm

Parameters *vapp-id* — Specifies the ESA and VM ID of the configured ESA-VM.

Values

vapp-id:	*esa-id*/*vm-id*	
	esa-id	1 to 16
	vm-id	1 to 4

Platforms 7750 SR-14s, 7750 SR-7/12/12e

9.141 esi

esi

Syntax **esi** *value*
no esi

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg esi)

Full Context configure service system bgp-evpn ethernet-segment esi

Description This command configures the 10-byte Ethernet Segment identifier (ESI) associated to the Ethernet-Segment that will be signaled in the BGP-EVPN routes. The ESI value cannot be changed unless the Ethernet-Segment is shutdown. Reserved esi values (0 and MAX-ESI) are not allowed.

Default no esi

Parameters *value* — Specifies the 10-byte esi.

Values 00-11-22-33-44-55-66-77-88-99
Using any of these separators ('-',':')

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.142 esm

esm

Syntax [**no**] **esm**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>ue-state esm)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ue-state esm

Description This command enables matching on ESM UEs.

The **no** form of this command disables matching on DSM UEs, unless UE state matching is disabled altogether.

Default no esm

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

esm

Syntax [**no**] **esm**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state esm)

Full Context configure subscriber-mgmt wlan-gw ue-query state esm

Description This command enables matching on UEs in an ESM state.

The **no** form of this command disables matching on UEs in an ESM state, unless all state matching is disabled.

Default no esm

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.143 esmc-tunnel

esmc-tunnel

Syntax [**no**] **esmc-tunnel**

Context **[Tree]** (config>port>ethernet>ssm esmc-tunnel)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet ssm esmc-tunnel

Description This command allows ESMC frames that are received into the Ethernet port to be tunneled in an Epipe or VPLS service. This is not recommended because it breaks the concepts inherent in Synchronous Ethernet, however it is required for compliance to MEF 6.1.1 EPL Option 2.

The **no** form of this command extracts the ESMC frames upon reception by the port. The ESMC frames are not tunneled through the service.

Default no esmc-tunnel

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.144 esp-auth-algorithm

esp-auth-algorithm

Syntax **esp-auth-algorithm** {**null** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** | **aes-xcbc** | **auth-encryption**}
no esp-auth-algorithm

Context **[Tree]** (config>ipsec>transform esp-auth-algorithm)

Full Context configure ipsec ipsec-transform esp-auth-algorithm

Description This command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a manually configured tunnel must share the same configuration parameters for the IPsec tunnel to enter the operational state.

The **no** form of this command disables the authentication.

Default esp-auth-algorithm sha1

Parameters **null** — This is a very fast algorithm specified in RFC 2410, which provides no authentication.

md5 — This parameter configures ESP to use the **hmac-md5** algorithm for authentication.

sha1 — This parameter configures ESP to use the **hmac-sha1** algorithm for authentication.

sha256 — This parameter configures ESP to use the **sha256** algorithm for authentication.

sha384 — This parameter configures ESP to use the **sha384** algorithm for authentication.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sha512 — This parameter configures ESP to use the **sha512** algorithm for authentication.

aes-xcbc — Specifies the **aes-xcbc** algorithm for authentication.

auth-encryption — This parameter must be configured when **esp-encryption-algorithm** is either **aes-gcm** or **aes-gmac**.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

esp-auth-algorithm

Syntax **esp-auth-algorithm** {**sha256** | **sha512**}
no esp-auth-algorithm

Context **[Tree]** (config>grp-encryp>encryp-keygrp esp-auth-algorithm)

Full Context configure group-encryption encryption-keygroup esp-auth-algorithm

Description This command specifies the hashing algorithm used to perform authentication on the Encapsulating Security Payload (ESP) within NGE packets for services configured using this key group. All SPI entries must be deleted before the **no** form of the command may be entered or the **esp-auth-algorithm** value changed from its current value.

The **no** form of the command reverts to the default value.

Default esp-auth-algorithm sha256

Parameters **sha256** — Configures the ESP to use the HMAC-SHA-256 algorithm for authentication.

sha512 — Configures the ESP to use the HMAC-SHA-512 algorithm for authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.145 esp-encryption-algorithm

esp-encryption-algorithm

Syntax **esp-encryption-algorithm** {**null** | **des** | **3des** | **aes128** | **aes192** | **aes256**| **aes128-gcm8** | **aes128-gcm12** | **aes128-gcm16** | **aes192-gcm8** | **aes192-gcm12** | **aes192-gcm16** | **aes256-gcm8** | **aes256-gcm12** | **aes256-gcm16** | **null-aes128-gmac** | **null-aes192-gmac** | **null-aes256-gmac**}
no esp-encryption-algorithm

Context **[Tree]** (config>ipsec>ipsec-transform esp-encryption-algorithm)

Full Context configure ipsec ipsec-transform esp-encryption-algorithm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the encryption algorithm to use for the IPsec session. Encryption only applies to esp configurations. If encryption is not defined, esp will not be used.

For IPsec tunnels to come up, both ends need to be configured with the same encryption algorithm.

The **no** form of this command removes the specified encryption algorithm.

Note: When **aes-gcm** or **aes-gmac** is configured:

- **esp-auth-algorithm** must be set to **auth-encryption**
- the system will not include the authentication algorithm in the ESP proposal of the SA payload
- **ipsec-transform** cannot be used for manual keying

Default esp-encryption-algorithm aes128

Parameters **null** — This parameter configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on.

des — This parameter configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

3des — This parameter configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make things more secure.

aes128 — This parameter configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes. As of today, this is a very strong algorithm choice.

aes192 — This parameter configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

aes256 — This parameter configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

aes128-gcm8 — Configures ESP to use aes-gcm with a 128-bit key size and an 8-byte ICV for encryption and authentication.

aes128-gcm12 — Configures ESP to use aes-gcm with a 128-bit key size and a 12-byte ICV for encryption and authentication.

aes128-gcm16 — Configures ESP to use aes-gcm with a 128-bit key size and a 16-byte ICV for encryption and authentication.

aes192-gcm8 — Configures ESP to use aes-gcm with a 192-bit key size and an 8-byte ICV for encryption and authentication.

aes192-gcm12 — Configures ESP to use aes-gcm with a 192-bit key size and a 12-byte ICV for encryption and authentication.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

aes192-gcm16 — Configures ESP to use aes-gcm with a 192-bit key size and a 16-byte ICV for encryption and authentication.

aes256-gcm8 — Configures ESP to use aes-gcm with a 256-bit key size and an 8-byte ICV for encryption and authentication.

aes256-gcm12 — Configures ESP to use aes-gcm with a 256-bit key size and a 12-byte ICV for encryption and authentication.

aes128-gcm16 — Configures ESP to use aes-gcm with a 256-bit key size and a 16-byte ICV for encryption and authentication.

null-aes128gmac — Configures ESP to use aes-gmac with a 128-bit key size for authentication only.

null-aes192gmac — Configures ESP to use aes-gmac with a 192-bit key size for authentication only.

null-aes256gmac — Configures ESP to use aes-gmac with a 256-bit key size for authentication only.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

esp-encryption-algorithm

Syntax **esp-encryption-algorithm** {**aes128** | **aes256**}
no esp-encryption-algorithm

Context **[Tree]** (config>grp-encryp>encryp-keygrp esp-encryption-algorithm)

Full Context configure group-encryption encryption-keygroup esp-encryption-algorithm

Description This command specifies the encryption algorithm used to perform encryption on the Encapsulating Security Payload (ESP) within NGE packets for services configured using this key group. All SPI entries must be deleted before the **no** form of the command may be entered or the **esp-encryption-algorithm** value changed from its current value.

The **no** form of the command resets the parameter to the default value.

Default esp-encryption-algorithm aes128

Parameters **aes128** — Configures the AES algorithm with a block size of 128 bits—a very strong algorithm choice.

aes256 — Configures the AES algorithm with a block size of 256 bits—the strongest available version of AES.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.146 esp-ext-hdr

esp-ext-hdr

Syntax **esp-ext-hdr** {**true** | **false**}
no esp-ext-hdr

Context **[Tree]** (config>filter>ipv6-filter>entry>match esp-ext-hdr)

Full Context configure filter ipv6-filter entry match esp-ext-hdr

Description This command enables match on existence of ESP Extension Header in the IPv6 filter policy.

The **no** form of this command ignores ESP Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default no esp-ext-hdr

Parameters **true** — Matches a packet with an ESP Extension Header.

false — Matches a packet without an ESP Extension Header.

Platforms All

9.147 ess-system-type

ess-system-type

Syntax [**no**] **ess-system-type**

Context **[Tree]** (bof ess-system-type)

Full Context bof ess-system-type

Description This command allows a new RoHS compliant 7750 SR-12 or 7750 SR-7 chassis to operate as an 7450 ESS-12 or 7450 ESS-7 system.

After entering this command, the system must be rebooted for the change to take effect.

If the RoHS compliant 7750 SR-12 or 7750 SR-7 chassis is operating as an 7450 ESS system, it can operate with either the 7750 SR or 7450 ESS CPM (subject to SR OS support) but both should always be the same type.

In addition, the system can operate with supported 7450 ESS or 7750 SR IOMs, MDAs, and IMMs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables this mode of operation and returns the system to a 7750 SR chassis type operation on the next reboot.

Default no ess-system-type

Platforms 7750 SR-7/12

9.148 est

est

Syntax **est**

Context **[Tree]** (admin>certificate est)

Full Context admin certificate est

Description Commands in this context configure Enrollment over Secure Transport (EST) parameters.

Platforms All

9.149 ete-fragment-threshold

ete-fragment-threshold

Syntax **ete-fragment-threshold** *threshold*
no ete-fragment-threshold

Context **[Tree]** (config>service>epipe>sap>frame-relay>frf-12 ete-fragment-threshold)
[Tree] (config>service>ipipe>sap>frame-relay>frf-12 ete-fragment-threshold)

Full Context configure service epipe sap frame-relay frf-12 ete-fragment-threshold
configure service ipipe sap frame-relay frf-12 ete-fragment-threshold

Description This command specifies the maximum length of a fragment to be transmitted.

The **no** form of this command reverts to the default.

Parameters *threshold* — The maximum length of a fragment to be transmitted.

Values 128 to 512

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ete-fragment-threshold

Syntax **ete-fragment-threshold** *threshold*
no ete-fragment-threshold

Context **[Tree]** (config>service>vpls>sap>fr>frf-12 ete-fragment-threshold)

Full Context configure service vpls sap frame-relay frf-12 ete-fragment-threshold

Description This command configures the FRF.12 fragmentation threshold.

The **no** form of this command removes the value.

Default ete-fragment-threshold 128

Parameters *threshold* — Specifies the maximum length of a fragment to be transmitted.

Values 128 to 512

Platforms All

ete-fragment-threshold

Syntax **ete-fragment-threshold** *fragment-threshold*
no ete-fragment-threshold

Context **[Tree]** (config>service>ies>if>sap>frame-relay>frf-12 ete-fragment-threshold)
[Tree] (config>service>vprn>if>sap>frame-relay>frf-12 ete-fragment-threshold)

Full Context configure service ies interface sap frame-relay frf-12 ete-fragment-threshold
configure service vprn interface sap frame-relay frf-12 ete-fragment-threshold

Description This command sets the maximum length, in bytes, of a fragment transmitted across a Frame Relay SAP with the FRF.12 end-to-end fragmentation enabled.

The no form of this command resets the fragment threshold back to the default value.

Default ete-fragment-threshold 128

Parameters *fragment-threshold* — Specifies the maximum fragment length, in bytes, to be transmitted across the FR SAP.

Values 128 to 512 bytes

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ete-fragment-threshold

Syntax **ete-fragment-threshold** *threshold*
no ete-fragment-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>if>sap>frf-12 ete-fragment-threshold)

Full Context configure service vprn interface sap frf-12 ete-fragment-threshold

Description This command specifies the maximum length of a fragment to be transmitted.

The **no** form of this command reverts to the default.

Parameters *threshold* — Specifies the maximum length of a fragment to be transmitted.

Values 128 to 512

Default 0

9.150 eth-bn

eth-bn

Syntax **eth-bn**

Context [Tree] (config>port>ethernet>eth-cfm>mep eth-bn)

Full Context configure port ethernet eth-cfm mep eth-bn

Description Commands in this context configure Ethernet Bandwidth Notification (ETH-BN) message handling.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.151 eth-bn-egress-rate-changes

eth-bn-egress-rate-changes

Syntax **eth-bn-egress-rate-changes**
no eth-bn-egress-rate-changes

Context [Tree] (config>port>ethernet eth-bn-egress-rate-changes)

Full Context configure port ethernet eth-bn-egress-rate-changes

Description This command allows rate changes received in ETH-BN messages on a port-based MEP to update the egress rate used on the port. The egress rate is capped by the minimum of the configured **egress-rate** and the maximum port rate, and the minimum egress rate is 1 kb/s. The **no** form of this command returns the value to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no eth-bn-egress-rate-changes

Platforms All

9.152 eth-cfm

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>eth-tunnel>path eth-cfm)

Full Context configure eth-tunnel path eth-cfm

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>port>ethernet eth-cfm)
[Tree] (config>lag eth-cfm)

Full Context configure lag eth-cfm
configure port ethernet eth-cfm

Description Commands in this context configure 802.1ag CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>service>epipe eth-cfm)
[Tree] (config>service>epipe>sap eth-cfm)
[Tree] (config>service>epipe>spoke-sdp eth-cfm)
[Tree] (config>service>ipipe>sap eth-cfm)

Full Context configure service epipe eth-cfm
configure service epipe sap eth-cfm
configure service epipe spoke-sdp eth-cfm
configure service ipipe sap eth-cfm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>service>vpls eth-cfm)
[Tree] (config>service>vpls>mesh-sdp eth-cfm)
[Tree] (config>service>vpls>spoke-sdp eth-cfm)
[Tree] (config>service>vpls>sap eth-cfm)

Full Context configure service vpls eth-cfm
configure service vpls mesh-sdp eth-cfm
configure service vpls sap eth-cfm
configure service vpls spoke-sdp eth-cfm

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>service>ies eth-cfm)
[Tree] (config>service>ies>sub-if>grp-if>sap eth-cfm)
[Tree] (config>service>ies>if>sap eth-cfm)
[Tree] (config>service>ies>if>spoke-sdp eth-cfm)

Full Context configure service ies eth-cfm
configure service ies interface sap eth-cfm
configure service ies interface spoke-sdp eth-cfm
configure service ies subscriber-interface group-interface sap eth-cfm

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies eth-cfm
- configure service ies interface spoke-sdp eth-cfm
- configure service ies interface sap eth-cfm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>service>vprn eth-cfm)
[Tree] (config>service>vprn>if>sap eth-cfm)
[Tree] (config>service>vprn>if>spoke-sdp eth-cfm)
[Tree] (config>service>vprn>sub-if>grp-if>sap eth-cfm)

Full Context configure service vprn eth-cfm
configure service vprn interface sap eth-cfm
configure service vprn interface spoke-sdp eth-cfm
configure service vprn subscriber-interface group-interface sap eth-cfm

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm
- configure service vprn eth-cfm
- configure service vprn interface spoke-sdp eth-cfm

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (debug eth-cfm)

Full Context debug eth-cfm

Description Commands in this context configure ETH-CFM debugging functions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>router>if eth-cfm)

Full Context configure router interface eth-cfm

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config>eth-ring>path eth-cfm)

Full Context configure eth-ring path eth-cfm

Description Commands in this context configure ETH-CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax **eth-cfm**

Context **[Tree]** (config eth-cfm)

Full Context configure eth-cfm

Description Commands in this context configure 802.1ag CFM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-cfm

Syntax [**no**] **eth-cfm**

Context **[Tree]** (config>sys>security>cpu-protection>policy eth-cfm)

Full Context configure system security cpu-protection policy eth-cfm

Description Provides the construct under which the different entries within CPU policy can define the match criteria and overall arrival rate of the Ethernet Configuration and Fault Management (ETH-CFM) packets at the CPU.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

9.153 eth-cfm-linktrace

eth-cfm-linktrace

Syntax **eth-cfm-linktrace** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**ttl** *ttl-value*] [**fc** {*fc-name*} [**profile** {**in** | **out**}]] [**count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>saa>test>type eth-cfm-linktrace)

Full Context configure saa test type eth-cfm-linktrace

Description This command configures a CFM linktrace test in SAA.

Parameters *mac-address* — Specifies the Layer 2 unicast MAC address of the destination MEP.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID as an alternative to the static *mac-address*. When the **remote-mepid** parameter is used in place of the *mac-address*, the domain and association information of the **source mep** for the test is used to check for a locally-stored unicast MAC address for the peer. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

ttl-value — Specifies the maximum number of hops traversed in the linktrace.

Values 1 to 255

Default 64

fc-name — Specifies the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

Values be, l2, af, l1, h2, ef, h1, nc

Default nc

profile {in | **out}** — Specifies the profile state of the MPLS echo request encapsulation.

Default in

send-count — Specifies the number of messages to send, expressed as a decimal integer. The **count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must be expired before the next message request is sent.

Values 1 to 10

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout — Specifies the time, to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of the time out, the test is marked complete and no more packets are processed for any of those request probes.

Values 1 to 10

Default 5

interval — Specifies the time, in seconds, to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

Values 1 to 10

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.154 eth-cfm-loopback

eth-cfm-loopback

Syntax **eth-cfm-loopback** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**size** *data-size*] [**fc** {*fc-name*} [**profile** {**in** | **out**}]] [**count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (config>saa>test>type eth-cfm-loopback)

Full Context configure saa test type eth-cfm-loopback

Description This command configures an Ethernet CFM loopback test in SAA.

Parameters *mac-address* — Specifies the Layer 2 unicast MAC address of the destination MEP.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID as an alternative to the static *mac-address*. When the **remote-mepid** parameter is used in place of the *mac-address*, the domain and association information of the **source mep** for the test is used to check for a locally-stored unicast MAC address for the peer. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ma-index — Specifies the MA index.

Values 1 to 4294967295

data-size — This is the size of the data portion of the data TLV. If 0 is specified, no data TLV is added to the packet.

Values 0 to 1500

Default 0

fc-name — Specifies the **fc** parameter that is used to indicate the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

Values be, l2, af, l1, h2, ef, h1, nc

Default nc

profile {in | out} — Specifies the profile state of the MPLS echo request encapsulation.

Default in

send-count — Specifies the number of messages to send, expressed as a decimal integer. The **count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must be expired before the next message request is sent.

Values 1 to 100

Default 1

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of time out, the test is marked complete and no more packets are processed for any of those request probes.

Values 1 to 10

Default 5

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

Values 1 to 10

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.155 eth-cfm-two-way-delay

eth-cfm-two-way-delay

Syntax **eth-cfm-two-way-delay** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**fc** {*fc-name*} [**profile** {**in** | **out**}]] [**count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (config>saa>test>type eth-cfm-two-way-delay)

Full Context configure saa test type eth-cfm-two-way-delay

Description This command configures an Ethernet CFM two-way delay test in SAA.

Parameters *mac-address* — Specifies the Layer 2 unicast MAC address of the destination MEP.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID as an alternative to the static *mac-address*. When the **remote-mepid** parameter is used in place of the *mac-address*, the domain and association information of the **source mep** for the test is used to check for a locally-stored unicast MAC address for the peer. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

fc-name — Specifies the **fc** parameter that is used to indicate the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

Values be, l2, af, l1, h2, ef, h1, nc

Default nc

send-count — Specifies the number of messages to send, expressed as a decimal integer. The count parameter is used to override the default number of message requests sent. The message interval value must be expired before the next message request is sent.

Values 1 to 100

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of time out, the test is marked complete and no more packets are processed for any of those request probes.

Values 1 to 10

Default 5

interval — Specifies the time, in seconds, expressed as a decimal integer. This parameter is used to configure the spacing between probes within a test run.

Values 0.1 to 0.9, 1 to 10

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.156 eth-cfm-two-way-slm

eth-cfm-two-way-slm

Syntax **eth-cfm-two-way-slm** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**fc** {*fc-name*} [**profile** {**in** | **out**}]] [**count** *send-count*] [**size** *data-size*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (config>saa>test>type eth-cfm-two-way-slm)

Full Context configure saa test type eth-cfm-two-way-slm

Description This command configures an Ethernet CFM two-way SLM test in SAA.

Parameters *mac-address* — Specifies the Layer 2 unicast MAC address of the destination MEP.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID as an alternative to the static *mac-address*. When the **remote-mepid** parameter is used in place of the *mac-address*, the domain and association information of the **source mep** for the test is used to check for a locally-stored unicast MAC address for the peer. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ma-index — Specifies the MA index.

Values 1 to 4294967295

fc-name — Specifies the **fc** parameter that is to indicate the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

Values be, l2, af, l1, h2, ef, h1, nc

Default nc

profile {in | **out}** — The profile state of the MPLS echo request encapsulation.

Default in

send-count — Specifies the number of messages to send, expressed as a decimal integer. The count parameter is used to override the default number of message requests sent. The message interval value must be expired before the next message request is sent.

Values 1 to 1000

Default 1

data-size — Specifies the size of the data portion of the data TLV. If 0 is specified, no data TLV is added to the packet.

Values 0 to 1500

Default 0

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of the time out, the test is marked complete and no more packets are processed for any of those request probes.

Values 1 to 10

Default 5

interval — Specifies the time, in seconds, used to configure the spacing between probes within a test run.

Values 0.1 to 0.9, 1 to 10

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.157 eth-ed

eth-ed

Syntax **eth-ed**

Context [Tree] (config>eth-ring>path>eth-cfm>mep>grace eth-ed)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace eth-ed)
[Tree] (config>lag>eth-cfm>mep>grace eth-ed)
[Tree] (config>port>ethernet>eth-cfm>mep>grace eth-ed)

Full Context configure eth-ring path eth-cfm mep grace eth-ed
configure eth-tunnel path eth-cfm mep grace eth-ed
configure lag eth-cfm mep grace eth-ed
configure port ethernet eth-cfm mep grace eth-ed

Description Commands in this context configure ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-ed

Syntax **eth-ed**

Context [Tree] (config>service>epipe>sap>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace eth-ed)

Full Context configure service epipe sap eth-cfm mep grace eth-ed
configure service epipe spoke-sdp eth-cfm mep grace eth-ed
configure service ipipe sap eth-cfm mep grace eth-ed

Description Commands in this context configure ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-ed

Syntax **eth-ed**

Context [Tree] (config>service>vpls>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace eth-ed)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls eth-cfm mep grace eth-ed
configure service vpls mesh-sdp eth-cfm mep grace eth-ed
configure service vpls sap eth-cfm mep grace eth-ed
configure service vpls spoke-sdp eth-cfm mep grace eth-ed

Description Commands in this context configure ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-ed

Syntax **eth-ed**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace eth-ed)

Full Context configure service ies interface sap eth-cfm mep grace eth-ed
configure service ies interface spoke-sdp eth-cfm mep grace eth-ed
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed

Description Commands in this context configure ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep grace eth-ed
- configure service ies interface spoke-sdp eth-cfm mep grace eth-ed

eth-ed

Syntax **eth-ed**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace eth-ed)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace eth-ed)

Full Context configure service vprn interface sap eth-cfm mep grace eth-ed
configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed

Description Commands in this context configure ITU-T Y.1731 ETH-ED expected defect functional parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm mep grace eth-ed
- configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed

eth-ed

Syntax **eth-ed**

Context **[Tree]** (config>router>if>eth-cfm>mep>grace eth-ed)

Full Context configure router interface eth-cfm mep grace eth-ed

Description Commands in this context configure ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.158 eth-legacy-fault-notification

eth-legacy-fault-notification

Syntax **eth-legacy-fault-notification**

Context **[Tree]** (config>service>ipipe eth-legacy-fault-notification)

Full Context configure service ipipe eth-legacy-fault-notification

Description This is the top level of the hierarchy containing Ethernet to Legacy fault notification parameters. This context must activate using the no shutdown command before Ethernet to legacy fault notification can occur for Ipipe services that make use of PPP, MLPPP or HDLC. This is only applicable to Ipipe services with one legacy (PPP, MLPPP or HDLC) connection and an Ethernet SAP. No other services, not other combinations are supported.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.159 eth-ring

eth-ring

Syntax **eth-ring** *ring-id*
no eth-ring

Context **[Tree]** (config>service>vpls eth-ring)

Full Context configure service vpls eth-ring

Description This command configures a VPLS SAP to be associated with an Ethernet ring. The SAP port ID is associated with the corresponding Ethernet ring path configured on the same port ID. The encapsulation type must be compatible with the Ethernet ring path encapsulation.

The **no** form of this command removes the Ethernet ring association from this SAP.

Default no eth-ring

Parameters *ring-id* — Specifies the ring ID.

Values 1 to 128

eth-ring

Syntax **eth-ring** *ring-index*
no eth-ring

Context **[Tree]** (config eth-ring)

Full Context configure eth-ring

Description This command configures a G.8032 protected Ethernet ring. G.8032 Rings may be configured as major rings with two paths (a&b) or as sub-rings with two paths, or in the case of an interconnection node a single path.

The **no** form of this command deletes the Ethernet ring specified by the ring-id.

Default no eth-ring

Parameters *ring-index* — Specifies the ring ID.

Values 1 to 128

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.160 eth-sat

eth-sat

Syntax **eth-sat** *sat-id* [**create**]
no eth-sat *sat-id*

Context **[Tree]** (config>system>satellite eth-sat)

Full Context configure system satellite eth-sat

Description This command enables the specified Ethernet satellite configuration context.

The **no** form of the command deletes the specified Ethernet satellite.

Parameters *sat-id* — Specifies the satellite ID for the associated Ethernet satellite.

Values 1 to 20

create — Creates a new Ethernet satellite context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-sat

Syntax **eth-sat** *sat-id*

Context **[Tree]** (admin>satellite eth-sat)

Full Context admin satellite eth-sat

Description This command can be used to perform administrative functions on the specified Ethernet-satellite chassis.

Parameters *sat-id* — Specifies the Ethernet-satellite chassis.

Values 1 to 20

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.161 eth-tag

eth-tag

Syntax **eth-tag** *tag-value*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no eth-tag

Context [Tree] (config>service>epipe>bgp-evpn>local-attachment-circuit eth-tag)
[Tree] (config>service>epipe>bgp-evpn>remote-attachment-circuit eth-tag)

Full Context configure service epipe bgp-evpn local-attachment-circuit eth-tag
configure service epipe bgp-evpn remote-attachment-circuit eth-tag

Description This command configures the Ethernet tag value. When configured in the **local-attachment-circuit** context, the system uses the value in the advertised AD per-EVI route sent for the attachment circuit. When configured in the **remote-attachment-circuit** context the system compares that value with the eth-tag value of the imported AD per-EVI routes for the service. If there is a match, the system creates an EVPN destination for the Epipe.

Parameters *tag-value* — Specifies the Ethernet tag value of the attachment circuit.

Values 1 to 16777215

Platforms All

9.162 eth-test

eth-test

Syntax **eth-test** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**data-length** *data-length*]

Context [Tree] (oam>eth-cfm eth-test)

Full Context oam eth-cfm eth-test

Description This command initiates an ETH-CFM test. The implementation supports a single ETH-TST PDU to check unidirectional reachability, launched from a source MEP and terminated on the remote MEP with no response PDU toward the source.

Parameters *mac-address* — Specifies a unicast destination MAC address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID of the peer within the association. The domain and association information are derived from the **source mep** for the session. The Layer 2 IEEE MAC address is resolved from previously-learned remote MAC addressing, derived from the reception and processing of the ETH-CC PDU. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

priority — Specifies the priority of the frame. The priority can be manipulated by QoS policies.

Values 0 to 7

Default 7

data-length — Specifies the size of the padding to be added to the frame.

Values 64 to 1500

Default 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.163 eth-test-enable

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep eth-test-enable)

Full Context configure eth-tunnel path eth-cfm mep eth-test-enable

Description This command enables eth-test functionality on MEP. For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**data-length** *data-length*]

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-test-enable

Syntax [**no**] **eth-test-enable**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>lag>eth-cfm>mep eth-test-enable)
[Tree] (config>port>ethernet>eth-cfm>mep eth-test-enable)
[Tree] (config>router>if>eth-cfm>mep eth-test-enable)

Full Context configure lag eth-cfm mep eth-test-enable
configure port ethernet eth-cfm mep eth-test-enable
configure router interface eth-cfm mep eth-test-enable

Description For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [priority *priority*] [data-length *data-length*]

The **no** form of this command disables eth-test capabilities.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context [Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep eth-test-enable)
[Tree] (config>service>epipe>sap>eth-cfm>mep eth-test-enable)
[Tree] (config>service>ipipe>sap>eth-cfm>mep eth-test-enable)

Full Context configure service epipe sap eth-cfm mep eth-test-enable
configure service epipe spoke-sdp eth-cfm mep eth-test-enable
configure service ipipe sap eth-cfm mep eth-test-enable

Description For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [priority *priority*] [data-length *data-length*]

A check is performed for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP indicates the problem.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context [Tree] (config>service>vpls>sap>eth-cfm>mep eth-test-enable)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep eth-test-enable)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep eth-test-enable)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls mesh-sdp eth-cfm mep eth-test-enable
configure service vpls sap eth-cfm mep eth-test-enable
configure service vpls spoke-sdp eth-cfm mep eth-test-enable

Description For ETH-test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**data-length** *data-length*]

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep eth-test-enable)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep eth-test-enable)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep eth-test-enable)

Full Context configure service ies interface sap eth-cfm mep eth-test-enable
configure service ies interface spoke-sdp eth-cfm mep eth-test-enable
configure service ies subscriber-interface group-interface sap eth-cfm mep eth-test-enable

Description For ETH-test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**data-length** *data-length*]

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep eth-test-enable

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep eth-test-enable
- configure service ies interface sap eth-cfm mep eth-test-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep eth-test-enable)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep eth-test-enable)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm eth-test-enable)

Full Context configure service vprn interface sap eth-cfm mep eth-test-enable
configure service vprn interface spoke-sdp eth-cfm mep eth-test-enable
configure service vprn subscriber-interface group-interface sap eth-cfm eth-test-enable

Description This command enables eth-test functionality on MEP. For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [**priority** *priority*] [**data-length** *data-length*]

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep eth-test-enable)

Full Context configure eth-ring path eth-cfm mep eth-test-enable

Description This command enables eth-test functionality on MEP. For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test is then performed using the following OAM commands:

oam eth-cfm eth-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [priority *priority*] [data-length *data-length*]

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.164 eth-tunnel

eth-tunnel

Syntax **eth-tunnel**

Context **[Tree]** (config>router>l2tp eth-tunnel)
[Tree] (config>router>l2tp>group eth-tunnel)
[Tree] (config>service>vprn>l2tp eth-tunnel)
[Tree] (config>service>vprn>l2tp>group eth-tunnel)

Full Context configure router l2tp eth-tunnel
configure router l2tp group eth-tunnel
configure service vprn l2tp eth-tunnel
configure service vprn l2tp group eth-tunnel

Description Commands in this context configure Ethernet tunnel client parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

eth-tunnel

Syntax [**no**] **eth-tunnel** *tunnel-index*

Context **[Tree]** (config eth-tunnel)

Full Context configure eth-tunnel

Description This command configures a G.8031 protected Ethernet tunnel.

The **no** form of this command deletes the Ethernet tunnel specified by the tunnel-id.

Parameters *tunnel-index* — Specifies the tunnel index.

Values 1 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-tunnel

Syntax **eth-tunnel** *tunnel-id*

Context **[Tree]** (config>service>vpls eth-tunnel)

Full Context configure service vpls eth-tunnel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates a BVPLS SAP with the global Ethernet tunnel object specified by tunnel-id. Only one-to-one mapping between SAP and Ethernet tunnel is supported in the initial implementation. The global eth-tunnel tunnel-id with at least a member port must be configured in advance for the command to be successful. A SAP will be instantiated using the active path components (member port and control-tag) for VPLS forwarding. The last member port in the Ethernet tunnel cannot be deleted if there is a SAP configured on that eth-tunnel. This command is only available in the BVPLS context.

The **no** form of this command removes the sap from the Ethernet tunnel object.

Default no sap is specified

Parameters *tunnel-id* — Specifies the value of the Ethernet tunnel identifier to be used for the SAP.

Values 1 to 64

eth-tunnel

Syntax **eth-tunnel**

Context **[Tree]** (config>service>epipe>sap eth-tunnel)
[Tree] (config>service>ipipe>sap eth-tunnel)

Full Context configure service epipe sap eth-tunnel
configure service ipipe sap eth-tunnel

Description Commands in this context configure Ethernet tunnel SAP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-tunnel

Syntax **eth-tunnel**

Context **[Tree]** (config>service>vpls>sap eth-tunnel)

Full Context configure service vpls sap eth-tunnel

Description Commands in this context configure Ethernet tunnel SAP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.165 eth-vsm-grace

eth-vsm-grace

Syntax **eth-vsm-grace**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>lag>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>port>ethernet>eth-cfm>mep>grace eth-vsm-grace)

Full Context configure eth-ring path eth-cfm mep grace eth-vsm-grace
configure eth-tunnel path eth-cfm mep grace eth-vsm-grace
configure lag eth-cfm mep grace eth-vsm-grace
configure port ethernet eth-cfm mep grace eth-vsm-grace

Description Commands in this context configure Nokia ETH-CFM Grace functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-vsm-grace

Syntax **eth-vsm-grace**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace eth-vsm-grace)

Full Context configure service epipe sap eth-cfm mep grace eth-vsm-grace
configure service epipe spoke-sdp eth-cfm mep grace eth-vsm-grace
configure service ipipe sap eth-cfm mep grace eth-vsm-grace

Description Commands in this context configure Nokia ETH-CFM Grace functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-vsm-grace

Syntax **eth-vsm-grace**

Context **[Tree]** (config>service>vpls>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace eth-vsm-grace)

Full Context configure service vpls eth-cfm mep grace eth-vsm-grace

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp eth-cfm mep grace eth-vsm-grace
configure service vpls sap eth-cfm mep grace eth-vsm-grace
configure service vpls spoke-sdp eth-cfm mep grace eth-vsm-grace

Description Commands in this context configure Nokia ETH-CFM Grace functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

eth-vsm-grace

Syntax **eth-vsm-grace**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace eth-vsm-grace)

Full Context configure service ies interface sap eth-cfm mep grace eth-vsm-grace
configure service ies interface spoke-sdp eth-cfm mep grace eth-vsm-grace
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace

Description Commands in this context configure Nokia ETH-CFM Grace functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep grace eth-vsm-grace
- configure service ies interface sap eth-cfm mep grace eth-vsm-grace

eth-vsm-grace

Syntax **eth-vsm-grace**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace eth-vsm-grace)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace eth-vsm-grace)

Full Context configure service vprn interface sap eth-cfm mep grace eth-vsm-grace
configure service vprn interface spoke-sdp eth-cfm mep grace eth-vsm-grace
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace

Description Commands in this context configure Nokia ETH-CFM Grace functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm mep grace eth-vsm-grace
- configure service vprn interface spoke-sdp eth-cfm mep grace eth-vsm-grace

eth-vsm-grace

Syntax **eth-vsm-grace**

Context **[Tree]** (config>router>if>eth-cfm>mep>grace eth-vsm-grace)

Full Context configure router interface eth-cfm mep grace eth-vsm-grace

Description Commands in this context configure Nokia ETH-CFM Grace functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.166 ethernet

ethernet

Syntax **ethernet**

Context **[Tree]** (config>port ethernet)

Full Context configure port ethernet

Description This command the context to configure Ethernet port attributes.

This context can only be used when configuring Fast Ethernet, gigabit or 10-G Fast Ethernet or Ethernet LAN ports on an appropriate MDA.

Platforms All

ethernet

Syntax **ethernet**

Context **[Tree]** (config>eth-tunnel ethernet)

Full Context configure eth-tunnel ethernet

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure Ethernet parameters for the Ethernet tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ethernet

Syntax **ethernet**

Context **[Tree]** (config>service>epipe>sap ethernet)

Full Context configure service epipe sap ethernet

Description Commands in this context configure Ethernet properties in this SAP.

Platforms All

ethernet

Syntax **ethernet**

Context **[Tree]** (config>test-oam>build-packet>header ethernet)
[Tree] (debug>oam>build-packet>packet>field-override>header ethernet)

Full Context configure test-oam build-packet header ethernet
debug oam build-packet packet field-override header ethernet

Description This command causes the associated header to be defined as an Ethernet header template and enables the context to define the Ethernet parameters.

The **no** form of this command removes the Ethernet header association.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ethernet

Syntax **ethernet**

Context **[Tree]** (config>oam-pm>session ethernet)

Full Context configure oam-pm session ethernet

Description Commands in this context configure the Ethernet specific source and destination information, the priority, and the Ethernet tests tools on the launch point.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.167 ethernet-ctag

ethernet-ctag

Syntax [**no**] **ethernet-ctag**

Context **[Tree]** (config>qos>sap-egress ethernet-ctag)

Full Context configure qos sap-egress ethernet-ctag

Description This command specifies that the top customer tag should be used for egress reclassification based on dot1p criteria. This command applies to all dot1p criteria configured in a given SAP egress QoS policy.

The **no** form of this command means that a service delimiting tag will be used for egress reclassification based on dot1p criteria.

Default no ethernet-ctag

Platforms All

9.168 ethernet-header

ethernet-header

Syntax **ethernet-header** [**da** *ieee-address*] [**sa** *ieee-address*] [**etype** *ethertype*]
no ethernet-header

Context **[Tree]** (config>li>li-source>nat ethernet-header)

Full Context configure li li-source nat ethernet-header

Description This command configures the Ethernet header for the NAT sources.

The **no** form of this command removes the values from the configuration.

Parameters **da** *ieee-address* — Specifies the destination MAC address field of the of the Ethernet encapsulation used for the NAT subscribers associated with this mirror source up to 30 characters.

sa *ieee-address* — Specifies the source MAC address field of the of the Ethernet encapsulation used for the NAT subscribers associated with this mirror source up to 30 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ethertype — Specifies the ethertype of the ethernet encapsulation used for the NAT subscribers associated with this mirror source that have an intercept identifier.

Values 1536 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.169 ethernet-segment

ethernet-segment

Syntax **ethernet-segment** *name* [**virtual**] [**create**]
no ethernet-segment *name*

Context **[Tree]** (config>service>system>bgp-evpn ethernet-segment)

Full Context configure service system bgp-evpn ethernet-segment

Description This command configures an Ethernet Segment instance and its corresponding name. The configuration of the dot1q or qinq nodes is only allowed if the Ethernet Segment (ES) is created as **virtual**.

For a virtual ES, a port, LAG, or SDP must be created for the ES before configuring a VLAN or vc-id association.

When a port or LAG is added, the **type** and **encap-type** values are checked. If the **encap-type** is **dot1q**, then only the dot1q node can be configured; the qinq context is not allowed. In the same way, if the **encap-type** is **qinq**, then only the qinq node is allowed. A dot1q, qinq, or vc-id range is required for a virtual ES to be operationally active.

Parameters *name* — Specifies the 32-character ES name.

virtual — This keyword specifies that the ES is virtual and is associated to logical interfaces, in addition to ports, LAGs, or SDPs.

create — Mandatory keyword for creating an ES.

Platforms All

9.170 etype

etype

Syntax **etype** *etype-value*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no etype

Context [Tree] (config>qos>sap-ingress>mac-criteria>entry>match etype)

Full Context configure qos sap-ingress mac-criteria entry match etype

Description Configures an Ethernet type II value to be used as a service ingress QoS policy match criterion.

The Ethernet type field is a 2-byte field used to identify the protocol carried by the Ethernet frame. For e.g. 0800 is used to identify the IPv4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. For IEEE 802.3 frames, use the dsap, ssap, or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap, and dsap fields are mutually exclusive and cannot be part of the same match criteria.

The no form of this command removes the previously entered etype field as the match criteria.

Default no etype

Parameters *etype-value* — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

Values 0x0600 to 0xFFFF

Platforms All

etype

Syntax **etype** *0x0600..0xffff*
no etype

Context [Tree] (config>filter>mac-filter>entry>match etype)

Full Context configure filter mac-filter entry match etype

Description Configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.

The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify the IPv4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. For IEEE 802.3 frames, use the dsap, ssap or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the previously entered etype field as the match criteria.

Default no etype

Parameters *0x0600..0xffff* — Specifies the Ethernet type II frame Ethertype value to be used as a match criterion expressed in decimal integer or hexadecimal format.

Values 1536 to 65535 or 0x0600 to 0xFFFF

Platforms All

etype

Syntax **etype** *0x0600xx0xffff*
no etype

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match etype)

Full Context configure system security management-access-filter mac-filter entry match etype

Description Configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.

The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify the IPv4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. For IEEE 802.3 frames, use the dsap, ssap or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide* for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

The **no** form of this command removes the previously entered etype field as the match criteria.

Default no etype

Parameters *ethernet-type* — Specifies the Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

Values 0x0600 to 0xFFFF

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.171 event

event

Syntax [**no**] **event**

Context **[Tree]** (debug>gtp event)

Full Context debug gtp event

Description This command configures detailed debugging of all events in the GTP system.

The **no** form of this command disables event debugging.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

event

Syntax [**no**] **event**

Context **[Tree]** (debug>router>l2tp event)
[Tree] (debug>router>l2tp>assignment-id event)
[Tree] (debug>router>l2tp>group event)
[Tree] (debug>router>l2tp>peer event)
[Tree] (debug>router>l2tp>tunnel event)

Full Context debug router l2tp assignment-id event
debug router l2tp event
debug router l2tp group event
debug router l2tp peer event
debug router l2tp tunnel event

Description This command configures an L2TP debugging event.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

event

Syntax [**no**] **event**

Context **[Tree]** (debug>service>id>ppp event)

Full Context debug service id ppp event

Description This command enables the PPP event debug context.

The **no** form of this command disables PPP event debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

event

Syntax [**no**] **event**

Context **[Tree]** (debug>dynsvc>scripts event)
[Tree] (debug>dynsvc>scripts>inst event)
[Tree] (debug>dynsvc>scripts>script event)

Full Context debug dynamic-services scripts event
debug dynamic-services scripts instance event
debug dynamic-services scripts script event

Description This command enables/disables the generation of all dynamic data service script debugging events output: cli, errors, executed-cmd, warnings, state-change.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

event

Syntax **event** *event-type* [**create**]
no event *event-type*

Context **[Tree]** (config>card>mda event)

Full Context configure card mda event

Description This command allows the user to control the action to be taken when a specific hardware error event is raised against the target MDA.

If no event action has been created for a specific event type, then the hardware errors related to that event type are ignored by the management plane of the router.

The **no** form of this command clears any action defined for the event.

Parameters *event-type* — Specifies the event type, up to 32 characters.

Values soft-error — Defines the action to be taken when soft errors are detected on the MDA

internal-frame-loss — System detected frame loss in the traffic transiting the MDA.

memory-error — Provides the user options to handle MDA memory error events on MDAs. This feature is supported on FP2- and FP3-based Ethernet MDAs and IMMs.

data-link-error — Provides the user options to handle datapath link errors on an MDA.

create — Keyword used to create an event.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

event

Syntax [**no**] **event**

Context **[Tree]** (debug>vsd>scripts event)

Full Context debug vsd scripts event

Description This command enables/disables the generation of all script debugging event output: cli, errors, execute-cmd, warnings, state-change.

Platforms All

event

Syntax [**no**] **event**

Context **[Tree]** (debug>router>gmpls event)

Full Context debug router gmpls event

Description This command enables and disables debugging for specific GMPLS events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

event

Syntax [**no**] **event**

Context **[Tree]** (debug>router>ldp>if event)
[Tree] (debug>router>ldp>peer event)

Full Context debug router ldp interface event
debug router ldp peer event

Description This command configures debugging for specific LDP events.

Platforms All

event

Syntax [**no**] **event**

Context **[Tree]** (debug>router>mpls event)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (debug>router>rsvp event)

Full Context debug router mpls event
debug router rsvp event

Description This command enables debugging for specific events.

The **no** form of the command disables the debugging.

Platforms All

event

Syntax [**no**] **event**

Context **[Tree]** (debug>router>ip event)

Full Context debug router ip event

Description This command enables debugging for specific IP events.

The **no** form of this command disables debugging for the specified IP events.

Platforms All

event

Syntax **event** *rmon-event-id* [*event-type*] [**description** *description-string*] [**owner** *owner-string*]
no event *rmon-event-id*

Context **[Tree]** (config>system>thresholds>rmon event)

Full Context configure system thresholds rmon event

Description The event command configures an entry in the RMON-MIB event table. The event command controls the generation and notification of threshold crossing events configured with the alarm command. When a threshold crossing event is triggered, the **rmon>event** configuration optionally specifies if an entry in the RMON-MIB log table should be created to record the occurrence of the event. It may also specify that an SNMP notification (trap) should be generated for the event. The RMON-MIB defines two notifications for threshold crossing events: Rising Alarm and Falling Alarm.

Creating an event entry in the RMON-MIB log table does not create a corresponding entry in the SR OS event logs. However, when the **event-type** is set to trap, the generation of a Rising Alarm or Falling Alarm notification creates an entry in the SR OS event logs and that is distributed to all the SR OS log destinations that are configured: CONSOLE, session, memory, file, syslog, or SNMP trap destination.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SR OS logger message includes a rising or falling threshold crossing event indicator, the sample type (absolute or delta), the sampled value, the threshold value, the RMON-alarm-id, the associated RMON-event-id and the sampled SNMP object identifier.

Use the **no** form of this command to remove an rmon-event-id from the configuration.

Parameters *rmon-event-id* — Specifies an identifier for this event. Alarm ID values above 65400 are used for dynamic system threshold commands and should be avoided.

Values 1 to 65535

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values **log** — An entry is made in the RMON-MIB log table for each event occurrence.

This does **not** create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

description-string — Specifies a user configurable string that can be used to identify the purpose of this event. This is an optional parameter and can be up to 80 characters long. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

owner-string — Specifies the owner string; the owner identifies the creator of this alarm. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarmTable by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner will not normally be configured by CLI users and can be up 80 characters long.

Default TiMOS CLI

Configuration example:

```
event 5 rmon-event-type both description "alarm testing" owner "TiMOS CLI"
```

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

event

Syntax [**no**] **event** *application-id event-name-id*

Context **[Tree]** (config>log>event-trigger event)

Full Context configure log event-trigger event

Description This command configures a specific log event as a trigger for one or more EHS handlers. Further matching criteria can be applied to only trigger certain handlers with certain instances of the log event.

The **no** form of this command removes the specified trigger event.

Parameters *application-id* — Specifies the type of application that triggers the event.

Values application_assurance, aps, atm, bgp, calltrace, cflowd, chassis, debug, dhcp, dhcps, diameter, dynsvc, efm_oam, elmi, ering, eth_cfm, etun, filter, gsmp, gmpls, igh, igmp, igmp_snooping, ip, ipsec, isis, l2tp, lag, ldp, li, lldp, lmp, logger, mcpath, mc_redundancy, mirror, mld, mld_snooping, mpls, mpls_tp, msdp, nat, ntp, oam, open_flow, ospf, pim, pim_snooping, port, ppp, pppoe, radius, rip, rip_ng, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, video, vrrp, vrtr, wlan_gw, wpp

event-name-id — Specifies the name or numerical identifier of the event.

Values 0 to 4294967295 | *event-name*: 32 characters max

Platforms All

9.172 event-control

event-control

Syntax **event-control** *application-id* [*event-name* | *event-number*] [**generate**] [*severity-level*] [throttle] [**specific-throttle-rate** *events-limit* **interval** *seconds* | **disable-specific-throttle**] [**repeat** | **no-repeat**]
event-control *application-id* [*event-name* | *event-number*] **suppress**
no event-control *application-id* [*event-name* | *event-number*]

Context **[Tree]** (config>log event-control)

Full Context configure log event-control

Description This command is used to specify that a particular event or all events associated with an application is either generated or suppressed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Events are generated by an application and contain an event number and description explaining the cause of the event. Each event has a default designation which directs it to be generated or suppressed.

Events are generated with a default severity level that can be modified by using the *severity-level* option.

Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are squelched. In reverse, indiscriminate application may cause excessive overhead.

The rate of event generation can be throttled by using the **throttle** parameter.

The **no** form of this command reverts the parameters to the default setting for events for the application or a specific event within the application. The severity, generate, suppress, and throttle options will also be reset to the initial values.

Default Each event has a set of default settings. To display a list of all events and the current configuration use the **event-control** command.

Parameters *application-id* — The application whose events are affected by this event control filter.

Values A valid application name. To display a list of valid application names, use the **show log applications** command. Some examples of valid applications are:

```
application_assurance| aps| atm| auto_prov| bfd| bgp| bier|
bmp| calltrace| ccag| cflowd| chassis| cpmhwfilter|
cpmhwqueue| debug| dhcp| dhcps| diameter| dot1x| dynsvc|
efm_oam| elmi| ering| eth_cfm| etun| filter| fpe| gsmp| gmpls|
gtp| gtungrp| icl| igh| igmp| igmp_snooping| ip| ipfix| ipsec|
ipsec_cpm| isis| l2tp| lag| ldap| ldp| li| lldp| lmp| logger|
macsec| mcac| mcpath| mc_redundancy| mgmt_core| mirror| mld|
mld_snooping| mpls| mpls_tp| mpls_lmgr| mrp| msdp| nat| nge|
ntp| oam| open_flow| ospf| pcap| pcep| pfcp| pim|
pim_snooping| port| ppp| pppoe| pppoe_clnt| profile| ptp|
pxc| python| qos| radius| rip| rip_ng| route_next_hop|
route_policy| rpki| rsvp| security| sflow| snmp| sr_policy|
stp| subscr_mgmt| sub_host_trk| svcmgr| system| tip| tls|
user| user_db| video| vrrp| vrtr| wlan_gw| wpp
```

Default None, this parameter must be explicitly specified.

event-name — To generate, suppress, or revert to default for a single event, enter the specific event short name up to 32 characters. If no event name is specified, the command applies to all events in the application. To display a list of all event short names use the **event-control** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

event-number — To generate, suppress, or revert to default for a single event, enter the specific number. If no event number is specified, the command applies to all events in the application.

Default none

Values 0 to 4294967295

generate — Specifies that logger event is created when this event occurs. The generate keyword can be used with two optional parameters, *severity-level* and **throttle**.

Default generate

severity-level — An ASCII string representing the severity level to associate with the specified generated events

Default The system assigned severity name

Values One of: cleared, indeterminate, critical, major, minor, warning.

throttle — Specifies whether or not events of this type will be throttled. By default, event throttling is on for most event types.

suppress — This keyword indicates that the specified events will not be logged. If the **suppress** keyword is not specified then the events are generated by default. For example on the 7750 SR, **event-control bgp suppress** will suppress all BGP events. If a log event is a raising event for a Facility Alarm, and the associated Facility Alarm is raised, then changing the log event to **suppress** clears the associated Facility Alarm.

Default generate

specific-throttle-rate *events-limit* — The log event throttling rate can be configured independently for each log event using this keyword. This specific-throttle-rate overrides the globally configured throttle rate (**config**>**log**>**throttle-rate**) for the specific log event.

Values 1 to 20000

interval *seconds* — Specifies the number of seconds that the specific throttling intervals lasts.

Values 1 to 1200

disable-specific-throttle — Specifies to disable the **specific-throttle-rate**.

repeat — Specifies that the log event should be repeated every minute until the underlying condition is cleared. Only supported for the following log events: BGP tBgpMaxNgPfxLmtThresholdReached and PORT tmnxEqPortEtherCrcAlarm (for **degrade** threshold only)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.173 event-damping

event-damping

Syntax [**no**] **event-damping**

Context **[Tree]** (config>log event-damping)

Full Context configure log event-damping

Description This command allows the user to set the event damping algorithm to suppress QoS or filter change events.

The **no** form of this command removes the event damping algorithm.

Note: While this event damping is original behavior for some modules such as service manager, QoS, and filters, it can result in the NMS system database being out of sync because of missed change events. On the other hand, if the damping is disabled (**no event-damping**), it may take much longer to **exec** a large CLI configuration file after system bootup.

Platforms All

9.174 event-handler

event-handler

Syntax **event-handler** *event-handler*
no event-handler

Context **[Tree]** (config>log>event-trigger>event>trigger-entry event-handler)

Full Context configure log event-trigger event trigger-entry event-handler

Description This command configures the event handler to be used for this trigger entry.

The **no** form of this command removes the event handler configuration.

Parameters *event-handler* — Specifies the name of the event handler, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

event-handler

Syntax **event-handler**

Context **[Tree]** (config>system>security>cli-script>authorization event-handler)

Full Context configure system security cli-script authorization event-handler

Description Commands in this context configure authorization for the Event Handling System (EHS). EHS allows user-controlled programmatic exception handling by allowing a CLI script to be executed upon the detection of a log event.

Platforms All

9.175 event-handling

event-handling

Syntax **event-handling**

Context **[Tree]** (config>log event-handling)

Full Context configure log event-handling

Description Commands in this context configure event handling within the Event Handler System (EHS).

Platforms All

9.176 event-log

event-log

Syntax **event-log** *event-log-name* [**create**]
no event-log *event-log-name*

Context **[Tree]** (config>app-assure>group event-log)

Full Context configure application-assurance group event-log

Description This command configures an event log.

Parameters *event-log-name* — Specifies the name of the event log.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

event-log

Syntax **event-log** *event-log-name* [**all**]
no event-log

Context **[Tree]** (config>app-assure>group>tcp-validate event-log)

Full Context configure application-assurance group tcp-validate event-log

Description This command enables logging of traffic dropped by TCP validation.

The **no** form of this command disables logging of traffic dropped by TCP validation.

Default no event-log

Parameters *event-log-name* — Specifies the name of the event log up to 32 characters.

all — Logs all dropped traffic. Using the **all** option allows the operator to capture all discards made by the TCP validation policy, including those related to:

- packets that were received after an RST and discarded
- packets received before TCP session establishment (before SYN) and discarded

Without the **all** option, discards related to these cases are not captured in any event log.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

event-log

Syntax **event-log** *event-log-name*
no event-log

Context **[Tree]** (config>app-assure>group>gtp event-log)
[Tree] (config>app-assure>group>gtp>gtp-filter event-log)

Full Context configure application-assurance group gtp event-log
configure application-assurance group gtp gtp-filter event-log

Description This command allows AA to treat traffic on UDP port number 2152 as GTP-u. Without further specifying any other parameters within this GTP context, AA performs basic GTP-u header sanity checks and discards packets that are malformed. This GTP context allows the operator to configure various GTP filters (maximum of 128 GTP filters).

Default no event-log

Parameters *event-log-name* — Specifies the event log name to be used to log discards due to GTP-u basic header sanity checks.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

event-log

Syntax **event-log** *event-log-name*
no event-log

Context **[Tree]** (config>app-assure>group>sctp-filter event-log)

Full Context configure application-assurance group sctp-filter event-log

Description This command configures an event log for packets dropped by the SCTP filter.

Default no event-log

Parameters *event-log-name* — Specifies the event log name to be used.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.177 event-mon

event-mon

Syntax **event-mon**

Context **[Tree]** (config>oam-pm>session>measurement-interval event-mon)

Full Context configure oam-pm session measurement-interval event-mon

Description This command enables the different threshold events on a specific measurement interval. Only one measurement interval with a configured OAM PM session can have events enabled using the **no shutdown** command.

9.178 event-notification

event-notification

Syntax [**no**] **event-notification**

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame event-notification)
[Tree] (config>port>ethernet>efm-oam>link-mon>errored-frame-period event-notification)
[Tree] (config>port>ethernet>efm-oam>link-mon>errored-frame-seconds event-notification)

Full Context configure port ethernet efm-oam link-monitoring errored-frame event-notification
configure port ethernet efm-oam link-monitoring errored-frame-period event-notification

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet efm-oam link-monitoring errored-frame-seconds event-notification

Description Allows the frame error **sf-threshold** crossing events to transmit the Event Notification OAMPDU with the specific Link Event TLV information. The Event Notification OAM PDU will only be generated when the initial **sf-threshold** is reached. No subsequent notification will be sent until the event that triggered until the event is manually cleared. The burst parameter under the **local-sf-action** will determine the number of Event Notification OAMPDUs to generate when the event occurs. The reception of the event notification will be processed regardless of this parameter.

The **no** version of this command will disable the transmission of the Event Notification OAMPDU for this event type.

Default event-notification

Platforms All

event-notification

Syntax [**no**] **event-notification**

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-symbols event-notification)

Full Context configure port ethernet efm-oam link-monitoring errored-symbols event-notification

Description This command allows the symbol error event threshold crossing actions to transmit the Event Notification OAM PDU with the specific Link Event TLV information. The Event Notification OAM PDU will only be generated on the initial sf-threshold is reached. No subsequent notification will be sent until the event that triggered the notification clears, through manual intervention or a window where the configured sd-threshold is not reached. The burst parameter under the local-sf-action will determine the number of Event Notification OAM PDUs to generate when the event occurs. The reception of the event notification will be processed regardless of this parameter.

The **no** version of this command will disable the transmission of the Event Notification OAM PDU for this event type.

Default event-notification

Platforms All

event-notification

Syntax **event-notification local-port-action** {**log-only** | **out-of-service**}

Context **[Tree]** (config>port>ethernet>efm-oam>peer-rdi-rx event-notification)

Full Context configure port ethernet efm-oam peer-rdi-rx event-notification

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines how to react to the reception of event TLVs contained in the Event Notification OAMPDU. The event TLVs contained in the event notification OAMPDU will be analyzed to determine if the peer has crossed the error threshold for the window. The analysis does not consider any local signal degrades or signal failure threshold. The analysis is based solely on the information receive form the peer. The analysis is performed on all event TLVs contained in the Event Notification OAMPDU without regard for support of a specific error counters or local configuration of any thresholds. In the case of symbol errors only, a threshold below the error rate can be used to return the port to service.

Default event-notification local-port-action log-only

Parameters **local-port-action** — Defines whether or not the local port will be affected when the Event Notification OAM PDU is received from a peer based on the threshold computation for the included TLVs.

log-only — Keyword that prevents the port from being affected when the local peer receives an Event Notification OAM PDU. The event will be logged but the port will remain operational.

out-of-service — Keyword that causes the port to enter a non-operation down state with a port state of link up. The error will be logged upon reception of Event Notification. The port will not be available to service data but will continue to carry Link OAM traffic to ensure the link is monitored. All this assumes the error threshold exceeds the error rate in the TLV.

Platforms All

9.179 event-notification-burst

event-notification-burst

Syntax **event-notification-burst** *packets*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>local-sf-action event-notification-burst)

Full Context configure port ethernet efm-oam link-monitoring local-sf-action event-notification-burst

Description This command defines the number of the Event Notification OAM PDU to be send to the peer if the local signal failure threshold (sf-threshold) has been reached. The sending of the Event Notification OAMPDU is configured under the individual monitors.

Interactions: The **sf-thresh** threshold will trigger these actions.

Parameters *packets* — Specifies the number of Event Notification OAM PDUs to send to a peer when the signal failure threshold has been reached.

Values 1 to 5

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.180 event-trigger

event-trigger

Syntax **event-trigger**

Context **[Tree]** (config>log event-trigger)

Full Context configure log event-trigger

Description Commands in this context configure log events as triggers for Event Handling System (EHS) handlers.

Platforms All

9.181 event-type

event-type

Syntax [**no**] **event-type** {**arp** | **config-change** | **oper-status-change** | **neighbor-discovery**}

Context **[Tree]** (debug>service>id>sap event-type)

Full Context debug service id sap event-type

Description This command enables a particular debugging event type.

The **no** form of this command disables the event type debugging.

Parameters **arp** — Displays ARP events.

config-change — Debugs configuration change events.

oper-status-change — Debugs service operational status changes.

neighbor-discovery — Displays the status of IPv6 neighbor discovery for the sap or the spoke-sdp for the 7450 ESS or 7750 SR only.

Output The following output is an example of event-type information.

Sample Output

```
A:bksim180# debug service id 1000 sap 1/7/1 event-type arp
DEBUG OUTPUT show on CLI is as follows:
3 2008/11/17 18:13:24.35 UTC MINOR: DEBUG #2001 Base Service 1000 SAP
1/7/1 "Service 1000 SAP 1/7/1:
RX: ARP_REQUEST (0x0001)
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
hwType      : 0x0001
prType      : 0x0800
hwLength    : 0x06
prLength    : 0x04
srcMac      : 8c:c7:01:07:00:03
destMac     : 00:00:00:00:00:00
srcIp       : 10.1.1.2
destIp      : 10.1.1.1
"

4 2008/11/17 18:13:24.35 UTC MINOR: DEBUG #2001 Base Service 1000
SAP 1/7/1 "Service 1000 SAP 1/7/1:
TX: ARP_RESPONSE (0x0002)
hwType      : 0x0001
prType      : 0x0800
hwLength    : 0x06
prLength    : 0x04
srcMac      : 00:03:0a:0a:0a:0a
destMac     : 8c:c7:01:07:00:03
srcIp       : 10.1.1.1
destIp      : 10.1.1.2
"
```

Platforms All

event-type

Syntax [**no**] **event-type** {**config-change** | **oper-status-change** | **neighbor-discovery** | **control-channel-status**}

Context **[Tree]** (debug>service>id>sdp event-type)

Full Context debug service id sdp event-type

Description This command enables a particular debugging event type.

The **no** form of this command disables the event type debugging.

Parameters **config-change** — Debugs configuration change events.

oper-status-change — Debugs service operational status changes.

neighbor-discovery — Displays the status of IPv6 neighbor discovery for the sap or the spoke-sdp for the 7450 ESS or 7750 SR only.

control-channel-status — Debugs control channel status events.

Platforms All

event-type

Syntax [**no**] **event-type** {**config-change** | **svc-oper-status-change** | **sap-oper-status-change** |

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sdpbind-oper-status-change}

Context [Tree] (debug>service>id event-type)

Full Context debug service id event-type

Description This command enables a particular debugging event type. The **no** form of this command disables the event type debugging.

Parameters **config-change** — Debugs configuration change events

svc-oper-status-change — Debugs service operational status changes

sap-oper-status-change — Debugs SAP operational status changes

sdpbind-oper-status-change — Debugs SDP operational status changes

Platforms All

9.182 events

events

Syntax **events** {**none** | **public-only** | **all**}

Context [Tree] (config>call-trace-trace-profile events)

Full Context configure call-trace trace-profile events

Description This command configures whether captured traces include events that occurred on the SR OS router, such as mobility and idle-timeout.

Default events none

Parameters **none** — Specifies that no events is traced.

public-only — Specifies that only events that are readable by everyone is traced.

all — Specifies that all events is traced, including events that are encrypted for use by customer support only. Encrypted events are not readable by end-users.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

events

Syntax [**no**] **events** [**interface** *ip-int-name*]

Context [Tree] (debug>router>srrp events)

Full Context debug router srrp events

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for SRRP packets.

The **no** form of this command disables debugging.

Platforms All

events

Syntax [**no**] **events**
[**no**] **events interface** *ip-int-name* [**vrid** *virtual-router-id*]
[**no**] **events interface** *ip-int-name* **vrid** *virtual-router-id* **ipv6**

Context **[Tree]** (debug>router>vrrp events)

Full Context debug router vrrp events

Description This command enables debugging for VRRP events.

The **no** form of the command disables debugging.

Parameters *ip-int-name* — Displays the specified interface name.

virtual-router-id — Displays the specified VRID.

ipv6 — Debugs the specified IPv6 VRRP interface.

Platforms All

events

Syntax **events** [**neighbor** *ip-address* | **group** *name*]
no events

Context **[Tree]** (debug>router>bgp events)

Full Context debug router bgp events

Description This command logs all events changing the state of a BGP peer.

The **no** form of this command disables the debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

events

Syntax **events** [**station** *station-name*]
no events

Context **[Tree]** (debug>router>bmp events)

Full Context debug router bmp events

Description This command enables debugging for all BMP events.

The **no** form of the command disables debugging for all BMP events.

Parameters *station-name* — Specifies the station name of the BMP monitoring station, up to 32 characters.

Platforms All

events

Syntax [**no**] **events** [**neighbor** *ip-int-name* | *ip-addr*]

Context **[Tree]** (debug>router>rip events)

Full Context debug router rip events

Description This command enables debugging for RIP events.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP events sent on the neighbor IP address or interface.

Platforms All

events

Syntax [**no**] **events** [**neighbor** *ip-int-name*]

Context **[Tree]** (debug>router>ripng events)

Full Context debug router ripng events

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for RIPng events.

Parameters *ip-int-name* — Debugs the RIPng events sent on the neighbor IP interface.

Platforms All

9.183 evi

evi

Syntax **evi** *value*
no evi

Context **[Tree]** (config>service>epipe>bgp-evpn evi)
[Tree] (config>service>vpls>bgp-evpn evi)

Full Context configure service epipe bgp-evpn evi
configure service vpls bgp-evpn evi

Description This command allows the configuration of a 2-byte EVPN instance (EVI) unique in the system. It is used for the service-carving algorithm for multi-homing and auto-deriving route target and route distinguishers.

If not specified, the value is zero and no route distinguisher or route targets are auto-derived from it. If the *evi* value is specified and no other **route-distinguisher** or **route-target** is configured in the service, the following rules apply:

- the route distinguisher is derived from <system_ip>:evi
- the route target is derived from <autonomous-system>:evi

If VSI import and export policies are configured, the route target must be configured in the policies and those values take preference over the auto-derived route targets. If **bgp-ad**>**vpls-id** and **bgp-evpn**>**evi** are both configured on the same service, the VPLS ID auto-derived route target or route distinguisher takes precedence over the values auto-derived from the EVI. The operational route target for a service is displayed in the **show service id bgp** command.

The **no** form of this command sets the EVI value back to zero.

Parameters *value* — Specifies the EVPN instance.

Values 1 to 16777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

evi

Syntax **evi** *start* [**to** *to*]
no evi *start*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>service-carving>manual evi)

Full Context configure service system bgp-evpn ethernet-segment service-carving manual evi

Description This command configures the EVI ranges for which the PE is the primary Designated Forwarder, or uses the lowest preference algorithm.

Note: Multiple individual EVI values and ranges are allowed.

There are two service-carving manual algorithms for DF election:

- manual non-preference

  A **preference** command is not configured for this algorithm. The primary PE for the configured EVIs is determined by the EVI range. The manual non-preference algorithm only supports two PEs in the Ethernet Segment
- manual preference-based

  If a **preference** command is configured, the algorithm uses the configured value to determine the DF election. For EVIs not defined in the range, the highest-preference algorithm is used. For configured EVIs, the lowest-preference algorithm is used.

The **no** form of this command removes the PE from the primary Designated Forwarder role for the range, or sets the preference algorithm back to highest preference.

Parameters *start* — Specifies the initial EVI value of the range.

Values 1 to 65535

to — Specifies the end EVI value of the range. If not configured, only the individual start value is considered.

Values 1 to 16777215

Platforms All

9.184 evi-three-byte-auto-rt

evi-three-byte-auto-rt

Syntax [**no**] **evi-three-byte-auto-rt**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>service>epipe>bgp-evpn>mpls evi-three-byte-auto-rt)
[Tree] (config>service>epipe>bgp-evpn>srv6 evi-three-byte-auto-rt)
[Tree] (config>service>epipe>bgp-evpn>vxlan evi-three-byte-auto-rt)
[Tree] (config>service>vpls>bgp-evpn>mpls evi-three-byte-auto-rt)
[Tree] (config>service>vpls>bgp-evpn>vxlan evi-three-byte-auto-rt)

Full Context
configure service epipe bgp-evpn mpls evi-three-byte-auto-rt
configure service epipe bgp-evpn segment-routing-v6 evi-three-byte-auto-rt
configure service epipe bgp-evpn vxlan evi-three-byte-auto-rt
configure service vpls bgp-evpn mpls evi-three-byte-auto-rt
configure service vpls bgp-evpn vxlan evi-three-byte-auto-rt

Description
This command specifies that the BGP-EVPN instance import and export route target is auto-derived as described in RFC 8365 (Global-Administrator:A/Type/D-ID/Service-ID).

Where:

- Global Administrator — is the configured 2-octet AS Number. If the configured ASN exceeds the 2 byte limit, the low order 16-bit value will be taken.
- A=0 (for auto-derivation)
- Type=4 (EVI-based route target)
- D-ID= [1..2] — encodes the BGP instance. This allows the auto-derivation of different route targets in multi-instance services. The value is inherited from the corresponding BGP instance.
- Service ID= 3-octet EVI

The **no** form of this command disallows the derivation of the route target.

Default
no evi-three-byte-auto-rt

Platforms
7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service epipe bgp-evpn segment-routing-v6 evi-three-byte-auto-rt

All

- configure service vpls bgp-evpn vxlan evi-three-byte-auto-rt
- configure service vpls bgp-evpn mpls evi-three-byte-auto-rt
- configure service epipe bgp-evpn mpls evi-three-byte-auto-rt
- configure service epipe bgp-evpn vxlan evi-three-byte-auto-rt

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.185 evpn

evpn

Syntax **evpn** *service-id* [**import-mode** *import-mode*] [**create**]
no evpn *service-id*

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain evpn)

Full Context configure subscriber-mgmt isa-service-chaining evpn

Description This command configures the import mode for the service chaining EVPN service. The **import-mode** controls the EPVN route types that are imported by the EVPN system.

The **no** form of this command removes the configuration parameters.

Parameters *service-id* — Specifies the service ID of the EVPN.

Values 1 to 2147483647

import-mode — Specifies the import mode of the EVPN.

Values bridged — The specified EVPN instance imports EVPN route type-2 and type-1 from the peer.

routed — The specified EVPN instance imports EVPN type-1, type-2 and type-5 routes from the peer. Also, the EVPN instance can be configured to export EVPN type-5 routes for NAT pools to the peer.

none — The specified EVPN instance does not import any EVPN routes from the peer but can be configured with NAT pools that are exported to the peer in EVPN type-5 routes.

create — Keyword used to create the EVPN service instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

evpn

Syntax **evpn send** *send-limit*
evpn send *send-limit* **receive** [**none**]
no evpn

Context **[Tree]** (config>router>bgp>add-paths evpn)
[Tree] (config>router>bgp>group>add-paths evpn)
[Tree] (config>router>bgp>group>neighbor>add-paths evpn)

Full Context configure router bgp add-paths evpn
configure router bgp group add-paths evpn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group neighbor add-paths evpn

Description This command configures the Add-Paths capability for EVPN routes.

The **no** form of this command disables Add-Paths support for EVPN routes. This causes sessions that are established using Add-Paths for EVPN to go down and come back up without the Add-Paths capability.

Default no evpn

Parameters *send-limit* — Specifies the maximum number of EVPN paths to send.

Values 1 to 16, none, multipaths

receive — Keyword used to allow multiple EVPN paths per prefix from a peer.

none — Keyword used to specify that the router does not negotiate to receive multiple unlabeled unicast routes per EVPN prefix.

Platforms All

evpn

Syntax **evpn**

Context **[Tree]** (config>service>ies>if>vpls evpn)
[Tree] (config>service>vprn>if>vpls evpn)

Full Context configure service ies interface vpls evpn
configure service vprn interface vpls evpn

Description Commands in this context configure EVPN parameters.

Platforms All

evpn

Syntax [**no**] **evpn**

Context **[Tree]** (config>router>ldp>import-pmsi-routes evpn)

Full Context configure router ldp import-pmsi-routes evpn

Description This command specifies that the SR OS is to cache inter-as EVPN PMSI AD routes for option B.

The **no** form of this command disables caching of EVPN PMSI AD routes. The default is disabled, however when an upgrade from a software load that does not supports this command is performed, this command will be enabled after the upgrade.

This command is not enabled if the user is using an older configuration file.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no evpn

9.186 evpn-etree-leaf-label

evpn-etree-leaf-label

Syntax **evpn-etree-leaf-label** [[*32..524256*]]
no evpn-etree-leaf-label

Context **[Tree]** (config>service>system>bgp-evpn evpn-etree-leaf-label)

Full Context configure service system bgp-evpn evpn-etree-leaf-label

Description This command enables EVPN Ethernet-Tree (E-Tree) VPLS services on the router (not B-VPLS). It allocates an E-Tree leaf label for the Provider Edge (PE) device and configures the ILM entry.

The command ensures that in-flight traffic can perform an ILM entry lookup at any time, and avoid the discards during **shutdown** or **no shutdown** services (or at least reduce the timing window so that it does not occur during normal operation or configuration).

The E-Tree leaf label can optionally be statically configured with a value. The label value must be in the static label range of the system.

Note: The **evpn-etree-leaf-label** command must be configured to execute **bgp-evpn mpls no shutdown**.

The **no** form of this command removes the value from the configuration.

Default no evpn-etree-leaf-label

Parameters *32..524256* — Specifies the E-Tree leaf label

Values 32 to 524256

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.187 evpn-mcast-gateway

evpn-mcast-gateway

Syntax **evpn-mcast-gateway** [**create**]
no evpn-mcast-gateway

Context **[Tree]** (config>service>vpls>bind evpn-mcast-gateway)

Full Context configure service vpls allow-ip-int-bind evpn-mcast-gateway

Description Commands in this context configure the EVPN multicast gateway.

The **no** form of this command sets the PE back to a non-EVPN multicast gateway.

Parameters **create** — Keyword used to create an EVPN multicast gateway.

Platforms All

9.188 evpn-mpls

evpn-mpls

Syntax [**no**] **evpn-mpls**

Context **[Tree]** (debug>service>id>igmp-snooping evpn-mpls)

Full Context debug service id igmp-snooping evpn-mpls

Description This command shows IGMP packets for EVPN-MPLS destinations. The **no** form of this command disables the debugging for EVPN-MPLS destinations

Platforms All

9.189 evpn-nd-advertise

evpn-nd-advertise

Syntax **evpn-nd-advertise** {**host** | **router**}

Context **[Tree]** (config>service>vpls>proxy-nd evpn-nd-advertise)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls proxy-nd evpn-nd-advertise

Description This command enables the advertisement of static or dynamic entries that are learned as host or routers (only one option is possible in a specified service), and determines the R flag (host or router) when sending Neighbor Advertisement (NA) messages for existing EVPN entries in the proxy-ND table.

This command cannot be modified without **proxy-nd** *shutdown*.

Default evpn-nd-advertise router

Parameters **host** — Enables the advertisement of static or dynamic entries that are learned as host.

router — Enables the advertisement of static or dynamic entries that are learned as routers.

Platforms All

9.190 evpn-proxy

evpn-proxy

Syntax [**no**] **evpn-proxy**

Context **[Tree]** (config>service>vpls>igmp-snooping evpn-proxy)
[Tree] (config>service>vpls>mld-snooping evpn-proxy)

Full Context configure service vpls igmp-snooping evpn-proxy
configure service vpls mld-snooping evpn-proxy

Description This command enables EVPN proxy for IGMP and MLD snooping.

This **no** form of this command disables EVPN proxy for IGMP and MLD snooping.

Platforms All

9.191 evpn-route-tag

evpn-route-tag

Syntax **evpn-route-tag** *tag*
no evpn-route-tag

Context **[Tree]** (config>service>vpls>proxy-arp evpn-route-tag)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>proxy-nd evpn-route-tag)

Full Context configure service vpls proxy-arp evpn-route-tag
configure service vpls proxy-nd evpn-route-tag

Description This command configures a local route tag that can be used on export policies to match MAC/IP routes generated by the proxy-ARP or proxy-ND module. For example, if a new active dynamic proxy-ARP entry is added to the proxy-ARP table and **evpn-route-tag** is 10, an export policy that matches on tag 10 and adds a site-of-origin community SOO-1, allows the router to advertise the MAC/IP route for the proxy-ARP entry with community SOO-1.

The **no** form of this command removes the route tag for the generated EVPN MAC/IP routes.

Parameters *tag* — Specifies the route tag, in either decimal or hexadecimal form.

Values 1 to 255

Platforms All

9.192 evpn-tunnel

evpn-tunnel

Syntax **evpn-tunnel** [**ipv6-gateway-address** {**ip** | **mac**}] [**supplementary-broadcast-domain**]
no evpn-tunnel

Context [Tree] (config>service>vprn>if>vpls evpn-tunnel)

Full Context configure service vprn interface vpls evpn-tunnel

Description This command sets the evpn-tunnel mode for the attached R-VPLS. When enabled for an IPv4 interface, no IPv4 address is required under the same interface. When enabled on an IPv6 interface, the **ipv6-gateway-address** parameter can be configured as **ip** or **mac**.

When configured as **evpn-tunnel ipv6-gateway-address ip** or simply **evpn-tunnel**, then:

- on transmission, the router populates the GW IP field of the route type 5 with a Link-Local-Address (LLA) if an explicit global IPv6 address is not configured. Otherwise, the configured IPv6 address is used.
- on reception of routes type 5 for IPv6 prefixes, only routes with non-zero GW IP are processed; the rest of the routes will be **treated-as-withdraw**.

When configured as **evpn-tunnel ipv6-gateway-address mac,** then:

- on transmission, the router sends routes type 5 with zero GW IP field, and a MAC extended community of the router, containing the VPRN interface MAC.
- on reception of IPv6 prefix routes, only routes with zero GW IP and non-zero router's MAC are processed; the rest of the routes will be **treated-as-withdraw**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **supplementary-broadcast-domain** option instructs the data path to exclude EVPN destinations in the Layer 3 lookup for packets coming from an RVPLS SAP and configures the entire set of VPRN as well as attached RVPLS services in OISM mode. Only one SBD RVPLS can exist in a given VPRN. In order to add or remove the **supplementary-broadcast-domain** option, the entire **evpn-tunnel** command must first be removed.

The configuration of **evpn-tunnel** without options is equivalent to the **ipv6-gateway-address ip** option.

The **no** form of this command disables the evpn-tunnel mode.

Default no evpn-tunnel

Parameters **ipv6-gateway-address** — Indicates whether the IPv6 Prefix route uses a GW IP or a GW MAC as gateway.

Values **ip, mac**

supplementary-broadcast-domain — Specifies to use the EVPN tunnel as a Supplementary Broadcast Domain (SBD). The SBD is used in EVPN OISM to advertise the SMET routes and receive the multicast traffic on egress PEs that are not attached to the source R-VPLS service.

Platforms All

9.193 evpn-type

evpn-type

Syntax **evpn-type** *type*
no evpn-type

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from evpn-type)

Full Context configure router policy-options policy-statement entry from evpn-type

Description This command matches BGP routes based on the EVPN route type. The route types supported in SR OS are the following:

- Type 1 or Auto-Discovery Ethernet Tag route, including both the AD per-ES and AD per-EVI routes Type 2 or MAC/IP route
- Type 2 or MAC/IP route
- Type 3 or IMET route, including Multicast Ethernet Tag
- Type 4 or ES (Ethernet Segment) routeType 5 of IP-prefix route, including IPv4 and IPv6 prefixes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Type 6 or Selective Multicast Ethernet Tag route, including IPv4 and IPv6 multicast groups
- Type 7 or Multicast Join Synch route, including IPv4 and IPv6 multicast group
- Type 8 or Multicast Leave Synch route, including IPv4 and IPv6 multicast groups

The **no** form of this command removes the **evpn-type** matching.

Parameters *name* — Specifies the EVPN route type.

Values 1 to 8

Platforms All

9.194 exceed

exceed

Syntax **exceed**

Context **[Tree]** (config>qos>sap-egress>queue>drop-tail exceed)

Full Context configure qos sap-egress queue drop-tail exceed

Description Commands in this context configure the queue exceed drop tail parameters. The exceed drop tail defines the queue depth beyond which exceed-profile packets will not be accepted into the queue and will be discarded.

Platforms All

exceed

Syntax **exceed**

Context **[Tree]** (cfg>qos>qgrps>egr>qgrp>queue>drop-tail exceed)

Full Context configure qos queue-group-templates egress queue-group queue drop-tail exceed

Description Commands in this context configure the queue exceed drop-tail parameters. The exceed drop tail defines the queue depth beyond which exceed-profile packets will not be accepted into the queue and will be discarded.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.195 exceed-action

exceed-action

Syntax **exceed-action** {**discard** | **low-priority** | **none**}

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>local-monitoring-policer exceed-action)

Full Context configure system security dist-cpu-protection policy local-monitoring-policer exceed-action

Description This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.

Default exceed-action none

Parameters **discard** — Discards packets that are nonconforming.

low-priority — Marks packets that are nonconforming as low-priority (discard eligible or out-profile). If there is congestion in the control plane of the SR OS then unmarked (green, hi-prio or in-profile) control packets are given preferential treatment.

none — no hold-down

Platforms All

exceed-action

Syntax **exceed-action** {**discard** [**hold-down** *seconds*] | **low-priority** [**hold-down** *seconds*] | **none**}

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>protocol>dynamic-parameters exceed-action)
[Tree] (config>sys>security>dist-cpu-protection>policy>static-policer exceed-action)

Full Context configure system security dist-cpu-protection policy protocol dynamic-parameters exceed-action
configure system security dist-cpu-protection policy static-policer exceed-action

Description This command controls the action performed upon the extracted control packets when the configured policer rates are exceeded.

Default exceed-action none

Parameters **discard** — Discards packets that are nonconforming.

low-priority — Marks packets that are nonconforming as low-priority (for example, discard eligible or out-profile). If there is congestion in the control plane of the SR OS then unmarked (for example, green, hi-prio or in-profile) control packets are given preferential treatment.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hold-down *seconds* — When this optional parameter is specified, it causes the following "hold-down" behavior.

When the SR OS software detects that an enforcement policer has marked or discarded one or more packets (software may detect this some time after the packets are actually discarded), and an optional **hold-down** *seconds* value has been specified for the **exceed-action**, then the policer will be set into a "mark-all" or "drop-all" mode that cause the following:

- the policer state to be updated as normal
- all packets to be marked (if the action is "low-priority") or dropped (action = discard) regardless of the results of the policing decisions/actions/state.

The **hold-down** is cleared after approximately the configured time in seconds after it was set. The **hold-down** *seconds* option should be selected for protocols that receive more than one packet in a complete handshake/negotiation (for example, DHCP, PPP). **hold-down** is not applicable to a local monitoring policer. The "detection-time" will only start after any **hold-down** is complete. During the **hold-down** (and the detection-time), the policer is considered as in an "exceed" state. The policer may re-enter the hold-down state if an exceed packet is detected during the detection-time countdown.

Configuring the **indefinite** parameter value will cause hold down to remain in place until the operator clears it manually using a tools command (**tools perform security dist-cpu-protection release-hold-down**) or removes the dist-cpu-protection policy from the object.

Configuring the **none** parameter value will disable hold down.

Values 1 to 10080, indefinite, none

Platforms All

9.196 exceed-profile-octets-discarded-count

exceed-profile-octets-discarded-count

Syntax [**no**] **exceed-profile-octets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters exceed-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters exceed-profile-octets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters exceed-profile-octets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters exceed-profile-octets-discarded-count

Description This command includes the exceed profile octets discarded count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command excludes the exceed profile octets discarded count.

Default no exceed-profile-octets-discarded-count

Platforms All

9.197 exceed-profile-octets-forwarded-count

exceed-profile-octets-forwarded-count

Syntax [**no**] **exceed-profile-octets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters exceed-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters exceed-profile-octets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters exceed-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters exceed-profile-octets-forwarded-count

Description This command includes the exceed profile octets forwarded count.

The **no** form of this command excludes the exceed profile octets forwarded count.

Default no exceed-profile-octets-forwarded-count

Platforms All

9.198 exceed-profile-octets-offered-count

exceed-profile-octets-offered-count

Syntax [**no**] **exceed-profile-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters exceed-profile-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters exceed-profile-octets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters exceed-profile-octets-offered-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log accounting-policy custom-record ref-policer e-counters exceed-profile-octets-offered-count

Description This command includes the exceed profile octets offered count.

The **no** form of this command excludes the exceed profile octets offered count.

Default no exceed-profile-octets-offered-count

Platforms All

9.199 exceed-profile-packets-discarded-count

exceed-profile-packets-discarded-count

Syntax [**no**] **exceed-profile-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters exceed-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters exceed-profile-packets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters exceed-profile-packets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters exceed-profile-packets-discarded-count

Description This command includes the exceed profile packets discarded count.

The **no** form of this command excludes the exceed profile packets discarded count.

Default no exceed-profile-packets-discarded-count

Platforms All

9.200 exceed-profile-packets-forwarded-count

exceed-profile-packets-forwarded-count

Syntax [**no**] **exceed-profile-packets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters exceed-profile-packets-forwarded-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>log>acct-policy>cr>ref-policer>e-counters exceed-profile-packets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters exceed-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters exceed-profile-packets-forwarded-count

Description This command includes the exceed profile packets forwarded count.

The **no** form of this command excludes the exceed profile packets forwarded count.

Default no exceed-profile-packets-forwarded-count

Platforms All

9.201 exceed-profile-packets-offered-count

exceed-profile-packets-offered-count

Syntax [**no**] **exceed-profile-packets-offered-count**

Context [Tree] (config>log>acct-policy>cr>policer>e-counters exceed-profile-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters exceed-profile-packets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters exceed-profile-packets-offered-count
configure log accounting-policy custom-record ref-policer e-counters exceed-profile-packets-offered-count

Description This command includes the exceed profile packets offered count.

The **no** form of this command excludes the exceed profile packets offered count.

Default no exceed-profile-packets-offered-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.202 exceed-slope

exceed-slope

Syntax [**no**] **exceed-slope**

Context **[Tree]** (config>qos>slope-policy exceed-slope)

Full Context configure qos slope-policy exceed-slope

Description The **exceed-slope** context contains the commands and parameters for defining the exceed Random Early Detection (RED) slope graph. Each egress buffer pool supports an exceed RED slope for managing access to the shared portion of the buffer pool for exceed-profile packets.

The **exceed-slope** parameters can be changed at any time and the affected buffer pool exceed RED slopes are adjusted appropriately.

The **no** form of this command restores the exceed slope configuration commands to the default values. If the leaf commands within **exceed-slope** are set to the default parameters, the **exceed-slope** node will not appear in save config and show config output unless the detail parameter is present.

Platforms All

9.203 exception

exception

Syntax [**no**] **exception**

Context **[Tree]** (debug>service>id>stp exception)

Full Context debug service id stp exception

Description This command enables STP debugging for exceptions.

The **no** form of the command disables debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.204 exclude

exclude

Syntax **exclude**

Context **[Tree]** (config>service>vprn>isis>loopfree-alternates exclude)

Full Context configure service vprn isis loopfree-alternates exclude

Description This command excludes from LFA SPF calculation prefixes that match a prefix entry or a tag entry in a prefix policy.

The user can exclude an interface in IS-IS or OSPF, an OSPF area, or an IS-IS level from the LFA SPF.

If a prefix is excluded from LFA, then it will not be included in LFA calculation regardless of its priority. The prefix tag will, however, be used in the main SPF.

Note: Prefix tags are defined for the IS-IS protocol but not for the OSPF protocol.

The default action of the **exclude** command, when not explicitly specified by the user in the prefix policy, is a “reject”. Thus, regardless of whether the user has explicitly added the statement “default-action reject” to the prefix policy, a prefix that does not match any entry in the policy is accepted into LFA SPF.

The **no** form of this command deletes the exclude prefix policy.

Default no exclude

Platforms All

exclude

Syntax **exclude**

Context **[Tree]** (config>service>vprn>ospf>loopfree-alternates exclude)
[Tree] (config>service>vprn>ospf3>loopfree-alternates exclude)

Full Context configure service vprn ospf loopfree-alternates exclude
configure service vprn ospf3 loopfree-alternates exclude

Description This command excludes from LFA SPF calculation prefixes that match a prefix entry or a tag entry in a prefix policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The implementation already allows the user to exclude an interface in IS-IS or OSPF, an OSPF area, or an IS-IS level from the LFA SPF.

If a prefix is excluded from LFA, then it will not be included in LFA calculation regardless of its priority. The prefix tag will, however, be used in the main SPF.

Note: Prefix tags are defined for the IS-IS protocol but not for the OSPF protocol.

The default action of the **exclude** command, when not explicitly specified by the user in the prefix policy, is a “reject”. Thus, regardless if the user did or did not explicitly add the statement “default-action reject” to the prefix policy, a prefix that did not match any entry in the policy will be accepted into LFA SPF.

The **no** form of this command deletes the exclude prefix policy.

Default no exclude

Platforms All

exclude

Syntax **exclude** *group-name* [*group-name*]
no exclude [*group-name* [*group-name*]]

Context **[Tree]** (config>router>mpls>lsp exclude)
[Tree] (config>router>mpls>lsp-template exclude)
[Tree] (config>router>mpls>lsp>primary exclude)
[Tree] (config>router>mpls>lsp>primary-p2mp-instance exclude)
[Tree] (config>router>mpls>lsp>secondary exclude)

Full Context configure router mpls lsp exclude
configure router mpls lsp primary exclude
configure router mpls lsp primary-p2mp-instance exclude
configure router mpls lsp secondary exclude
configure router mpls lsp-template exclude

Description This command specifies the admin groups to be excluded when an LSP is set up. Up to five groups per operation can be specified, up to 32 maximum. The admin groups are defined in the **config>router>if-attribute>admin-group** context.

The config>router>mpls>lsp>primary-p2mp-instance>exclude command is not supported on the 7450 ESS.

Use the **no** form of this command to remove the exclude command.

Default no exclude

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-name* — Specifies the existing group-name to be excluded when an LSP is set up.

Platforms All

exclude

Syntax [**no**] **exclude** *tag*

Context **[Tree]** (config>router>admin-tags>route-admin-tag-policy exclude)

Full Context configure router admin-tags route-admin-tag-policy exclude

Description This configures an admin tag to be excluded when matching a route against an LSP.

Up to eight exclusion statements are supported per policy.

The **no** form of this command removes the admin tag from the exclude statement.

Parameters *tag* — Specifies the value of the admin tag, up to 32 characters.

Platforms All

exclude

Syntax **exclude**

Context **[Tree]** (config>router>fad>flex-algo exclude)

Full Context configure router flexible-algorithm-definitions flex-algo exclude

Description Commands in this context configure administrative groups that will be excluded from the flexible algorithm topology graph.

If the defined FAD includes administrative groups link in its exclude list, the specified links are excluded from the topology graph.

Platforms All

exclude

Syntax **exclude**

Context **[Tree]** (config>router>isis>loopfree-alternates exclude)

Full Context configure router isis loopfree-alternates exclude

Description Commands in this context configure a prefix policy for excluding specific prefixes in the LFA calculation by ISIS or OSPF.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

exclude

Syntax **exclude**

Context **[Tree]** (config>router>ospf>loopfree-alternates exclude)
[Tree] (config>router>ospf3>loopfree-alternates exclude)

Full Context configure router ospf loopfree-alternates exclude
configure router ospf3 loopfree-alternates exclude

Description Commands in this context configure a prefix policy for excluding specific prefixes in the LFA calculation by ISIS or OSPF.

Platforms All

9.205 exclude-addresses

exclude-addresses

Syntax [**no**] **exclude-addresses** *start-ip-address* [*end-ip-address*]

Context **[Tree]** (config>router>dhcp>server>pool>subnet exclude-addresses)
[Tree] (config>service>vprn>dhcp>server>pool>subnet exclude-addresses)

Full Context configure router dhcp local-dhcp-server pool subnet exclude-addresses
configure service vprn dhcp local-dhcp-server pool subnet exclude-addresses

Description This command specifies a range of IP addresses that excluded from the pool of IP addresses in this subnet.

The **no** form of the removes the parameters from the configuration.

Parameters *start-ip-address* — Specifies the start address of this range to exclude. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

end-ip-address — Specifies the end address of this range to exclude. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.206 exclude-avps

exclude-avps

Syntax **exclude-avps** [**calling-number**] [**initial-rx-lcp-conf-req**]
no exclude-avps

Context **[Tree]** (config>router>l2tp exclude-avps)
[Tree] (config>service>vprn>l2tp exclude-avps)

Full Context configure router l2tp exclude-avps
configure service vprn l2tp exclude-avps

Description This command configures the L2TP AVPs to exclude.

Default no exclude-avps

Parameters **calling-number** — Specifies to exclude the AVP calling-number.

initial-rx-lcp-conf-req — Specifies to exclude the AVP initial-rx-lcp-conf-req.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.207 exclude-from-avg

exclude-from-avg

Syntax **exclude-from-avg** {**forward** | **backward** | **round-trip**} **bins** *bin-numbers*
no exclude-from-avg (**forward** | **backward** | **round-trip**}

Context **[Tree]** (config>oam-pm>bin-group>bin-type exclude-from-avg)

Full Context configure oam-pm bin-group bin-type exclude-from-avg

Description This optional command allows the results from probes that map to the specified bins within the bin type to be excluded from the average calculation. Individual counters are incremented in the bin, but the average is not affected by the value of the excluded delay metric for the individual probes in this bin. The bin group does not allow this command to be added, modified, or deleted when a test is actively referencing the bin group. Sessions that reference the bin group must have the bin group and tests shut down before changes can be made.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the exclusion, and all bins are included in the average calculation.

Default no exclude-from-avg forward

no exclude-from-avg backward

no exclude-from-avg round-trip

Parameters **forward** — Specifies the forward direction bin.

backward — Specifies the backward direction bin.

round-trip — Specifies the round-trip direction bin.

bin-numbers — Specifies the bin numbers to be excluded from the average calculation. The values typically represent, but are not restricted to, the highest and lowest configured bins in order to eliminate outlying results that are not representative of network performance.

A hyphen can be entered between bin numbers to include a continuous sequence of bins; for example, entering 7-9 would specify bins 7, 8, and 9. Commas can be entered between bin numbers to include separate or non-continuous bins; for example, entering 0,8,9 would specify bins 0, 8, and 9. Both hyphens and commas can be used in this manner in the same configuration; for example, entering 0,7-9 would include bins 0, 7, 8, and 9. All bin numbers specified as part of this command must be configured. If a specified bin does not exist, the command fails.

Values 0 to 9

Platforms All

9.208 exclude-group

exclude-group

Syntax [**no**] **exclude-group** *ip-admin-group-name*

Context **[Tree]** (config>router>route-next-hop-policy>template exclude-group)

Full Context configure router route-next-hop-policy template exclude-group

Description This command configures the admin group constraint into the route next-hop policy template.

Each group is entered individually. The **include-group** statement instructs the LFA SPF selection algorithm to pick up a subset of LFA next-hops among the links that belong to one or more of the specified admin groups. A link that does not belong to at least one of the admin-groups is excluded. However, a link can still be selected if it belongs to one of the groups in an include-group statement but also belongs to other groups that are not part of any include-group statement in the route next-hop policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **pref** option is used to provide a relative preference for the admin group to select. A lower preference value means that LFA SPF will first attempt to select an LFA backup next-hop that is a member of the corresponding admin group. If none is found, then the admin group with the next highest preference value is evaluated. If no preference is configured for a given admin group name, then it is supposed to be the least preferred, that is, numerically the highest preference value.

When evaluating multiple **include-group** statements within the same preference, any link that belongs to one or more of the included admin groups can be selected as an LFA next-hop. There is no relative preference based on how many of those included admin groups the link is a member of.

The **exclude-group** statement simply prunes all links belonging to the specified admin group before making the LFA backup next-hop selection for a prefix.

If the same group name is part of both include and exclude statements, the exclude statement will win. It other words, the exclude statement can be viewed as having an implicit preference value of zero (0).

The admin-group criteria are applied before running the LFA next-hop selection algorithm.

The **no** form deletes the admin group constraint from the route next-hop policy template.

Parameters *ip-admin-group-name* — Specifies the name of the group, up to 32 characters.

Platforms All

9.209 exclude-mac-policy

exclude-mac-policy

Syntax **exclude-mac-policy** *mac-policy-id*
no exclude-mac-policy

Context **[Tree]** (config>port>ethernet>dot1x>macsec exclude-mac-policy)

Full Context configure port ethernet dot1x macsec exclude-mac-policy

Description This command specifies the MAC policy to be excluded from MACsec encryption.

The **no** form of this command removes the policy from the MACsec and allows all destination MAC addresses.

Default no exclude-mac-policy

Parameters *mac-policy-id* — Specifies the MAC policy to exclude from the configuration.

Values 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

9.210 exclude-node

exclude-node

Syntax **exclude-node** *ip-address*
no exclude-node

Context **[Tree]** (config>router>mpls>lsp exclude-node)

Full Context configure router mpls lsp exclude-node

Description This command enables the option to include XRO object in the bypass LSP PATH message object. The exclude-node option is required for manual bypass LSP with XRO to FRR protect ABR node in a multi-vendor network deployment. This command must be configured on the PLR node that protects the ABR node. The ABR node IP address must be configured as exclude-node.

Default no exclude-node

Platforms All

9.211 exclude-prefix

exclude-prefix

Syntax [**no**] **exclude-prefix** *ipv6-prefix/prefix-length*

Context **[Tree]** (config>router>dhcp6>server>pool exclude-prefix)
[Tree] (config>service>vprn>dhcp6>server>pool exclude-prefix)

Full Context configure router dhcp6 local-dhcp-server pool exclude-prefix
configure service vprn dhcp6 local-dhcp-server pool exclude-prefix

Description This command defines a prefix that to be excluded from available prefix in the pool for DHCP6. The typical use case is to exclude the interface address.

- A held lease is deleted if it got excluded by an exclude prefix.
- An exclude range can never exclude only a part of an existing lease. If for example a /63 PD is assigned, an exclude of /64 which belongs to this /63 cannot be configured.
- A single exclude prefix can never exclude a whole include prefix.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- When applying or removing an exclude prefix, the threshold stats are adjusted to reflect the actual address space and its usage.

The **no** form of this command removes the prefix that is to be excluded from available prefix in the pool.

Parameters *ipv6-prefix/prefix-length* — Specifies an IPv6 prefix and prefix length.

Values

ipv6-prefix	x:x:x:x:x:x:x:x	(eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D
	prefix-length	0 to 128

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.212 exclude-protocol

exclude-protocol

Syntax [**no**] **exclude-protocol** {*protocol-name*}

Context **[Tree]** (config>port>ethernet>dot1x>macsec exclude-protocol)

Full Context configure port ethernet dot1x macsec exclude-protocol

Description Specifies protocols whose packets are not secured using Media Access Control Security (MACsec) when MACsec is enabled on a port.

When this option is enabled in a connectivity association that is attached to an interface, MACsec is not enabled for all packets of the specified protocols that are sent and received on the link.

When this option is enabled on a port where MACsec is configured, packets of the specified protocols will be sent and accepted in clear text.

Default no exclude-protocol

Parameters *protocol-name* — Specifies the protocol name.

Values **cdp**, **lacp**, **lldp**, **eapol-start**, **efm-oam**, **eth-cfm**, **ptp**, or **ubfd**

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.213 exclude-srlg

exclude-srlg

Syntax **exclude-srlg** *group-name* [*group-name*]
no exclude-srlg [*group-name* [*group-name*]]

Context **[Tree]** (config>router>gmpls>lsp>working-path exclude-srlg)
[Tree] (config>router>gmpls>lsp>protect-path exclude-srlg)

Full Context configure router gmpls lsp protect-path exclude-srlg
configure router gmpls lsp working-path exclude-srlg

Description This command specifies a list of one to five SRLG groups in the optical network which the router can request to the UNI-N that the GMPLS LSP path should avoid by signaling it in the XRO of the RSVP path message. Each *group-name* must have been defined under **config>router>if-attribute>srlg-group**.

The **no** form of the command removes the list of SRLG groups to exclude.

Parameters *group-name* — Specifies the name of the SRLG. Up to 5 groups names can be specified.

Values 32 characters maximum text string

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

9.214 exclude-tcp-retrans

exclude-tcp-retrans

Syntax [**no**] **exclude-tcp-retrans**

Context **[Tree]** (config>app-assure>group>statistics>aa-sub exclude-tcp-retrans)

Full Context configure application-assurance group statistics aa-sub exclude-tcp-retrans

Description This command is to only to EPC. When enabled, TCP errors and retransmission packets are not counted for the purpose of CBC. This setting has no impact on app/app-group aggregate AA stats.

Default no exclude-tcp-retrans

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.215 exclusive-lock-time

exclusive-lock-time

Syntax **exclusive-lock-time** *seconds*
no exclusive-lock

Context **[Tree]** (config>router>policy-options exclusive-lock-time)

Full Context configure router policy-options exclusive-lock-time

Description This command specifies the inactivity timer for the exclusive lock time for policy editing. When a session is idle for greater than this time, the lock is removed and the configuration changes is aborted.

Default exclusive-lock-time 300

Parameters *seconds* — Specifies the duration the session with exclusive lock may be inactive.

Values Values: 1 to 3600

Platforms All

9.216 exec

exec

Syntax **exec** [**-echo**] [**-syntax**] {*file-name* | *eof-marker-string*} [**-argument** [*256 chars max*] [[*256 chars max*]]

Context **[Tree]** (global exec)

Full Context global exec

Description This command executes the contents of a text file as if they were CLI commands entered at the console.

exec commands do not have **no** versions.

Related Commands:

boot-bad-exec: Use this command to configure a URL for a CLI script to exec following a failed configuration boot.

boot-good-exec: Use this command to configure a URL for a CLI script to exec following a successful configuration boot.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

stdin can be used as the source of commands for the **exec** command. When **stdin** is used as the **exec** command input, the command list is terminated with <Ctrl-C>, “EOF<Return>” or “*eof_string*<Return>”.

If an error occurs entering an exec file sourced from stdin, all commands after the command returning the error will be silently ignored. The **exec** command will indicate the command error line number when the stdin input is terminated with an end-of-file input.

Example:

Assume the *test.cfg* file has the following commands:

echo $(1)

echo $(2)

echo $(3)

Enter the following command:

exec test.cfg –arguments 10 20 30

The output from this command will be:

```
10
20
30
```

Parameters **-echo** — Echoes the contents of the **exec** file to the session screen as it executes.

Default echo disabled

-syntax — Performs a syntax check of the file without executing the commands. Syntax checking will be able to find invalid commands and keywords, but it will not be able to validate erroneous user- supplied parameters.

Default execute file commands

file-name — Specifies the text file with CLI commands to execute, up to 256 characters.

eof-marker-string — Specifies the ASCII printable string used to indicate the end of the exec file when stdin is used as the exec file source. <Ctrl-C> and “EOF” can always be used to terminate an exec file sourced from stdin up to 254 characters.

Default EOF

-argument — Specifies up to five arguments, each up to 256 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.217 executed-cmd

executed-cmd

Syntax [**no**] **executed-cmd**

Context **[Tree]** (debug>dynsvc>scripts>event executed-cmd)
[Tree] (debug>dynsvc>scripts>inst>event executed-cmd)
[Tree] (debug>dynsvc>scripts>script>event executed-cmd)

Full Context debug dynamic-services scripts event executed-cmd
debug dynamic-services scripts instance event executed-cmd
debug dynamic-services scripts script event executed-cmd

Description This command enables/disables the generation of a specific dynamic data service script debugging event output: executed-cmd.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

executed-cmd

Syntax [**no**] **executed-cmd**

Context **[Tree]** (debug>vsd>scripts>event executed-cmd)
[Tree] (debug>vsd>scripts>instance executed-cmd)

Full Context debug vsd scripts event executed-cmd
debug vsd scripts instance executed-cmd

Description This command enables/disables the generation of a specific script debugging event output: **execute-cmd**.

Platforms All

9.218 exhausted-credit-service-level

exhausted-credit-service-level

Syntax [**no**] **exhausted-credit-service-level**

Context **[Tree]** (config>subscr-mgmt>cat-map>category exhausted-credit-service-level)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the exhausted credit service level.

The **no** form of this command reverts to the default.

Default exhausted-credit-service-level

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.219 exit

exit

Syntax **exit** [**all**]

Context **[Tree]** (global exit)

Full Context global exit

Description This command returns to the context from which the current level was entered. For example, to navigate to the current level on a context by context basis, then the **exit** command only moves the cursor back one level.

```
A:ALA-1# configure
A:ALA-1>config# router
A:ALA-1>config>router# ospf
A:ALA-1>config>router>ospf# exit
A:ALA-1>config>router# exit
A:ALA-1>config# exit
```

When navigating to the current level by entering a command string, the **exit** command returns the cursor to the context in which the command was initially entered.

```
A:ALA-1# configure router ospf
A:ALA-1>config>router>ospf# exit
A:ALA-1#
```

The **exit all** command moves the cursor all the way back to the root level.

```
A:ALA-1# configure
A:ALA-1>config# router
A:ALA-1>config>router# ospf
A:ALA-1>config>router>ospf# exit all
A:ALA-1#
```

Parameters **all** — Exits back to the root CLI context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.220 expected

expected

Syntax **expected auto-generated**
expected bytes *byte-string* [*byte-string* (up to 64 bytes-strings max, 64 bytes max)]
expected string *identifier*
expected use-rx

Context **[Tree]** (config>port>otu>pm-tti expected)

Full Context configure port otu pm-tti expected

Description This command allows the user to configure the expected RX trail trace identifier (TTI) for path monitoring (PM) in the ODU overhead. This identifier can be a string or a non-printable sequence of bytes. The length of the string or sequence of bytes cannot exceed 64 bytes. This trace should match the far-end port's PM trace. When this trace does not match the received PM trace, the ODU-TIM alarm will be reported if enabled.

Default Blank (all zeros)

Parameters **auto-generated** — Sets the default.

identifier — Sets the PM TTI to the string provided by the user. If the string is less than 64 bytes, the remaining bytes will be set to 0. Up to 64 byte strings can be specified in a single statement.

byte-string — [byte1 byte2 to byte64]. Sets the PM TTI to the sequence of bytes provided by the user. If the user provides less than 64 bytes, the remaining bytes will be set to 0.

use-rx — Copies the received pm-tti to the expected either as a string or a sequence of bytes depending on the received pm-tti data.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

expected

Syntax **expected** *byte*
expected auto

Context **[Tree]** (config>port>otu>psi-payload expected)

Full Context configure port otu psi-payload expected

Description This command allows the user to configure the expected received payload type value in byte 0 of the Payload structure identifier (PSI) of the OPU overhead. When this values does not match the received value, the OPU-PLM alarm will be reported if it is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default 3 for 10GE-LAN/WAN or OC192 with OTU encapsulation; 5 for GFP framed 10GE-LAN with OTU encapsulation.

Parameters **auto** — Sets the expected value to the standard value in the payload type field.

byte — Specifies the expected received payload type value in bytes.

Values [00 to FF] Hexadecimal notation

Default 00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

expected

Syntax **expected auto-generated**
expected bytes *byte-string* [*byte-string*...(up to 64 byte-strings max, 64 bytes max)]
expected string *identifier*
expected use-rx

Context **[Tree]** (config>port>otu>sm-tti expected)

Full Context configure port otu sm-tti expected

Description This command enables the user to configure the expected RX Trail Trace Identifier (TTI) for Section Monitoring (SM) in the OTU overhead. This identifier can be a string or a non-printable sequence of bytes. The length of the string or sequence of bytes cannot exceed 64 bytes. This trace should match the expected far-end port's SM trace. When this trace does not match the received SM trace, the OTU-TIM alarm will be reported if enabled.

Default Blank (all zeros)

Parameters **auto-generated** — Sets the default.

identifier — Sets the PM TTI to the string provided by the user. If the string is less than 64 bytes, the remaining bytes will be set to 0. Up to 64 byte strings can be specified in a single statement.

byte-string — [byte1 byte2 to byte64]. Sets the PM TTI to the sequence of bytes provided by the user. If the user provides less than 64 bytes, the remaining bytes will be set to 0.

use-rx — Copies the received pm-tti to the expected either as a string or a sequence of bytes depending on the received pm-tti data.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.221 expire-time

expire-time

Syntax **expire-time** {*seconds* | **forever**}

Context **[Tree]** (config>system>script-control>script-policy expire-time)

Full Context configure system script-control script-policy expire-time

Description This command is used to configure the maximum amount of time to keep the run history status entry from a script run.

Default expire-time 3600

Parameters *seconds* — Specifies the time to keep the run history status entry, in seconds.

Values 0 to 21474836

Default 3600 (1 hour)

forever — Specifies to keep the run history status entry indefinitely.

Platforms All

9.222 expiry-time

expiry-time

Syntax **expiry-time** *expiry-time*
no expiry-time

Context **[Tree]** (config>subscr-mgmt>msap-policy>igmp-host-tracking expiry-time)

Full Context configure subscriber-mgmt msap-policy igmp-host-tracking expiry-time

Description This command configures the time that the system continues to track inactive hosts.

The **no** form of this command removes the values from the configuration.

Parameters *expiry-time* — Specifies the time, in seconds, that this system continues to track an inactive host.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

expiry-time

Syntax **expiry-time** *expiry-time*
no expiry-time

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-snooping expiry-time)

Full Context configure service vprn subscriber-interface group-interface sap igmp-snooping expiry-time

Description This command configures the time that the system continues to track inactive hosts.

The **no** form of this command removes the values from the configuration.

Parameters *expiry-time* — Specifies the time, in seconds, that this system continues to track an inactive host.

Values 1 to 65535

expiry-time

Syntax **expiry-time** *expiry-time*
no expiry-time

Context **[Tree]** (config>service>vpls>igmp-host-tracking expiry-time)
[Tree] (config>service>vpls>sap>igmp-host-tracking expiry-time)

Full Context configure service vpls igmp-host-tracking expiry-time
configure service vpls sap igmp-host-tracking expiry-time

Description This command configures the time that the system continues to track inactive hosts.

The **no** form of this command removes the values from the configuration.

Default no expiry-time

Parameters *expiry-time* — Specifies the time, in seconds, that this system continues to track an inactive host

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

expiry-time

Syntax **expiry-time** *expiry-time*
no expiry-time

Context **[Tree]** (config>service>ies>igmp-host-tracking expiry-time)
[Tree] (config>service>ies>sub-if>grp-if>sap>igmp-host-tracking expiry-time)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies igmp-host-tracking expiry-time
configure service ies subscriber-interface group-interface sap igmp-host-tracking expiry-time

Description This command configures the time that the system continues to track inactive hosts.

The **no** form of this command removes the values from the configuration.

Default no expiry-time

Parameters *expiry-time* — Specifies the time, in seconds, that this system continues to track an inactive host.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

expiry-time

Syntax **expiry-time** *expiry-time*
no expiry-time

Context **[Tree]** (config>service>vprn>igmp-trk expiry-time)
[Tree] (config>service>vprn>sap>igmp-trk expiry-time)

Full Context configure service vprn igmp-host-tracking expiry-time
configure service vprn sap igmp-trk expiry-time

Description This command configures the time that the system continues to track inactive hosts.

The **no** form of this command removes the values from the configuration.

Default no expiry-time

Parameters *expiry-time* — Specifies the time, in seconds, that this system continues to track an inactive host.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.223 explicit-sf-path

explicit-sf-path

Syntax **explicit-sf-path** {**primary** | **secondary**}
no explicit-sf-path

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel explicit-sf-path)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>source-override explicit-sf-path)

Full Context configure mcast-management multicast-info-policy bundle channel explicit-sf-path
configure mcast-management multicast-info-policy bundle source-override explicit-sf-path

Description This command defines an explicit ingress switch fabric multicast path assigned to a multicast channel. When defined, the channel is setup with the explicit path as its inactive path. When an explicit path is not defined, all multicast channels are initialized on the secondary path and when they start to consume bandwidth, they are moved to the appropriate path based on the channel attributes and path limitations. Explicit path channels are not allowed to move from their defined path.

The **explicit-sf-path** command in the bundle context defines the initial path for all channels associated with the bundle unless the channel has an overriding **explicit-sw-path** defined in the channel context. The channel context may also be overridden by the **explicit-sf-path** command in the **source-override** context. The channel and **source-override explicit-sf-path** settings default to null (undefined) and have no effect unless explicitly set.

The **no** form of this command restores default path association behavior (dynamic or null depending on the context).

Parameters **primary** — The **primary** and **secondary** keywords are mutually exclusive to one another. One keyword must be specified when executing the explicit-sf-path command. The **primary** keyword specifies that the primary ingress multicast path should be used as the explicit path for the channel.

secondary — The **primary** and **secondary** keywords are mutually exclusive to one another. One keyword must be specified when executing the explicit-sf-path command. The **secondary** keyword specifies that the secondary ingress multicast path should be used as the explicit path for the channel.

Override sequence — The channel setting overrides the bundle setting. The source-override setting overrides the channel and bundle settings.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

9.224 explicit-subscriber-map

explicit-subscriber-map

Syntax **explicit-subscriber-map**

Context [Tree] (config>subscriber-mgmt explicit-subscriber-map)

Full Context configure subscriber-mgmt explicit-subscriber-map

Description This command configures an explicit subscriber mapping.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

9.225 exponential-backoff

exponential-backoff

Syntax [**no**] **exponential-backoff**

Context **[Tree]** (config>system>login-control exponential-backoff)

Full Context configure system login-control exponential-backoff

Description This command enables the exponential-backoff of the login prompt. The exponential-backoff command is used to deter dictionary attacks, when a malicious user can gain access to the CLI by using a script to try **admin** with any conceivable password.

The **no** form of this command disables exponential-backoff.

Default no exponential-backoff

Platforms All

9.226 exponential-backoff-retry

exponential-backoff-retry

Syntax **exponential-backoff-retry**
no exponential-backoff-retry

Context **[Tree]** (config>router>mpls exponential-backoff-retry)

Full Context configure router mpls exponential-backoff-retry

Description This command enables the use of an exponential back-off timer when re-trying an LSP. When an LSP path establishment attempt fails, the path is put into retry procedures and a new attempt will be performed at the expiry of the user-configurable retry timer (config>router>mpls>lsp>retry-timer). By default, the retry time is constant for every attempt. The exponential back-off timer procedures will double the value of the user configured retry timer value at every failure of the attempt to adjust to the potential network congestion that caused the failure. An LSP establishment fails if no Resv message was received and the Path message retry timer expired or a PathErr message was received before the timer expired.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.227 export

export

Syntax [**no**] **export**

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>evpn export)

Full Context configure subscriber-mgmt isa-service-chaining evpn export

Description Commands in this context configure information related to the export of EVPN BGP routes related to service chaining.

The **no** form of this command disables exporting EVPN BGP routes related to service chaining

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

export

Syntax **export** *policy* [*policy*]
no export

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy export)

Full Context configure subscriber-mgmt bgp-peering-policy export

Description This command specifies the export policies to be used to control routes advertised to BGP neighbors.

When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be configured. The first policy that matches is applied.

Note: If a non-existent route policy is applied to a VPRN instance, the CLI generates a warning message. This message is only generated at an interactive CLI session and the route policy association is made. No warning message is generated when a non-existent route policy is applied to a VPRN instance in a configuration file or when SNMP is used.

The **no** form of this command removes all route policy names from the export list.

Default no export — BGP advertises routes from other BGP routes but does not advertise any routes from other protocols unless directed by an export policy.

Parameters *policy* — Specifies a route policy statement name, up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

export

Syntax **export** *ip-prefix/length*
no export

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>redundancy export)

Full Context configure service ies subscriber-interface wlan-gw redundancy export

Description This command specifies an IPv4 route (prefix/length) per subscriber-interface to be exported (announced) to indicate liveness of the subscriber-interface on the WLAN-GW. This route is the one that is monitored in routing by the peer WLAN-GW to decide its state with respect.

The no form of this command reverts to the default.

Parameters *ip-prefix/length* — Specifies the IP prefix and length.

Values ip-prefix:a.b.c.d
ip-prefix-length: 0 to 32

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

export

Syntax **export** *plcy-or-long-expr* [*plcy-or-expr*]
no export

Context **[Tree]** (config>service>vprn>bgp export)
[Tree] (config>service>vprn>bgp>group export)
[Tree] (config>service>vprn>bgp>group>neighbor export)

Full Context configure service vprn bgp export
configure service vprn bgp group export
configure service vprn bgp group neighbor export

Description This command is used to specify route policies that control how outbound routes transmitted to certain peers are handled. Route policies are configured in the **config>router>policy-options** context.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in a peer-group) or neighbor level (only applies to the specified peer). The most specific level is used.

The **export** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine the modifications of each route and the final action to accept or reject the route.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Only one of the 15 objects referenced by the **export** command can be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters while the remaining 14 objects have a maximum length of 64 characters each.

When multiple **export** commands are issued, the last command entered overrides the previous command.

When an export policy is not specified, BGP-learned routes are advertised by default; non-BGP routes are not advertised.

The **no** form of this command removes the policy association.

Default no export

Parameters *plcy-or-long-expr* — Specifies the route policy name, up to 64 characters in length, or a policy logical expression, up to 255 characters in length.

plcy-or-expr — Specifies the route policy name, up to 64 characters in length, or a policy logical expression, up to 255 characters in length.

Platforms All

export

Syntax [**no**] **export** *policy-name* [*policy-name*...**up to 5 max**]

Context **[Tree]** (config>service>vprn>isis export)

Full Context configure service vprn isis export

Description This command configures export routing policies that determine the routes exported from the routing table to IS-IS.

If no export policy is defined, non IS-IS routes are not exported from the routing table manager to IS-IS.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered overrides the previous command. A maximum of five policy names can be specified.

If an **aggregate** command is also configured in the **config>router** context, then the aggregation is applied before the export policy is applied.

Routing policies are created in the **config>router>policy-options** context.

The **no** form of this command removes the specified *policy-name* or all policies from the configuration if no *policy-name* is specified.

Default no export — No export policy name is specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — The export policy name. Up to five *policy-name* arguments can be specified.

Platforms All

export

Syntax **export** *policy-name* [*policy-name*...(**up to 5 max**)]
no export

Context **[Tree]** (config>service>vprn>msdp export)
[Tree] (config>service>vprn>msdp>group export)
[Tree] (config>service>vprn>msdp>group>peer export)
[Tree] (config>service>vprn>msdp>peer export)

Full Context configure service vprn msdp export
configure service vprn msdp group export
configure service vprn msdp group peer export
configure service vprn msdp peer export

Description This command specifies the policies to export source active state from the source active list into Multicast Source Discovery Protocol (MSDP).

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no export

Parameters *policy-name* — Specifies the export policy name, up to 32 characters. Up to five policy-name arguments can be specified.

If you configure an export policy at the global level, each individual peer inherits the global policy. If you configure an export policy at the group level, each individual peer in a group inherits the group's policy. If you configure an export policy at the peer level, then policy only applies to the peer where it is configured.

Platforms All

export

Syntax **export** {**unicast** | *ext-community*}

Context **[Tree]** (config>service>vprn>mvpn>vrf-target export)

Full Context configure service vprn mvpn vrf-target export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies communities to be sent to peers.

Parameters **unicast** — Specifies to use unicast vrf-target ext-community for the multicast VPN.

ext-comm — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values

target:{*ip-address*:*comm-val* | *2byte-asnumber:ext-comm-val* | 4byte-asnumber:comm-val}

ip-address:	a.b.c.d
comm-val:	0 to 65535
2byte-asnumber:	1 to 65535
4byte-asnumber	0 to 4294967295

Platforms All

export

Syntax **export** *ip-prefix/length*
no export

Context **[Tree]** (config>service>vprn>nat>outside>pool>redundancy export)

Full Context configure service vprn nat outside pool redundancy export

Description This command installs the export route in the routing table for active NAT pools.

Once the export route is in the routing table, it can be advertised in the network via a routing protocol. NAT pools in the standby or disabled state will not advertise the export route.

A NAT pool becomes active when it becomes operationally UP, and there is no monitoring route (which is also the export route from the peer) present in the routing node (as received from the network). The pool will transition into standby state in case that the monitoring route (or export route from the peer) is already present in the routing table. In other words, the monitoring route is already advertised as an export route from the peering node with active NAT pool.

The export route can be advertised only from:

- The active lead pool.
- Active pool for which fate-sharing is disabled.

Default no export

Parameters *ip-prefix/length* — Specifies the IP prefix and length.

Syntax:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-prefix/length:	ip-prefix	a.b.c.d
	ip-prefix-length	0 to 32

Values 0, 4, 16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

export

Syntax **export** *policy-name* [*policy-name*]
no export

Context **[Tree]** (config>service>vprn>ospf>area export)
[Tree] (config>service>vprn>ospf3>area export)

Full Context configure service vprn ospf area export
configure service vprn ospf3 area export

Description This command configures ABR export policies to filter OSPFv2 Type 3 Summary-LSAs or OSPFv3 Inter-Area-Prefix-LSA between areas, in to only permit the export of specified routes into an area.

This command cannot be used in OSPF area 0.

The **no** form of this command reverts to the default value.

Default no export

Parameters *policy-name* — Specifies the export route policy name. A maximum of five policy names may be specified. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), enclose the entire string in double quotes.

The specified policy names must be predefined and already exist in the system.

Platforms All

export

Syntax **export** *policy-name* [*policy-name*]
no export

Context **[Tree]** (config>service>vprn>ospf export)
[Tree] (config>service>vprn>ospf3 export)

Full Context configure service vprn ospf export
configure service vprn ospf3 export

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates export route policies to determine which routes are exported from the route table to OSPF. Export polices are only in effect if OSPF is configured as an ASBR.

If no export policy is specified, non-OSPF routes are not exported from the routing table manager to OSPF.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no export — No export route policies specified.

Parameters *policy-name* — Specifies the export route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

The specified policy name(s) must be predefined and already exist in the system.

Platforms All

export

Syntax **export** *policy-name* [*policy-name*...(up to 5 max)]
no export

Context **[Tree]** (config>service>vprn>rip export)
[Tree] (config>service>vprn>rip>group export)
[Tree] (config>service>vprn>rip>group>neighbor export)
[Tree] (config>service>vprn>ripng export)
[Tree] (config>service>vprn>ripng>group export)
[Tree] (config>service>vprn>ripng>group>neighbor export)

Full Context configure service vprn rip export
configure service vprn rip group export
configure service vprn rip group neighbor export
configure service vprn ripng export
configure service vprn ripng group export
configure service vprn ripng group neighbor export

Description This command specifies the export route policies used to determine routes that are exported to RIP. If no export policy is specified, non-RIP routes will not be exported from the routing table manager to RIP; RIP-learned routes will be exported to RIP neighbors.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no export

Parameters *policy-name* — The export route policy name. Allowed values are any string up to 32 characters in length and composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the string must be enclosed between double quotes. The specified names must already be defined.

Platforms All

export

Syntax **export** *policy-name* [*policy-name*]
no export

Context **[Tree]** (config>router>ldp export)

Full Context configure router ldp export

Description This command specifies the export route policies used to determine which routes are exported to LDP. Policies are configured in the **config>router>policy-options** context.

If no export policy is specified, non-LDP routes will not be exported from the routing table manager to LDP. LDP-learned routes will be exported to LDP neighbors. Present implementation of export policy (outbound filtering) can be used “only” to add FECs for label propagation. The export policy does not control propagation of FECs that an LSR receives from its neighbors.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of 5 policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no export — No export route policies specified.

Parameters *policy-name* — Specifies up to five export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

export

Syntax **export** *ip-prefix/length*
no export

Context **[Tree]** (config>router>nat>outside>pool>redundancy export)

Full Context configure router nat outside pool redundancy export

Description This command configures the route to export to the peer. While the export prefix is configured and the value of the object tmnxNatPlLsnRedActive is equal to true, the system exports this prefix in the realm of the virtual router instance associated with this pool; to the NAT redundancy peer, the presence of this prefix is an indication that the Large Scale NAT function in this virtual router instance is active; hence, the export prefix of this system is the monitor prefix of the peer.

The export prefix must be different from the monitor prefix.

Default no export

Parameters *ip-prefix/length* — Specifies the IP address and length of the prefix to be exported.

Values

ip-prefix:	a.b.c.d
ip-prefix-length:	0 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

export

Syntax **export** *policy-name* [*policy-name*]
no export

Context **[Tree]** (config>router>msdp export)
[Tree] (config>router>msdp>peer export)
[Tree] (config>router>msdp>group export)
[Tree] (config>router>msdp>group>peer export)

Full Context configure router msdp export
configure router msdp group export
configure router msdp group peer export
configure router msdp peer export

Description This command specifies the policies to export source active state from the source active list into Multicast Source Discovery Protocol (MSDP).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command applies no export policies and all SA entries are announced.

Default no export

Parameters *policy-name* — Specifies the export policy name, up to 32 characters. Up to five policy-name arguments can be specified.

If you configure an export policy at the global level, each individual peer inherits the global policy. If you configure an export policy at the group level, each individual peer in a group inherits the group's policy. If you configure an export policy at the peer level, then policy only applies to the peer where it is configured.

Platforms All

export

Syntax **export type** {*type*} **input** *filename* **output** *url-string* **format** *output-format* [**password** [*32 chars max*]] [**pkey** *filename*]

Context **[Tree]** (admin>certificate export)

Full Context admin certificate export

Description This command performs certificate operations.

Parameters *url-string* — Specifies the local CF card url of the file.

Values

url-string	<local-url> [up to 99 characters]
local-url	<cflash-id>/<file-path>
cflash-id	cf1: | cf2: | cf3:

type — Specifies the type of input file.

Values cert, key, crl

format — Specifies the format of output file.

Values pkcs10, pkcs12, pkcs7-der, pkcs7-pem, pem, der

Platforms All

export

Syntax **export** *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no export [*plcy-or-long-expr*]

Context **[Tree]** (config>router>bgp export)
[Tree] (config>router>bgp>group export)
[Tree] (config>router>bgp>group>neighbor export)

Full Context configure router bgp export
configure router bgp group export
configure router bgp group neighbor export

Description This command specifies route policies that control the handling of outbound routes transmitted to all peers. Route policies are configured in the **config>router>policy-options** context.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific level is used.

The export command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine the modifications of each route and the final action to accept or reject the route.

Only one of the 15 objects referenced by the command can be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters; the remaining 14 objects have a maximum length of 64 characters each.

When multiple export commands are issued, the last command entered overrides the previous command.

When an export policy is not specified, BGP-learned routes are advertised by default and non-BGP routes are not advertised.

The **no** form of this command removes the policy association.

Default no export

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters long). Allowed values are any string up to 255 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

plcy-or-expr — Specifies up to 14 route policy names (up to 64 characters each) or a policy logical expression (up to 64 characters long). Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

export

Syntax [**no**] **export** *policy-name* [*policy-name*]

Context **[Tree]** (config>router>isis export)

Full Context configure router isis export

Description This command configures export routing policies that determine the routes exported from the routing table to IS-IS.

If no export policy is defined, non IS-IS routes are not exported from the routing table manager to IS-IS.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered overrides the previous command. A maximum of five policy names can be specified.

If an **aggregate** command is also configured in the **config>router** context, then the aggregation is applied before the export policy is applied.

Routing policies are created in the **config>router>policy-options** context.

The **no** form of this command removes the specified *policy-name* or all policies from the configuration if no *policy-name* is specified.

Parameters *policy-name* — Specifies up to five export policy names.

Platforms All

export

Syntax **export** *policy-name* [*policy-name*]
no export

Context **[Tree]** (config>router>ospf export)
[Tree] (config>router>ospf3 export)

Full Context configure router ospf export
configure router ospf3 export

Description This command associates export route policies to determine which routes are exported from the route table to OSPF. Export polices are only in effect if OSPF is configured as an ASBR.

If no export policy is specified, non-OSPF routes are not exported from the routing table manager to OSPF.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no export

Parameters *policy-name* — Specifies up to 5 export route policy names. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified names must already be defined.

Platforms All

export

Syntax [**no**] **export** *policy-name* [*policy-name*]

Context **[Tree]** (config>router>ospf>area export)
[Tree] (config>router>ospf3>area export)

Full Context configure router ospf area export
configure router ospf3 area export

Description This command configures ABR export policies to filter OSPFv2 Type 3 Summary-LSAs or OSPFv3 Inter-Area-Prefix-LSA between areas, in order to only permit the specified routes from being exported into an area.

This command cannot be used in OSPF area 0.

The **no** form of this command reverts to the default value.

Default no export

Parameters *policy-name* — Specifies up to five export route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified names must already be defined.

Platforms All

export

Syntax **export** *policy-name* [*policy-name*]
no export

Context **[Tree]** (config>router>rip export)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>rip>group export)
[Tree] (config>router>rip>group>neighbor export)
[Tree] (config>router>ripng export)
[Tree] (config>router>ripng>group export)
[Tree] (config>router>ripng>group>neighbor export)

Full Context configure router rip export
configure router rip group export
configure router rip group neighbor export
configure router ripng export
configure router ripng group export
configure router ripng group neighbor export

Description This command specifies the export route policies used to determine which routes are exported to RIP.

If no export policy is specified, non-RIP routes will not be exported from the routing table manager to RIP. RIP-learned routes will be exported to RIP neighbors.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

Default no export

Parameters *policy-name* — Specifies up to five export route policy names. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on.), the entire string must be enclosed within double quotes.

The specified names must already be defined.

Platforms All

9.228 export-addresses

export-addresses

Syntax **export-addresses** *policy-name* [*policy-name*]
no export-addresses

Context [Tree] (config>router>ldp>session-params>peer export-addresses)

Full Context configure router ldp session-parameters peer export-addresses

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the export prefix policy to local addresses advertised to this peer.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified.

The **no** form of this command removes the policy from the configuration.

Parameters *policy-name* — Specifies up to five export-prefix route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined.

Platforms All

9.229 export-filter

export-filter

Syntax **export-filter**

Context **[Tree]** (config>cflowd>collector export-filter)

Full Context configure cflowd collector export-filter

Description This command creates the CLI context to specify cflowd data filters. These filters allow the administrator to control which flows are sent or are not sent to an associated cflowd collector.

Platforms All

9.230 export-grt

export-grt

Syntax **export-grt** *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]
no export-grt

Context **[Tree]** (config>service>vprn>grt-lookup export-grt)

Full Context configure service vprn grt-lookup export-grt

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command uses route policy to determine which routes are exported from the VRF to the GRT along with all the forwarding information. These entries are marked as BGP-VPN routes in the GRT. Routes must be in the GRT in order for proper routing to occur from the GRT to the VRF.

Default no export-grt

Parameters *plcy-or-long-expr* — Specifies the route policy name, up to 64 characters, or a policy logical expression, up to 255 characters.

plcy-or-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Up to 4 policy names or logical expressions can be specified in a single statement.

Platforms All

9.231 export-host-routes

export-host-routes

Syntax [**no**] **export-host-routes**

Context **[Tree]** (config>service>ies>subscriber-interface export-host-routes)
[Tree] (config>service>vprn>subscriber-interface export-host-routes)

Full Context configure service ies subscriber-interface export-host-routes
configure service vprn subscriber-interface export-host-routes

Description This command controls the export of subscriber management host routes from a retail service to the corresponding forwarding wholesale VPRN service.

By default, subscriber management host routes are not exported.

The presence of retail subscriber management host routes in the wholesale VPRN service is required for downstream traffic forwarding in multi-chassis redundancy scenarios with a redundant interface and when the retail subscriber subnets are not leaked in the wholesale VPRN service (allow-unmatching-subnets or unnumbered retail subscriber interface).

This command fails if the subscriber interface is not associated with a forwarding wholesale service subscriber interface or if the subscriber interface is not configured to support address allocation outside the provisioned subnets (allow-unmatching-subnets or unnumbered subscriber interface).

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.232 export-id

export-id

Syntax **export-id** *export-id*
no export-id

Context **[Tree]** (config>app-assure>group>policy>application export-id)
[Tree] (config>app-assure>group>policy>application>charging-group export-id)
[Tree] (config>app-assure>group>policy>app-group export-id)

Full Context configure application-assurance group policy app-group export-id
configure application-assurance group policy application charging-group export-id
configure application-assurance group policy application export-id

Description This command assigns an export-id value to a charging group app-group or application to be used for accounting export identification in RADIUS accounting. This ID is encoded in the top 2 bytes of the RADIUS accounting VSA to identify which charging group the counter value represents.

If no export-id is assigned, that counter cannot be added to the aa-sub stats RADIUS export-type. Once a charging group index is referenced, it cannot be deleted without removing the reference.

The no form of this command removes the export-id from the configuration.

Default no export-id

Parameters *export-id* — Specifies an integer that identifies an export-id.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.233 export-inactive-bgp

export-inactive-bgp

Syntax [**no**] **export-inactive-bgp**

Context **[Tree]** (config>service>vprn export-inactive-bgp)

Full Context configure service vprn export-inactive-bgp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the preferred BGP route learned by a VPRN to be exported as the VPN route, even when if it is inactive in the route table because a preferred BGP VPRN route from another PE is present. This overrides the default state in which the VPRN cannot export an inactive BGP route.

For the BGP route to be exported, the VRF export policy must accept it.

This command applies to both MPLS VPN and SRv6 VPN routes. In SRv6 VPN routes the advertised instruction is an End.DT, while in MPLS VPN routes the advertised label is a per-next-hop label.

This “best-external” type of route advertisement is useful in active/standby multi-homing scenarios because it ensures that all PEs know about the backup path provided by the standby PE.

Default no export-inactive-bgp

Platforms All

9.234 export-limit

export-limit

Syntax **export-limit** *num-routes*
no export-limit

Context **[Tree]** (config>service>vprn>grt-lookup export-limit)
[Tree] (config>service>vprn>ospf export-limit)
[Tree] (config>service>vprn>ospf3 export-limit)

Full Context configure service vprn grt-lookup export-limit
configure service vprn ospf export-limit
configure service vprn ospf3 export-limit

Description This command provides the ability to limit the total number of routes exported from the VRF to the GRT. The value zero (0) provides an override that disables the maximum limit. Setting this value to zero (0) will not limit the number of routes exported from the VRF to the GRT. Configuring a range of one (1) to 1000 will limit the number of routes to the specified value.

The **no** form of this command sets the export-limit to a default of five (5).

Default export-limit 5

Parameters *num-routes* — Specifies the maximum number of routes that can be exported.

Values 0 to 1000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

export-limit

Syntax **export-limit** *number* [**log** *percentage*]
no export-limit

Context **[Tree]** (config>service>vprn>rip export-limit)
[Tree] (config>service>vprn>ripng export-limit)

Full Context configure service vprn rip export-limit
configure service vprn ripng export-limit

Description This command configures the maximum number of routes (prefixes) that can be exported into RIP from the route table.

The **no** form of this command removes the parameters from the configuration.

Default no export-limit

Parameters *number* — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.

Values 1 to 4294967295

log *percentage* — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values 1 to 100

Platforms All

export-limit

Syntax **export-limit** *number* [**log** *percentage*]
no export-limit

Context **[Tree]** (config>service>vprn>isis export-limit)

Full Context configure service vprn isis export-limit

Description This command configures the maximum number of routes (prefixes) that can be exported into IS-IS from the route table for the VPRN instance.

The **no** form of this command removes the parameters from the configuration.

Default no export-limit - The export limit for routes or prefixes is disabled.

Parameters *number* — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

log *percentage* — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values 1 to 100

Platforms All

export-limit

Syntax **export-limit** *number* [**log** *percentage*]
no export-limit

Context **[Tree]** (config>router>isis export-limit)

Full Context configure router isis export-limit

Description This command configures the maximum number of routes (prefixes) that can be exported into IS-IS from the route table. After the maximum is reached, a warning log message is sent and additional routes are ignored.

The **no** form of this command removes the parameters from the configuration.

Parameters *number* — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.

Values 1 to 4294967295

percentage — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values 1 to 100

Platforms All

export-limit

Syntax **export-limit** *number* [**log** *percentage*]
no export-limit

Context **[Tree]** (config>router>ospf export-limit)
[Tree] (config>router>ospf3 export-limit)

Full Context configure router ospf export-limit
configure router ospf3 export-limit

Description This command configures the maximum number of routes (prefixes) that can be exported into OSPF from the route table. After the maximum is reached, a warning log message is sent and additional routes are ignored.

The **no** form of this command removes the parameters from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no export-limit

Parameters *number* — Specifies the maximum number of routes (prefixes) that can be exported into OSPF from the route table.

Values 1 to 4294967295

percentage — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values 1 to 100

Platforms All

export-limit

Syntax **export-limit** *number* [**log** *percentage*]
no export-limit

Context **[Tree]** (config>router>rip export-limit)
[Tree] (config>router>ripng export-limit)

Full Context configure router rip export-limit
configure router ripng export-limit

Description This command configures the maximum number of routes (prefixes) that can be exported into RIP from the route table.

The **no** form of the command removes the parameters from the configuration.

Default no export-limit

Parameters *number* — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.

Values 1 to 4294967295

percentage — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values 1 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.235 export-mode

export-mode

Syntax **export-mode** {**automatic** | **manual**}

Context **[Tree]** (config>cflowd export-mode)

Full Context configure cflowd export-mode

Description This command can be used to control how exports are generated by the cflowd process. The default behavior is for flow data to be exported automatically based on the active and inactive time-out values. The alternative mode is manual in which case flow data is only exported when the command “tools perform cflowd manual-export” is issued. The only exception is if the cflowd cache overflows, in which case the normal automatic export process is used.

Default export-mode automatic

Parameters **automatic** — cflowd flow data is automatically generated.

manual — cflowd flow data is exported only when manually triggered.

Platforms All

9.236 export-override

export-override

Syntax **export-override** *mode*
no export-override

Context **[Tree]** (configure>app-assure>group>cflowd export-override)

Full Context configure application-assurance group cflowd export-override

Description This command configures the AA sub-type used in cflowd record export. The cflowd stats exported to the cflowd collector to look identical to when AA is on the type of system defined by the mode. The following cflowd export fields are affected:

a. cflowd export observation point (field 138), the mode will be derived from the export-override category that is selected.
b. cflowd export AA_Subscriber_Type (field 12) modified as configured, using existing field types.
c. cflowd interface name is used as the sub-ID field, optionally modified to use the **export-override** *mode* **prefix** as a global identifier.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All AA cflowd record types are affected by export-override. To change any of the export-override or prefix, cflowd must be shutdown first. When the **export-override** is set back to default (**no export-override**) the prefix is set back to the default.

The **no** form of this command removes the export override.

Default no export-override

Parameters *mode* — The type of system emulated by stats export.

Values mobile(mobile gateway mode, cflowd field 138 = 2)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.237 export-prefixes

export-prefixes

Syntax [**no**] **export-prefixes** *policy-name*

Context **[Tree]** (config>router>ldp>session-params>peer export-prefixes)

Full Context configure router ldp session-parameters peer export-prefixes

Description This command specifies the export route policy used to determine which prefixes received from other LDP and T-LDP peers are re-distributed to this LDP peer via the LDP/T-LDP session to this peer. A prefix that is filtered out (deny) is not exported. A prefix that is filtered in (accept) will be exported.

If no export policy is specified, all FEC prefixes learned will be exported to this LDP peer. This policy is applied in addition to the global LDP policy and targeted session policy.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified. Peer address has to be the peer LSR-ID address.

The **no** form of this command removes the policy from the configuration.

Default no export-prefixes - no export route policy is specified

Parameters *policy-name* — Specifies up to five export-prefix route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

export-prefixes

Syntax **export-prefixes** *policy-name* [*policy-name*]
no export-prefixes

Context **[Tree]** (config>router>ldp>targeted-session export-prefixes)

Full Context configure router ldp targeted-session export-prefixes

Description This command specifies the export route policy used to determine which FEC prefix label bindings are exported from a targeted LDP session. A route that is filtered out (deny) will not be exported. A route that is filtered in (accept) will be exported.

If no export policy is specified, all bindings learned through a targeted LDP session will be exported to all targeted LDP peers. This policy is applied in addition to the global LDP policy.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified.

The **no** form of this command removes the policy from the configuration.

Parameters *policy-name* — Specifies up to five export policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

9.238 export-tunnel-table

export-tunnel-table

Syntax **export-tunnel-table** *policy-name* [*policy-name*...(up to 5 max)]
no export-tunnel-table

Context **[Tree]** (config>router>ldp export-tunnel-table)

Full Context configure router ldp export-tunnel-table

Description This command enables exports BGP label route and SR tunnels from the TTM into LDP for the purpose of stitching an LDP FEC to a BGP or SR tunnel for the same destination prefix.

To enable route stitching between LDP and BGP, separately configure tunnel table route export policies in both protocols and enable the advertisement of RFC 3107, *Carrying Label Information in BGP-4*, formatted labeled routes for prefixes learned from LDP FECs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The BGP route export policy instructs BGP to listen to LDP route entries in the CPM Tunnel Table. If a /32 LDP FEC prefix matches an entry in the export policy, BGP originates a BGP labeled route, stitches it to the LDP FEC, and re-distributes the BGP labeled route to its Interior Border Gateway Protocol (IBGP) neighbors.

Using the following commands to add LDP FEC prefixes with the **from protocol ldp** statement in the existing BGP export policy configuration at the global level, peer-group level, or peer level:

- **config>router>bgp>export** *policy-name*
- **config>router>bgp>group>export** *policy-name*
- **config>router>bgp>group>neighbor>export** *policy-name*

To indicate to BGP to evaluate the entries with the **from protocol ldp** statement in the export policy when applied to a specific BGP neighbor, use commands:

- **config>router>bgp>group>neighbor>family label-ipv4** and
- **config>router>bgp>group>neighbor>advertise-ldp-prefix**

Without the latter configuration, only core IPv4 routes learned from RTM are advertised as BGP labeled routes to the neighbor. No stitching of LDP FEC to the BGP labeled route will be performed for this neighbor even if the same prefix was learned from LDP.

The LDP tunnel table route export policy instructs LDP to listen to BGP route entries in the CPM Tunnel Table. If a /32 BGP labeled route matches a prefix entry in the export policy, LDP originates an LDP FEC for the prefix, stitches it to the BGP labeled route, and re-distributes the LDP FEC to its IBGP neighbors.

The user can add BGP labeled route prefixes with the **from protocol bgp** statement in the configuration of the LDP tunnel table export policy. The **from protocol** statement is applied only when the protocol value is **ldp**. Policy entries with protocol values of **rsvp**, **bgp**, or any value other than **ldp** are ignored at the time the policy is applied to LDP.

In the LDP-to-SR data path direction, LDP listens to SR tunnel entries in the TTM. The user can restrict the export of SR tunnels to LDP from a specific prefix list. The user can also restrict the export to a specific IGP instance by optionally specifying the instance ID in the “from protocol” statement. The statement has an effect only when the protocol value is **isis** or **bgp**. Policy entries with any other protocol value are ignored at the time the policy is applied. If the user configures multiple **from protocol** statements in the same policy or does not include the **from protocol** statement but adds a default action of accept, then LDP will follow the TTM selection rules to select a tunnel to which it will stitch the LDP ILM:

1. LDP selects the tunnel from the lowest TTM preference protocol.
2. If two or more of IS-IS or OSPF protocol instances and BGP protocol have the same preference, then LDP selects the protocol using the default TTM protocol preference.
3. Within the same IGP protocol, LDP selects the lowest instance ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If an LDP FEC primary next-hop cannot be resolved using an RTM route and a SR tunnel of type SR-ISIS to the same destination prefix matches a prefix entry in the export policy, LDP programs an LDP ILM and stitches it to the SR node-SID tunnel endpoint. LDP also originates an FEC for the prefix and re-distributes it to its LDP peers. When an LDP FEC is stitched to a SR tunnel, packets forwarded will benefit from the protection of the LFA/remote LFA backup next-hop of the SR tunnel.

When resolving a FEC, LDP will prefer RTM over TTM when both resolutions are possible. That is, swapping the LDP ILM to a LDP NHLFE is preferred over stitching it to an SR tunnel endpoint.

Nokia recommends that the user should enable the bfd-enable option on the interfaces in LDP, IGP instance, and BGP contexts to speed up failure detection and activation of the SR LFA/remote-LFA backup next-hop or the BGP backup, depending on the stitching operation.

This feature is limited to IPv4 /32 prefixes in LDP, BGP and SR.

The **no** form of this command disables the export of BGP and SR tunnels to LDP.

Default no export-tunnel-table — no tunnel table export route policy is specified.

Parameters *policy-name* — Specifies up to five export-tunnel-table route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined.

Platforms All

export-tunnel-table

Syntax **export-tunnel-table ldp**
no export-tunnel-table

Context **[Tree]** (config>router>isis>segment-routing export-tunnel-table)

Full Context configure router isis segment-routing export-tunnel-table

Description This command exports the LDP tunnels to an IGP instance for the purpose of stitching a SR tunnel to a LDP FEC for the same destination IPv4 /32 prefix.

In the SR-to-LDP data path direction, the SR mapping server provides a global policy for the prefixes corresponding to the LDP FECs the SR stitches to.

When this command is enabled in the segment-routing context of an IGP instance, IGP listens to LDP tunnel entries in the TTM. Whenever a LDP tunnel destination matches a prefix for which IGP received a prefix-SID sub-TLV from a mapping server, it instructs the SR module to program the SR ILM and to stitch it to the LDP tunnel endpoint. The LDP FEC can be resolved via a static route, a IS-IS instance, or an OSPF instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an SR tunnel is stitched to a LDP FEC, packets forwarded will benefit from the protection of the LFA backup next-hop of the LDP FEC.

When resolving a node SID, IGP will prefer resolution of prefix SID received in a IP Reach TLV over a prefix SID received via the mapping server. That is, swapping the SR ILM to a SR NHLFE is preferred over stitching it to a LDP tunnel endpoint.

Nokia recommends that the user should enable the bfd-enable option on the interfaces in both LDP and IGP instance contexts to speed up the failure detection and the activation of the LFA/remote-LFA backup next-hop in either direction of the stitching.

This feature is limited to IPv4 /32 prefixes in both LDP and SR.

The **no** form of this command disables the exporting of LDP tunnels to the IGP instance.

Default no export-tunnel-table

Parameters **ldp** — Exports LDP tunnels from the tunnel table into an IGP instance.

Platforms All

export-tunnel-table

Syntax [**no**] **export-tunnel-table ldp**

Context **[Tree]** (config>router>ospf>segm-rtng export-tunnel-table)

Full Context configure router ospf segment-routing export-tunnel-table

Description This command enables exporting, to an IGP instance, the LDP tunnels for the purpose of stitching a SR tunnel to a LDP FEC for the same destination IPv4 /32 prefix.

In the SR-to-LDP data path direction, the SR mapping server provides a global policy for the prefixes corresponding to the LDP FECs that the SR stitches to.

When this command is enabled in the segment-routing context of an IGP instance, IGP listens to LDP tunnel entries in the TTM. Whenever a LDP tunnel destination matches a prefix for which IGP received a prefix-SID sub-TLV from a mapping server, it instructs the SR module to program the SR ILM and to stitch it to the LDP tunnel endpoint. The LDP FEC can be resolved via a static route, a IS-IS instance, or an OSPF instance.

When an SR tunnel is stitched to a LDP FEC, packets forwarded will benefit from the protection of the LFA backup next hop of the LDP FEC.

When resolving a node SID, IGP will prefer resolution of prefix SID received in a IP Reach TLV over a prefix SID received via the mapping server. In other words, the swapping of the SR ILM to a SR NHLFE is preferred over stitching it to a LDP tunnel endpoint.

It is recommended to enable the **bfd-enable** option on the interfaces in both LDP and IGP instance contexts, to speed up the failure detection and the activation of the LFA/remote-LFA backup next hop in either direction of the stitching.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This feature is limited to IPv4 /32 prefixes in both LDP and SR.

The **no** form of this command disables the exporting of LDP tunnels to the IGP instance.

Platforms All

9.239 export-v6-limit

export-v6-limit

Syntax **export-v6-limit** *num-routes*
no export-v6-limit

Context **[Tree]** (config>service>vprn>grt-lookup export-v6-limit)

Full Context configure service vprn grt-lookup export-v6-limit

Description This command limits the total number of IPv6 routes exported from the VPRN to the GRT. The value “0” provides an override that disables the maximum limit. Setting this value to “0” does not limit the number of routes exported from the VPRN to the GRT. Configuring a range of 1 to 1000 limits the number of routes to the specified value.

The **no** form of this command sets the export-limit to a default of 5.

Default export-v6-limit 5

Parameters *num-routes* — Specifies maximum number of routes that can be exported.

Values 0 to 1000

Platforms All

9.240 expression

expression

Syntax **expression** *expr-index expr-type* {**eq** | **neq**} *expr-string*
no expression *expr-index*

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry expression)

Full Context configure application-assurance group policy app-filter entry expression

Description This command configures string values to use in the application definition.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *expr-index* — Specifies an index value which represents expression substrings.

Values 1 to 4

expr-type — Represents a type (and thereby the expression substring).

http-host — Matches the string against the HTTP Host field or TLS Server Name Indicator (SNI).

http-uri — Matches the string against the HTTP URI field.

http-referer — Matches the string against the HTTP Referer field.

http-user-agent — Matches the string against the HTTP User Agent field.

sip-ua — Matches the string against the SIP UA field.

sip-uri — Matches the string against the SIP URI field.

sip-mt — Matches the string against the SIP MT field.

citrix-app — Matches the string against the Citrix app field.

h323-product-id — Matches the string against the h323-product-id field.

tls-cert-subj-org-name — Matches the TLS Certificate Subject Organization Name substring.

tls-cert-subj-common-name — Matches the TLS Certificate Subject Common Name substring.

rtsp-host — Matches the Real Time Streaming Protocol (RTSP) substring host.

rtsp-uri — Matches the RTSP URI substring.

rtsp-ua — Matches the RTSP UA substring.

rtmp-page-host — Matches against the RTMP Page Host field

rtmp-page-uri — Matches against the RTMP Page URI field

rtmp-swf-host — Matches against the RTMP Swf Host field

rtmp-swf-uri — Matches against the RTMP Swf URI field

dns-domain-name — Matches the string against the DNS Name field.

eq — Specifies the equal to comparison operator to match the specified HTTP string.

neq — Specifies the not equal to comparison operator to match the specified HTTP string.

expr-string — Specifies an expression string, up to 64 characters, used to define a pattern match. Denotes a printable ASCII substring used as input to an application assurance filter match criteria object.

The following syntax is permitted within the substring to define the pattern match criteria:

^<substring>* - matches when <substring> is at the beginning of the object.

<substring> - matches when <substring> is at any place within the object.

*<substring>$ - matches when <substring> is at the end of the object.

^<substring>$ - matches when <substring> is the entire object.

* - matches zero to many of any character. A single wildcard as infix in the expression is allowed.

\. - matches any single character

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

\d - matches any single decimal digit [0-9]

\I - forces case sensitivity (by default, the expression match are case insensitive), the \I can be specified anywhere between

the leading [^*] and trailing [$*]

* - matches the asterisk character

Rules for <substring> characters:

<substring> must contain printable ASCII characters.

<substring> must not contain the “double quote” character or the “ ” (space) character on its own.

<substring> match is case in sensitive by default.

<substring> must not include any regular expression meta-characters other than "*", "\I", "\.", "*" and "\d".

The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the <substring>:

Character to match <substring> input

Hexadecimal Octet YY \xYY

A <substring> that uses the '\' (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

Operational notes:

- When matching a TCP flow against HTTP-string based applications, the HTTP header fields are collected from the first HTTP request (for example a GET or a POST) for a given TCP flow. The collected strings are then evaluated against each HTTP flow created within the given TCP flow to determine whether a given HTTP flow matches the application. By not specifying a protocol, the HTTP expressions are matched against all protocols in the HTTP family. By specifying a specific HTTP protocol (for example, http_video) the expression match can be constrained to a subset of the HTTP protocols.
- To uniquely identify a SIP-based application a protocol match is not required in the app-filter entry with the SIP expression. The SIP expression match is performed against any protocol in the SIP family (such as sip and rtp_sip). By specifying a specific SIP protocol (like rtp_sip) the expression match can be constrained to a subset of the SIP protocols.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

expression

Syntax **expression** *expr-index* **eq** *expr-string* **offset** *payload-octet-offset* **direction** *direction*
no expression *expr-index*

Context **[Tree]** (config>app-assure>group>policy>custom-protocol expression)

Full Context configure application-assurance group policy custom-protocol expression

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an expression string value for pattern-based custom protocols match. A flow matches a custom protocol if the specified string is found at an offset of a TCP/UDP of the first payload packet.

Options:

- client-to-server — A pattern will be matched against a flow from a TCP client.
- server-to-client — A pattern will be matched against a flow from a TCP server.
- any – A pattern will be matched against a TCP/UDP flow in any direction (towards or from AA subscriber)

The **no** form of this command deletes a specified string expression from the definition.

Parameters *expr-index* — Specifies the expression substring index.

Values 1

expr-string — Denotes a printable ASCII string, up to 16 characters, used to define a custom protocol match. Rules for expr-string characters:

- Must contain printable ASCII characters.
- Must not contain the “double quote” character or the “ ” (space) character on its own.
- Match is case sensitive.
- Must not include any regular expression meta-characters.

The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the expr-string:

Character to match expr-string input

Hexadecimal Octet YY \xYY

An expr-string that uses the '\' (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

offset *payload-octet-offset* — specifies the offset (in octets) into the protocol payload, where the expr-string match criteria will start.

Values 0 to 127

direction *direction* — Specifies the protocol direction to match against to resolve to a custom protocol.

Values client-to-server, server-to-client, any

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

expression

Syntax **expression** *expr-index expr-type* **eq** *expr-string* {**record** | **no-record**}
no expression expr-index

Context **[Tree]** (debug>app-assure>group>http-host>filter expression)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug application-assurance group http-host-recorder filter expression

Description This command configures the recorder filter expressions.

Parameters *expr-index* — Specifies the expression index value.

Values 1 to 4

expr-type — Specifies the expression type.

Values http-host

expr-string — Specifies the HTTP host filter expression string.

Values format *<expression>$ (33 chars max)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

expression

Syntax **expression** *regular-expression*
no expression

Context **[Tree]** (config>router>policy-options>as-path expression)

Full Context configure router policy-options as-path expression

Description This command creates a route policy AS path regular expression statement to use in route policy entries.

The **no** form of this command deletes the AS path regular expression statement.

Parameters *reg-exp* — The AS path regular expression. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

null — The AS path expressed as an empty regular expression string.

Platforms All

expression

Syntax **expression** *expression* [**exact**]
no expression

Context **[Tree]** (config>router>policy-options>community expression)

Full Context configure router policy-options community expression

Description This command creates a logical expression to match a route policy community.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the logical expression.

Default no expression

Parameters **expression** *expression* — Specifies a logical expression containing terms and operators. It can contain sub-expressions enclosed in round brackets.

Values up to 900 characters

<expression> is one of the following: <expression> {AND| OR} <expression> [NOT] (<expression>) [NOT] <comm-id>

For example:

from community expression "[community list A] OR ([community list B] AND [community list C])"

exact — All the communities indicated by the expression must be present in the route in order for a match to occur.

Platforms All

9.241 expression-match

expression-match

Syntax **[no] expression-match**

Context **[Tree]** (config>app-assure>group>url-list expression-match)

Full Context configure application-assurance group url-list expression-match

Description This command configures a URL list that contains hostnames with wildcards.

The **no** form of this command removes the URL list containing hostnames with wildcards.

Default no expression-match

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.242 extended-action

extended-action

Syntax [**no**] **extended-action**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>ip-filter>entry>action extended-action)
[Tree] (config>filter>ipv6-filter>entry>action extended-action)

Full Context configure filter ip-filter entry action extended-action
configure filter ipv6-filter entry action extended-action

Description Commands in this context configure an extended action for a filter entry's PBR action (configured under **config**>**filter**>**ip-filter**>**entry**>**action** and **config**>**filter**>**ipv6-filter**>**entry**>**action** contexts). The extended action is executed in addition to the configured PBR action.

The **no** form of the command removes the extended action.

Default no extended-action

Platforms All

9.243 extended-bw

extended-bw

Syntax [**no**] **extended-bw**

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx>features extended-bw)

Full Context configure subscriber-mgmt diameter-application-policy gx features extended-bw

Description This command specifies whether extended bandwidth AVPs are supported. Extended bandwidth AVPs are capable of supporting bandwidth values greater than (2^{32} - 1) b/s. The extended AVPs allow bitrates in kb/s and are as follows:

- Extended-GBR-DL (AVP code 2850)
- Extended-GBR-UL (AVP code 2851)
- Extended-Max-Requested-BW-DL (AVP code 554)
- Extended-Max-Requested-BW-UL (AVP code 555)
- Extended-APN-AMBR-DL (AVP code 2848)
- Extended-APN-AMBR-UL (AVP code 2849)

The **no** form of this command disables the extended bandwidth AVP support.

Default no extended-bw

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.244 extended-community

extended-community

Syntax [**no**] **extended-community**

Context **[Tree]** (config>router>bgp>outbound-route-filtering extended-community)
[Tree] (config>router>bgp>group>outbound-route-filtering extended-community)
[Tree] (config>router>bgp>group>neighbor>outbound-route-filtering extended-community)

Full Context configure router bgp group neighbor outbound-route-filtering extended-community
configure router bgp group outbound-route-filtering extended-community
configure router bgp outbound-route-filtering extended-community

Description The extended-community command opens the configuration tree for sending or accepting extended-community based BGP filters.

For the **no** version of the command to work, all sub-commands (**send-orf**, **accept-orf**) must be removed first.

Default no extended-community

Platforms All

9.245 extended-failure-handling

extended-failure-handling

Syntax **extended-failure-handling**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy extended-failure-handling)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling

Description Commands in this context configure Extended Failure Handling (EFH), a mechanism to establish a new Diameter Gy session with the Online Charging Server (OCS) after Credit Control Failure Handling (CCFH) CONTINUE is triggered.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.246 extended-lsa

extended-lsa

Syntax **extended-lsa** {**sparse** | **only**}
no extended-lsa

Context **[Tree]** (config>router>ospf3 extended-lsa)

Full Context configure router ospf3 extended-lsa

Description This command configures the use of extended LSA format in OSPFv3 as per *draft-ietf-ospf-ospfv3-lsa-extend*.

Prior to this feature, SR OS used the fixed format LSA to carry the prefix and link information as per RFC 5340, *OSPF for IPv6*. The fixed format is not extensible and the TLV format of the extended LSA must be used.

With this feature, the default mode of operation for OSPFv3 is referred to as **sparse** mode, meaning that the router will always advertise the fixed format for existing LSAs and will add the TLV-based extended LSA only when it needs to advertise new sub-TLVs. This mode of operation is similar to the way OSPFv2 advertises the segment routing information. It sends the prefix in the original fixed-format prefix LSA and then follows with the extended prefix TLV which is sent in an extended prefix opaque LSA containing the prefix SID sub-TLV.

The **extended-lsa only** value enables the full extended LSA mode. This causes all existing and new LSAs to use the extended LSA format.

The OSPFv3 instance must first be shut down before the user can change the mode of operation since the protocol must flush all LSAs and re-establish all adjacencies.

The **no** form at the OSPFv3 instance level reverts the OSPFv3 instance into the default sparse mode of operation.

Default extended-lsa sparse

Parameters **sparse** — Enables the sparse mode of operation in an OSPFv3 instance.

only — Enables the full extended LSA mode of operation in an OSPFv3 instance.

Platforms All

extended-lsa

Syntax **extended-lsa** {**inherit** | **only**}
no extended-lsa

Context **[Tree]** (config>router>ospf3>area extended-lsa)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ospf3 area extended-lsa

Description This command configures the use of extended LSA format in a OSPFv3 area as per *draft-ietf-ospf-ospfv3-lsa-extend*.

By default, the area inherits the instance level configuration. The latter defaults to **sparse** mode of operation. The **extended-lsa only** value enables the full extended LSA mode and this will cause all existing and new LSAs to use the extended LSA format.

The OSPFv3 instance must first be shut down before the user can change the mode of operation since the protocol must flush all LSAs and re-establish all adjacencies.

The **no** form at the area level returns the area into the default mode of inheriting the mode from the OSPFv3 instance level.

Default extended-lsa inherit

Parameters **inherit** — Configures the area to inherit the mode of operation enabled at the OSPFv3 instance level.

only — Enables the full extended LSA mode of operation in an OSPFv3 area.

Platforms All

9.247 extended-nh-encoding

extended-nh-encoding

Syntax **extended-nh-encoding** [**ipv4**]
no extended-nh-encoding

Context **[Tree]** (config>service>vprn>bgp extended-nh-encoding)
[Tree] (config>service>vprn>bgp>group extended-nh-encoding)
[Tree] (config>service>vprn>bgp>group>neighbor extended-nh-encoding)

Full Context configure service vprn bgp extended-nh-encoding
configure service vprn bgp group extended-nh-encoding
configure service vprn bgp group neighbor extended-nh-encoding

Description This command configures BGP to advertise (at session OPEN) the capability to receive IPv4 routes with IPv6 next-hops from the VPRN BGP peers included in the scope of the command. These peers should not send these routes unless they receive the capability. If the SR OS router receives an IPv4 route from a peer to which it did not advertise the necessary capability, the UPDATE message will be considered malformed and causes either a session reset or treat as withdraw behavior depending on the error handling settings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command causes the sending of an extended NH encoding BGP capability to the associated BGP peers to be inherited from a higher configuration level or disabled (if configured at the BGP level).

Default no extended-nh-encoding

Parameters **ipv4** — Specifies that the command should be applied to unlabeled unicast IPv4 routes.

Platforms All

extended-nh-encoding

Syntax **extended-nh-encoding** [**label-ipv4**] [**vpn-ipv4**] [**ipv4**]
no extended-nh-encoding

Context **[Tree]** (config>router>bgp extended-nh-encoding)
[Tree] (config>router>bgp>group extended-nh-encoding)
[Tree] (config>router>bgp>group>neighbor extended-nh-encoding)

Full Context configure router bgp extended-nh-encoding
configure router bgp group extended-nh-encoding
configure router bgp group neighbor extended-nh-encoding

Description This command configures BGP to advertise (at session OPEN) the capability to receive label IPv4, VPN IPv4 routes, or IPv6 next hops from the peers. These peers should not send such routes unless they receive notification of this capability. If the SR OS router receives a label IPv4 or VPN IPv4 route from a peer to which it did not advertise the necessary capability, the UPDATE message will be considered malformed and this will cause either session reset or **treat-as-withdraw** behavior depending on the error handling settings.

The **no** form of this command causes the sending of an extended NH encoding BGP capability to the associated BGP peers to be inherited from a higher configuration level or disabled (if configured at the BGP level).

Default no extended-nh-encoding

Parameters **label-ipv4** — Instructs BGP to advertise an extended NH encoding capability for NLRI AFI=1, NLRI SAFI=4, and next-hop AFI=2.

vpn-ipv4 — Instructs BGP to advertise an extended NH encoding capability for NLRI AFI=1, NLRI SAFI=128, and next-hop AFI=2.

ipv4 — Instructs BGP to advertise an extended NH encoding capability for NLRI AFI=1, NLRI SAFI=1 and next-hop AFI=2.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.248 extended-sequence-number

extended-sequence-number

Syntax **[no] extended-sequence-number**

Context **[Tree]** (config>ipsec>ipsec-transform extended-sequence-number)

Full Context configure ipsec ipsec-transform extended-sequence-number

Description This command enables 64-bit extended sequence numbering support. This numbering is used for high throughput CHILD_SA to avoid frequent rekeying caused by sequence numbering wrap around.

The **no** form of this command disables extended sequence numbering support. Only 32-bit sequence numbering is supported.

Default no extended-seq-number

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.249 extended-unicast

extended-unicast

Syntax **[no] extended-unicast**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if extended-unicast)

Full Context configure mcast-management multicast-info-policy video-policy video-interface extended-unicast

Description This command delays video unicast from switching over to multicast for 5 minutes. The unicast session can be extended further by sending an RTCP extension request, which resets the 5-minute timer. This is ideal for services that require unicast video and end devices that require extended time to switch over from unicast to multicast.

The **no** form of this command disables extended unicast. The unicast session switches over to multicast 1.5 seconds after the IGMP request is sent. Most Fast Channel Change deployments do not require a time extension.

Default no extended-unicast

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.250 extension

extension

Syntax [**no**] **extension start** [*0 to 4095*] **end** [*0 to 4095*]

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>extensions extension)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range extensions extension

Description This command configures an additional VLAN range extension that is used for matching. Any traffic within the extension range is considered part of the same VLAN range for purposes of intra-SSID mobility.

Default none

Parameters **start** [*0 to 4095*] — Specifies the start of the VLAN extension range

Values 0 to 4095

end [*0 to 4095*] — Specifies the end of VLAN extension range

Values 0 to 4095

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.251 extensions

extensions

Syntax [**no**] **extensions**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range extensions)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range extensions

Description This command enables VLAN range extensions on this VLAN tag range.

The **no** form of the command disables VLAN extensions.

Default no extensions

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.252 external

external

Syntax [**no**] **external**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from external)

Full Context configure router policy-options policy-statement entry from external

Description This command specifies the external route matching criteria for the entry.

Default no external

Platforms All

9.253 external-assignment

external-assignment

Syntax [**no**] **external-assignment**

Context **[Tree]** (config>router>nat>outside>pool external-assignment)
[Tree] (config>service>vprn>nat>outside>pool external-assignment)

Full Context configure router nat outside pool external-assignment
configure service vprn nat outside pool external-assignment

Description This command enables external allocation of L2-Aware NAT outside IP addresses from the pool.

The **no** form of the command disables the allocation.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

9.254 external-db-overflow

external-db-overflow

Syntax **external-db-overflow** *limit interval*
no external-db-overflow

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>ospf external-db-overflow)
[Tree] (config>service>vprn>ospf3 external-db-overflow)

Full Context configure service vprn ospf external-db-overflow
configure service vprn ospf3 external-db-overflow

Description This command enables limits on the number of non-default AS-external-LSA entries that can be stored in the LSDB and specifies a wait timer before processing these after the limit is exceeded.

The *limit* value specifies the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database (LSDB). Placing a limit on the non-default AS-external-LSAs in the LSDB protects the router from receiving an excessive number of external routes that consume excessive memory or CPU resources. If the number of routes reach or exceed the *limit*, the table is in an overflow state. When in an overflow state, the router does not originate any new AS-external-LSAs and it withdraws all self-originated non-default external LSAs.

The *interval* specifies the amount of time to wait after an overflow state before regenerating and processing non-default AS-external-LSAs. The waiting period acts like a dampening period, which prevents the router from continuously running Shortest Path First (SPF) calculations caused by the excessive number of non-default AS-external LSAs.

The **external-db-overflow** must be set identically on all routers attached to any regular OSPF area. OSPF stub areas and not-so-stubby areas (NSSAs) are excluded.

The **no** form of this command disables limiting the number of non-default AS-external-LSA entries.

Default no external-db-overflow — No limit on non-default AS-external-LSA entries.

Parameters *limit* — The maximum number of non-default AS-external-LSA entries that can be stored in the LSDB before going into an overflow state expressed as a decimal integer.

Values -1 to 2147483647

Note: Setting a value of -1 is equivalent to **no external-db-overflow**.

interval — The number of seconds after entering an overflow state before attempting to process non-default AS-external-LSAs expressed as a decimal integer.

Values 0 to 2147483647

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

external-db-overflow

Syntax **external-db-overflow** *limit interval*
no external-db-overflow

Context **[Tree]** (config>router>ospf external-db-overflow)
[Tree] (config>router>ospf3 external-db-overflow)

Full Context configure router ospf external-db-overflow
configure router ospf3 external-db-overflow

Description This command enables limits on the number of non-default AS-external-LSA entries that can be stored in the LSDB and specifies a wait timer before processing these after the limit is exceeded.

The *limit* value specifies the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database (LSDB). Placing a limit on the non-default AS-external-LSAs in the LSDB protects the router from receiving an excessive number of external routes that consume excessive memory or CPU resources. If the number of routes reach or exceed the *limit*, the table is in an overflow state. When in an overflow state, the router will not originate any new AS-external-LSAs. In fact, it withdraws all the self-originated non-default external LSAs.

The *interval* specifies the amount of time to wait after an overflow state before regenerating and processing non-default AS-external-LSAs. The waiting period acts like a dampening period preventing the router from continuously running Shortest Path First (SPF) calculations caused by the excessive number of non-default AS-external LSAs.

The **external-db-overflow** must be set identically on all routers attached to any regular OSPF area. OSPF stub areas and not-so-stubby areas (NSSAs) are excluded.

The **no** form of this command disables limiting the number of non-default AS-external-LSA entries.

Default no external-db-overflow

Parameters *limit* — Specifies the maximum number of non-default AS-external-LSA entries that can be stored in the LSDB before going into an overflow state expressed as a decimal integer.

Values 0 to 2147483647

interval — The number of seconds after entering an overflow state before attempting to process non-default AS-external-LSAs expressed as a decimal integer.

Values 0 to 2147483647

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

9.255 external-preference

external-preference

Syntax **external-preference** *preference*
no external-preference

Context **[Tree]** (config>service>vprn>isis>level external-preference)

Full Context configure service vprn isis level external-preference

Description This command configures the external route preference for the IS-IS level.

The **external-preference** command configures the preference level of either IS-IS level 1 or IS-IS level 2 external routes. By default, the preferences are as listed in the table below.

A route can be learned by the router by different protocols, in which case, the costs are not comparable. When this occurs, the preference decides the route to use.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is dependent on the default preference table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of the route to use is determined by the configuration of the **ecmp** in the **config>router** context.

Default Default preferences are listed in Table 52.

Table 52 **Default Preferences**

Route Type	Preference	Configurable
Direct attached	0	No
Static route	5	Yes
MPLS	7	—
OSPF internal routes	10	No
IS-IS Level 1 internal	15	Yes [1]
IS-IS Level 2 internal	18	Yes [1]
OSPF external	150	Yes
IS-IS Level 1 external	160	Yes
IS-IS Level 2 external	165	Yes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 52 **Default Preferences**

Route Type	Preference	Configurable
BGP	170	Yes
BGP	170	Yes

Note:

1. Internal preferences are changed using the **preference** command in the **config>router>isis>level** *level-number* context.

Parameters *preference* — The preference for external routes at this level as expressed.

Values 1 to 255

Platforms All

external-preference

Syntax **external-preference** *preference*
no external-preference

Context **[Tree]** (config>service>vprn>ospf external-preference)
[Tree] (config>service>vprn>ospf3 external-preference)

Full Context configure service vprn ospf external-preference
configure service vprn ospf3 external-preference

Description This command configures the preference for OSPF external routes.

A route can be learned by the router from different protocols, in which case the costs are not comparable. If this occurs, preference is used to decide which route is used.

Different protocols should not be configured with the same preference. If this occurs, the tiebreaker is per the default preference table as defined in Table 53. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of the **ecmp** in the **config**>**router** context.

The **no** form of this command reverts to the default value.

Table 53 **Default External Route Preferences**

Route Type	Preference	Configurable
Direct attached	0	No

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 53 **Default External Route Preferences**

Route Type	Preference	Configurable
Static routes	5	Yes
OSPF internal	10	Yes [1]
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes

Note:

1. Preference for OSPF internal routes is configured with the **preference** command.

Default external-preference 150 — OSPF external routes have a default preference of 150.

Parameters *preference* — The preference for external routes expressed as a decimal integer.

Values 1 to 255

Platforms All

external-preference

Syntax **external-preference** *preference*
no external-preference

Context **[Tree]** (config>router>isis>level external-preference)

Full Context configure router isis level external-preference

Description This command configures the external route preference for the IS-IS level.

The **external-preference** command configures the preference level of either IS-IS level 1 or IS-IS level 2 external routes. By default, the preferences are as listed in the table below.

A route can be learned by the router by different protocols, in which case, the costs are not comparable. When this occurs, the preference decides the route to use.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is dependent on the default preference table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of the route to use is determined by the configuration of the **ecmp** in the **config>router** context.

The **no** form of this command reverts to the default value.

Default external-preference (Level 1) — 160

external-preference (Level 2) — 165

Parameters *preference* — Specifies the preference for external routes at this level as expressed.

Default preferences are listed in the Table 54:

Table 54 **Default External Route Preferences**

Route Type	Preference	Configurable
Direct attached	0	—
Static-route	5	Yes
OSPF internal routes	10	—
IS-IS Level 1 internal	15	Yes [1]
IS-IS Level 2 internal	18	Yes [1]
OSPF external	150	Yes
IS-IS Level 1 external	160	Yes
IS-IS Level 2 external	165	Yes
BGP	170	Yes

Note:

1. Internal preferences are changed using the preference command in the config>router>isis>level *level-number* context.

Values 1 to 255

Platforms All

external-preference

Syntax **external-preference** *preference*
no external-preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ospf external-preference)
[Tree] (config>router>ospf3 external-preference)

Full Context configure router ospf external-preference
configure router ospf3 external-preference

Description This command configures the preference for OSPF external routes.

A route can be learned by the router from different protocols, in which case, the costs are not comparable. When this occurs, the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the Table 55. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the **ecmp** in the **config**>**router** context.

The **no** form of this command reverts to the default value.

Default external-preference 150

Parameters *preference* — Specifies the preference for external routes expressed as a decimal integer. Defaults for different route types are listed in Table 55.

Table 55 **Route Preference Defaults by Route Type**

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes [1]
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

Note:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

1. Preference for OSPF internal routes is configured with the **preference** command.

Values 1 to 255

Platforms All

9.256 extranet

extranet

Syntax **extranet** [**detail**]
no extranet

Context **[Tree]** (debug>router>pim extranet)

Full Context debug router pim extranet

Description This command enables debugging for extranet PIM.

The **no** form of this command disables PIM extranet debugging.

Parameters **detail** — Debugs detailed extranet PIM information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10 f Commands

10.1 facility

facility

Syntax **facility** *syslog-facility*
no facility

Context **[Tree]** (config>service>vprn>log>syslog facility)

Full Context configure service vprn log syslog facility

Description This command configures the facility code for messages sent to the syslog target host.

Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last *facility-code* entered overwrites the previous facility-code.

If multiple facilities need to be generated for a single syslog target host, then multiple **log-id** entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.

The **no** form of this command reverts to the default value.

Default local7 — Syslog entries are sent with the local7 facility code.

Parameters *syslog-facility* — Specifies syslog facility name represents a specific numeric facility code. The code should be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.

Values kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Valid responses per RFC3164, *The BSD syslog Protocol,* are listed in Table 56.

Table 56 **Syslog Facility Codes**

Numerical Code	Facility Code
0	kernel
1	user

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 56 **Syslog Facility Codes**

Numerical Code	Facility Code
2	mail
3	systemd
4	auth
5	syslogd
6	printer
7	net-news
8	uucp
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

Values: 0 to 23

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

facility

Syntax **facility** *syslog-facility*

Context **[Tree]** (config>app-assure>group>evt-log>syslog facility)

Full Context configure application-assurance group event-log syslog facility

Description This command configures the syslog facility. The syslog facility is an information field associated with a syslog message. It is defined by the syslog protocol and provides an indication of which part of the system originated the message.

Default facility local7

Parameters *syslog-facility* — Specifies the syslog facility keyword.

Values kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

facility

Syntax **facility** *syslog-facility*

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy facility)

Full Context configure service nat syslog syslog-export-policy facility

Description This command configures a syslog facility. For more information, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. The **config>log>syslog>level** hierarchy also applies to this context.

Default facility local0

Parameters *syslog-facility* — Specifies a syslog facility name which represents a specific numeric facility code. The code must be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.

Values kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

facility

Syntax **facility** *syslog-facility*
no facility

Context **[Tree]** (config>log>syslog facility)

Full Context configure log syslog facility

Description This command configures the facility code for messages sent to the syslog target host.

Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last *facility-code* entered overwrites the previous facility-code.

If multiple facilities need to be generated for a single syslog target host, then multiple **log-id** entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.

The **no** form of this command reverts to the default value.

Default facility local7

Parameters *syslog-facility* — Specifies a syslog facility name which represents a specific numeric facility code. The code must be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.

Values kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Valid responses per RFC 3164, *The BSD syslog Protocol,* are listed in Table 57.

Table 57 **Syslog Protocol Valid Responses**

Numerical Code	Facility Code
0	kernel
1	user
2	mail
3	systemd
4	auth
5	syslogd
6	printer
7	net-news

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 57 **Syslog Protocol Valid Responses**

Numerical Code	Facility Code
8	uucp
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

Platforms All

10.2 facility-fault

facility-fault

Syntax [**no**] **facility-fault**

Context **[Tree]** (config>lag>eth-cfm>mep facility-fault)
[Tree] (config>port>ethernet>eth-cfm>mep facility-fault)

Full Context configure lag eth-cfm mep facility-fault
configure port ethernet eth-cfm mep facility-fault

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Allows the facility MEP to move from alarming only to network actionable function. This means a facility MEP will not merely report the defect conditions but will be able to action based on the transition of the MEP state. Without this command the facility MEP will only monitor and report and conditions of the MEP do not affect related services.

Default no facility-fault

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

facility-fault

Syntax [**no**] **facility-fault**

Context **[Tree]** (config>router>if>eth-cfm>mep facility-fault)

Full Context configure router interface eth-cfm mep facility-fault

Description This command allows the facility MEP to move from alarming only to network actionable function. This means that a MEP facility reports both the defect conditions and the actions that are based on the transition of the MEP state.

The **no** form of this command causes the facility MEP to only monitor and report conditions on the MEPs that do not affect related services.

Default no facility-fault

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.3 facility-id-permission

facility-id-permission

Syntax **facility-id-permission** {**chassis**}
no facility-id-permission

Context **[Tree]** (config>eth-cfm>domain>assoc facility-id-permission)

Full Context configure eth-cfm domain association facility-id-permission

Description This command allows the operator to include the sender-id TLV information that was specified under the **config>eth>system>sender-id** context for facility base MEPs. When this option is present under the maintenance association, the specific MPs in the association included the **sender-id** TLV information in ETH-CFM PDUs. MEPs include the **sender-id** TLV for CCM (not sub second CCM enabled MEPs), LBM/LBR, and LTM/LTR. MIPs include this value in the LBR and LTR PDUs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: LBR functions reflect all TLVs received in the LBM unchanged including the SenderID TLV. This command produces an error when a bridge-identifier is configured under the association. Facility MEPs do not support the bridge-identifier. Transmission of the Management Domain and Management Address fields are not supported in this TLV.

Parameters **chassis** — Sends the configured chassis information defined under **eth-cfm>system** using the **sender-id** option.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.4 fail-action

fail-action

Syntax **fail-action** {**continue** | **drop**}
no fail-action

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>match-radprox-cache fail-action)

Full Context configure subscriber-mgmt local-user-db ipoe host match-radius-proxy-cache fail-action

Description This command specifies the action to take when no match is found in the cache.

The **no** form of this command reverts to the default.

Default fail-action drop

Parameters **continue** — Specifies to continue when no match is found.

drop — Specifies to drop when no match is found.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

fail-action

Syntax **fail-action** *fail-action*
no fail-action

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action fail-action)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action fail-action

Description This command configures the fail action when a packet matches with a VAS filter entry in a specific direction, but no mapping exists for the specified SF-IP or ESI in the specified EVPN service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the fail action from the configuration.

Parameters *fail-action* — Specifies the fail action.

Values drop, forward

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.5 fail-on-error

fail-on-error

Syntax [**no**] **fail-on-error**

Context **[Tree]** (config>card fail-on-error)
[Tree] (config>card>xiom fail-on-error)

Full Context configure card fail-on-error
configure card xiom fail-on-error

Description This command controls the behavior of the card when any one of a specific set of card level errors is encountered in the system. When the **fail-on-error** command is enabled, and any one (or more) of the specific errors is detected, then the Operational State of the card is set to Failed. This Failed state will persist until the clear card command is issued (reset) or the card is removed and re-inserted (re-seat). If the condition persists after re-seating the card, then Nokia support should be contacted for further investigation.

Enabling **fail-on-error** is only recommended when the network is designed to be able to route traffic around a failed card (redundant cards, nodes or other paths exist).

The list of specific errors includes:

- CHASSIS event ID# 2063 – tmnxEqCardPChipMemoryEvent
- CHASSIS event ID# 2076 – tmnxEqCardPChipCamEvent
- CHASSIS event ID# 2059 – tmnxEqCardPChipError (for ingress Ethernet only)
- CHASSIS event ID# 2098 tmnxEqCardQChipBufMemoryEvent
- CHASSIS event ID# 2099 tmnxEqCardQChipStatsMemoryEvent
- CHASSIS event ID# 2101 tmnxEqCardQChipIntMemoryEvent
- CHASSIS event ID# 2103 tmnxEqCardChipIfCellEvent

On platforms without independent IOM/IMM and CPM cards, the node is rebooted if fail-on-error is enabled and one of the card level errors is encountered.

The tmnxEqCardPChipError is only considered as a trigger for card fail-on-error for ingress FCS errors (not egress FCS errors), and only for Ethernet MDAs or IMMs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note that upon the detection of the event/error in the system, the reporting of the event (logs) and the **fail-on-error** behavior of the card are independent. Log event control configuration will determine whether the events are reported in logs (or SNMP traps, and so on) and the **fail-on-error** configuration will determine the behavior of the card. This implies that the card can be configured to **fail-on-error** even if the events are suppressed (some may be suppressed in the system by default). In order to facilitate post-failure analysis, Nokia recommends that you enable the reporting of the specific events/errors (**configure log event-control**) when **fail-on-error** is enabled.

Default no fail-on-error

Platforms 7750 SR-s

- configure card xiom fail-on-error

All

- configure card fail-on-error

fail-on-error

Syntax [**no**] **fail-on-error**

Context **[Tree]** (config>card>mda fail-on-error)

Full Context configure card mda fail-on-error

Description This command enables the fail-on-error feature. If an MDA is experiencing too many Egress XPL Errors, this feature causes the MDA to fail. This can force an APS switchover or **traffic re-route**. The purpose of this feature is to avoid situations where traffic is forced to use a physical link that suffers from errors but is still technically operational.

The feature uses values configured in the **config>card>mda>egress-xpl** context. When this feature is enabled on a MDA, if *window* consecutive minutes pass in which the MDA experiences more than *threshold* Egress XPL Errors per minute, then the MDA will be put in the *failed* state.

The **no** form of this command disables the feature on the MDA.

Platforms All

10.6 fail-to-open

fail-to-open

Syntax [**no**] **fail-to-open**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>isa>aa-grp fail-to-open)

Full Context configure isa application-assurance-group fail-to-open

Description This command configures the mode of operation during an operational failure of this application assurance group when no application assurance engines are available to service traffic. When enabled, all traffic that was to be inspected will be dropped. When disabled, all traffic that was to be inspected will be forwarded without any inspection as if the group was not configured at all.

Default no fail-to-open

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.7 failed-mda-limit

failed-mda-limit

Syntax **failed-mda-limit** *number*
no failed-mda-limit

Context [Tree] (config>isa>nat-group failed-mda-limit)

Full Context configure isa nat-group failed-mda-limit

Description This command configures the maximum number of supported simultaneously failures in the active-active intra-chassis NAT redundancy model. Traffic from the failed ISAs is distributed over the remaining ISA in the system. Memory resources are reserved in every ISA to accommodate new mappings from the failed ISA. However, bandwidth is not reserved and each ISA operates at max speed in all conditions (with failure or without the failure).

NAT translations are not preserved across switchovers and consequently they will have to be re-initiated by the clients.

For this command to take effect, the intra-chassis redundancy mode must be set to active-active (**config>isa>nat-group>redundancy active-active**).

Default no failed-mda-limit

Parameters *number* — Specifies the number of simultaneous ISA failures supported in active-active intra-chassis NAT redundancy model.

Values 1 to 2

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.8 failed-threshold

failed-threshold

Syntax **failed-threshold** [1 to 1000]
failed-threshold all

Context **[Tree]** (config>service>vpls>site failed-threshold)

Full Context configure service vpls site failed-threshold

Description This command defines the number of objects should be down for the site to be declared down. Both administrative and operational status must be evaluated and if at least one is down, the related object is declared down.

Default failed-threshold all

Parameters *1 to 1000* — Specifies the threshold for the site to be declared down.

Platforms All

10.9 failover

failover

Syntax **failover**

Context **[Tree]** (config>router>dhcp>server failover)
[Tree] (config>router>dhcp>server>pool failover)
[Tree] (config>router>dhcp6>server failover)
[Tree] (config>router>dhcp6>server>pool failover)
[Tree] (config>service>vprn>dhcp>server failover)
[Tree] (config>service>vprn>dhcp>server>pool failover)
[Tree] (config>service>vprn>dhcp6>server failover)
[Tree] (config>service>vprn>dhcp6>server>pool failover)

Full Context configure router dhcp local-dhcp-server failover
configure router dhcp local-dhcp-server pool failover
configure router dhcp6 local-dhcp-server failover
configure router dhcp6 local-dhcp-server pool failover
configure service vprn dhcp local-dhcp-server failover
configure service vprn dhcp local-dhcp-server pool failover
configure service vprn dhcp6 local-dhcp-server failover
configure service vprn dhcp6 local-dhcp-server pool failover

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure failover parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

failover

Syntax **failover**

Context **[Tree]** (config>router>l2tp failover)
[Tree] (config>router>l2tp>group failover)
[Tree] (config>router>l2tp>group>tunnel failover)
[Tree] (config>service>vprn>l2tp failover)
[Tree] (config>service>vprn>l2tp>group failover)
[Tree] (config>service>vprn>l2tp>group>tunnel failover)

Full Context configure router l2tp failover
configure router l2tp group failover
configure router l2tp group tunnel failover
configure service vprn l2tp failover
configure service vprn l2tp group failover
configure service vprn l2tp group tunnel failover

Description Commands in this context configure LAC multi-chassis redundancy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.10 failure-action

failure-action

Syntax **failure-action down**
no failure-action

Context **[Tree]** (config>router>ldp>lsp-bfd failure-action)

Full Context configure router ldp lsp-bfd failure-action

Description This command configures the action to take when LSP BFD fails on an LDP LSP.

The system generates an SNMP trap if BFD goes down on an LSP, regardless of whether a failure action is configured or not.

The **no** form of this command removes the failure action.

Default no failure-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **down** — Specifies the LSP is marked as unusable in the TTM. If the LSP appears as a shortcut in RTM, then the route is removed.

Platforms All

failure-action

Syntax **failure-action down**
no failure-action

Context **[Tree]** (config>service>epipe>spoke-sdp>bfd failure-action)
[Tree] (config>service>ies>interface>spoke-sdp>bfd failure-action)
[Tree] (config>service>vpls>spoke-sdp>bfd failure-action)
[Tree] (config>service>vprn>interface>spoke-sdp>bfd failure-action)

Full Context configure service epipe spoke-sdp bfd failure-action
configure service ies interface spoke-sdp bfd failure-action
configure service vpls spoke-sdp bfd failure-action
configure service vprn interface spoke-sdp bfd failure-action

Description This command configures the ability to bind the operational state of a spoke-SDP to the state of its VCCV BFD session.

If **failure-action down** is configured, the spoke-SDP is taken operationally down if the associated VCCV BFD session goes down. This configuration also allows BFD packets to be forwarded on an otherwise operationally down spoke-SDP in order to test the spoke-SDP connectivity.

The **no** form of this command removes the failure action.

Default no failure-action

Parameters **down** — Specifies that the spoke-SDP is taken operationally down if the associated VCCV BFD session goes down.

Platforms All

failure-action

Syntax **failure-action** *failure-action*
no failure-action

Context **[Tree]** (config>router>mpls>lsp>bfd failure-action)

Full Context configure router mpls lsp bfd failure-action

Description This command configures what action occurs when LSP BFD fails on an RSVP, SR-TE, or LDP LSP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A failure action of **down** means an LSP is marked as unusable in TTM. If it appears as a shortcut in RTM, the route is removed. This failure action can only be configured on RSVP LSPs.

A failure action of **failover** causes the active path of an RSVP LSP to switch to the secondary or next-preference available secondary path. This option is only available for RSVP LSPs. It is not applicable to **one-hop-p2p** and **mesh-p2p** auto LSPs.

A failure action of **failover-or-down** means that a switchover from the active path is triggered on failure of the BFD session on the active path (primary or standby). If there is no available path to switch to, then the LSP is taken operationally down. For RSVP-TE LSPs, this failure action causes the two best-preference standby paths to be programmed in the data path, in addition to the primary.

The system generates an SNMP trap if BFD goes down on an LSP, regardless of whether a failure action is configured or not.

The **no** form of this command removes the failure action.

Default no failure-action

Parameters **down** — Specifies that the LSP will be marked as unusable in the TTM. If it appears as a shortcut in RTM, then the route will be removed.

failover — Specifies that the active path of an RSVP LSP will switch to the secondary path or next-preference available secondary path. This option is only available for RSVP LSPs. It is not applicable in the LSP template.

failover-or-down — Specifies that the active path of an SR-TE or RSVP-TE LSP switches to the secondary or next-preference available secondary path, or for the LSP to go operationally down if no other path is available.

Platforms All

failure-action

Syntax **failure-action** {**down** | **failover-or-down**}
no failure-action

Context **[Tree]** (config>router>mpls>lsp-template>bfd failure-action)

Full Context configure router mpls lsp-template bfd failure-action

Description This command configures the action to take when LSP BFD fails on an RSVP LSP.

The system generates an SNMP trap if BFD goes down on an LSP, regardless of whether or not a failure action is configured.

The **no** form of this command removes the failure action.

Default no failure-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **down** — Specifies that the LSP is marked as unusable in the TTM. If it appears as a shortcut in RTM, then the route is removed.

failover-or-down — Specifies that the active path of an SR-TE LSP switches to the secondary or next-preference available secondary path, or for the LSP to go operationally down if no other path is available. This option is only available for SR-TE LSPs.

Platforms All

10.11 failure-mode

failure-mode

Syntax **failure-mode** [**discard** | **per-link-hash**]
no failure-mode

Context **[Tree]** (config>lag>link-map-profile failure-mode)

Full Context configure lag link-map-profile failure-mode

Description This command defines the failure mode for egress traffic of SAPs/network interfaces that use this link-map-profile when neither primary nor secondary links of this profile are available.

Default failure-mode per-link-hash

Parameters **discard** — Specifies egress traffic for SAPs/network interfaces using this link-map-profile is discarded to protect SAP/network interface traffic on other LAG links from impact of re-hashing the affected SAPs/network interfaces.

per-link-hash — Specifies egress traffic for SAPs/network interfaces using this link-map-profile is rehashed on remaining, available LAG links using per-link-hash algorithm. SAP/network interface QoS configurations dictate what traffic is discarded on any link that may become oversubscribed as result of the re-hash.

Platforms All

10.12 failure-recovery

failure-recovery

Syntax [**no**] **failure-recovery**

Context **[Tree]** (config>sys>switch-fabric failure-recovery)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system switch-fabric failure-recovery

Description Commands in this context configure attributes related to the automatic switch fabric recovery process.

The automatic switch fabric recovery process is triggered when there are two resets of an IOM/XCM due to ICC failures within a small time frame. The recovery process involves the sequential resetting of SFM in case the issues are due to one of the SFM in the ICC communication path. As the final step in the recovery process, a CPM switchover is triggered to reset the active CPM.

Platforms 7450 ESS, 7750 SR-7, 7950 XRS

10.13 failure-threshold

failure-threshold

Syntax **failure-threshold** *number*
no failure-threshold

Context **[Tree]** (config>test-oam>icmp>ping-template failure-threshold)

Full Context configure test-oam icmp ping-template failure-threshold

Description This command configures the count, when reached, that causes the transition of the IPv4 interface from operationally up to operationally down because of a ping template failure.

The **no** form of this command reverts to the default value.

Default failure-threshold 3

Parameters *number* — Specifies a count that causes the transition of the IP interface from operationally up to operationally down because of ping template failure.

Values 2 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.14 fallback-action

fallback-action

Syntax **fallback-action accept** [**force-probing**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fallback-action user-db *local-user-db-name* [**force-probing**]
no fallback-action

Context **[Tree]** (config>subscr-mgmt>auth-plcy fallback-action)

Full Context configure subscriber-mgmt authentication-policy fallback-action

Description This command configures the action when no RADIUS server is available; servers are either out of service or are in a probing state.

The **no** form of this command removes the action from the configuration.

Parameters **accept** — Specifies that all authentication requests are automatically accepted.

local-user-db-name — Specifies that the LUDB is used to authenticate to the server.

force-probing — Specifies that a subscriber or a test user Access-Request**,** depending which arrives first, is used to probe a RADIUS server before continuing with the configured **fallback-action**. This forces an out-of-service server to transition to a probing state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.15 fallback-path-computation-method

fallback-path-computation-method

Syntax **fallback-path-computation-method** {**none** | **local-cspf**}
no fallback-path-computation-method

Context **[Tree]** (config>router>mpls>lsp fallback-path-computation-method)
[Tree] (config>router>mpls>lsp-template fallback-path-computation-method)

Full Context configure router mpls lsp fallback-path-computation-method
configure router mpls lsp-template fallback-path-computation-method

Description This command specifies the fallback path computation method used if all configured PCEs are down or the signaling overload and the redelegation timer has expired. This method is used regardless of whether the LSP is PCE-controlled and PCE-computed, or just PCE-computed.

The **no** form of this command removes the fallback path computation method used.

Default fallback-path-computation-method none

Parameters **none** — Specifies to fall back to using the named path for RSVP-TE LSPs.

local-cspf — Specifies to fall back to using local CSPF computation.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.16 falling-percent-reset

falling-percent-reset

Syntax **falling-percent-reset** *percent-of-highest*
no falling-percent-reset

Context **[Tree]** (config>mcast-mgmt>bw-plcy falling-percent-reset)

Full Context configure mcast-management bandwidth-policy falling-percent-reset

Description This command is configures the percentage of bandwidth decrease that must occur to reset the dynamic bandwidth monitoring function for a multicast channel. When a channel is configured to use the ingress dynamic bandwidth as the in-use bandwidth for ingress multicast path management, the system maintains a sliding window in time that defines how long the last highest bandwidth value associated with the channel should be used. The sliding window duration is derived from the channels bw-activity dynamic falling-delay parameter within the multicast information policy. Each time the system detects a current bandwidth for a channel that is equal to or greater than the current highest bandwidth for the channel, the sliding window is reset and the highest value is used when managing the ingress multicast paths. If the system does not detect a higher or equal bandwidth value for the channel within the window period, the system resets the sliding window and uses the next highest rate seen during the duration of the window period. In this way, the system delays relinquishing bandwidth for a dynamic bandwidth channel for a configurable period. If a momentary fluctuation (decrease) in ingress bandwidth occurs, the system ignores the bandwidth change.

While this is useful for momentary fluctuations in bandwidth, it may be desirable to react faster when the current bandwidth monitored for a channel drops significantly relative to the currently in-use bandwidth. When the bandwidth decrease is equal to or greater than the falling-percent-reset value, the system immediately stops using the highest bandwidth and starts using the current bandwidth while resetting the sliding window.

If falling-percent-reset is set to 50%, when the current ingress dynamic bandwidth is 50% of the current in-use highest bandwidth, the system immediately uses the current dynamic ingress bandwidth as the highest bandwidth for the channel.

By default, the falling-percent-reset is 50% when a new bandwidth policy is created. The default bandwidth policy also has a hard configured value of 50%. Setting falling-percent-reset to 100 is equivalent to specifying no falling-percent-reset.

The **no** form of this command restores the default value of 50%.

Default falling-percent-reset 50

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent-of-highest* — The percent-of-highest parameter is required and defines the percentage of decline between the current ingress dynamic bandwidth and the current in-use highest bandwidth at which the system resets the dynamic ingress bandwidth monitoring for the channel. When reset in this case, the system uses the current ingress dynamic bandwidth as the highest rate and continues monitoring. The parameter must be defined as an integer value representing a percentage.

Values 1 to 100 percent

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

10.17 family

family

Syntax **family** [**ipv4** | **ipv6**]

Context **[Tree]** (config>lag>bfd family)

Full Context configure lag bfd family

Description This command specifies the address family for the micro-BFD session over the associated LAG links.

Default family ipv4

Parameters **ipv4** — Specifies that IPv4 encapsulation be used for the micro-BFD session.

ipv6 — Specifies that IPv6 encapsulation be used for the micro-BFD session.

Platforms All

family

Syntax **family** *family*

Context **[Tree]** (config>service>vprn>bgp>convergence family)

Full Context configure service vprn bgp convergence family

Description This command specifies the convergence family used for route convergence.

Parameters *family* — Specifies the convergence family used for route convergence

Values ipv4, ipv6

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

family

Syntax [**no**] **family** {**ipv4** | **ipv6** | **label-ipv4** | **flow-ipv4** | **flow-ipv6**}

Context **[Tree]** (config>service>vprn>bgp>graceful-restart>long-lived family)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived family)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived family)

Full Context configure service vprn bgp graceful-restart long-lived family
configure service vprn bgp group graceful-restart long-lived family
configure service vprn bgp group neighbor graceful-restart long-lived family

Description This command configures family-specific LLGR parameters for BGP peers.

Default no family

Parameters **ipv4** — Specifies the IPv4 family.

ipv6 — Specifies the IPv6 family.

label-ipv4 — Specifies the label IPv4 family.

flow-ipv4 — Specifies the flow IPv4 family.

flow-ipv6 — Specifies the flow IPv6 family.

Platforms All

family

Syntax **family** [**ipv4**] [**label-ipv4**] [**ipv6**] [**mcast-ipv4**] [**flow-ipv4**] [**mcast-ipv6**] [**flow-ipv6**]
no family

Context **[Tree]** (config>service>vprn>bgp family)
[Tree] (config>service>vprn>bgp>group family)
[Tree] (config>service>vprn>bgp>group>neighbor family)

Full Context configure service vprn bgp family
configure service vprn bgp group family
configure service vprn bgp group neighbor family

Description This command configures the set of BGP address families (AFI plus SAFI) to be supported by the applicable VPRN BGP sessions.

The **no** form of this command restores the default, which corresponds to unlabeled IPv4 unicast routes (AFI 1, SAFI 1) only.

Default family ipv4

Parameters **ipv4** — Adds support for the IPv4 unicast (unlabeled) address family.

label-ipv4 — Adds support for the IPv4 unicast (labeled) address family.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6 — Adds support for the IPv6 unicast (unlabeled) address family.

mcast-ipv4 — Adds support for the IPv4 multicast SAFI address family.

flow-ipv4 — Adds support for the IPv4 FlowSpec address family.

mcast-ipv6 — Adds support for the IPv6 multicast SAFI address family.

flow-ipv6 — Adds support for the IPv6 FlowSpec address family.

Platforms All

family

Syntax **family** [**ipv4** | **ipv6**]

Context **[Tree]** (config>router>mpls>lsp-template family)

Full Context configure router mpls lsp-template family

Description This command specifies if the lsp-template is for use in IPv4 or IPv6 SR-TE LSP.

This command is optional in a IPv4 SR-TE auto-LSP but must be set to **ipv6** value in a IPv6 SR-TE auto-LSP. By default, this command is set to **ipv4** value for backward compatibility.

When establishing both IPv4 and IPv6 SR-TE mesh auto-LSPs with the same parameters and constraints, a separate LSP template of type **mesh-p2p-srte** must be configured for each address family with the **family** CLI leaf set to the IPv4 or IPv6 value. SR-TE one-hop auto-LSPs can only be established for either IPv4 or IPv6 family, but not both. The **family** leaf in the LSP template of type **one-hop-p2p-srte** should be set to the desired IP family value.

The **no** form of this command reverts to the default value.

Default family ipv4

Parameters **ipv4** — Specifies the lsp-template is for use in IPv4 SR-TE LSP.

ipv6 — Specifies the lsp-template is for use in IPv6 SR-TE LSP.

Platforms All

family

Syntax [**no**] **family**

Context **[Tree]** (config>cflowd>collector>export-filter family)

Full Context configure cflowd collector export-filter family

Description This command defines the address family for the flow types that should not be sent to the associated cflowd collector.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Multiple family types can be defined in this context to filter out multiple address families to a given collector.

The **no** form of this command removes the address family definition, allowing all address family types to be exported to the associated collector.

Default no family

Platforms All

family

Syntax **family** *family*

Context **[Tree]** (config>router>bgp>convergence family)

Full Context configure router bgp convergence family

Description This command configures the IP family used for route convergence.

Parameters *family* — Specifies the convergence family.

Values ipv4, ipv6

Platforms All

family

Syntax **family** [**ipv4**] [**label-ipv4**] [**vpn-ipv4**] [**ipv6**] [**label-ipv6**] [**vpn-ipv6**] [**mcast-ipv4**] [**l2-vpn**] [**mvpn-ipv4**] [**mvpn-ipv6**] [**mdt-safi**] [**ms-pw**] [**flow-ipv4**] [**flow-ipv6**] [**route-target**] [**mcast-vpn-ipv4**] [**evpn**] [**bgp-ls**] [**mcast-ipv6**] [**mcast-vpn-ipv6**] [**sr-policy-ipv4**] [**sr-policy-ipv6**]
no family

Context **[Tree]** (config>router>bgp family)
[Tree] (config>router>bgp>group family)
[Tree] (config>router>bgp>group>neighbor family)

Full Context configure router bgp family
configure router bgp group family
configure router bgp group neighbor family

Description This command configures the set of BGP address families (AFI plus SAFI) to be supported by the base router BGP sessions.

The **no** form of this command restores the default, which corresponds to unlabeled IPv4 unicast routes (AFI 1, SAFI 1) only.

Default family ipv4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **ipv4** — Advertises MP-BGP support for the IPv4 unicast (unlabeled) address family.

label-ipv4 — Advertises MP-BGP support for the IPv4 unicast (labeled) address family.

vpn-ipv4 — Advertises MP-BGP support for the IPv4 VPN (SAFI 128) address family.

ipv6 — Advertises MP-BGP support for the IPv6 unicast (unlabeled) address family.

label-ipv6 — Advertises MP-BGP support for the IPv6 unicast (labeled) address family.

vpn-ipv6 — Advertises MP-BGP support for the IPv6 VPN (SAFI 128) address family.

mcast-ipv4 — Advertises MP-BGP support for the IPv4 multicast SAFI address family.

l2-vpn — Advertises MP-BGP support for the L2 VPN address family.

mvpn-ipv4 — Advertises MP-BGP support for the IPv4 multicast VPN address family.

mvpn-ipv6 — Advertises MP-BGP support for the IPv6 multicast VPN address family.

mdt-safi — Advertises MP-BGP support for the MDT SAFI address family.

ms-pw — Advertises MP-BGP support for the multi-segment pseudowire address family.

flow-ipv4 — Advertises MP-BGP support for the IPv4 FlowSpec address family.

flow-ipv6 — Advertises MP-BGP support for the IPv6 FlowSpec address family.

route-target — Advertises MP-BGP support for RT constraint routes.

mcast-vpn-ipv4 — Advertises MP-BGP support for the IPv4 VPN multicast (SAFI 129) address family.

evpn — Advertises MP-BGP support for the EVPN address family.

bgp-ls — Enables the advertisement of BGP-LS address family to the associated BGP neighbors.

mcast-ipv6 — Advertises MP-BGP support for the IPv6 multicast SAFI address family.

mcast-vpn-ipv6 — Advertises MP-BGP support for the IPv6 multicast routes from a VPRN over the provider network. This family is only applicable in the base BGP routing context.

sr-policy-ipv4 — Advertises MP-BGP support for AFI1/SAFI73 IP address families for BGP routes that encode a segment-routing policy to an IPv4 destination.

sr-policy-ipv6 — Advertises MP-BGP support for AF12/SAF173 IP address families for BGP routes that encode a segment-routing policy to an IPv6 destination.

Platforms All

family

Syntax [**no**] **family** {**ipv4** | **ipv6** | **label-ipv4** | **label-ipv6** | **vpn-ipv4** | **vpn-ipv6** | **l2-vpn** | **route-target** | **flow-ipv4** | **flow-ipv6**}

Context **[Tree]** (config>router>bgp>graceful-restart>long-lived family)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>bgp>group>graceful-restart>long-lived family)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived family)

Full Context configure router bgp graceful-restart long-lived family
configure router bgp group graceful-restart long-lived family
configure router bgp group neighbor graceful-restart long-lived family

Description This command configures family-specific LLGR parameters for BGP peers.

Default no family

Parameters **ipv4** — Specifies the IPv4 family.

ipv6 — Specifies the IPv6 family.

label-ipv4 — Specifies the label IPv4 family.

label-ipv6 — Specifies the label IPv6 family.

vpn-ipv4 — Specifies the VPN IPv4 family.

vpn-ipv6 — Specifies the VPN IPv6 family.

l2-vpn — Specifies the Layer 2 VPN family.

route-target — Specifies the route target family.

flow-ipv4 — Specifies the flow IPv4 family.

flow-ipv6 — Specifies the flow IPv6 family.

Platforms All

family

Syntax **family** {**label-ipv4** | **label-ipv6** | **vpn**}

Context [Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel family)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family

Description This command configures the address family context for configuring next-hop resolution of BGP label routes.

Parameters **label-ipv4** — Enters the context for configuring next-hop-resolution options for labeled-unicast IPv4 routes.

label-ipv6 — Enters the context for configuring next-hop-resolution options for labeled-unicast IPv6 routes.

vpn — Enters the context for configuring next-hop-resolution options for VPN-IPv4 and VPN-IPv6 routes when they are not imported into any VPRN service.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

family

Syntax **family** {**ipv4** | **ipv6**}

Context **[Tree]** (config>router>bgp>next-hop-res>shortcut-tunnel family)

Full Context configure router bgp next-hop-resolution shortcut-tunnel family

Description This command creates the context to configure next-hop resolution of unlabeled IPv4 or unlabeled IPv6 routes by certain tunnel types in the tunnel table.

Parameters **ipv4** — Specifies that the configuration applies to unlabeled IPv4 BGP routes.

ipv6 — Specifies that the configuration applies to unlabeled IPv6 BGP routes.

Platforms All

family

Syntax **family** [**ipv4**] [**ipv6**] [**label-ipv4**] [**label-ipv6**] [**vpn-ipv4**] [**vpn-ipv6**] [**mcast-ipv4**] [**mcast-ipv6**] [**mcast-vpn-ipv4**] [**mcast-vpn-ipv6**] [**evpn**] [**l2-vpn**]
no family

Context **[Tree]** (config>bmp>station family)

Full Context configure bmp station family

Description This command configures the address families that are reported to a BMP monitoring station.

The **no** form of this command reverts to the default.

Default family ipv4

Parameters **ipv4** — Adds support for the IPv4 unicast (unlabeled) address family.

ipv6 — Adds support for the IPv6 unicast (unlabeled) address family.

label-ipv4 — Adds support for the IPv4 unicast (labeled) address family.

label-ipv6 — Adds support for the IPv6 unicast (labeled) address family.

vpn-ipv4 — Adds support for the IPv4 VPN (SAFI 128) address family.

vpn-ipv6 — Adds support for the IPv6 VPN (SAFI 128) address family.

mcast-ipv4 — Adds support for the IPv4 multicast address family.

mcast-ipv6 — Adds support for the IPv6 multicast address family.

mcast-vpn-ipv4 — Adds support for the IPv4 VPN multicast address family.

mcast-vpn-ipv6 — Adds support for the IPv6 VPN multicast address family.

evpn — Adds support for the VPN address family.

l2-vpn — Adds support for the L2-VPN address family.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

family

Syntax **family** {**ipv4** | **ipv6** | **srv4** | **srv6**}

Context **[Tree]** (config>router>isis>igp-shortcut>tunnel-next-hop family)

Full Context configure router isis igp-shortcut tunnel-next-hop family

Description Commands in this context configure the resolution of IGP IPv4 and IGP IPv6 prefix families, as well as SR-ISIS IPv4 and SR-ISIS IPv6 tunnel families using IGP shortcuts.

Parameters **ipv4** — Selects the IPv4 address family.

ipv6 — Selects the IPv6 address family.

srv4 — Selects the SR-ISIS IPv4 tunnel family.

srv6 — Selects the SR-ISIS IPv6 tunnel family.

Platforms All

family

Syntax **family** {**ipv4** | **ipv6**}
no family

Context **[Tree]** (config>router>isis>segment-routing>adjacency-set family)

Full Context configure router isis segment-routing adjacency-set family

Description This command specifies the address family of an adjacency set in IS-IS.

The **no** form of this command reverts to the default.

Default family ipv4

Parameters **ipv4** — Specifies a family of IPv4.

ipv6 — Specifies a family of IPv6.

Platforms All

family

Syntax **family** {**ipv4** | **srv4**}

Context **[Tree]** (config>router>ospf>igp-shortcut>tunnel-next-hop family)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ospf igp-shortcut tunnel-next-hop family

Description Commands in this context configure the resolution of the IGP IPv4 prefix family or SR-OSPF IPv4 tunnel using IGP shortcuts.

Parameters **ipv4** — Selects the IPv4 address family.

srv4 — Selects the SR-OSPF IPv4 tunnel family.

Platforms All

family

Syntax **family ipv6**

Context **[Tree]** (config>router>ospf3>igp-shortcut>tunnel-next-hop family)

Full Context configure router ospf3 igp-shortcut tunnel-next-hop family

Description Commands in this context configure the resolution of the IGP IPv6 prefix family using IGP shortcuts.

Parameters **ipv6** — Selects the IPv6 address family.

Platforms All

family

Syntax **family** [**ipv4**] [**label-ipv4**] [**vpn-ipv4**] [**ipv6**] [**label-ipv6**] [**vpn-ipv6**] [**mcast-ipv4**] [**l2-vpn**] [**mvpn-ipv4**] [**mvpn-ipv6**] [**mdt-safi**] [**ms-pw**] [**flow-ipv4**] [**flow-ipv6**] [**route-target**] [**mcast-vpn-ipv4**] [**evpn**] [**bgp-ls**] [**mcast-ipv6**] [**mcast-vpn-ipv6**] [**sr-policy-ipv4**] [**sr-policy-ipv6**]
no family

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from family)

Full Context configure router policy-options policy-statement entry from family

Description This command specifies address families as matching conditions.

Default no family

Parameters **ipv4** — Matches routes belonging to the IPv4 unicast (unlabeled) address family.

label-ipv4 — Matches routes belonging to the IPv4 unicast (labeled) address family.

vpn-ipv4 — Matches routes belonging to the IPv4 VPN (SAFI 128) address family.

ipv6 — Matches routes belonging to the IPv6 unicast (unlabeled) address family.

label-ipv6 — Matches routes belonging to the IPv6 unicast (labeled) address family.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vpn-ipv6 — Matches routes belonging to the IPv6 VPN (SAFI 128) address family.

mcast-ipv4 — Matches routes belonging to the IPv4 multicast SAFI address family.

l2-vpn — Matches routes belonging to the L2 VPN address family.

mvpn-ipv4 — Matches routes belonging to the IPv4 multicast VPN address family.

mvpn-ipv6 — Matches routes belonging to the IPv6 multicast VPN address family.

mdt-safi — Matches routes belonging to the MDT SAFI address family.

ms-pw — Matches routes belonging to the multi-segment pseudowire address family.

flow-ipv4 — Matches routes belonging to the IPv4 FlowSpec address family.

flow-ipv6 — Matches routes belonging to the IPv6 FlowSpec address family.

route-target — Matches routes belonging to the address family for RT constrain routes.

mcast-vpn-ipv4 — Matches routes belonging to the IPv4 VPN multicast (SAFI 129) address family.

evpn — Matches routes belonging to the EVPN address family.

bgp-ls — Enables the advertisement of BGP-LS address family to the associated BGP neighbors.

mcast-ipv6 — Matches routes belonging to the IPv6 multicast SAFI address family.

mcast-vpn-ipv6 — Matches routes belonging to the IPv6 multicast routes from a VPRN over the provider network. This family is only applicable in the base BGP routing context.

sr-policy-ipv4 — Matches routes belonging to the segment routing policy IPv4 address family (AFI1/SAFI73).

sr-policy-ipv6 — Matches routes belonging to the segment routing policy IPv6 address family (AFI2/SAFI73).

Platforms All

family

Syntax [**no**] **family** {**ipv6 | ipv4**}

Context **[Tree]** (config>router>bgp>srv6 family)

Full Context configure router bgp segment-routing-v6 family

Description This command adds a configuration context for family-specific behaviors that relate to processing prefix SID attributes containing SRv6 TLVs.

The **no** form of this command deletes the family configuration context.

Parameters **ipv4** — Specifies a family of IPv4.

ipv6 — Specifies a family of IPv6.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

family

Syntax [**no**] **family** {**ipv6 | ipv4**}

Context **[Tree]** (config>router>bgp>group>srv6>route family)
[Tree] (config>router>bgp>group>neighbor>srv6>route family)

Full Context configure router bgp group neighbor segment-routing-v6 route-advertisement family
configure router bgp group segment-routing-v6 route-advertisement family

Description This command specifies an address family to use when configuring whether to strip SRv6 TLVs from BGP routes advertised to peers.

The **no** form of this command deletes the context.

Default no family

Parameters **ipv4** — Specifies a family of IPv4.

ipv6 — Specifies a family of IPv6.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

10.18 far-end

far-end

Syntax **far-end** *ip-address*
no far-end

Context **[Tree]** (config>gmpls-tun-grp far-end)

Full Context configure gmpls-tun-grp far-end

Description This command configures the IP address (GMPLS Loopback Address) of the far-end UNI-C router.

The **no** form of this command removes the far-end address

Default no far-end

Parameters *ip-address* — Specifies an IPv4 or IPv6 address of the far-end UNI-C router.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x:x:x:x:x:x:d.d.d.d
x — [0 to FFFF]H
d — [0 to 255]D

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

far-end

Syntax **far-end** *ip-address* [**vc-id** *vc-id*] [{**ing-svc-label** *ingress-vc-label* | **tldp**}] [**icb**]
no far-end *ip-address*

Context **[Tree]** (config>mirror>mirror-dest>remote-source far-end)

Full Context configure mirror mirror-dest remote-source far-end

Description This command is used on a destination router in a remote mirroring solution. See the description for the **remote-source** command for additional information.

When using L2TPv3, MPLS-TP or LDP IPv6 LSP SDPs in the remote mirroring solution, the destination node should be configured with **remote-src>spoke-sdp** entries. For all other types of SDPs, r**emote-source>far-end** entries are used.

Up to 50 far-end entries can be specified.

The **no** form of this command removes the IP address from the remote source configuration.

Parameters *ip-address* — Specifies the service IP address (system IP address) of the remote device sending mirrored traffic to this mirror destination service. If 0.0.0.0 is specified, any remote is allowed to send to this service.

Values 1.0.0.1 to 223.255.255.254

vc-id — Specifies the virtual circuit identifier of the remote source. For mirror services, the *vc-id* defaults to the *service-id*. However, if the *vc-id* is being used by another service a unique vc-id is required to create an SDP binding. For this purpose the mirror service SDP bindings accepts *vc-ids*. This VC ID must match the VC ID used on the spoke SDP that is configured on the source router.

ingress-vc-label — Specifies the ingress service label for mirrored service traffic on the **far end** device for manually configured mirror service labels.

The defined *ing-svc-label* is entered into the ingress service label table which causes ingress packet with that service label to be handled by this mirror destination service.

The specified *ing-svc-label* must not have been used for any other service ID and must match the egress service label being used on the spoke SDP that is configured on the source router. It must be within the range specified for manually configured service labels defined on this router. It may be reused for other far end addresses on this *mirror-dest-service-id*.

Values 2048 to 18431

tldp — Specifies that the label is obtained through signaling via the LDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

icb — Specifies that the remote source is an inter-chassis backup SDP binding.

Platforms All

far-end

Syntax **far-end node-id** *node-id* [**global-id** *global-id*]
far-end [*ip-address* | *ipv6-address*]
no far-end *ip-address* | *ipv6-address*

Context **[Tree]** (config>service>sdp far-end)

Full Context configure service sdp far-end

Description This command configures the system IP address of the far-end destination router for the Service Distribution Point (SDP) that is the termination point for a service.

The far-end IP address must be explicitly configured. The destination IP address must be that of an SR OS and for a GRE SDP it must match the system IP address of the far end router.

If the SDP uses GRE for the destination encapsulation, the IP address is checked against other GRE SDPs to verify uniqueness. If the IP address is not unique within the configured GRE SDPs, an error is generated and the IP address is not associated with the SDP. The local device may not know whether the IP address is actually a system IP interface address on the far-end device.

If the SDP uses MPLS encapsulation, the **far-end** address is used to check LSP names when added to the SDP. If the "**to** IP address" defined within the LSP configuration does not exactly match the SDP **far-end** address, the LSP will not be added to the SDP and an error will be generated. Alternatively, an SDP that uses MPLS can have an MPLS-TP node with an MPLS-TP node-id and (optionally) a global ID. In this case, the SDP must use an MPLS-TP LSP and the SDP **signaling** parameter must be set to **off**.

An SDP cannot be administratively enabled until a **far-end** *ip-address* or MPLS-TP node-id is defined. The SDP is operational when it is administratively enabled (**no shutdown**) and the **far-end** *ip-address* is contained in the IGP routing table as a host route. OSPF ABRs should not summarize host routes between areas. This can cause SDPs to become operationally down. Static host routes (direct and indirect) can be defined in the local device to alleviate this issue.

On a tunnel configured as SDP with delivery type of eth-gre-bridged, this command designates L2oGRE tunnel end points. This is the only configuration option allowed for this type of SDP.

The **no** form of this command removes the currently configured destination IP address for the SDP. The *ip-address* parameter is not specified and will generate an error if used in the **no far-end** command. The SDP must be administratively disabled using the **config service sdp shutdown** command before the **no far-end** command can be executed. Removing the far-end IP address will cause all *lsp-name* associations with the SDP to be removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default none

Parameters **far-end** — Specifies the far-end termination point for the GRE tunnel.

ip-address | *ipv6-address* — Specifies a IPv4 or IPv6 address of the far-end SR OS for the SDP in dotted decimal notation.

node-id — Specifies the MPLS-TP Node ID of the far-end system for the SDP, either in dotted decimal notation (a.b.c.d) or an unsigned 32-bit integer (1 to 4294967295). This parameter is mandatory for an SDP using an MPLS-TP LSP.

global-id — Specifies a MPLS-TP Global ID of the far-end system for the SDP, in an unsigned 32-bit integer (0 to 4294967295). This parameter is optional for an SDP using an MPLS-TP LSP. If not entered, a default value for the Global ID of '0' is used. A global ID of '0' indicates that the far-end node is in the same domain as the local node. The user must explicitly configure a Global ID if its value is non-zero.

Platforms All

10.19 fast-leave

fast-leave

Syntax [**no**] **fast-leave**

Context **[Tree]** (config>service>vpls>sap>igmp-snooping fast-leave)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping fast-leave)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping fast-leave)
[Tree] (config>service>vpls>sap>mld-snooping fast-leave)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping fast-leave)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping fast-leave)

Full Context configure service vpls mesh-sdp igmp-snooping fast-leave
configure service vpls mesh-sdp mld-snooping fast-leave
configure service vpls sap igmp-snooping fast-leave
configure service vpls sap mld-snooping fast-leave
configure service vpls spoke-sdp igmp-snooping fast-leave
configure service vpls spoke-sdp mld-snooping fast-leave

Description This command enables fast leave.

When IGMP fast leave processing is enabled, the 7450 ESS or 7750 SR immediately removes a SAP or SDP from the IP multicast group when it detects an IGMP leave message on that SAP or SDP. Fast leave processing allows the switch to remove a SAP or SDP that sends a leave message from the forwarding table without first sending out group-specific queries to the SAP or SDP, which speeds up the process of changing channels.

Fast leave should only be enabled when there is a single receiver present on the SAP or SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When fast leave is enabled, the configured **last-member-query-interval** value is ignored.

Default no fast-leave

Platforms All

fast-leave

Syntax [**no**] **fast-leave**

Context **[Tree]** (config>subscr-mgmt>igmp-policy fast-leave)

Full Context configure subscriber-mgmt igmp-policy fast-leave

Description This command enables IGMP fast-leave processing.

The **no** form of this command reverts to the default value.

Default fast-leave

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

fast-leave

Syntax [**no**] **fast-leave**

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp fast-leave)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping fast-leave

Description This command enables fast leave.

When IGMP fast leave processing is enabled, the 7450 ESS or 7750 SR will immediately remove a SAP or SDP from the IP multicast group when it detects an IGMP leave on that SAP or SDP. Fast leave processing allows the switch to remove a SAP or SDP that sends a leave from the forwarding table without first sending out group-specific queries to the SAP or SDP, and thus speeds up the process of changing channels (zapping).

Fast leave should only be enabled when there is a single receiver present on the SAP or SDP.

When fast leave is enabled, the configured **last-member-query-interval** value is ignored.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fast-leave

Syntax [**no**] **fast-leave**

Context **[Tree]** (config>subscr-mgmt>mld-policy fast-leave)

Full Context configure subscriber-mgmt mld-policy fast-leave

Description This command enables fast leave. When fast leave processing is enabled, the router immediately removes a SAP or SDP from the IP multicast group when it detects an MLD leave on that SAP or SDP. Fast leave processing allows the switch to remove a SAP or SDP that sends a leave from the forwarding table without first sending out group-specific queries to the SAP or SDP, and thus speeds up the process of changing channels (zapping).

Fast leave should only be enabled when there is a single receiver present on the SAP or SDP.

When fast leave is enabled, the configured last-member-query-interval value is ignored.

The **no** form of this command reverts to the default.

Default fast-leave

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

fast-leave

Syntax [**no**] **fast-leave**

Context **[Tree]** (config>service>pw-template>igmp-snooping fast-leave)

Full Context configure service pw-template igmp-snooping fast-leave

Description This command enables fast leave.

When IGMP fast leave processing is enabled, the 7750 SR will immediately remove a SAP or SDP from the IP multicast group when it detects an IGMP **leave** on that SAP or SDP. Fast leave processing allows the switch to remove a SAP or SDP that sends a **leave** from the forwarding table without first sending out group-specific queries to the SAP or SDP, and thus speeds up the process of changing channels (zapping).

Fast leave should only be enabled when there is a single receiver present on the SAP or SDP.

When fast leave is enabled, the configured last-member-query-interval value is ignored.

Default no fast-leave

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.20 fast-reroute

fast-reroute

Syntax **fast-reroute** [**backup-sr-tunnel**]
no fast-reroute

Context **[Tree]** (config>router>ldp fast-reroute)

Full Context configure router ldp fast-reroute

Description This command enables LDP Fast-Reroute (FRR) procedures. When enabled, LDP uses both the primary next-hop and LFA next-hop, when available, for resolving the next-hop of an LDP FEC against the corresponding prefix in the routing table. This will result in LDP programming a primary NHLFE and a backup NHLFE into the forwarding engine for each next-hop of a FEC prefix for the purpose of forwarding packets over the LDP FEC.

When any of the following events occurs, LDP instructs in the fast path the forwarding engines to enable the backup NHLFE for each FEC next-hop impacted by this event:

- An LDP interface goes operationally down, or is admin shutdown.
- An LDP session to a peer went down as the result of the Hello or Keep-Alive timer expiring.
- The TCP connection used by a link LDP session to a peer went down, due say to next-hop tracking of the LDP transport address in RTM, which brings down the LDP session.
- A BFD session, enabled on a T-LDP session to a peer, times-out and as a result the link LDP session to the same peer and which uses the same TCP connection as the T-LDP session goes also down.
- A BFD session enabled on the LDP interface to a directly connected peer, times out and brings down the link LDP session to this peer.

The **tunnel-down-dump-time** option or the **label-withdrawal-delay** option, when enabled, does not cause the corresponding timer to be activated for a FEC as long as a backup NHLFE is still available.

Because LDP can detect the loss of a neighbor/next-hop independently, it is possible that it switches to the LFA next-hop while IGP is still using the primary next-hop. Also, when the interface for the previous primary next-hop is restored, IGP may re-converge before LDP completed the FEC exchange with it neighbor over that interface. This may cause LDP to de-program the LFA next-hop from the FEC and blackhole traffic. In order to avoid this situation, it is recommended to enable IGP-LDP synchronization on the LDP interface.

When the SPF computation determines there is more than one primary next-hop for a prefix, it will not program any LFA next-hop in RTM. Thus, the LDP FEC will resolve to the multiple primary next-hops that provide the required protection.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **backup-sr-tunnel** option enables the use of SR tunnel, as a remote LFA or TI-LFA backup tunnel next-hop by an LDP FEC.

As a pre-requisite, the user must enable the stitching of LDP and SR in the LDP-to-SR direction. That is because the LSR must perform the stitching of the LDP ILM to SR tunnel when the primary LDP next-hop of the FEC fails. Thus LDP must listen to SR tunnels programmed by the IGP in TTM but the mapping server feature is not required.

Assuming the following:

- the **backup-sr-tunnel** option is enabled in LDP
- the {**loopfree-alternates remote-lfa**} and/or the {**loopfree-alternates ti-lfa**} option is enabled in the IGP instance
- LDP was able to resolve the primary next-hop of the LDP FEC in RTM

IGP SPF will run both the base LFA and the TI-LFA algorithms and if it does not find a backup next-hop for a prefix of an LDP FEC, it will also run the remote LFA algorithm. If IGP finds a TI-LFA or a remote LFA tunnel next-hop, LDP programs the primary next-hop of the FEC using a LDP NHLFE and programs the LFA backup next-hop using a LDP NHLFE pointing to the SR tunnel endpoint. Note that the LDP packet is not “tunneled” over the SR tunnel. The LDP label is actually stitched to the segment routing label stack. LDP points both the LDP ILM and the LTN to the backup LDP NHLFE which itself uses the SR tunnel endpoint.

The behavior of the feature is thus similar to the LDP-to-SR stitching feature, except the behavior is augmented to allow the stitching of an LDP ILM/LTN to a SR tunnel also when the primary LDP next-hop of the FEC fails.

If the LDP FEC primary next-hop failed and LDP has pre-programmed a remote LFA or TI-LFA next-hop with a LDP backup NHLFE pointing to SR tunnel, the LDP ILM/LTN switches to it. Note that if for some reason the failure impacted only the LDP tunnel primary next-hop but not the SR tunnel primary next-hop, the LDP backup NHLFE will effectively point to the primary next-hop of the SR tunnel and traffic of the LDP ILM/LTN will follow this path instead of the TI-LFA or remote LFA next-hop of the SR tunnel until the latter is activated.

This feature is limited to IPv4 /32 prefixes in both LDP and SR.

The **no** form of this command disables the use of SR tunnels as backups for LDP FECs and disables LDP FRR.

Default no fast-reroute

Platforms All

fast-reroute

Syntax **fast-reroute** *frr-method*
no fast-reroute

Context **[Tree]** (config>router>mpls>lsp fast-reroute)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>mpls>lsp-template fast-reroute)

Full Context
configure router mpls lsp fast-reroute
configure router mpls lsp-template fast-reroute

Description
This command creates a pre-computed detour LSP from each node in the path of the LSP. In case of failure of a link or LSP between two nodes, traffic is immediately rerouted on the pre-computed detour LSP, thus avoiding packet-loss.

When **fast-reroute** is enabled, each node along the path of the LSP tries to establish a detour LSP as follows:

- Each upstream node sets up a detour LSP that avoids only the immediate downstream node, and merges back on to the actual path of the LSP as soon as possible.

  If it is not possible to set up a detour LSP that avoids the immediate downstream node, a detour can be set up to the downstream node on a different interface.
- The detour LSP may take one or more hops (see **config>router>mpls>lsp hop-limit**, **config>router>mpls>lsp>primary-p2mp-instance hop-limit**) before merging back on to the main LSP path.
- When the upstream node detects a downstream link or node failure, the ingress router switches traffic to a standby path if one was set up for the LSP.

Fast reroute is available only for the primary path. No configuration is required on the transit hops of the LSP. The ingress router will signal all intermediate routers using RSVP to set up their detours. TE must be enabled for fast-reroute to work.

If an LSP is configured with **fast-reroute** *frr-method* specified but does not enable CSPF, then global revertive will not be available for the LSP to recover.

The **no** form of the **fast-reroute** command removes the detour LSP from each node on the primary path. This command will also remove configuration information about the hop-limit and the bandwidth for the detour routes.

The **no** form of **fast-reroute hop-limit** command reverts to the default value.

Note: A one-to-one detour backup LSP cannot be used at the PLR for ABR node protection. As a result, a PLR node does not signal a one-to-one detour LSP for ABR protection. In addition, the ABR node rejects a Path message that it has received from a third-party implementation configured with a detour object and a loose ERO next-hop. The Path message is rejected regardless of whether the **cspf-on-loose-hop** command is enabled on the node. When the router transits ABR for the detour path, the router rejects the signaling of an inter-area detour backup LSP.

Default
no fast-reroute — When fast-reroute is specified, the default fast-reroute method is one-to-one.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *frr-method* — Configures the fast-reroute method.

Values **one-to-one** — In the one-to-one technique, a label switched path is established which intersects the original LSP somewhere downstream of the point of link or node failure. For each LSP which is backed up, a separate backup LSP is established.

Values **facility** — This option, sometimes called many-to-one, takes advantage of the MPLS label stack. Instead of creating a separate LSP for every backed-up LSP, a single LSP is created which serves to backup up a set of LSPs. This LSP tunnel is called a bypass tunnel.

The bypass tunnel must intersect the path of the original LSP(s) somewhere downstream of the point of local repair (PLR). Naturally, this constrains the set of LSPs being backed-up through that bypass tunnel to those that pass through a common downstream node. All LSPs which pass through the PLR and through this common node which do not also use the facilities involved in the bypass tunnel are candidates for this set of LSPs.

Platforms All

fast-reroute

Syntax [**no**] **fast-reroute**

Context **[Tree]** (config>router>bier fast-reroute)

Full Context configure router bier fast-reroute

Description This command enables BIER Fast Reroute (FRR).

The **no** form of this command disables BIER FRR.

Default no fast-reroute

Platforms All

10.21 fast-start

fast-start

Syntax [**no**] **fast-start**

Context **[Tree]** (config>qos>adv-config-policy>child-control>offered-measurement fast-start)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos adv-config-policy child-control offered-measurement fast-start

Description This command is used to enable fast detection of initial bandwidth on a child policer or queue associated with the policy. Multiple offered rate counter reads may be performed per the sampling interval. The system accumulates these counter values and evaluates the delta at the conclusion of the sampling interval. When fast-start is enabled, the system identifies all children associated with the policy that enter the inactive state (current offered rate is zero). Any inactive 'fast start' child that has a positive offered counter during a sampling period bypasses the normal sampling interval and does an immediate offered rate evaluation.

This option is intended for use with children that would benefit from faster than normal startup detection, typically those of a real-time nature.

When this parameter is not enabled, the system uses the normal sampling interval behavior of both newly active and currently active children.

The **no** form of this command is used to restore the sampling-interval-based offered rate evaluation for newly active children.

Platforms All

10.22 fast-stop

fast-stop

Syntax [**no**] **fast-stop**

Context **[Tree]** (config>qos>adv-config-policy>child-control>offered-measurement fast-stop)

Full Context configure qos adv-config-policy child-control offered-measurement fast-stop

Description This command is used to enable fast detection of lack of offered rate on a child policer or queue associated with the policy. Multiple offered rate counter reads may be performed per sampling interval. The system accumulates these counter values and evaluates the delta at the conclusion of the sampling interval. When fast-stop is enabled, the system bypasses the sampling interval for any currently active 'fast stop' child that has a zero offered counter measurement and does an immediate offered rate evaluation using the zero value.

This option is intended for use with children where other children would benefit from faster than normal inactive detection, typically those of a real-time nature.

When this parameter is not enabled, the system uses the normal sampling interval behavior of both newly inactive and currently active children.

The **no** form of this command is used to restore the sampling-interval-based offered rate evaluation for newly inactive children.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.23 fate-sharing-group-template

fate-sharing-group-template

Syntax **fate-sharing-group-template** *name* **[create]**
no fate-sharing-group-template *name*

Context **[Tree]** (config>subscr-mgmt>up-resiliency fate-sharing-group-template)

Full Context configure subscriber-mgmt up-resiliency fate-sharing-group-template

Description This command creates a template that configures resiliency parameters per FSG.

The **no** form of this command deletes the template.

Parameters *name* — Specifies the FSG template ID, up to 32 characters.

create — Keyword used to create a template. The **create** keyword requirement can be disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.24 fault-propagation-bmac

fault-propagation-bmac

Syntax **fault-propagation-bmac** [*mac-name* | *ieee-address*] [**create**]
no fault-propagation-bmac [*mac-name* | *ieee-address*]

Context **[Tree]** (config>service>vpls>mesh-sdp fault-propagation-bmac)
[Tree] (config>service>vpls>sap fault-propagation-bmac)
[Tree] (config>service>vpls>spoke-sdp fault-propagation-bmac)

Full Context configure service vpls mesh-sdp fault-propagation-bmac
configure service vpls sap fault-propagation-bmac
configure service vpls spoke-sdp fault-propagation-bmac

Description This command configures associated B-MAC addresses for fault propagation on a B-VPLS SAP or SDP binding. The statement can appear up to four times in the configuration to support four remote B-MAC addresses in the same remote B-VPLS. The configured VPLS must be a B-VPLS.

The **no** form of this command removes the specified MAC name or MAC address from the list of Fault Propagation B-MAC addresses associated with the SAP (or SDP).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac-name* — Specifies a (predefined) MAC name to associate with the SAP or SDP, indirectly specifying a Fault Propagation B-MAC address. Up to 32 characters in length

ieee-address — Specifies a MAC address to associate with the SAP or SDP, directly specifying a Fault Propagation B-MAC address. The value should be input in either a xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format.

Platforms All

10.25 fault-propagation-enable

fault-propagation-enable

Syntax **fault-propagation-enable** {**use-if-tlv** | **suspend-ccm**}
no fault-propagation-enable

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>ipipe>sap>eth-cfm>mep fault-propagation-enable)

Full Context configure service epipe sap eth-cfm mep fault-propagation-enable
configure service epipe spoke-sdp eth-cfm mep fault-propagation-enable
configure service ipipe sap eth-cfm mep fault-propagation-enable

Description This command configures the fault propagation for the MEP.

Parameters **use-if-tlv** — Specifies to use the interface TLV.

suspend-ccm — Specifies to suspend continuity check messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fault-propagation-enable

Syntax **fault-propagation-enable** {**use-if-tlv** | **suspend-ccm**}
no fault-propagation-enable

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>vpls>sap>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep fault-propagation-enable)

Full Context configure service vpls mesh-sdp eth-cfm mep fault-propagation-enable
configure service vpls sap eth-cfm mep fault-propagation-enable
configure service vpls spoke-sdp eth-cfm mep fault-propagation-enable

Description This command configures the fault propagation for the MEP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **use-if-tlv** — Specifies to use the interface TLV.

suspend-ccm — Specifies to suspend the continuity check messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fault-propagation-enable

Syntax **fault-propagation-enable** {**use-if-tlv** | **suspend-ccm**}
no fault-propagation-enable

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep fault-propagation-enable)

Full Context configure service ies interface sap eth-cfm mep fault-propagation-enable
configure service ies interface spoke-sdp eth-cfm mep fault-propagation-enable
configure service ies subscriber-interface group-interface sap eth-cfm mep fault-propagation-enable

Description This command configures the fault propagation for the MEP.

Parameters **use-if-tlv** — Specifies to use the interface TLV.

suspend-ccm — Specifies to suspend the continuity check messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep fault-propagation-enable

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep fault-propagation-enable
- configure service ies interface spoke-sdp eth-cfm mep fault-propagation-enable

fault-propagation-enable

Syntax **fault-propagation-enable** {**use-if-tlv** | **suspend-ccm**}
no fault-propagation-enable

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep fault-propagation-enable)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm fault-propagation-enable)

Full Context configure service vprn interface sap eth-cfm mep fault-propagation-enable
configure service vprn interface spoke-sdp eth-cfm mep fault-propagation-enable
configure service vprn subscriber-interface group-interface sap eth-cfm fault-propagation-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the fault propagation for the MEP.

Parameters **use-if-tlv** — Specifies to use the interface TLV.

suspend-ccm — Specifies to suspend the continuity check messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.26 fc

fc

Syntax **fc** *fc-name* [*fc-name*]
no fc

Context **[Tree]** (config>service>epipe>sap>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>ipipe>sap>eth-cfm>collect-lmm-fc-stats fc)

Full Context configure service epipe sap eth-cfm collect-lmm-fc-stats fc
configure service epipe spoke-sdp eth-cfm collect-lmm-fc-stats fc
configure service ipipe sap eth-cfm collect-lmm-fc-stats fc

Description This command creates individual counters for the specified FCs without regard for profile. All countable packets that match a configured FC, regardless of profile, will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-aware FC using the **fc-in-profile** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-unaware counter. In order for the counter to be used, the **config**>**oam-pm**>**session**>**ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc

Syntax **fc** *fc-name* [*fc-name*]
no fc

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>vpls>sap>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc)

Full Context configure service vpls mesh-sdp eth-cfm collect-lmm-fc-stats fc
configure service vpls sap eth-cfm collect-lmm-fc-stats fc
configure service vpls spoke-sdp eth-cfm collect-lmm-fc-stats fc

Description This command creates individual counters for the specified FCs without regard for profile. All countable packets that match a configured FC, regardless of profile, will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-aware FC using the **fc-in-profile** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc

Parameters *fc-name* — Specifies up to eight names of the FC for which to create an individual profile-unaware counter. In order for the counter to be used, the **config**>**oam-pm**>**session**> **ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc

Syntax **fc** *fc-name* [*fc-name*]
no fc

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>collect-lmm-fc-stats fc)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>collect-lmm-fc-stats fc)

Full Context configure service ies interface sap eth-cfm collect-lmm-fc-stats fc
configure service ies interface spoke-sdp eth-cfm collect-lmm-fc-stats fc
configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc

Description This command creates individual counters for the specified FCs without regard for profile. All countable packets that match a configured FC, regardless of profile, will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

An FC that is specified as part of this command for this specific context cannot be specified as a profile-aware FC using the **fc-in-profile** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-unaware counter. Up to eight FCs may be specified. In order for the counter to be used, the **config**>**oam-pm**>**session**>**ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm collect-lmm-fc-stats fc
- configure service ies interface sap eth-cfm collect-lmm-fc-stats fc

fc

Syntax **fc** *fc-name* [*fc-name*]
no fc

Context [Tree] (config>service>vprn>if>sap>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>collect-lmm-fc-stats fc)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap eth-cfm collect-lmm-fc-stats fc
configure service vprn interface spoke-sdp eth-cfm collect-lmm-fc-stats fc
configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc

Description This command creates individual counters for the specified FCs without regard for profile. All countable packets that match a configured FC, regardless of profile, will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-aware FC using the **fc-in-profile** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-unaware counter. Up to 8 FCs can be named in a single statement. In order for the counter to be used, the **config**>**oam-pm**>**session**>**ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm collect-lmm-fc-stats fc
- configure service vprn interface spoke-sdp eth-cfm collect-lmm-fc-stats fc

fc

Syntax **fc** {**be** | **l2** | **af** | **l1** | **h2** | **ef** | **h1**| **nc**} **forwarding-set** *set-id*
no {**be** | **l2** | **af** | **l1** | **h2** | **ef** | **h1** | **nc**}

Context **[Tree]** (config>router>mpls>class-forwarding-policy fc)

Full Context configure router mpls class-forwarding-policy fc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the mapping of FCs to up to six forwarding sets for the class-based forwarding (CBF) of an LDP FEC or a BGP prefix over IGP shortcuts.

All FCs are mapped to set 1 as soon as the policy is created. The user can then make changes to the mapping of FCs as required. An FC that is not added to the class forwarding policy is thus always mapped to set 1. An FC can only be mapped to one forwarding set. One or more FCs can map to the same set. The user can indicate the initial default set by including the **default-set** option.

The default forwarding set forwards packets of an FC when all LSPs of the forwarding set that the FC maps to become operationally down. The router uses the user-configured default set as the initial default set if no default is configured; otherwise, it elects the lowest numbered set as the default forwarding set in a class forwarding policy. When the last LSP in a default forwarding set goes into an operationally down state, the router designates the next lowest numbered set as the new default forwarding set.

Parameters **{be | l2 | af | l1 | h2 | ef | h1 | nc}** — Specifies the name of the forwarding class.

set-id — Specifies the class forwarding set.

Values 1 to 4 (in system profile None/A)
1 to 6 (in system profile B)

Platforms All

fc

Syntax **fc** *fc-name* **sampling-weight** *sampling-weight*
no fc

Context **[Tree]** (config>router>mpls>lsp-template>auto-bandwidth fc)

Full Context configure router mpls lsp-template auto-bandwidth fc

Description This command configures the sampling weight.

Platforms All

fc

Syntax **fc** *fc-name* **class-type** *ct-number*
no fc fc-name

Context **[Tree]** (config>router>rsvp>diffserv-te fc)

Full Context configure router rsvp diffserv-te fc

Description This command maps one or more system forwarding classes to a Diff-Serv Class Type (CT). The default mapping is shown in Table 58.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 58 **Forwarding Classes Mapping**

FC ID	FC Name	FC Designation	Class Type (CT)
7	Network Control	NC	7
6	High-1	H1	6
5	Expedited	EF	5
4	High-2	H2	4
3	Low-1	L1	3
2	Assured	AF	2
1	Low-2	L2	1
0	Best Effort	BE	0

The **no** form of this command reverts to the default mapping for the forwarding class name.

Parameters **class-type** *ct-number* — The Diff-Serv Class Type number. One or more system forwarding classes can be mapped to a CT.

Values 0 to 7

Platforms All

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action>remark fc)

Full Context configure application-assurance group policy app-qos-policy entry action remark fc

Description This command configures remark FC action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured forwarding class.

The **no** form of this command stops FC remarking action on packets belonging to flows matching this AQP entry.

Default no fc

Parameters *fc-name* — Configure the FC remark action for flows matching this entry.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc

Syntax [**no**] **fc** *fc-name*

Context **[Tree]** (config>service>nat>nat-policy>priority-sessions fc)
[Tree] (config>service>nat>firewall-policy>priority-sessions fc)
[Tree] (config>service>nat>up-nat-policy>priority-sessions fc)

Full Context configure service nat firewall-policy priority-sessions fc
configure service nat nat-policy priority-sessions fc
configure service nat up-nat-policy priority-sessions fc

Description This command configures the forwarding classes that have their sessions prioritized.

Parameters *fc-name* — Specifies the forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy priority-sessions fc
- configure service nat up-nat-policy priority-sessions fc

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy priority-sessions fc

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>mirror>mirror-dest fc)

Full Context configure mirror mirror-dest fc

Description This command specifies a forwarding class for all mirrored packets transmitted to the destination SAP or SDP overriding the default (be) forwarding class. All packets are sent with the same class of service to minimize out-of-sequence issues. The mirrored packet does not inherit the forwarding class of the original packet.

When the destination is on a SAP, a single egress queue is created that pulls buffers from the buffer pool associated with the *fc-name*.

When the destination is on an SDP, the *fc-name* defines the DiffServ-based egress queue that is used to reach the destination. The *fc-name* also defines the encoded forwarding class of the encapsulation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The FC configuration also affects how mirrored packets are treated at the ingress queuing point on the line cards. One ingress queue is used per mirror destination (service) and that is an expedited queue if the configured FC is expedited (one of nc, h1, ef or h2). The ingress mirror queues have no CIR, but a line-rate PIR.

The **no** form of this command reverts the mirror-dest service ID forwarding class to the default forwarding class.

Default The best effort (be) forwarding class is associated with the mirror-dest service ID.

Parameters *fc-name* — The name of the forwarding class with which to associate mirrored service traffic. The forwarding class name must already be defined within the system. If the *fc-name* does not exist, an error is returned and the **fc** command has no effect. If the *fc-name* does exist, the forwarding class associated with *fc-name* overrides the default forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

fc

Syntax **fc** *fc-name* [**profile** {**in** | **out**}]
no fc

Context **[Tree]** (config>test-oam>ldp-treetrace fc)

Full Context configure test-oam ldp-treetrace fc

Description This command indicates the forwarding class and profile of the MPLS echo request packet.

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified FC and profile parameter values. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface.

When the MPLS echo request packet is received on the responding node, The FC and profile parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the FC and profile parameter values determined by the classification of the echo request packet, which is being replied to, at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. The ToS byte is not modified. Table 59 summarizes this behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 59 **fc Request Packet and Behavior**

CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • pkt queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet {tos=1, fc2, profile2}
Outgoing interface (responder node)	Echo reply packet: • pkt queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

Default no fc

Parameters *fc-name* — Specifies the forwarding class of the MPLS echo request packets.

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out} — Specifies the profile value to be used with the forwarding class specified in the **fc-name** parameter.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy fc)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy fc)

Full Context configure saa test type-multi-line lsp-ping sr-policy fc
configure saa test type-multi-line lsp-trace sr-policy fc

Description This command specifies the FC and profile parameters that are used to indicate the forwarding class and profile of the MPLS echo request packet.

The **no** form of this command reverts to the default value.

Default fc be

Parameters *fc-name* — Specifies the forwarding class name.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

Platforms All

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>oam-pm>session>ip fc)

Full Context configure oam-pm session ip fc

Description This command sets the forwarding class designation for TWAMP Light packets that are sent through the node and exposed to the various QoS functions on the network element.

The **no** form of this command restores the default value.

Default fc be

Parameters *fc-name* — Specifies the forwarding class name.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>oam-pm>session>mpls fc)

Full Context configure oam-pm session mpls fc

Description This command sets the forwarding class designation for DM packets sent through the node and exposed to the various QoS functions on the network element.

The **no** form of this command reverts the default value.

Default fc be

Parameters *fc-name* — Specifies the forwarding class name.

Values be — Specifies best effort
l2 — Specifies low-2
af — Specifies assured
l1 — Specifies low-1
h2 — Specifies high-2
ef — Specifies expedited
h1 — Specifies high-1
nc — Specifies network control

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc

Syntax **fc** *fc-name* **profile** *profile* [**create**]
no fc *fc-name* **profile** *profile*

Context **[Tree]** (config>qos>post-policer-mapping fc)

Full Context configure qos post-policer-mapping fc

Description This command specifies the forwarding class and profile state of an egress policed packet that is to be mapped to another forwarding class and profile, where the profile state is that of the resulting profile after the packet has been processed by the egress policer.

The new forwarding class and profile state is configured using the **maps-to** command.

The traffic remarking is based on the marking configured for the forwarding class and profile of the traffic after being policed but before it is remapped.

The **no** form of this command deletes the forwarding class and profile remapping statement, including the **maps-to** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *fc-name* — Specifies one of the eight forwarding classes supported by the system.

Values be, l2, af, l1, h2, ef, h1, nc

profile — Specifies one of the egress packet profile states.

Values exceed, in, inplus, out

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

fc

Syntax **fc** *fc-name* [**create**]
no fc *fc-name*

Context **[Tree]** (config>qos>sap-ingress fc)

Full Context configure qos sap-ingress fc

Description The **fc** command creates a class or subclass instance of the forwarding class fc-name. When the *fc-name* is created, classification actions can be applied and the subclass can be used in match classification criteria. Attempting to use an undefined subclass in a classification command will result in an execution error and the command will fail.

The **no** form of this command removes all the explicit queue mappings for *fc-name* forwarding types. The queue mappings revert to the default queues for *fc-name*. To successfully remove a subclass, all associations with the subclass in the classification commands within the policy must first be removed or diverted to another forwarding class or subclass.

Parameters *fc-name* — The parameter subclass-name is optional and must be defined using a dot separated notation with a preceding valid system-wide forwarding class name. Creating a subclass follows normal naming conventions. Up to sixteen ASCII characters may be used. If the same sub-name is used with two or more forwarding class names, each is considered a different instance of subclass. A subclass must always be specified with its preceding forwarding class name. When a forwarding class is created or specified without the optional subclass, the parent forwarding class is assumed.

Within the SAP ingress QoS policy, up to 56 subclasses may be created. Each of the 56 subclasses may be created within any of the eight parental forwarding classes. When the limit of 56 is reached, any further subclass creations will fail and the subclass will not exist.

Successfully creating a subclass places the CLI within the context of the subclass for further subclass parameter definitions. Within the subclass context, commands may be executed that define subclass priority (within the parent forwarding class queue mapping), subclass color aware profile settings, subclass in-profile and out-of-profile precedence or DSCP markings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The *subclass-name* parameter is optional and used with the *fc-name* parameter to define a pre-existing subclass. The *fc-name* and *subclass-name* parameters must be separated by a period (.). If *subclass-name* does not exist in the context of *fc-name*, an error will occur. If *subclass-name* is removed using the **no fc** *fc-name.subclass-name* **force** command, the **default-fc** command will automatically drop the *subclass-name* and only use *fc-name* (the parent forwarding class for the subclass) as the forwarding class.

Values

fc: *class*[.*subclass*]
class: be, l2, af, l1, h2, ef, h1, nc
subclass: 29 characters max

create — Required parameter when creating a SAP QoS ingress policy forwarding class.

Platforms All

fc

Syntax **fc** *fc-name* [**create**]
no fc *fc-name*

Context **[Tree]** (config>qos>sap-egress fc)

Full Context configure qos sap-egress fc

Description The **fc** fc-*name* node within the SAP egress QoS policy is used to contain the explicitly defined queue mapping and dot1p marking commands for *fc-name*. When the mapping for *fc-name* points to the default queue and the dot1p marking is not defined, the node for *fc-name* is not displayed in the **show configuration** or **save configuration** output unless the detail option is specified.

The **no** form of this command removes the explicit queue mapping and dot1p marking commands for *fc-name*. The queue mapping reverts to the default queue for *fc-name* and the dot1p marking (if appropriate) uses the default of 0.

Default no fc

Parameters *fc-name* — This parameter specifies that the forwarding class queue mapping or dot1p marking is to be edited. The value given for *fc-name* must be one of the predefined forwarding classes in the system.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc

Syntax **fc** *fc-name* **mlppp-class** *class-id*
no fc *fc-name*

Context **[Tree]** (config>qos>mlppp-profile-egress>class fc)

Full Context configure qos mlppp-profile-egress class fc

Description This command configures the mapping of the system forwarding class to the MLPPP classes for this profile. There is a many-to-one relationship between the system forwarding class and an MLPPP class.

Parameters *fc-name* — Specifies the forwarding class name.

Values b3, l2, af, l1, h2, ef, h1, nc

class-id — Specifies the class ID.

Values 0 to 3

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>qos>network>ingress fc)

Full Context configure qos network ingress fc

Description This command is used to enter the CLI node to configure QoS parameters for the specified forwarding class. The **fc** command overrides the default parameters for that forwarding class from the values defined in the network default policy.

The **no** form of this command removes the forwarding class name configuration. The forwarding class reverts to the parameters defined in the default network policy.

Parameters *fc-name* — The case-sensitive, system-defined forwarding class name for which policy entries will be created.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>qos>network>egress fc)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos network egress fc

Description This command is used to enter the CLI node to configure QoS parameters for the specified forwarding class. The FC name represents a CLI parent node that contains parameters describing the egress marking criteria of packets flowing through it. This command overrides the default parameters for that forwarding class from the values defined in the network default policy. It can also be used to redirect packets to a policer or queue in a network egress queue group instance.

The **no** form of this command removes the forwarding class name configuration. The forwarding class reverts to the parameters defined in the default network policy.

Parameters *fc-name* — The case-sensitive, system-defined forwarding class name for which policy entries will be created.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

fc

Syntax **fc** *fc-name* [**create**]
no fc *fc-name*

Context **[Tree]** (config>qos>network-queue fc)

Full Context configure qos network-queue fc

Description The **fc** command is used to enter the forwarding class mapping context for the given *fc-name*. Each forwarding class maps by default to queues 1 (unicast) and 9 (multipoint).

Parameters *fc-name* — A valid forwarding class must be specified as *fc-name* when the **fc** command is executed. When the **fc** *fc-name* command is successfully executed, the system will enter the specified forwarding class context where the **queue** *queue-id* command may be executed.

Values be, l2, af, l1, h2, ef, h1, nc

create — Required parameter when creating an FC node.

Platforms All

fc

Syntax **fc** *fc-name* [**create**]
no fc *fc-name*

Context **[Tree]** (cfg>qos>qgrps>egr>qgrp fc)

Full Context configure qos queue-group-templates egress queue-group fc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **fc** command is used to enter the forwarding class mapping context for the given fc-name. Each forwarding class has a default mapping depending on the egress queue group template. The system-created policer-output-queue template contains queues 1 and 2 by default with queue 1 being best-effort and queue 2 expedited. Forwarding classes be, l1, af and l2 all map to queue 1 by default. Forwarding classes h1, ef, h2 and nc all map to queue 2 by default. More queues may be created within the policer-output-queues template and the default forwarding classes may be changed to any defined queue within the template.

When all other user-defined egress queue group templates are created, only queue 1 (best-effort) exists and all forwarding classes are mapped to that queue. Other queues may be created and the forwarding classes may be changed to any defined queue within the template.

Besides the default mappings within the templates, the egress queue group template forwarding class queue mappings operate the same as the forwarding class mappings in a sap-egress QoS policy.

The template forwarding class mappings are the default mechanism for mapping egress policed traffic to a queue within an egress port queue group associated with the template. If a queue-id is explicitly specified in the QoS policy forwarding class policer mapping, and that queue exists within the queue group, the template forwarding class mapping is ignored.

On the 7450 ESS and 7750 SR, egress policed subscriber traffic works in a slightly different way. The subscriber and subscriber host support destination and organization strings are used to identify the egress port queue group. In this instance, the forwarding class mappings are always used and any queue overrides in the QoS policy are ignored. If neither string exists for the subscriber host, the egress queue group queue-id can be derived from either the QoS policy policer mapping or the template forwarding class queue mappings.

The **no** form of this command is used to return the specified forwarding class to its default template queue mapping.

Parameters *fc-name* — A valid forwarding class must be specified as *fc-name* when the **fc** command is executed. When the **fc** *fc-name* command is successfully executed, the system will enter the specified forwarding class context where the **queue** *queue-id* command may be executed.

Values **be**, **l1**, **af**, **l2**, **h1**, **ef**, **h2**, **nc**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

fc

Syntax **fc** *fc-name* [**create**]
no fc

Context **[Tree]** (config>qos>shared-queue fc)

Full Context configure qos shared-queue fc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the forwarding class name. The forwarding class name represents an egress queue. The **fc** *fc-name* represents a CLI parent node that contains sub-commands or parameters describing the egress characteristics of the queue and the marking criteria of packets flowing through it. The **fc** command overrides the default parameters for that forwarding class defined in the network default policy *policy-id* 1.

Default Refer to "Default Shared Queue Policy Values" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for undefined forwarding class values.

Parameters *fc-name* — The case-sensitive, system-defined forwarding class name for which policy entries will be created.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

fc

Syntax **fc** *fc-name*
no fc

Context **[Tree]** (config>filter>ip-filter>entry>action fc)
[Tree] (config>filter>ipv6-filter>entry>action fc)

Full Context configure filter ip-filter entry action fc
configure filter ipv6-filter entry action fc

Description This command assigns a forwarding class to packets matching the filter entry.

The **no** version of this command removes the forwarding class marking action.

Parameters *fc-name* — Specifies the forwarding class name.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms All

fc

Syntax **fc** *fc-name* [*fc-name*]
no fc

Context **[Tree]** (config>router>if>eth-cfm>mep>collect-lmm-fc-stats fc)

Full Context configure router interface eth-cfm mep collect-lmm-fc-stats fc

Description This command creates individual counters for the specified FCs without regard for profile. All countable packets that match a configured FC, regardless of profile, will be included in this counter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-aware FC using the **fc-in-profile** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-unaware counter. A maximum of eight fc-names can be specified in a single statement. In order for the counter to be used, the **config**>**oam-pm**>**session**> **ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc

Syntax **fc** {*fc*} **lsp** *lsp-name*
no fc {fc}

Context **[Tree]** (config>service>sdp>class-forwarding fc)

Full Context configure service sdp class-forwarding fc

Description This command makes an explicit association between a forwarding class and an LSP. The LSP name must exist and must have been associated with this SDP using the command config>service>sdp>lsp. Multiple forwarding classes can be associated with the same LSP. However, a forwarding class can only be associated with a single LSP in a given SDP. All subclasses will be assigned to the same LSP as the parent forwarding class.

Parameters **lsp** *lsp-name* — Specifies the RSVP or static LSP to use to forward service packets which are classified into the specified forwarding class.

fc — Specifies a forwarding class to LSP mapping.

Values be, l2, af, 1, h2, ef, h1, nc

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc

Syntax **fc** *fc* [**priority** {**low** | **high**}]
no fc

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action fc)

Full Context configure router policy-options policy-statement entry action fc

Description This command associates a forwarding-class and optionally priority with the routes matched by a route policy entry. The command takes effect when the action of the route policy entry is accept, next-entry, or next-policy. It has no effect except in route policies applied as VRF import policies, BGP import policies, or RIP import policies.

The **no** form of this command removes the QoS association of the routes matched by the route policy entry.

Default no fc

Parameters *fc* — Specify the name of one of the predefined forwarding classes in the system.

Values be, l2, af, l1, h2, ef, h1, nc

Default none (no QoS information is associated with matched routes)

priority {**low** | **high**} — This parameter associates an enqueuing priority with routes matched by the policy entry. Specifying a priority is optional.

Values **high** — Setting the enqueuing parameter to **high** for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. After the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

low — Setting the enqueuing parameter to **low** for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. After the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Default low

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc

Syntax **fc** *fc-name*

Context **[Tree]** (config>test-oam>link-meas>template>twl fc)

Full Context configure test-oam link-measurement measurement-template twamp-light fc

Description This command configures the FC name for the TWAMP Light packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default fc h1

Parameters *fc-name* — Specifies the forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.27 fc-in-profile

fc-in-profile

Syntax **fc-in-profile** *fc-name* [*fc-name*]
no fc-in-profile

Context **[Tree]** (config>service>epipe>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc-in-profile)
[Tree] (config>service>ipipe>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)

Full Context configure service epipe sap eth-cfm collect-lmm-fc-stats fc-in-profile
configure service epipe spoke-sdp eth-cfm collect-lmm-fc-stats fc-in-profile
configure service ipipe sap eth-cfm collect-lmm-fc-stats fc-in-profile

Description This command creates individual counters for the specified FCs with regard for profile. All countable packets that match a configured FC and are deemed to be in-profile will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-unaware FC using the **fc** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc-in-profile

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-aware counter. In order for the counter to be used, the **config**>**oam-pm**>**session**>**ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc-in-profile

Syntax **fc-in-profile** *fc-name* [*fc-name*]
no fc-in-profile

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>collect-lmm-fc-stats fc-in-profile)
[Tree] (config>service>vpls>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc-in-profile)

Full Context configure service vpls mesh-sdp eth-cfm collect-lmm-fc-stats fc-in-profile
configure service vpls sap eth-cfm collect-lmm-fc-stats fc-in-profile
configure service vpls spoke-sdp eth-cfm collect-lmm-fc-stats fc-in-profile

Description This command creates individual counters for the specified FCs with regard for profile. All countable packets that match a configured FC and are deemed to be in-profile will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-unaware FC using the **fc** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc-in-profile

Parameters *fc-name* — Specifies up to eight names of the FC for which to create an individual profile-aware counter. In order for the counter to be used, the **config**>**oam-pm**>**session**> **ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fc-in-profile

Syntax **fc-in-profile** *fc-name* [*fc-name*]
no fc-in-profile

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc-in-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)

Full Context configure service ies interface sap eth-cfm collect-lmm-fc-stats fc-in-profile
configure service ies interface spoke-sdp eth-cfm collect-lmm-fc-stats fc-in-profile
configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc-in-profile

Description This command creates individual counters for the specified FCs with regard for profile. All countable packets that match a configured FC and are deemed to be in profile will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

An FC that is specified as part of this command for this specific context cannot be specified as a profile-unaware FC using the **fc** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc-in-profile

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-aware counter. Up to eight FCs may be specified. In order for the counter to be used, the **config**>**oam-pm**>**session**>**ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc-in-profile

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm collect-lmm-fc-stats fc-in-profile
- configure service ies interface sap eth-cfm collect-lmm-fc-stats fc-in-profile

fc-in-profile

Syntax **fc-in-profile** *fc-name* [*fc-name*]
no fc-in-profile

Context [Tree] (config>service>vprn>if>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>collect-lmm-fc-stats fc-in-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>collect-lmm-fc-stats fc-in-profile)

Full Context configure service vprn interface sap eth-cfm collect-lmm-fc-stats fc-in-profile
configure service vprn interface spoke-sdp eth-cfm collect-lmm-fc-stats fc-in-profile
configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc-in-profile

Description This command creates individual counters for the specified FCs with regard for profile. All countable packets that match a configured FC and are deemed to be in profile will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-unaware FC using the **fc** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc-in-profile

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-aware counter. Up to 8 FCs can be named in a single statement. In order for the counter to be used, the **config>oam-pm>session>ethernet>priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config>oam-pm>session>ethernet>lmm>enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm collect-lmm-fc-stats fc-in-profile

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm collect-lmm-fc-stats fc-in-profile
- configure service vprn interface sap eth-cfm collect-lmm-fc-stats fc-in-profile

fc-in-profile

Syntax **fc-in-profile** *fc-name* [*fc-name*]
no fc-in-profile

Context [Tree] (config>router>if>eth-cfm>mep>collect-lmm-fc-stats fc-in-profile)

Full Context configure router interface eth-cfm mep collect-lmm-fc-stats fc-in-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates individual counters for the specified FCs with regard for profile. All countable packets that match a configured FC and are deemed to be in-profile will be included in this counter.

A differential is performed when this command is re-entered. Omitted FCs will stop counting, newly added FCs will start counting, and unchanged FCs will continue to count.

Up to eight FCs may be specified. An FC that is specified as part of this command for this specific context cannot be specified as a profile-unaware FC using the **fc** command under the same context.

The **no** form of this command removes all previously defined FCs and stops counting for those FCs.

Default no fc-in-profile

Parameters *fc-name* — Specifies the name of the FC for which to create an individual profile-aware counter. A maximum of eight fc-names can be specified in a single statement. In order for the counter to be used, the **config**>**oam-pm**>**session**> **ethernet**>**priority** command must be configured with a numerical value representing the FC name (7 = NC, 6 = H1, 5 = EF, 4 = H2, 3 = L1, 2 = AF, 1 = L2, 0 = BE), and the **config**>**oam-pm**>**session**>**ethernet**>**lmm**>**enable-fc-collection** command must be enabled.

Values nc, h1, ef, h2, l1, af, l2, be

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.28 fcc

fcc

Syntax **fcc** *percent*

Context **[Tree]** (config>isa>video-group>watermark>bandwidth fcc)
[Tree] (config>isa>video-group>watermark>session fcc)

Full Context configure isa video-group watermark bandwidth fcc
configure isa video-group watermark session fcc

Description This command sets the watermark to trigger the SNMP trap if the FCC bandwidth or session exceeds the configured percentage. The bandwidth is the available egress bandwidth of the ISA. The SNMP trap is cleared when the consumption is lowered by 10%. For example, if the system resource of the available bandwidth is 10 Gb/s and the watermark is configured to be 90%, the SNMP trap is raised as the bandwidth exceeds 9 Gb/s (90% of 10 Gb/s). The SNMP trap is cleared when the bandwidth drops below 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s). The default value of the watermark is set at 90% of the system resources for both bandwidth and session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default fcc 90

Parameters *percent* — Specifies the percentage of the system resources per ISA.

Values 1 to 99

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

10.29 fcc-burst

fcc-burst

Syntax **fcc-burst** *burst-percentage*
no fcc-burst

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd fcc-burst)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip fcc-burst)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd fcc-burst)

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd fcc-burst
configure mcast-management multicast-info-policy video-policy video-interface pip fcc-burst
configure mcast-management multicast-info-policy video-policy video-interface sd fcc-burst

Description This command sets the burst rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client above the received rate to allow the client to catchup to the multicast stream.

This parameter is only applicable if the FCC server mode is **burst**.

The **no** form of the command returns the parameter to the default value.

Default fcc-burst 25

Parameters *burst-percentage* — Specifies the percentage of nominal bandwidth used to catch up to the multicast stream.

Values

HD:	0 to 100
SD and PIP:	0 to 600

Default 25

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.30 fcc-channel-type

fcc-channel-type

Syntax **fcc-channel-type** {**hd** | **sd** | **pip**}
no fcc-channel-type

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video fcc-channel-type)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video fcc-channel-type)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video fcc-channel-type)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video fcc-channel-type
configure mcast-management multicast-info-policy bundle channel video fcc-channel-type
configure mcast-management multicast-info-policy bundle video fcc-channel-type

Description This command configures the channel type for the bundle/channel. The channel type is used in the video policy to set various Fast Channel Change (FCC) parameters including the type of FCC and various FCC rates.

The **no** form of this command returns the parameter to the default value.

Default no fcc-channel-type

Parameters **hd** — The channel type is High-Definition (HD) (Default).

sd — The channel type is Standard Definition (SD).

pip — The channel type is Picture in Picture (PIP).

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

10.31 fcc-min-duration

fcc-min-duration

Syntax **fcc-min-duration** *time*
no fcc-min-duration

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video fcc-min-duration)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video fcc-min-duration)

Full Context configure mcast-management multicast-info-policy bundle channel video fcc-min-duration
configure mcast-management multicast-info-policy bundle video fcc-min-duration

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the minimum time duration, in milliseconds, of the Fast Channel Change (FCC) burst. The value of this object determines the starting point of the FCC burst. If the current Group of Pictures (GOP) has less than the minimum duration worth of data, FCC burst begins from the previous GOP.

The **no** form of the command reverts to the default value.

Default fcc-min-duration 300

Parameters *time* — Specifies the FCC burst minimum duration, in milliseconds.

Values 300 to 8000

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

10.32 fcc-server

fcc-server

Syntax [**no**] **fcc-server**

Context **[Tree]** (config>isa>video-group fcc-server)

Full Context configure isa video-group fcc-server

Description This command enables the FCC server capability for the ISA video group. FCC server cannot be enabled if ad insertion or the local RET server is enabled.

FCC server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the FCC server is disabled or if the video group is administratively disabled (shutdown).

The **no** form of the command disables the FCC server.

Default no fcc-server

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

fcc-server

Syntax **fcc-server** [**mode** {**burst** | **dent** | **hybrid**}]
no fcc-server

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd fcc-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip fcc-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd fcc-server)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd fcc-server
configure mcast-management multicast-info-policy video-policy video-interface pip fcc-server
configure mcast-management multicast-info-policy video-policy video-interface sd fcc-server

Description This command enables the Fast Channel Change (FCC) server and sets the mode to send the FCC unicast stream.

The mode indicates how the FCC server will send information to the client. When **burst** is specified, the FCC server will send the channel at a nominally faster rate than the channel was received based on the applicable fcc-burst setting. When **dent** is specified, the FCC server will selectively discard frames from the original stream based on the applicable dent-threshold setting. If no mode is specified, burst is the default mode.

The **no** form of the command disables the FCC server at that context and subordinate contexts.

Default no fcc-server

Parameters **mode burst** — Sets the mode of the FCC server to burst when sending the channel to the FCC client.

mode dent — Sets the mode of the FCC server to dent when sending the channel to the FCC client.

mode hybrid — Combines the burst and dent modes.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

fcc-server

Syntax **fcc-server** [**disable**]
no fcc-server

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video fcc-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video fcc-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video fcc-server)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video fcc-server
configure mcast-management multicast-info-policy bundle channel video fcc-server
configure mcast-management multicast-info-policy bundle video fcc-server

Description This command enables Fast Channel Change (FCC) for a multicast bundle or channel. Additional parameters such as **fcc-channel-type** should also be configured to match the characteristics of the bundle/channel.

The **no** form of the command disables removes the FCC configuration for the bundle/channel context and implies the setting is inherited from a higher context or the default policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no fcc-server

Parameters **disable** — Explicitly disables the FCC server within the policy. For the default bundle within the default multicast information policy, the **no** form of the command and the **disable** keyword have the same meaning and imply that the server is disabled.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

fcc-server

Syntax **fcc-server** [**client** *client-ip* [**source-port** *src-port*]]
no fcc-server

Context **[Tree]** (debug>service>id>video-interface fcc-server)

Full Context debug service id video-interface fcc-server

Description This command enables debugging the FCC server.

Parameters **client** *client-ip* — Specifies the client IP address.

source-port *src-port* — Specifies the source port's IP address.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

10.33 fcc-session-timeout

fcc-session-timeout

Syntax **fcc-session-timeout** *seconds*
no fcc-session-timeout

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if fcc-session-timeout)

Full Context configure mcast-management multicast-info-policy video-policy video-interface fcc-session-timeout

Description By default, the video ISA will wait for 5 minutes before closing the RTCP session from the subscriber. The RTCP session can be adjusted from 5 second to 5 minutes. The timeout is applicable to both RET and FCC RTCP sessions.

The **no** form of the command reverts to the default.

Default fcc-session-timeout 300

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the FCC session timeout in seconds.

Values 5 to 300

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

10.34 fd-avg

fd-avg

Syntax [**no**] **fd-avg** {**forward** | **backward** | **round-trip**}

Context **[Tree]** (config>oam-pm>streaming>delay-template fd-avg)

Full Context configure oam-pm streaming delay-template fd-avg

Description This command specifies the sending of average frame delay for a specified direction.

The **no** form of this command deletes the specified average direction.

Note: All directions can be specified if all directions are important for reporting. However, only enable those directions that are required.

Parameters **forward** — Specifies the measurement in the forward direction.

backward — Specifies the measurement in the backward direction.

round-trip — Specifies the measurement for the round trip.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.35 fdb-table-high-wmark

fdb-table-high-wmark

Syntax [**no**] **fdb-table-high-wmark** *high-water-mark*

Context **[Tree]** (config>service>vpls fdb-table-high-wmark)
[Tree] (config>service>template>vpls-template fdb-table-high-wmark)

Full Context configure service template vpls-template fdb-table-high-wmark
configure service vpls fdb-table-high-wmark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the value to send logs and traps when the threshold is reached.

The **no** form of this command reverts to the default value.

Default fdb-table-high-wmark 95

Parameters *high-water-mark* — Specifies the value as a percentage.

Values 0 to 100

Platforms All

10.36 fdb-table-low-wmark

fdb-table-low-wmark

Syntax [**no**] **fdb-table-low-wmark** *low-water-mark*

Context **[Tree]** (config>service>vpls fdb-table-low-wmark)
[Tree] (config>service>template>vpls-template fdb-table-low-wmark)

Full Context configure service template vpls-template fdb-table-low-wmark
configure service vpls fdb-table-low-wmark

Description This command specifies the value to send logs and traps when the threshold is reached.

The **no** form of this command reverts to the default value.

Default fdb-table-low-wmark 90

Parameters *low-water-mark* — Specifies the value as a percentage.

Values 0 to 100

Platforms All

10.37 fdb-table-size

fdb-table-size

Syntax **fdb-table-size** *table-size*
no fdb-table-size [*table-size*]

Context **[Tree]** (config>service>vpls fdb-table-size)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>template>vpls-template fdb-table-size)

Full Context configure service template vpls-template fdb-table-size
configure service vpls fdb-table-size

Description This command specifies the maximum number of MAC entries in the forwarding database (FDB) for the VPLS instance on this node.

The **fdb-table-size** specifies the maximum number of forwarding database entries for both learned and static MAC addresses for the VPLS instance.

The **no** form of this command returns the maximum FDB table size to default.

Default fdb-table-size 250

Parameters *table-size* — Specifies the number of entries permitted in the forwarding database for this VPLS instance.

Values 7450 ESS, 7950 XRS, or 7750 SR-7, SR-12, SR-12e: 1 to 511999
7750 SR-e, SR-a: 1 to 250000

Platforms All

fdb-table-size

Syntax **fdb-table-size** *table-size*
no fdb-table-size

Context [Tree] (config>service>system fdb-table-size)

Full Context configure service system fdb-table-size

Description This command configures the maximum system FDB table size, which is dependent on the chassis type. CPMs with at least 16 GB of memory are required when exceeding 500k MAC addresses in a system. The table size cannot be reduced below its default value, which is also chassis-dependent.

The maximum system FDB table size also limits the maximum FDB table size of any card within the system.

The **no** version of this command sets the table size to its default.

The command default depends on the chassis type and available memory.

Parameters *table-size* — Specifies the maximum system FDB table size.

Values 255999 to 2047999

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.38 feac-loop-respond

feac-loop-respond

Syntax [**no**] **feac-loop-respond**

Context **[Tree]** (config>port>tdm>ds3 feac-loop-respond)

Full Context configure port tdm ds3 feac-loop-respond

Description This command enables the associated DS-3 interface to respond to remote loop signals.

The DS-3 far-end alarm and control (FEAC) signal is used to send alarm or status information from the far-end terminal back to the local terminal. DS-3 loopbacks at the far-end terminal from the local terminal are initiated.

The **no** form of this command prevents the associated DS-3 interface from responding to remote loop signals.

Default no feac-loop-respond

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

10.39 feature

feature

Syntax [**no**] **feature** *feature-name*

Context **[Tree]** (config>system>satellite>eth-sat feature)

Full Context configure system satellite eth-sat feature

Description This command enables specific satellite functionality that may have specific satellite requirements, such as software version.

The **no** form of this command disables the specific satellite functionality.

Parameters *feature-name* — Specifies the functionality to enable.

Values local-forward

Values transparent-clock-eth

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.40 features

features

Syntax **features**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx features)

Full Context configure subscriber-mgmt diameter-application-policy gx features

Description Commands in this context configure the Gx features.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.41 fec

fec

Syntax **fec** {**g709** | **enhanced**}
no fec

Context **[Tree]** (config>port>otu fec)

Full Context configure port otu fec

Description This command enables the Forwarding Error Correction (FEC) encoder/decoder and specifies the FEC encoder/decoder mode to use when enabled.

The following rules must be followed:

- The port's OTU must be enabled to set or change the FEC mode.
- The port must be shut down before changing the FEC mode.
- The sf-sd-method must be changed to BIP8 before setting the FEC mode to disabled.

Note that FEC cannot be disabled on OTU3 encapsulated OC768 or 40-Gigabit Ethernet by the **no fec** command. Therefore, the default depends on the port type. The default for OTU3 encapsulated OC768 or 40-Gigabit Ethernet is **fec enhanced**.

The **no** form of this command disables FEC encoder and decoder.

Default no fec

Parameters **enhanced** — Enables the FEC encoder and decoder with a proprietary enhanced FEC algorithm.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

g709 — Enables the FEC encoder and decoder with the standard G.709 FEC algorithm.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.42 fec-limit

fec-limit

Syntax **fec-limit** *limit* [**log-only**] [**threshold** *percentage*]
no fec-limit

Context **[Tree]** (config>router>ldp>session-params>peer fec-limit)

Full Context configure router ldp session-parameters peer fec-limit

Description This command configures a limit on the number of FECs which an LSR will accept from a given peer and add into the LDP label database. The limit applies to the aggregate count of all FEC types including service FEC. Once the limit is reached, any FEC received will be released back to the peer. This behavior is different from the per-peer import policy which will still accept the FEC into the label database but will not resolve it.

When the FEC limit for a peer is reached, the LSR performs the following actions:

1. Generates a trap and a syslog message.
2. Generates a LDP notification message with the LSR overload status TLV, for each LDP FEC type including service FEC, to this peer only if this peer advertised support for the LSR overload sub-TLV via the LSR Overload Protection Capability TLV at session initialization.
3. Releases, with LDP Status Code of "No_Label_Resources", any new FEC, including service FEC, from this peer which exceeds the limit.

If a legitimate FEC is released back to a peer, while the FEC limit was exceeded, the user must have a means to replay that FEC back to the router LSR once the condition clears. This is done automatically if the peer is an SR OS-based router and supports the LDP overload status TLV (SR OS 11.0R5 and higher). Third-party peer implementations must support the LDP overload status TLV or provide a manual command to replay the FEC.

The **threshold** option allows to set a threshold value when a trap and an syslog message are generated as a warning to the user in addition to when the limit is reached. The default value for the threshold when not configured is 90%.

The **log-only** option causes a trap and syslog message to be generated when reaching the threshold and limit. However, LDP labels are not released back to the peer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the user decreases the limit value such that it is lower than the current number of FECs accepted from the peer, the LDP LSR raises the trap for exceeding the limit. In addition, it will set overload for peers which signaled support for LDP overload protection capability TLV. However, no existing resolved FECs from the peer which does not support the overload protection capability TLV should be de-programmed or released.

A different trap is released when crossing the threshold in the upward direction, when reaching the FEC limit, and when crossing the threshold in the downward direction. However the same trap will not be generated more often than 2 minutes apart if the number of FECs oscillates around the threshold or the FEC limit.

Default no fec-limit

Parameters *limit* — Specifies the aggregate count of FECs of all types which can be accepted from this LDP peer.

log-only — Specifies that only a trap and syslog message are generated when reaching the threshold and limit. However, LDP labels are not released back to the peer.

percentage — Specifies the threshold value (as a percentage) that triggers a warning syslog message and trap to be sent.

Platforms All

10.43 fec-originate

fec-originate

Syntax **fec-originate** *ip-prefix/mask* [**advertised-label** *in-label*] [**swap-label** *out-label*] **interface interface-name**
fec-originate *ip-prefix/mask* [**advertised-label** *in-label*] **next-hop** *ip-address* [**swap-label** *out-label*]
fec-originate *ip-prefix/mask* [**advertised-label** *in-label*] **next-hop** *ip-address* [**swap-label** *out-label*] **interface interface-name**
fec-originate *ip-prefix/mask* [**advertised-label** *in-label*] **pop**
no fec-originate *ip-prefix/mask* **interface interface-name**
no fec-originate *ip-prefix/mask* **next-hop** *ip-address*
no fec-originate *ip-prefix/mask* **next-hop** *ip-address* **interface interface-name**
no fec-originate *ip-prefix/mask* **pop**

Context **[Tree]** (config>router>ldp fec-originate)

Full Context configure router ldp fec-originate

Description This command defines a way to originate a FEC (with a swap action) for which the LSR is not egress, or to originate a FEC (with a pop action) for which the LSR is egress.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix/mask* — Specifies information for the specified IP prefix and mask length.

Values

<ip-address/mask>	ipv4-prefix - a.b.c.d	
	ipv4-prefix-le - [0..32]	
	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0..FFFF]H
		d - [0..255]D
		ipv6-prefix-le - [0..128]

next-hop — Specifies the IP address of the next hop of the prefix.

advertised-label — Specifies the label advertised to the upstream peer. If not configured, then the label advertised should be from the label pool. If the configured static label is not available then the IP prefix is not advertised.

out-label — Specifies the LSR to swap the label. If configured, then the LSR should swap the label with the configured swap-label. If not configured, then the default action is pop if the next-hop parameter is not defined.

The next-hop, advertised-label, swap-label parameters are all optional. If next-hop is configured but no swap label specified, it will be a swap with label 3, such as, pop and forward to the next-hop. If the next-hop and swap-label are configured, then it is a regular swap. If no parameters are specified, a pop and route is performed.

Values 16 to 1048575

in-label — Specifies the number of labels to send to the peer associated with this FEC.

Values 32 to 1023

pop — Specifies to pop the label and transmit without the label.

interface *interface-name* — Specifies the name of the interface the label for the originated FEC is swapped to. For an unnumbered interface, this parameter is mandatory since there is no address for the next-hop. For a numbered interface, it is optional.

Platforms All

10.44 fec-prefix

fec-prefix

Syntax [**no**] **fec-prefix** *ip-prefix*[*mask*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ldp>egr-stats fec-prefix)

Full Context configure router ldp egress-statistics fec-prefix

Description This command configures statistics in the egress data path at the ingress LER or LSR for an LDP FEC. The user must execute the **no shutdown** command for this command to effectively enable statistics. The egress data path counters will be updated for both originating and transit packets. Originating packets may be service packets or IP user and control packets forwarded over the LDP LSP when used as an IGP shortcut. Transit packets of the FEC which are label switched on this node.

When ECMP is enabled and multiple paths exist for a FEC, the same set of counters are updated for each packet forwarded over any of the NHLFEs associated with this FEC and for as long as this FEC is active.

The statistics can be enabled on prefix FECs imported from both LDP neighbors and T-LDP neighbors (LDP over RSVP). LDP sets up egress statistics collection for the LDP tunnels whose FECs match the exact prefix specified in this command. Service FECs, that is, FEC 128 and FEC 129, are not valid. LDP FEC egress statistics are collected at the Penultimate-Popping Hop (PHP) node for a LDP FEC using an implicit null egress label.

The **no** form of this command disables the statistics in the egress data path and removes the accounting policy association from the LDP FEC.

Parameters *ip-prefix* — Specifies the IP address representing the FEC.

Values

IPv4 prefix:	*a.b.c.d*	*a*, *b*, *c*, *d* - 0 to 255; decimal
IPv6 prefix:	*x:x:x:x:x:x:x:x* (eight 16-bit pieces) *x:x:x:x:x:x:d.d.d.d*	*x* - 0 to FFFF; hexadecimal

mask — Specifies the mask of the IP address.

Values IPv4: 0 to 32
IPv6: 0 to 128

Platforms All

10.45 fec-type-capability

fec-type-capability

Syntax **fec-type-capability**

Context [Tree] (config>router>ldp>session-params>peer fec-type-capability)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ldp>if-params>if>ipv4 fec-type-capability)
[Tree] (config>router>ldp>if-params>if>ipv6 fec-type-capability)

Full Context configure router ldp interface-parameters interface ipv4 fec-type-capability
configure router ldp interface-parameters interface ipv6 fec-type-capability
configure router ldp session-parameters peer fec-type-capability

Description This command enables or disables the advertisement of a FEC type on a given LDP session or Hello adjacency to a peer.

The config>router>ldp>if-params>if>ipv6>fec-type-capability command is not supported on the 7450 ESS.

Platforms All

10.46 fec129-cisco-interop

fec129-cisco-interop

Syntax [**no**] **fec129-cisco-interop**

Context [Tree] (config>router>ldp>session-params>peer fec129-cisco-interop)

Full Context configure router ldp session-parameters peer fec129-cisco-interop

Description This command specifies whether LDP will provide translation between non-compliant FEC 129 formats of Cisco. Peer LDP sessions must be manually configured towards the non-compliant Cisco PEs.

When enabled, Cisco non-compliant format will be used to send and interpret received label release messages that is the FEC129 SAII and TAII fields will be reversed.

When the disabled, Cisco non-compliant format will not be used or supported. Peer address has to be the peer LSR-ID address.

The **no** form of this command returns the default.

Default no fec129-cisco-interop

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.47 fib-priority

fib-priority

Syntax **fib-priority** {**high** | **standard**}

Context **[Tree]** (config>service>vprn fib-priority)

Full Context configure service vprn fib-priority

Description This command specifies the FIB priority for VPRN BGP routes.

Parameters **high** — Specifies high FIB priority for VPRN.

standard — Specifies standard FIB priority for VPRN.

Platforms All

fib-priority

Syntax **fib-priority** {**high** | **standard**}

Context **[Tree]** (config>router fib-priority)

Full Context configure router fib-priority

Description This command specifies the FIB priority for VPRN BGP routes.

Default fib-priority standard

Parameters **high** — Specifies the high FIB priority.

standard — Specifies the standard FIB priority.

Platforms All

10.48 fib-telemetry

fib-telemetry

Syntax [**no**] **fib-telemetry**

Context **[Tree]** (config>router fib-telemetry)

Full Context configure router fib-telemetry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the collection of extra state information related to the forwarding table state of certain IP routes, TTM tunnels, and MPLS LFIB entries. This extra state can be retrieved by gNMI telemetry subscriptions targeted to the following YANG paths:

- /state/router/route-fib
- /state/router/tunnel-fib
- /state/router/label-fib

If this command is not configured, no information is displayed by the following **show** commands:

- **show**>**router**>**fib-telemetry**>**route**
- **show**>**router**>**fib-telemetry**>**tunnel**

The **no** form of this command disables the collection of this extra state.

Default no fib-telemetry

Platforms All

10.49 field

field

Syntax [**no**] **field** *field-name*

Context **[Tree]** (config>app-assure>group>cflowd>comp>template>dynamic-fields field)
[Tree] (config>app-assure>group>cflowd>rtp-perf>audio-template>dynamic-fields field)
[Tree] (config>app-assure>group>cflowd>rtp-perf>video-template>dynamic-fields field)
[Tree] (config>app-assure>group>cflowd>rtp-perf>voice-template>dynamic-fields field)
[Tree] (config>app-assure>group>cflowd>tcp-perf>template>dynamic-fields field)
[Tree] (config>app-assure>group>cflowd>volume>template>dynamic-fields field)

Full Context configure application-assurance group cflowd comprehensive template dynamic-fields field
configure application-assurance group cflowd rtp-performance audio-template dynamic-fields field
configure application-assurance group cflowd rtp-performance video-template dynamic-fields field
configure application-assurance group cflowd rtp-performance voice-template dynamic-fields field
configure application-assurance group cflowd tcp-performance template dynamic-fields field
configure application-assurance group cflowd volume template dynamic-fields field

Description This command specifies which fields to include in the exported cflowd template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Certain fields, such as source and destination IP addresses, are always included in the exported template, so they are not optional.

The **no** form of this command removes the specified field from the template.

Parameters *field-name* — Specifies the name of the field to include in the exported cflowd template, up to 256 characters.

Values

Common to all templates	session/flowStartSeconds, session/flowDurationMilliseconds, postIpPrecedence, ipTTL, aaProt, aaApp, aaAppGrp, hostName, deviceId, deviceMfgId, deviceOsId, ipFamily, deviceOsVer1, deviceOsVer2, deviceOsVer3, anlType, anlTopology, anlCongestionState, timeZone, aaChargingGrp, flowAttr_video, flowAttr_abr_service, flowAttr_audio, flowAttr_encrypted, flowAttr_download, flowAttr_upload, flowAttr_realtime_communication, aaSubTetheringState When AA is deployed in FWA SR: ApnExtended
For the TCP and comprehensive templates only	tcpSessionEstDelay, tcpRetransmittedBytes, tcpRetransmittedPackets
For the rtp-voice template only	rtpBurstCount, rtpAvgBurstLengthMs, rtpGapCount, rtpAvgGapLengthMs, MAPDV, RBurst, RGap, SSRC
For the rtp-video template only	rtpRefClockRate, MOSAV, VSTQ, estimatedPSNR, GoPType, avgGoPLength, avgInterIFrameGap, imageWidth, imageHeight, frameRate, slicesPerIFrame, SSRC, videoInterlaced, IFrameReceived, IFrameImpaired, PFrameReceived, PFrameImpaired, BFrameReceived, BFrameImpaired, SIFrameReceived, SIFrameImpaired, SPFrameReceived, SPFrameImpaired, frameInterArrivalJitter, IFrameInterArrivalJitter, avgFrameArrivalDelay
For the rtp-audio template only	frtpBurstCount, rtpAvgBurstLengthPkts, rtpGapCount, rtpAvgGapLengthPkts, PPDVM, rtpNumAudioChannels, rtpRefClockRate, rtpPeakAudioBw, SSRC, hostName

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

field

Syntax [**no**] **field** *field-name*

Context **[Tree]** (config>app-assure>group>http-enrich field)

Full Context configure application-assurance group http-enrich field

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the fields to insert into the HTTP header. The command must be repeated for each field to be inserted. The same field cannot be inserted twice into the header under different header names.

Note: AA can insert two copies of the following fields in the same HTTP header (with a different header name): **imei-hyphenated**, i**mei-hyphenated-2**, **imsi**, **imsi-2**, **static-string**, **static-string-2**, **user-location-raw**, and **user-location-raw2**.

The **no** form of this command removes the specified field so that it is not inserted into the HTTP header.

Parameters *field-name* — Specifies the fields to insert into the HTTP header.

Values The following parameters are supported in any deployment:

- **static-string** — header name for the inserted string
- **static-string-2** — header name for the inserted string
- **subscriber-id** — header name for the subscriber ID
- **subscriber-ip** — header name for the subscriber IP address

The following parameters are supported in Fixed Wireless Access (FWA) deployments only:

- **apn** — APN used by the UE
- **apn-ni** — APN Network Identifier (APN-NI) used by the UE
- **billing-type** — UE charging type (charging characteristics)
- **dynamic-acr** — dynamic Anonymous Customer Record (ACR)
- **static-acr** — static ACR
- **imei-sv** — subscriber IMEI with format AABBBBBBCCCCCCEE
- **imei-hyphenated** — subscriber IMEI with format AABBBBBB-CCCCCC-EE
- **imei-hyphenated-2** — subscriber IMEI with format AABBBBBB-CCCCCC-EE
- **imsi** — subscriber IMSI
- **imsi-2** — subscriber IMSI
- **msisdn** — subscriber MSISDN
- **msisdn-without-cc** — subscriber MSISDN without a country code
- **pgw_ggsn-address** — PGW/GGSN address serving the UE
- **plmn-id** — Public Land Mobile Network (PLMN) ID of the SGSN/MME
- **rat-type** — Radio Access Technology (RAT) type
- **timestamp** — timestamp inserted in UNIX time format Example: 1531204313
- **user-location** — UE LOCATION (ULI)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **user-location-3gpp** — ULI encoded as defined in 3GPP 29.061
- **user-location-raw** — ULI in raw format <ULI-TYPE1>[+<ULI-TYPE2>]=<ULI HEX>

  Example: x-locinfo: TAI+ECGI= 1300622c46130062014adf16
- **user-location-raw-2** — ULI in raw format <ULI-TYPE1>[+<ULI-TYPE2>]=<ULI HEX>

  Example: x-locinfo: TAI+ECGI= 1300622c46130062014adf16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.50 field-override

field-override

Syntax **field-override**

Context **[Tree]** (debug>oam>build-packet field-override)

Full Context debug oam build-packet field-override

Description Commands in this context configure an override value for a field within a header within a packet to be launched by the OAM **find-egress** tool.

10.51 field-selection

field-selection

Syntax **field-selection** *field-selection*
no field-selection

Context **[Tree]** (config>app-assure>group>cflowd>comp>template field-selection)
[Tree] (config>app-assure>group>cflowd>rtp-perf>audio-template field-selection)
[Tree] (config>app-assure>group>cflowd>rtp-perf>video-template field-selection)
[Tree] (config>app-assure>group>cflowd>rtp-perf>voice-template field-selection)
[Tree] (config>app-assure>group>cflowd>tcp-perf>template field-selection)
[Tree] (config>app-assure>group>cflowd>volume>template field-selection)

Full Context configure application-assurance group cflowd comprehensive template field-selection
configure application-assurance group cflowd rtp-performance audio-template field-selection
configure application-assurance group cflowd rtp-performance video-template field-selection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group cflowd rtp-performance voice-template field-selection
configure application-assurance group cflowd tcp-performance template field-selection
configure application-assurance group cflowd volume template field-selection

Description This command configures how fields included in the exported cflowd template are selected.

The **no** form of this command reverts to the **legacy** field selection type.

Default field-selection legacy

Parameters *field-selection* — Specifies how fields are selected.

legacy	Specifies that the fields within the cflowd template are set and fixed and as per SR OS release 17 (or earlier).
dynamic	Specifies that the operator can select which fields are included in the cflowd template.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.52 file

file

Syntax **file** *file-url*
no file

Context **[Tree]** (config>app-assure>group>url-list file)

Full Context configure application-assurance group url-list file

Description This command specifies the file for the URL list.

The **no** form of this command removes the url-list object.

Default no file

Parameters *file-url* — Specifies the flash ID or file path.

Values [*cflash-id*/] *file-path*: [200 chars max]
cflash-id: - cf1: | cf1-A: | cf1-B: | cf2: | cf2-A: | cf2-B: | cf3: | cf3-A: | cf3-B:

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

file

Syntax **file**

Context **[Tree]** (file file)

Full Context file

Description Specifies the context to enter and perform file system operations. When entering the **file** context, the prompt changes to reflect the present working directory. Navigating the file system with the **cd ..** command results in a changed prompt.

The **exit all** command leaves the file system/file operation context and returns to the operational root CLI context. The state of the present working directory is maintained for the CLI session. Entering the **file** command returns the cursor to the working directory where the **exit** command was issued.

Platforms All

10.53 file-id

file-id

Syntax [**no**] **file-id** *file-id* [**name** *file-policy-name*]

Context **[Tree]** (config>log file-id)

Full Context configure log file-id

Description This command creates the context to configure a file policy that is used as the destination for an event log or billing (accounting) file.

This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting/billing information. The file defined in this context is subsequently specified in the **to** command under **log-id** or **accounting-policy** to direct specific logging or billing source streams to the file destination.

A file policy can only be assigned to either *one* **log-id** or *one* **accounting-policy**. It cannot be reused for multiple instances. A file policy and associated file definition must exist for each log and billing file that must be stored in the file system.

A file is created when the file policy defined in this command is selected as the destination type for a specific log or accounting record. Log files are collected in a “log” directory. Accounting files are collected in an “act” directory.

The file names for a log are created by the system as summarized in Table 60.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 60 **Log File Names**

File Type	File Name
Log File	log*llff-timestamp*
Accounting File	act*aaff-timestamp*

Where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the file-id
- The *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
  - *yyyy* is the year (for example, 2006)
  - *mm* is the month number (for example, 12 for December)
  - *dd* is the day of the month (for example, 03 for the 3rd of the month)
  - *hh* is the hour of the day in 24 hour format (for example, 04 for 4 a.m.)
  - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
  - *ss* is the number of seconds (for example, 14 for 14 seconds)
- The accounting file is compressed and has a gz extension.

When initialized, each file contains:

- The *log-id* description.
- The time the file was opened.
- The reason the file was created.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

The **no** form of this command removes the file policy from the configuration. A file policy can only be removed from the configuration if the policy is not the designated output for a log destination. The actual log or accounting file remain on the file system when a file policy is deleted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *file-id* — The file identification number for the file policy, expressed as a decimal integer.

Values 1 to 99

name *file-policy-name* — Configures an optional file policy name, up to 64 characters, that can be used to refer to the file policy after it is created. If the name begins with a numerical digit (from 1 to 9), the name is a number from 1 to 99.

Platforms All

10.54 file-transfer

file-transfer

Syntax **file-transfer** *file-transfer-mode* [*file-transfer-mode*]
no file-transfer

Context **[Tree]** (config>system>satellite file-transfer)

Full Context configure system satellite file-transfer

Description This command specifies the file transfer protocol to use between the 7750 SR or 7950 XRS host and 7210 SAS Ethernet satellite.

The **no** form of this command reverts to the default value.

Default file-transfer ftp

Parameters *file-transfer-mode* — Specifies up to two satellite secure file transfer protocols.

Values ftp – The file transfer FTP protocol is used between 7750 SR or 7950 XRS host and the 7210 SAS Ethernet satellite.

scp - The file transfer SCP protocol is used between the 7750 SR or 7950 XRS host and the 7210 SAS Ethernet satellite.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.55 file-transmission-profile

file-transmission-profile

Syntax **file-transmission-profile** *name* [**create**]
no file-transmission-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>system file-transmission-profile)

Full Context configure system file-transmission-profile

Description This command creates a new file transmission profile or enters the configuration context of an existing file-transmission-profile.

The **file-transmission-profile** context defines transport parameters for protocol such as HTTP, include routing instance, source address, timeout value, and so on.

The **no** form of the command removes the profile name from the configuration.

Default no file-transmission-profile

Parameters *name* — Specifies the file transmission profile name, up to 32 characters.

create — Keyword used to create the transmission profile. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms All

file-transmission-profile

Syntax **file-transmission-profile** *profile-name*
no file-transmission-profile

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update>crl-urls>url-entry file-transmission-profile)

Full Context configure system security pki ca-profile auto-crl-update crl-urls url-entry file-transmission-profile

Description This command specifies the file-transmission-profile for the **url-entry**. When the system downloads a CRL from the configured URL in the **url-entry** it will use the transportation parameter configured in the **file-transmission-profile**. **auto-crl-update** supports Base/Management/VPRN routing instance. **vpls-management** is not supported. In case of VPRN, the HTTP server port can only be 80 or 8080.

The **no** form of this command removes the specified profile name.

Default no file-transmission-profile

Parameters *profile-name* — Specifies the name of the file transmission profile to be matched up to 32 characters. The profile name is configured in the **config>system>file-transmission-profile** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.56 file-url

file-url

Syntax **file-url** *file-url*
no file-url

Context **[Tree]** (config>mirror>mirror-dest>pcap file-url)

Full Context configure mirror mirror-dest pcap file-url

Description This command specifies a file URL for the FTP or TFTP server, including the filename for packet capture transfer. After the file URL is entered, the system attempts to establish a connection and creates a file using the filename specified. The command prompt displays an error and rejects the file URL if the session establishment fails, if write privilege to remote server fails, or if the session experiences a sudden termination. If the FTP or TFTP server is unreachable, the command prompt is halted for further input until the retires are timed out after 24 seconds (after four attempts of about six seconds each). This command overwrites any file on the FTP or TFTP server with the same filename.

The **no** form of this command removes the *file-url* instance and stops the packet capture and file transfer session.

Parameters *file-url* — Specifies the URL for the file to direct the search.

Values [*local-url* | *remote-url*]
where:

- *local-url* — [*cflash-id*/] [*file-path*]
  180 chars max, including *cflash-id*
  directory length 99 chars max each
- *remote-url* — [{ftp://| tftp://} *login*:*pswd*@*remote-locn*/][*file-path*]
  180 chars max
  directory length 99 chars max each
  where: *remote-locn* — [*hostname* | *ipv4-address* | *ipv6-address*]

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x[-interface] x:x:x:x:x:x:d.d.d.d[-interface] x - [0..FFFF]H d - [0..255]D interface - 32 chars max, for link local addresses
cflash-id	cf1:| cf1-A:| cf1-B:| cf2:| cf2-A:| cf2-B:| cf3:| cf3-A:| cf3-B:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

10.57 filter

filter

Syntax **filter** *filter-id*
no filter

Context **[Tree]** (config>service>ies>sub-if>grp-if>dhcp filter)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp filter)

Full Context configure service ies subscriber-interface group-interface dhcp filter
configure service vprn subscriber-interface group-interface dhcp filter

Description This command assigns a DHCP filter to the group-interface. This feature is used where the SR 7750 is the second DHCP relay or where DHCP messages are snooped for subscriber management. The filter can be used to bypass host creation, drop DHCP message, or perform no action.

The **no** form of this command reverts to the default.

Parameters *filter-id* — Specifies the DHCP filter ID for this interface.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

filter

Syntax **filter** *filter-id*
no filter

Context **[Tree]** (config>service>ies>sub-if>grp-if>dhcp6 filter)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp6 filter)

Full Context configure service ies subscriber-interface group-interface dhcp6 filter
configure service vprn subscriber-interface group-interface dhcp6 filter

Description This command assigns a DHCP6 filter to the group interface. This feature is used where the SR 7750 is the second DHCP6 relay or where DHCP6 messages are snooped for subscriber management. The filter can be used to bypass host creation, drop DHCP6 message, or perform no action.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *filter-id* — Specifies the DHCP6 filter ID for this interface

Values 1 to 65535

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>vprn>nw-if>egress filter)
[Tree] (config>service>vprn>if>spoke-sdp>egress filter)
[Tree] (config>service>vprn>if>spoke-sdp>ingress filter)
[Tree] (config>service>vprn>red-if>spoke-sdp>ingress filter)
[Tree] (config>service>vprn>red-if>spoke-sdp>egress filter)
[Tree] (config>service>vprn>nw-if>egress filter)

Full Context configure service vprn interface spoke-sdp egress filter
configure service vprn interface spoke-sdp ingress filter
configure service vprn network-interface egress filter
configure service vprn redundant-interface spoke-sdp egress filter
configure service vprn redundant-interface spoke-sdp ingress filter

Description This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface. An IP filter policy can be associated with spoke SDPs. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria.

The filter command is used to associate a filter policy with a specified ip-filter-id with an ingress or egress SAP. The ip-filter-id must already be defined before the filter command is executed. If the filter policy does not exist, the operation fails and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use scope command within the filter definition to change the scope to local or global. The default scope of a filter is local.

Parameters **ip** *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp egress filter
- configure service vprn redundant-interface spoke-sdp ingress filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service vprn interface spoke-sdp ingress filter
- configure service vprn interface spoke-sdp egress filter
- configure service vprn network-interface egress filter

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
filter mac *mac-filter-id*
no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>ies>if>sap>egress filter)
[Tree] (config>service>ies>if>sap>ingress filter)
[Tree] (config>service>ies>red-if>egress filter)
[Tree] (config>service>ies>red-if>ingress filter)
[Tree] (config>service>ies>red-if>egress filter)
[Tree] (config>service>ies>red-if>ingress filter)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress filter)
[Tree] (config>service>ies>sub-if>grp-if>sap>ingress filter)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress filter)
[Tree] (config>service>vprn>sub-if>grp-if>sap>ingress filter)

Full Context configure service ies interface sap egress filter
configure service ies interface sap ingress filter
configure service ies red-if egress filter
configure service ies red-if ingress filter
configure service ies subscriber-interface group-interface sap egress filter
configure service ies subscriber-interface group-interface sap ingress filter
configure service vprn subscriber-interface group-interface sap egress filter
configure service vprn subscriber-interface group-interface sap ingress filter

Description This command associates a filter policy with an ingress or egress Service Access Point (SAP). Filter policies control the forwarding and dropping of packets based on the matching criteria. MAC filters are only allowed on Epipe and Virtual Private LAN Service (VPLS) SAPs.

The **filter** command is used to associate a filter policy with a specified *ip-filter-id* or *ipv6-filter-id* (7750 SR) with an ingress or egress SAP. The filter policy must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation fails and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes any configured filter ID association with the SAP. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Special Cases **IES —** Only IP filters are supported on an IES IP interface, and the filters only apply to routed traffic.

Parameters **ip** *ip-filter-id* — Specifies the ID for the IP filter policy and corresponds to a previously created IP filter policy in the **config>filter>ip-filter** context.

Values 1 to 65535

ipv6 *ipv6-filter-id* — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

mac *mac-filter-id* — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap ingress filter
- configure service ies subscriber-interface group-interface sap egress filter
- configure service ies subscriber-interface group-interface sap ingress filter
- configure service vprn subscriber-interface group-interface sap egress filter

All

- configure service ies interface sap ingress filter
- configure service ies interface sap egress filter

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
filter mac *mac-filter-id*
no filter [**ip** *ip-filter-id*] [**mac** *mac-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>vpls>sap>egress filter)
[Tree] (config>service>vpls>sap>ingress filter)
[Tree] (config>service>vpls>mesh-sdp>egress filter)
[Tree] (config>service>vpls>mesh-sdp>ingress filter)
[Tree] (config>service>vpls>spoke-sdp>egress filter)
[Tree] (config>service>vpls>spoke-sdp>ingress filter)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context
configure service vpls mesh-sdp egress filter
configure service vpls mesh-sdp ingress filter
configure service vpls sap egress filter
configure service vpls sap ingress filter
configure service vpls spoke-sdp egress filter
configure service vpls spoke-sdp ingress filter

Description
This command associates an IP filter policy or MAC filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There are two types of filter policies: IP and MAC. Only one type may be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified *filter ID* with an ingress or egress SAP. The *filter ID* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Special Cases
VPLS — Both MAC and IP filters are supported on a VPLS service SAP. However, concurrent MAC-based QoS or filter policy match criteria and IPv6-based QoS or filter policy match criteria are not supported on access interfaces. On ingress, IPv6 routed packets ignore MAC-based QoS classification criteria, while switched packets ignore IPv6-based ACL match criteria. On egress, IPv6 QoS-based classification criteria are ignored when MAC-based ACLs are configured.

Parameters
ip *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

ipv6 *ipv6-filter-id* — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

mac *mac-filter-id* — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

filter

Syntax **filter** *filter-name*
no filter

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext filter)

Full Context configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext filter

Description This command applies to VPRN services only to filter for ingress home traffic.

Default no filter

Parameters *filter-name* — Specifies an IP filter name, up to 32 characters.

filter

Syntax **filter** *filter-name*
no filter

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>xconnect filter)

Full Context configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext xconnect filter

Description This command applies to VPRN services only to filter for cross-connect traffic.

Default no filter

Parameters *filter-name* — Specifies an filter name, up to 32 characters.

filter

Syntax **filter** *filter-name*
no filter

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network filter)

Full Context configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext network filter

Description This command applies to VPRN services only to filter for ingress data center traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no filter

Parameters *filter-name* — Specifies an IP filter name, up to 32 characters.

filter

Syntax **filter** [**ip** *ip-filter-id*]
filter [**ipv6** *ipv6-filter-id*]
no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>fpipe>sap>egress filter)
[Tree] (config>service>fpipe>sap>ingress filter)
[Tree] (config>service>cpipe>spoke-sdp>egress filter)
[Tree] (config>service>cpipe>spoke-sdp>ingress filter)
[Tree] (config>service>fpipe>spoke-sdp>egress filter)
[Tree] (config>service>fpipe>spoke-sdp>ingress filter)
[Tree] (config>service>ipipe>spoke-sdp>egress filter)
[Tree] (config>service>ipipe>sap>ingress filter)
[Tree] (config>service>ipipe>sap>egress filter)
[Tree] (config>service>ipipe>spoke-sdp>ingress filter)

Full Context configure service cpipe spoke-sdp egress filter
configure service cpipe spoke-sdp ingress filter
configure service fpipe sap egress filter
configure service fpipe sap ingress filter
configure service fpipe spoke-sdp egress filter
configure service fpipe spoke-sdp ingress filter
configure service ipipe sap egress filter
configure service ipipe sap ingress filter
configure service ipipe spoke-sdp egress filter
configure service ipipe spoke-sdp ingress filter

Description This command associates a filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP matching criteria. Only one filter can be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified *ip-filter-id* with an ingress or egress SAP. The *ip-filter-id* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets will not be subject to the filter and will always be passed, even if the filter's default action is to drop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Parameters *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

ipv6-filter-id — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp ingress filter
- configure service fpipe spoke-sdp egress filter
- configure service fpipe sap egress filter
- configure service fpipe sap ingress filter

All

- configure service ipipe sap ingress filter
- configure service ipipe spoke-sdp egress filter
- configure service ipipe sap egress filter
- configure service ipipe spoke-sdp ingress filter

filter

Syntax **filter** [**ip** *ip-filter-id*]
filter [**ipv6** *ipv6-filter-id*]
filter [**mac** *mac-filter-id*]
no filter [**ip** *ip-filter-id*]
no filter [**ipv6** *ipv6-filter-id*]
no filter [**mac** *mac-filter-id*]

Context **[Tree]** (config>service>epipe>sap>egress filter)
[Tree] (config>service>epipe>sap>ingress filter)
[Tree] (config>service>epipe>spoke-sdp>egress filter)
[Tree] (config>service>epipe>spoke-sdp>ingress filter)

Full Context configure service epipe sap egress filter
configure service epipe sap ingress filter
configure service epipe spoke-sdp egress filter
configure service epipe spoke-sdp ingress filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP matching criteria. Only one filter can be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified *filter-id* with an ingress or egress SAP. The *filter-id* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets will not be subject to the filter and will always be passed, even if the filter's default action is to drop.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

IPv6 filters are only supported by the 7450 ESS and 7750 SR but are not supported on a Layer 2 SAP that is configured with QoS MAC criteria. Also, MAC filters are not supported on a Layer 2 SAP that is configured with QoS IPv6 criteria.

Special Cases **Epipe —** Both MAC and IP filters are supported on an Epipe service SAP.

Parameters *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

ipv6-filter-id — Specifies the IPv6 filter policy for 7450 ESS or 7750 SR. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

mac-filter-id — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

Platforms All

filter

Syntax [**no**] **filter**

Context **[Tree]** (config>service>template>epipe-sap-template>egress filter)
[Tree] (config>service>template>epipe-sap-template>ingress filter)

Full Context configure service template epipe-sap-template egress filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service template epipe-sap-template ingress filter

Description Commands in this context configure filter parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

filter

Syntax **filter ip** *ip-filter-id*
no filter

Context **[Tree]** (config>service>ies>aarp-interface>spoke-sdp>egress filter)
[Tree] (config>service>ies>aarp-interface>spoke-sdp>ingress filter)

Full Context configure service ies aarp-interface spoke-sdp egress filter
configure service ies aarp-interface spoke-sdp ingress filter

Description This command associates an IP filter policy with an ingress or egress IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.

The *filter-id* must already be defined before the filter command is executed. If the filter policy does not exist, the operation fails and an error message returned.

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets will not be subject to the filter and will always be passed, even if the filter's default action is to drop.

The **no** form of this command removes any configured filter ID association with the IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local.

Parameters *ip-filter-id* — Specifies the filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535 or a string up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter

Context **[Tree]** (config>service>ies>if>spoke-sdp>egress filter)
[Tree] (config>service>ies>if>spoke-sdp>ingress filter)

Full Context configure service ies interface spoke-sdp egress filter
configure service ies interface spoke-sdp ingress filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates an IP filter policy filter policy with an ingress or egress spoke SDP.

Filter policies control the forwarding and dropping of packets based on matching criteria.

MAC filters are only allowed on Epipe and Virtual Private LAN Service (VPLS) SAPs.

The **filter** command is used to associate a filter policy with a specified *ip-filter-id* with an ingress or egress spoke SDP. The *ip-filter-id* must already be defined in the **config>filter** context before the **filter** command is executed. If the filter policy does not exist, the operation fails and an error message returned.

In general, filters applied to SAPs or spoke SDPs (ingress or egress) apply to all packets on the SAP or spoke SDPs. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Special Cases **IES —** Only IP filters are supported on IES IP interfaces, and the filters only apply to routed traffic.

Parameters **ip** — Keyword indicating the filter policy is an IP filter.

ip-filter-id — The filter name acts as the ID for the IP filter policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP filter policy. The filter ID must already exist within the created IP filters.

Platforms All

filter

Syntax **filter ip** *ip-filter-id*
no filter

Context **[Tree]** (config>service>vprn>aarp-interface>spoke-sdp>egress filter)
[Tree] (config>service>vprn>aarp-interface>spoke-sdp>ingress filter)

Full Context configure service vprn aarp-interface spoke-sdp egress filter
configure service vprn aarp-interface spoke-sdp ingress filter

Description This command associates an IP filter policy with an ingress or egress IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.

The *filter-id* must already be defined before the filter command is executed. If the filter policy does not exist, the operation fails and an error message returned.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets will not be subject to the filter and will always be passed, even if the filter's default action is to drop.

The **no** form of this command removes any configured filter ID association with the IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local.

Parameters *ip-filter-id* — Specifies the filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535 or a string up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>vprn>if>sap>egress filter)
[Tree] (config>service>vprn>if>sap>ingress filter)

Full Context configure service vprn interface sap egress filter
configure service vprn interface sap ingress filter

Description This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.

The **filter** command is used to associate a filter policy with a specified filter ID with an ingress or egress SAP. The filter ID must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation fails and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Parameters **ip** *ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values ip-filter-id: 1 to 65535
name: up to 64 characters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6 *ipv6-filter-id* — Specifies IPv6 filter policy. The filter ID must already exist within the created IP filters.

Values ip-filter-id: 1 to 65535
name: up to 64 characters

Platforms All

filter

Syntax **filter** *filter-id* [**name** *filter-name*]
no filter *filter-id*

Context **[Tree]** (config>service>vprn>log filter)
[Tree] (config>service>vprn>log>log-id filter)

Full Context configure service vprn log filter
configure service vprn log log-id filter

Description This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.

Filters are configured in the **filter** *filter-id* context and then applied to a log in the **log-id** *log-id* context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.

Changes made to an existing filter using any of the sub-commands are immediately applied to the destinations where the filter is applied.

By default, no event filters are defined. Event filters must be explicitly configured.

The **no** form of this command removes the filter association from log IDs, which causes those logs to forward all events.

Default No event filters are defined.

Parameters *filter-id* — Specifies the unique filter ID.

Values 1 to 1500

name *filter-name* — Configures an optional filter name, up to 64 characters, that can be used to refer to the filter after it is created.

Platforms All

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>vprn>network>ingress filter)

Full Context configure service vprn network ingress filter

Description This command configures a network ingress filter for IPv4 or IPv6 traffic arriving over explicitly defined spokes or auto-bind network interfaces for the VPRN service.

The **no** form of this command removes an IPv4, IPv6, or both filters.

Default no filter

Parameters *ip-filter-id/ipv6-filter-id* — Specifies an existing IP/IPv6 filter policy of a scope template.

Values 1 to 65535, *name*
name: 64 characters maximum

Platforms All

filter

Syntax **filter ip** *ip-filter-id*
no filter [**ip** *ip-filter-id*]

Context **[Tree]** (config>service>ies>aa-if>sap>egress filter)
[Tree] (config>service>vprn>aa-if>sap>egress filter)

Full Context configure service ies aa-interface sap egress filter
configure service vprn aa-interface sap egress filter

Description This command applies an IP filter to the SAP.

Default no filter

Parameters *ip-filter-id* — Specifies an existing IP filter ID.

Values 1 to 65535, or name up to 64 characters maximum

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

filter

Syntax **filter**

Context **[Tree]** (debug>app-assure>group>http-host filter)

Full Context debug application-assurance group http-host-recorder filter

Description This command configures recorder filter settings. This command specifies the filtering parameter for the http-host-recorder feature.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

filter

Syntax **filter ip** *ip-filter-id*
no filter

Context **[Tree]** (config>service>ies>video-interface>video-sap>egress filter)
[Tree] (config>service>vpls>video-interface>video-sap>egress filter)
[Tree] (config>service>vprn>video-interface>video-sap>egress filter)
[Tree] (config>service>ies>video-interface>video-sap>ingress filter)
[Tree] (config>service>vpls>video-interface>video-sap>ingress filter)
[Tree] (config>service>vprn>video-interface>video-sap>ingress filter)

Full Context configure service ies video-interface video-sap egress filter
configure service ies video-interface video-sap ingress filter
configure service vpls video-interface video-sap egress filter
configure service vpls video-interface video-sap ingress filter
configure service vprn video-interface video-sap egress filter
configure service vprn video-interface video-sap ingress filter

Description This command associates an existing IP filter policy with an ingress or egress video SAP. Filter policies control the forwarding and dropping of packets based on the matching criteria.

Filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP. The filter ID itself is not removed from the system.

Parameters **ip** *ip-filter-id* — Specifies the ID for the IP filter policy.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

filter

Syntax **filter ip** *ip-filter-id*
no filter

Context **[Tree]** (config>service>vprn>ipmirrorif>spoke-sdp filter)

Full Context configure service vprn ipmirrorif spoke-sdp filter

Description This command places a filter on the IP mirror interface spoke SDP. It is recommended to configure this filter with a PBR filter to redirect the mirror traffic to the proper egress interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the filter ID from the configuration.

Parameters *ip-filter-id* — Specifies the IP filter ID.

Values 1 to 65525 or a name, up to 64 characters.

filter

Syntax **filter** *filter-id*
no filter

Context **[Tree]** (config>li>log>log-id filter)

Full Context configure li log log-id filter

Description This command adds an event filter policy with the log destination.

The **filter** command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.

An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination **snmp-trap-group**.

The application of filters for debug messages is limited to application and subject only.

Accounting records cannot be filtered using the **filter** command.

Only one filter-id can be configured per log destination.

The **no** form of this command removes the specified event filter from the *log-id*.

Parameters *filter-id* — Specifies the event filter policy ID used to associate the filter with the *log-id* configuration. The event filter policy ID must already be defined in **config>log>filter** *filter-id*.

Values 1 to 1000

Platforms All

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>router>if>ingress filter)
[Tree] (config>router>if>egress filter)

Full Context configure router interface egress filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface ingress filter

Description This command associates an IP filter policy with an IP interface.

Filter policies control packet forwarding and dropping based on IP match criteria.

The *ip-filter-id* must have been preconfigured before this **filter** command is executed. If the filter ID does not exist, an error occurs.

Only one filter ID can be specified.

The **no** form of this command removes the filter policy association with the IP interface.

Default no filter

Parameters *ip-filter-id* — The filter name acts as the ID for the IP filter policy expressed as a decimal integer. The filter policy must already exist within the **config>filter>ip** context.

Values 1 to 16384

ipv6-filter-id — The filter name acts as the ID for the IPv6 filter policy expressed as a decimal integer. The filter policy must already exist within the **config>filter>ipv6** context. This parameter only applies to the 7750 SR and 7950 XRS.

Values 1 to 65535

Platforms All

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
filter mac *mac-filter-id*
no filter [**ip** *ip-filter-id*] [**mac** *mac-filter-id*] [**ipv6** *ipv6-filter-id*]

Context **[Tree]** (config>service>pw-template>egress filter)
[Tree] (config>service>pw-template>ingress filter)

Full Context configure service pw-template egress filter
configure service pw-template ingress filter

Description This command associates an IP filter policy or MAC filter policy on egress or ingress. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There are two types of filter policies: IP and MAC. Only one type may be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified *filter ID* with an ingress or egress SAP. The *filter ID* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **filter-name** command can be used in all configuration modes.

This command is mutually exclusive with the **filter-name** command. Only one or the other can be configured.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Parameters *ip-filter-id* — Specifies the IP filter policy.

Values 1 to 65535

ipv6-filter-id — Specifies the IPv6 filter policy.

Values 1 to 65535

mac-filter-id — Specifies the MAC filter policy.

Values 1 to 65535

Platforms All

filter

Syntax **filter** *filter-id* [**name** *filter-name*]
no filter *filter-id*

Context **[Tree]** (config>log filter)

Full Context configure log filter

Description This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.

Filters are configured in the **filter** *filter-id* context and then applied to a log in the **log-id** *log-id* context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.

Changes made to an existing filter using any of the sub-commands are immediately applied to the destinations where the filter is applied.

By default, no event filters are defined. Event filters must be explicitly configured.

The **no** form of this command removes the filter association from log IDs, which causes those logs to forward all events.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *filter-id* — Specifies the unique filter ID.

Values 1 to 1500

name *filter-name* — Configures an optional filter name, up to 64 characters, that can be used to refer to the filter after it is created.

Platforms All

filter

Syntax **filter** *filter-id*
no filter

Context **[Tree]** (config>log>log-id filter)

Full Context configure log log-id filter

Description This command adds an event filter policy with the log destination.

The **filter** command is optional. If an event filter is not configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.

An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination **snmp-trap-group**.

The application of filters for debug messages is limited to application and subject only.

Accounting records cannot be filtered using the **filter** command.

Only one filter ID can be configured per log destination.

The **no** form of this command removes the specified event filter from the *log-id*.

Parameters *filter-id* — Specifies the event filter policy ID is used to associate the filter with the *log-id* configuration. The event filter policy ID must already be defined in **config>log>filter** *filter-id*.

Values 1 **to** 1000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.58 filter-cam-type

filter-cam-type

Syntax **filter-cam-type** {**normal** | **packet-length**}

Context **[Tree]** (config>service>vprn>flowspec filter-cam-type)

Full Context configure service vprn flowspec filter-cam-type

Description This command specifies the filter type that is required to embed FlowSpec entries to this VPRN. The filter type defines the match criteria that are available in the filter policy.

Default normal

Parameters **normal** — Specifies that the filter policy is of type normal.

packet-length — Specifies that the filter policy is of type packet-length.

Platforms All

filter-cam-type

Syntax **filter-cam-type** {**normal** | **packet-length**}

Context **[Tree]** (config>router>flowspec filter-cam-type)

Full Context configure router flowspec filter-cam-type

Description This command specifies the filter type that is required to embed FlowSpec entries. The filter type defines the match criteria that are available in the filter policy.

Default normal

Parameters **normal** — Specifies that the filter policy is of type normal.

packet-length — Specifies that the filter policy is of type packet-length.

Platforms All

10.59 filter-id-range

filter-id-range

Syntax **filter-id-range start** *filter-id* **end** *filter-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no filter-id-range

Context [Tree] (config>filter>md-auto-id filter-id-range)

Full Context configure filter md-auto-id filter-id-range

Description This command specifies the range of IDs used by SR OS to automatically assign an ID to filters that are created in model-driven interfaces without an ID explicitly specified by the user or client.

A filter created with an explicitly-specified ID cannot use an ID in this range. In classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed, which causes any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **config>filter md-auto-id** command for further details.

Default no filter-id-range

Parameters **start** *filter-id* — Specifies the lower value of the ID range. The value must be less than or equal to the **end** value.

Values 1 to 2147483647

end *filter-id* — Specifies the upper value of the ID range. The value must be greater than or equal to the **start** value.

Values 1 to 2147483647

Platforms All

10.60 filter-name

filter-name

Syntax [**no**] **filter-name**

Context [Tree] (config>service>template>epipe-sap-template>egress filter-name)
[Tree] (config>service>template>epipe-sap-template>ingress filter-name)

Full Context configure service template epipe-sap-template egress filter-name
configure service template epipe-sap-template ingress filter-name

Description Commands in this context configure filter parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

filter-name

Syntax [**no**] **filter-name**

Context **[Tree]** (config>service>template>vpls-sap-template>egress filter-name)
[Tree] (config>service>template>vpls-sap-template>ingress filter-name)

Full Context configure service template vpls-sap-template egress filter-name
configure service template vpls-sap-template ingress filter-name

Description Commands in this context configure filter parameters.

Platforms All

filter-name

Syntax **filter-name** *filter-name*
no filter-name

Context **[Tree]** (config>filter>ip-exception filter-name)

Full Context configure filter ip-exception filter-name

Description This command configures filter-name attribute of a given filter. filter-name, when configured, can be used instead of filter ID to reference the given policy in the CLI.

Default no filter-name

Parameters *filter-name* — Specifies a string up to 64 characters in length that uniquely identifies this filter policy.

The following restrictions apply to the *filter-name*:

- Policy names may not begin with a number (0-9).
- Policy names may not begin with the underscore "_" character (e.g. _myPolicy). Names that start with underscore are reserved for system generated names.
- "fSpec-x" (where x is any number) cannot be used as a user defined filter name.

filter-name

Syntax **filter-name ip** *ip-name*
filter-name ipv6 *ipv6-name*
filter-name mac *mac-name*
no filter-name [**ip**] [**ipv6**] [**mac**]

Context **[Tree]** (config>service>pw-template>egress filter-name)
[Tree] (config>service>pw-template>ingress filter-name)

Full Context configure service pw-template egress filter-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service pw-template ingress filter-name

Description This command associates an IP filter policy or MAC filter policy on egress or ingress. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There are two types of filter policies: IP and MAC. Only one type may be applied to a SAP at a time.

The **filter-name** command is used to associate a filter policy with a specified *filter name* with an ingress or egress SAP. The *filter name* must already be defined before the **filter-name** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

This command is mutually exclusive with the **filter** command. Only one or the other can be configured.

The **no** form of this command removes any configured filter name association with the SAP or IP interface. The filter name itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter name and only break the association with the service object, use **scope** command within the filter definition to change the scope to **local** or **global**. The default scope of a filter is **local**.

Parameters *ip-name* — Specifies the IP filter policy. The filter name must already exist within the created IP filters, up to 64 characters.

ipv6-name — Specifies the IPv6 filter policy. The filter name must already exist within the created IPv6 filters, up to 64 characters.

mac-name — Specifies the MAC filter policy. The specified filter name must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters, up to 64 characters.

Platforms All

10.61 filter-profile

filter-profile

Syntax **filter-profile** {**none** | **profile-a**}

Context **[Tree]** (config>card filter-profile)

Full Context configure card filter-profile

Description This command controls the resources allocated to ingress and egress IPv4 and IPv6 filters on a per-linecard basis on the SR-a platform. You must shutdown the card prior to changing the filter profile.

Default filter-profile none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **none** — Sets the card filter profile to its default value.

profile-a — Sets the card filter profile to **profile-a**.

Platforms 7750 SR-a

10.62 filter-sample

filter-sample

Syntax [**no**] **filter-sample**

Context **[Tree]** (config>filter>ip-filter>entry filter-sample)
[Tree] (config>filter>ipv6-filter>entry filter-sample)

Full Context configure filter ip-filter entry filter-sample
configure filter ipv6-filter entry filter-sample

Description This command enables cflowd sampling for packets matching this filter entry.

If the cflowd is either not enabled or set to **cflowd interface** mode, this command is ignored.

The **no** form disables the cflowd sampling using this filter entry.

Default no filter-sample

Platforms All

10.63 filtering

filtering

Syntax **filtering** *filtering-mode*
no filtering

Context **[Tree]** (config>service>nat>nat-policy filtering)
[Tree] (config>service>nat>firewall-policy filtering)
[Tree] (config>service>nat>up-nat-policy filtering)

Full Context configure service nat firewall-policy filtering
configure service nat nat-policy filtering
configure service nat up-nat-policy filtering

Description This command configures the filtering of the NAT or residential firewall policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default filtering endpoint-independent

Parameters *filtering-mode* — Specifies the method used to filter the inbound traffic.

Values address-and-port-dependent, endpoint-independent

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy filtering
- configure service nat nat-policy filtering

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy filtering

10.64 find-egress

find-egress

Syntax **find-egress packet** *packet-number* **ingress-port** *physical-port-id*

Context **[Tree]** (oam find-egress)

Full Context oam find-egress

Description This command executes the OAM find-egress test, injecting the specified packet ID into the specified ingress port.

Parameters *packet-number* — Specifies the build-packet to be injected into the associated ingress port.

Values 1 to 65535

physical-port-id — Specifies the physical port ID that is injected into the specified build-packet.

Values *slot*/*mda*/*port*

esat-<sat-id>/slot/port?

esat	keyword
id	1 to 20
slot	always 1
port	Ethernet satellite client port number

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.65 fips-140-2

fips-140-2

Syntax [**no**] **fips-140-2**

Context **[Tree]** (bof fips-140-2)

Full Context bof fips-140-2

Description This command is used to configure the node in FIPS-140-2 mode. Before using this command, the operator must ensure that no current configuration exists in the config file that is not supported in FIPS-140-2 mode. Failing to remove unsupported configuration will result in the node being unable to boot up. The node must be rebooted after executing this command in order for the node to begin operating in FIPS-140-2 mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.66 fir-burst-limit

fir-burst-limit

Syntax **fir-burst-limit** *size* **[bytes | kilobytes]**
no fir-burst-limit

Context **[Tree]** (config>qos>sap-egress>queue fir-burst-limit)

Full Context configure qos sap-egress queue fir-burst-limit

Description This command configures a burst limit for the FIR of the specified queue.

The **no** version of this command returns the limit to the default value.

Parameters *size* — Specifies the size of the FIR burst limit.

Values 1 to 102400, default

Platforms 7750 SR-1, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.67 firewall

firewall

Syntax **firewall**

Context **[Tree]** (config>router firewall)
[Tree] (config>service>vprn firewall)

Full Context configure router firewall
configure service vprn firewall

Description Commands in this context configure firewall parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.68 firewall-info

firewall-info

Syntax [**no**] **firewall-info**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute firewall-info)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute firewall-info

Description This command enables inclusion of the Firewall Information VSA in AAA protocols.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.69 firewall-policy

firewall-policy

Syntax **firewall-policy** *policy-name*
no firewall-policy

Context **[Tree]** (config>subscr-mgmt>sub-prof firewall-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt sub-profile firewall-policy

Description This command enables the IPv6 firewall for this subscriber profile using the specified firewall policy.

The **no** form of this command disables the IPv6 firewall for this subscriber profile.

Default no firewall-policy

Parameters *policy-name* — Specifies the name of the firewall policy, up to 32 characters maximum.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

firewall-policy

Syntax **firewall-policy** *name* [**create**]
no firewall-policy

Context **[Tree]** (config>service>nat firewall-policy)

Full Context configure service nat firewall-policy

Description This command configures a firewall policy that can be used in contexts where basic protection from outside attack vectors is required.

The **no** form of the command removes the policy, and can only be performed when the policy is not in use.

Default no firewall-policy

Parameters **create** — Mandatory keyword used when creating a firewall policy.

name — Specifies the name of the firewall policy, up to 32 characters maximum.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.70 flags-tlv

flags-tlv

Syntax **[no] flags-tlv**

Context **[Tree]** (config>router>fad>flex-algo flags-tlv)

Full Context configure router flexible-algorithm-definitions flex-algo flags-tlv

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command advertises the FAD Flags TLV to provide additional context on how the router must run a constrained SPF (cSPF). The IETF definition includes only the M-flag for use in the FAD Flags TLV. When it is set, the M-flag specifies the use of a Flex-Algorithm specific prefix metric. The M-flag is important for inter-area or inter-domain routing support with Flex-Algorithms.

When a router advertises a FAD, it is optional to advertise the FAD Flags TLV. However, when a FAD that includes the FAD Flags TLV is received, then the router must decode the flags before participating in the Flex-Algorithm.

By default, the following considerations apply to the FAD Flags TLV.

- SR OS sets the M-flag and advertises the FAD Flags TLV.
- When a FAD Flags TLV is received, SR OS decodes the flags and modifies the cSPF computation based upon the M-flag status.

The **no** form of this command prevents the advertisement of the FAD Flags TLV within a FAD.

Default flags-tlv

Platforms All

10.71 flex-algo

flex-algo

Syntax **flex-algo** *flex-algo*
no flex-algo

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop flex-algo)

Full Context configure router static-route-entry indirect tunnel-next-hop flex-algo

Description This command instructs the tunnel towards the indirect static-route next-hop to use the specified flexible algorithm.

It is assumed that the router using this command is participating in the flexible algorithm. This command instructs the router to lookup the indirect next-hop using flexible algorithm tunnels. If flexible algorithm aware tunnel to the indirect next-hop does not exist, then the static-route is not activated.

The expected outcome of this command is that when the router receives an IP payload packet, that it is steered towards the indirect next-hop using a flexible algorithm aware segment-routing tunnel if such tunnel exists. If such tunnel does not exist, then the route is not active, and the received IP packet will be dropped, if no other Longest Prefix Match (LPM) route exists.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the *flex-algo* parameter is specified, the resolution filter can only use matching flexible algorithm-aware segment routing tunnels created by flexible algorithm-aware routing protocols (for example, SR IS-IS).

The **no** form of this command disables flexible algorithm-aware indirect next-hop resolution.

Default no flex-algo

Parameters *flex-algo* — Configures or deconfigures tunnel-next-hop flexible algorithm for resolving indirect static-route-entry.

Values 128 to 255

Platforms All

flex-algo

Syntax **flex-algo** *fad-name* [**create**]
no flex-algo *fad-name*

Context **[Tree]** (config>router>fad flex-algo)

Full Context configure router flexible-algorithm-definitions flex-algo

Description This command configures the definition context for a Flexible Algorithm Definition (FAD). Parameters, including the FAD priority, metric type, links to construct a flexible algorithm topology graph, and a description of the algorithm. Up to 256 local FADs can be configured on a router.

The FAD configuration parameters are grouped using the *fad-name* as the reference anchor. When an IGP is configured to use and advertise a local configured FAD, the *fad-name* is used as the reference anchor.

The **no** form of this command deletes the configured parameters and removes the defined FAD.

Default no flex-algo

Parameters *fad-name* — Specifies the name of the flexible algorithm, up to 32 characters, that is used as reference anchor for the configured parameters.

create — Specifies the mandatory keyword to create a router instance.

Platforms All

flex-algo

Syntax [**no**] **flex-algo** *flex-algo*

Context **[Tree]** (config>router>isis>flex-algos flex-algo)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router isis flexible-algorithms flex-algo

Description This command enters the configuration context for an IS-IS flexible algorithm.

A maximum of seven unique flexible algorithms can be configured on a router across all configured IS-IS instances. In each IS-IS flexible algorithm configuration context, the IS-IS instance participation can be either enabled or disabled, and it configures the advertising of a locally-configured flexible algorithm definition.

When flexible algorithm is enabled in an IS-IS instance, it is enabled for all levels (Level 1 and Level 2) within the IS-IS instance.

The **no** form of this command removes the IS-IS flexible algorithm configuration context.

Default no flex-algo

Parameters *flex-algo* — Specifies the number of the IS-IS flexible algorithm.

Values 128 to 255

Platforms All

flex-algo

Syntax [**no**] **flex-algo** *flex-algo-id*

Context **[Tree]** (config>router>ospf>flex-algos flex-algo)

Full Context configure router ospf flexible-algorithms flex-algo

Description This command enters the configuration context for an OSPFv2 flexible algorithm.

A maximum of seven unique flexible algorithms can be configured on a router across all configured OSPFv2 instances. The supported flexible algorithms are in the range of 128 to 255. In each OSPF flexible algorithm configuration context, the OSPFv2 instance participation can be either enabled or disabled, and it configures the advertising of a locally-configured flexible algorithm definition.

When flexible algorithm is enabled in an OSPF instance, it is enabled for all areas within the OSPF instance.

The **no** form of this command removes the OSPF flexible algorithm configuration context.

Default no flex-algo

Parameters *flex-algo-id* — Specifies the OSPF flexible algorithm number.

Values 128 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

flex-algo

Syntax [**no**] **flex-algo** *flex-algo-id*

Context **[Tree]** (config>router>ospf>area>if flex-algo)

Full Context configure router ospf area interface flex-algo

Description This command enters the OSPFv2 flexible algorithms configuration context on the interface.

The **no** form of this command removes the OSPF flexible algorithm configuration context.

Default no flex-algo

Parameters *flex-algo-id* — Specifies the number of the OSPF flexible algorithm.

Values 128 to 255

Platforms All

flex-algo

Syntax **flex-algo** *flex-algo-id* | *param-name*
no flex-algo

Context **[Tree]** (config>router>policy-options>policy-statement>default-action flex-algo)
[Tree] (config>router>policy-options>policy-statement>entry>action flex-algo)

Full Context configure router policy-options policy-statement default-action flex-algo
configure router policy-options policy-statement entry action flex-algo

Description This command configures the Flex-Algorithm for use in the BGP next-hop autobind operation in a BGP import policy. A Flex-Algorithm aware autobind of the BGP next-hop is enabled when the route is matched by the policy statement entry.

Note:

- Flex-Algorithm aware next-hop lookup is supported for unicast BGP, VPRN, and BGP-LU.
- This command is not supported for multicast address families.

The **no** form of this command removes the Flex-Algorithm aware next-hop lookup.

Default no flex-algo

Parameters *flex-algo-id* — Specifies the flexible algorithm forwarding path.

Values 128 to 255

param-name — Specifies the parameter name, up to 32 characters, that starts and ends with an at-sign (@) symbol.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

10.72 flexible-algorithm-definitions

flexible-algorithm-definitions

Syntax **flexible-algorithm-definitions**

Context **[Tree]** (config>router flexible-algorithm-definitions)

Full Context configure router flexible-algorithm-definitions

Description Commands in this context locally configure algorithm definitions.

Platforms All

10.73 flexible-algorithms

flexible-algorithms

Syntax **flexible-algorithms**

Context **[Tree]** (config>router>isis flexible-algorithms)

Full Context configure router isis flexible-algorithms

Description Commands in this context configure the IS-IS parameters for flexible algorithm participation.

Platforms All

flexible-algorithms

Syntax **flexible-algorithms**

Context **[Tree]** (config>router>ospf flexible-algorithms)

Full Context configure router ospf flexible-algorithms

Description Commands in this context configure the OSPFv2 parameters for flexible algorithm participation.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.74 flood-garp-and-unknown-req

flood-garp-and-unknown-req

Syntax [**no**] **flood-garp-and-unknown-req**

Context **[Tree]** (config>service>ies>if>vpls>evpn>arp flood-garp-and-unknown-req)
[Tree] (config>service>vprn>if>vpls>evpn>arp flood-garp-and-unknown-req)

Full Context configure service ies interface vpls evpn arp flood-garp-and-unknown-req
configure service vprn interface vpls evpn arp flood-garp-and-unknown-req

Description This command controls whether CPM-originated ARP frames are flooded in the R-VPLS service. Any frames that are data path flooded, such as the ARP messages received on a SAP, are flooded regardless of the command.

The **no** form of this command disables flooding GARP and unknown requests.

Default flood-garp-and-unknown-req

Platforms All

10.75 flood-time

flood-time

Syntax **flood-time** *flood-time*
no flood-time

Context **[Tree]** (config>service>vpls>mrp flood-time)

Full Context configure service vpls mrp flood-time

Description This command configures the amount of time, in seconds, after a status change in the VPLS service during which traffic is flooded. When that time expires, traffic will be delivered according to the MMRP registrations that exist in the VPLS. When “no flood-time” is executed, flooding behavior is disabled.

Default no flood-time

Parameters *flood-time* — Specifies the MRP flood time, in seconds.

Values 3 to 600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

flood-time

Syntax **flood-time** *flood-time*
no flood-time

Context **[Tree]** (config>service>vpls>mrp>mmrp flood-time)

Full Context configure service vpls mrp mmrp flood-time

Description This command configures the amount of time, in seconds, after a status change in the VPLS service during which traffic is flooded. Once that time expires, traffic will be delivered according to the MMRP registrations that exist in the VPLS.

Default flood-time 3

Parameters *flood-time* — Specifies the MRP flood time, in seconds

Values 3 to 600

Platforms All

10.76 flow-attribute

flow-attribute

Syntax [**no**] **flow-attribute** *flow-attribute-name*

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match flow-attribute)

Full Context configure application-assurance group policy app-qos-policy entry match flow-attribute

Description This command configures a flow attribute to use as match criteria.

The **no** form of this command reverts to the default value.

Default no flow-attribute

Parameters *flow-attribute-name* — Specifies the name of the flow attribute, up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

flow-attribute

Syntax [**no**] **flow-attribute** *flow-attribute-name*

Context **[Tree]** (config>isa>aa-grp flow-attribute)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure isa application-assurance-group flow-attribute

Description This command enables the specified flow attribute.

The **no** form of this command disables the attribute.

Parameters *flow-attribute-name* — Specifies the name of the flow attribute, up to 256 characters.

Values

video	This attribute specifies streaming or real-time video media traffic transferred between a sender and receiver. It does not differentiate adaptive and nonadaptive video streaming. Assigned to flows based on packet payload inspection (many protocols) or behavioral mechanisms, and may be used together with the RTC attribute to identify video call traffic.
abr_service	This attribute is assigned to adaptive bit rate traffic exchanges where the traffic rate or behavior can be automatically adjusted based on changes in network conditions. Assigned by application filter configuration or by behavioral mechanisms.
audio	This attribute is assigned to streaming or real-time audio media traffic transferred between a sender and receiver. Assigned to flows based on packet payload inspection or behavioral mechanisms, and may be used together with the RTC attribute to identify voice call traffic.
encrypted	This attribute is assigned to traffic exchanges where the initial payload or the entirety of the exchange is encrypted. Assigned to sessions based on packet payload inspection or by behavioral mechanisms.
download	This attribute is assigned to traffic that has a high likelihood of exchanging data predominantly in the network to subscriber direction over the lifetime of a session. May be assigned to sessions based on behavioral mechanisms.
upload	This attribute is assigned to traffic that has a high likelihood of exchanging data predominantly in the subscriber to network direction over the lifetime of the session. The upload and download attributes are mutually exclusive. Assigned to sessions based on behavioral mechanisms.
real_time_communication	This attribute is assigned to traffic that provides a low latency or real-time exchange of information between two or more communicating endpoints. Assigned by packet payload inspection of an RTP protocol being used or by behavioral mechanisms.
esni	This attribute is assigned to traffic that uses an encrypted server name indication (eSNI), as part of the TLS layer negotiation

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.77 flow-count

flow-count

Syntax **flow-count** *flow-count*
no flow-count

Context **[Tree]** (config>app-assure>group>policer flow-count)
[Tree] (config>app-assure>group>tod-override flow-count)

Full Context configure application-assurance group policer flow-count
configure application-assurance group policer tod-override flow-count

Description This command configures the flow count for the flow-count-limit policer. It is recommended to configure flow count subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

Default no flow-count

Parameters *flow-count* — Specifies the flow count for the flow-count-limit policer.

Values 0 to 100000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.78 flow-count-limit

flow-count-limit

Syntax **flow-count-limit** *policer-name* [**event-log** *event-log-name*]
no flow-count-limit

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action flow-count-limit)

Full Context configure application-assurance group policy app-qos-policy entry action flow-count-limit

Description This command assigns an existing flow count limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When multiple policers apply to a single flow, the final action on a packet is the worst case of all policer outcomes (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of this command removes this flow policer from actions on flows matching this AQP entry.

Default no flow-count-limit

Parameters *policer-name* — Specifies the name of the existing flow setup rate policer for this application assurance profile. The *policer-name* is configured in the **config>app-assure>group>policer** context.

event-log-name — Specifies the name of the event log used when event logging is enabled, up to 32 characters, which is used when event logging is enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.79 flow-label

flow-label

Syntax **flow-label** *flow-label* [*mask*]
no flow-label

Context **[Tree]** (config>filter>ipv6-filter>entry>match flow-label)

Full Context configure filter ipv6-filter entry match flow-label

Description This command configures the flow-label and optional mask match condition.

The **no** form of the command reverts to the default.

Default no flow-label

Parameters *flow-label* — Specifies the flow label to be used as a match criterion. Value can be expressed as a decimal integer, as well as in hexadecimal or binary format. The following value shows decimal integer format only.

Values 0 to 1048575

mask — Specifies the flow label mask value for this policy IPv6 Filter entry. Value can be expressed as a decimal integer, as well as in hexadecimal or binary format. The following value shows decimal integer format only.

Values 0 to 1048575

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

flow-label

Syntax **flow-label** *value*
no flow-label

Context **[Tree]** (config>system>security>mgmt-access-filter>ipv6-filter>entry flow-label)

Full Context configure system security management-access-filter ipv6-filter entry flow-label

Description This command configures flow label match conditions. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service or real-time service. This command only applies to the 7750 SR and 7950 XRS.

Parameters *value* — Specifies the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (See RFC 3595, *Textual Conventions for IPv6 Flow Label*.)

Values 0 to 1048575

Platforms All

flow-label

Syntax **flow-label** *value*
no flow-label

Context **[Tree]** (cfg>sys>sec>cpm>ipv6-filter>entry>match flow-label)

Full Context configure system security cpm-filter ipv6-filter entry match flow-label

Description This command configures flow label match conditions. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default quality of service or real-time service.

Parameters *value* — Specifies the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (See RFC 3595, *Textual Conventions for IPv6 Flow Label*.)

Values 0 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.80 flow-label-load-balancing

flow-label-load-balancing

Syntax [**no**] **flow-label-load-balancing**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>if>load-balancing flow-label-load-balancing)
[Tree] (config>service>ies>if>load-balancing flow-label-load-balancing)
[Tree] (config>service>vprn>if>load-balancing flow-label-load-balancing)
[Tree] (config>service>vprn>nw-if>load-balancing flow-label-load-balancing)

Full Context configure router interface load-balancing flow-label-load-balancing
configure service ies interface load-balancing flow-label-load-balancing
configure service vprn interface load-balancing flow-label-load-balancing
configure service vprn network-interface load-balancing flow-label-load-balancing

Description This command enables load balancing in ECMP and LAG that is based on the output of a hash performed on the triplet {SA, DA, flow label} in the header of an IPv6 packet received on a IES, VPRN, R-VPLS, CsC, or network interface.

The **no** form of this command disables load balancing in ECMP and LAG based on the hash of triplet fields {SA, DA, flow label} in an IPv6 packet header.

Default no flow-label-load-balancing

Platforms All

10.81 flow-rate

flow-rate

Syntax **flow-rate** *sample-rate*
no flow-rate

Context [Tree] (config>app-assure>group>cflowd>rtp-perf flow-rate)
[Tree] (config>app-assure>group>cflowd>tcp-perf flow-rate)
[Tree] (config>app-assure>group>cflowd>comp flow-rate)

Full Context configure application-assurance group cflowd comprehensive flow-rate
configure application-assurance group cflowd rtp-performance flow-rate
configure application-assurance group cflowd tcp-performance flow-rate

Description This command specifies the per-flow sampling rate for the cflowd export of Application Assurance performance statistics.

The **no** form of this command reverts to the default.

Default no flow-rate

Parameters *sample-rate* — Specifies the rate at which to sample flows that are eligible for TCP performance measurement.

Values 1 to 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.82 flow-rate-limit

flow-rate-limit

Syntax **flow-rate-limit** *policer-name* [**event-log** *event-log-name*]
no flow-rate-limit

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action flow-rate-limit)

Full Context configure application-assurance group policy app-qos-policy entry action flow-rate-limit

Description This command assigns an existing flow setup rate limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worst case of all policer outcomes (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of this command removes this flow policer from actions on flows matching this AQP entry.

Default no flow-rate-limit

Parameters *policer-name* — Specifies the policer name up to 32 characters.

event-log *event-log-name* — Specifies the event-log-name up to 32 characters, which will be used when event logging is enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.83 flow-rate2

flow-rate2

Syntax **flow-rate2** *sample-rate*
no flow-rate2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>cflowd>rtp-perf flow-rate2)
[Tree] (config>app-assure>group>cflowd>tcp-perf flow-rate2)
[Tree] (config>app-assure>group>cflowd>comp flow-rate2)

Full Context configure application-assurance group cflowd comprehensive flow-rate2
configure application-assurance group cflowd rtp-performance flow-rate2
configure application-assurance group cflowd tcp-performance flow-rate2

Description This command specifies the per-flow second sampling rate for the cflowd export of Application Assurance performance statistics.

The **no** form of this command reverts to the default.

Default no flow-rate2

Parameters *sample-rate* — Specifies the rate at which to sample flows that are eligible for TCP and/or RTP performance measurement.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.84 flow-setup-direction

flow-setup-direction

Syntax **flow-setup-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}

Context [Tree] (config>app-assure>group>policy>app-filter>entry flow-setup-direction)

Full Context configure application-assurance group policy app-filter entry flow-setup-direction

Description This command configures the direction of flow setup to which the application filter entry is to be applied.

Default flow-setup-direction both

Parameters **subscriber-to-network** — Specifies that the app-filter entry will be applied to flows initiated by a local subscriber.

network-to-subscriber — Specifies that the app-filter entry will be applied to flows initiated from a remote destination towards a local subscriber.

both — Specifies that the app filter entry will be applied for subscriber-to-network and network-to-subscriber traffic.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.85 flow-setup-high-wmark

flow-setup-high-wmark

Syntax **flow-setup-high-wmark** *high-watermark*

Context **[Tree]** (config>app-assure flow-setup-high-wmark)

Full Context configure application-assurance flow-setup-high-wmark

Description This command configures the system wide high watermark threshold for per-ISA throughput in packets/second when an alarm will be raised by the agent. The value must be larger than or equal to the packet-rate-low-wmark parameter.

Default flow-setup-high-wmark max

Parameters *high-watermark* — Specifies the high watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-low-wmark value.

Values 1 to 800000, **max** flows/sec (disabled)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.86 flow-setup-low-wmark

flow-setup-low-wmark

Syntax **flow-setup-low-wmark** *low-watermark*
no flow-setup-low-wmark

Context **[Tree]** (config>app-assure flow-setup-low-wmark)

Full Context configure application-assurance flow-setup-low-wmark

Description This command configures the flow setup rate on the ISA-AA when a flow setup alarm will be raised by the agent.

Default flow-setup-low-wmark 0

Parameters *low-watermark* — Specifies the low watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-high-wmark value.

Values 1 to 799999 flows/sec

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.87 flow-spec-dest

flow-spec-dest

Syntax **flow-spec-dest** *prefix-list-name*
no flow-spec-dest

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from flow-spec-dest)

Full Context configure router policy-options policy-statement entry from flow-spec-dest

Description This command is used to match BGP FlowSpec routes on the basis of the destination IP prefix in the flow specification. An IPv4 FlowSpec route is matched by this command if its NLRI contains a type 1 subcomponent encoding a prefix and prefix-length that is covered by an entry in the referenced prefix-list. An IPv6 FlowSpec route is matched by this command if its NLRI contains a type 1 component encoding prefix-offset=0 and a prefix & prefix-length that is covered by an entry in the referenced prefix-list.

The **flow-spec-dest** command has no effect when the policy is not applied as a BGP import or export policy.

Default no flow-spec-dest

Parameters *prefix-list-name* — Specifies the name of a prefix-list containing IPv4 and/or IPv6 prefix entries [up to 32 characters].

Platforms All

10.88 flow-spec-source

flow-spec-source

Syntax **flow-spec-source** *prefix-list-name*
no flow-spec-source

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from flow-spec-source)

Full Context configure router policy-options policy-statement entry from flow-spec-source

Description This command is used to match BGP FlowSpec routes on the basis of the source IP prefix in the flow specification. An IPv4 FlowSpec route is matched by this command if its NLRI contains a type 2 subcomponent encoding a prefix and prefix-length that is covered by an entry in the referenced prefix-list. An IPv6 FlowSpec route is matched by this command if its NLRI contains a type 2 component encoding prefix-offset=0 and a prefix & prefix-length that is covered by an entry in the referenced prefix-list.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **flow-spec-source** command has no effect when the policy is not applied as a BGP import or export policy.

Default no flow-spec-source

Parameters *prefix-list-name* — Specifies the name of a prefix-list containing IPv4 and/or IPv6 prefix entries, up to 32 characters.

Platforms All

10.89 flow-table-high-wmark

flow-table-high-wmark

Syntax **flow-table-high-wmark** *high-watermark*
no flow-table-high-wmark

Context **[Tree]** (config>app-assure flow-table-high-wmark)

Full Context configure application-assurance flow-table-high-wmark

Description This command configures the system-wide high watermark threshold as a percentage of the flow table size for the per-ISA utilization of the flow records when a full alarm will be raised by the agent.

Default flow-table-high-wmark 95

Parameters *high-watermark* — Specifies the high watermark for flow table full alarms, in percent.

Values 0 to 100

Default 95

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.90 flow-table-low-wmark

flow-table-low-wmark

Syntax **flow-table-low-wmark** *low-watermark*
no flow-table-low-wmark

Context **[Tree]** (config>app-assure flow-table-low-wmark)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance flow-table-low-wmark

Description This command configures the system-wide low watermark threshold as a percentage of the flow table size for per-ISA. The value must be lower than or equal to the **flow-table-high-wmark** *high-watermark* parameter.

Default flow-table-low-wmark 90

Parameters *low-watermark* — Specifies the low watermark for flow table full alarms, in percent.

Values 0 to 100

Default 90

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.91 flow-timeout-on-switchover

flow-timeout-on-switchover

Syntax **flow-timeout-on-switchover** *percent*

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy flow-timeout-on-switchover)

Full Context configure isa nat-group inter-chassis-redundancy flow-timeout-on-switchover

Description This command configures an initial flow timeout on the newly activated node for the **nat-group** after a switchover. This timeout stays in effect only if there is no traffic present over this flow; otherwise, the first packet over the flow after the switchover resets the flow timeout to the originally configured value (under the NAT policy configuration).

This command configuration restricts the flow timeout to a portion of the originally configured value.

Default flow-timeout-on-switchover 50

Parameters *percent* — Specifies the percentage of the originally configured timeout value for the flow under the **nat-policy**.

Values 1 to 50

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.92 flows-active-count

flows-active-count

Syntax [**no**] **flows-active-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr flows-active-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr flows-active-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters flows-active-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters flows-active-count

Description This command includes the active flow count and only applies to the 7750 SR.

The **no** form of this command excludes the active flow count in the AA subscriber's custom record.

Default no flows-active-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.93 flows-admitted-count

flows-admitted-count

Syntax [**no**] **flows-admitted-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr flows-admitted-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr flows-admitted-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters flows-admitted-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters flows-admitted-count

Description This command includes the admitted flow count and only applies to the 7750 SR.

The **no** form of this command excludes the flow’s admitted count in the AA subscriber's custom record.

Default no flows-admitted-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.94 flows-denied-count

flows-denied-count

Syntax [**no**] **flows-denied-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr flows-denied-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr flows-denied-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters flows-denied-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters flows-denied-count

Description This command includes the flow's denied count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of this command excludes the flow's denied count.

Default no flows-denied-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.95 flowspec

flowspec

Syntax [**no**] **flowspec**

Context **[Tree]** (config>service>vprn>if>sap>ingress flowspec)
[Tree] (config>service>vprn>if>spoke-sdp>ingress flowspec)
[Tree] (config>service>ies>if>sap>ingress flowspec)
[Tree] (config>service>ies>if>spoke-sdp>ingress flowspec)

Full Context configure service ies interface sap ingress flowspec
configure service ies interface spoke-sdp ingress flowspec
configure service vprn interface sap ingress flowspec
configure service vprn interface spoke-sdp ingress flowspec

Description This command enables IPv4 FlowSpec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv4 FlowSpec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv4 traffic on an interface can be filtered by both a user-defined IPv4 filter and FlowSpec. Evaluation proceeds in this order:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- user-defined IPv4 filter entries
- FlowSpec derived filter entries
- user-defined IPv4 filter default-action

The **no** form of this command removes IPv4 FlowSpec filtering from an IP interface.

Default no flowspec. No access interfaces have IPv4 FlowSpec enabled.

flowspec

Syntax **flowspec**

Context **[Tree]** (config>service>vprn flowspec)

Full Context configure service vprn flowspec

Description Commands in this context configure FlowSpec related parameters for the specified routing instance.

Platforms All

flowspec

Syntax **flowspec**

Context **[Tree]** (config>service>vprn>bgp flowspec)

Full Context configure service vprn bgp flowspec

Description The context to enable and disable FlowSpec validations.

Platforms All

flowspec

Syntax **flowspec**

Context **[Tree]** (config>router flowspec)

Full Context configure router flowspec

Description Commands in this context configure FlowSpec related parameters for the specified routing instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

flowspec

Syntax **flowspec**

Context **[Tree]** (config>router>bgp flowspec)

Full Context configure router bgp flowspec

Description Commands in this context enable and disable FlowSpec validations.

Platforms All

10.96 flowtable

flowtable

Syntax [**no**] **flowtable** *of-table-id*

Context **[Tree]** (config>open-flow>of-switch flowtable)

Full Context configure open-flow of-switch flowtable

Description This command configures the flow table parameters for this OpenFlow switch instance.

The **no** form of this command restores flow table configuration default settings.

Default no flowtable

Parameters *of-table-id* — Specifies an identifier of the open flow table, a string up to 256 characters.

Platforms All

10.97 flr-threshold

flr-threshold

Syntax **flr-threshold** *percentage*
no flr-threshold

Context **[Tree]** (config>oam-pm>session>ethernet>lmm>availability flr-threshold)
[Tree] (config>oam-pm>session>ethernet>slm flr-threshold)

Full Context configure oam-pm session ethernet lmm availability flr-threshold
configure oam-pm session ethernet slm flr-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the frame loss threshold used to determine whether the delta-t is available or unavailable. An individual delta-t with a frame loss threshold equal to the configured threshold is marked unavailable. An individual delta-t with a frame loss threshold lower than the configured threshold is marked as available.

The **no** form of this command restores the default value of 50%.

Parameters *percentage* — Specifies the percentage of the threshold.

Values 0 to 100

Default 50

Platforms All

flr-threshold

Syntax **flr-threshold** *percentage*
no flr-threshold

Context **[Tree]** (config>oam-pm>session>ip>twamp-light>loss flr-threshold)

Full Context configure oam-pm session ip twamp-light loss flr-threshold

Description This command defines the frame loss threshold used to determine whether the delta-t is available or unavailable. An individual delta-t with a frame loss threshold equal to or higher than the configured threshold is marked unavailable. An individual delta-t with a frame loss threshold lower than the configured threshold is marked as available.

The **no** form of this command restores the default value of 50%.

Default flr-threshold 50

Parameters *percentage* — Specifies the percentage of the threshold.

Values 0 to 100

Default 50

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.98 fng-alarm-time

fng-alarm-time

Syntax **fng-alarm-time** *time*

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>alarm-notification fng-alarm-time)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>eth-tunnel>path>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>lag>eth-cfm>mep>alarm-notification fng-alarm-time)

Full Context configure eth-ring path eth-cfm mep alarm-notification fng-alarm-time
configure eth-tunnel path eth-cfm mep alarm-notification fng-alarm-time
configure lag eth-cfm mep alarm-notification fng-alarm-time

Description This command configures the Fault Notification Generation (FNG) alarm time.

Parameters *time* — The length of time, in centi-seconds, that must expire before a defect is alarmed.

Values 0, 250, 500, 1000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

fng-alarm-time

Syntax **fng-alarm-time** *time*

Context [Tree] (config>service>vpls>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>epipe>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vpls>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vpls>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>ies>if>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vprn>if>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>port>ethernet>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>lag>eth-cfm>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>router>if>eth-cfm>mep>alarm-notification fng-alarm-time)
[Tree] (config>service>vprn>sap>eth-cfm>mep>alarm-notification fng-alarm-time)

Full Context configure lag eth-cfm eth-cfm mep alarm-notification fng-alarm-time
configure port ethernet eth-cfm mep alarm-notification fng-alarm-time
configure router interface eth-cfm mep alarm-notification fng-alarm-time
configure service epipe sap eth-cfm mep alarm-notification fng-alarm-time
configure service epipe spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
configure service ies interface sap eth-cfm mep alarm-notification fng-alarm-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
configure service ies subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-alarm-time
configure service ipipe sap eth-cfm mep alarm-notification fng-alarm-time
configure service vpls eth-cfm mep alarm-notification fng-alarm-time
configure service vpls mesh-sdp eth-cfm mep alarm-notification fng-alarm-time
configure service vpls sap eth-cfm mep alarm-notification fng-alarm-time
configure service vpls spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
configure service vprn interface sap eth-cfm mep alarm-notification fng-alarm-time
configure service vprn interface spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
configure service vprn sap eth-cfm mep alarm-notification fng-alarm-time
configure service vprn subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-alarm-time

Description This command is used to configure the Fault Notification Generation time values for raising the alarm. This timer is used for network management processes and is not tied into delaying the notification to the fault management system on the network element. This timer does not affect fault propagation mechanisms.

Parameters *time* — Specifies the time, in centiseconds (10ms intervals), that a defect condition at or above the **low-priority-defect** must be present before raising alarm.

Values 0, 250, 500, 1000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-alarm-time
- configure service ies subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-alarm-time

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls eth-cfm mep alarm-notification fng-alarm-time
- configure service vpls mesh-sdp eth-cfm mep alarm-notification fng-alarm-time
- configure service epipe sap eth-cfm mep alarm-notification fng-alarm-time
- configure service ies interface sap eth-cfm mep alarm-notification fng-alarm-time
- configure service vpls sap eth-cfm mep alarm-notification fng-alarm-time
- configure router interface eth-cfm mep alarm-notification fng-alarm-time
- configure service ies interface spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
- configure service ipipe sap eth-cfm mep alarm-notification fng-alarm-time
- configure service vpls spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
- configure service epipe spoke-sdp eth-cfm mep alarm-notification fng-alarm-time
- configure service vprn interface sap eth-cfm mep alarm-notification fng-alarm-time
- configure port ethernet eth-cfm mep alarm-notification fng-alarm-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface spoke-sdp eth-cfm mep alarm-notification fng-alarm-time

fng-alarm-time

Syntax **fng-alarm-time** *time*

Context **[Tree]** (config>router>if>eth-cfm>mep fng-alarm-time)

Full Context configure router interface eth-cfm mep fng-alarm-time

Description This command configures the Fault Notification Generation (FNG) alarm time.

Parameters *time* — The length of time, in centi-seconds, that must pass before an alarm is raised for a defect.

Values 0, 250, 500, 1000

Default 0

10.99 fng-reset-time

fng-reset-time

Syntax **fng-reset-time** *time*

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>lag>eth-cfm>mep>alarm-notification fng-reset-time)

Full Context configure eth-ring path eth-cfm mep alarm-notification fng-reset-time
configure eth-tunnel path eth-cfm mep alarm-notification fng-reset-time
configure lag eth-cfm mep alarm-notification fng-reset-time

Description This command configure the Fault Notification Generation (FNG) reset time.

Parameters *time* — The length of time, in centiseconds, that must expire before a defect is reset.

Values 0, 250, 500, 1000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fng-reset-time

Syntax **fng-reset-time** *time*

Context **[Tree]** (config>service>vpls>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>epipe>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vpls>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vpls>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>ies>if>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vprn>if>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>port>ethernet>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>lag>eth-cfm>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>router>if>eth-cfm>mep>alarm-notification fng-reset-time)
[Tree] (config>service>vprn>sap>eth-cfm>mep>alarm-notification fng-reset-time)

Full Context configure lag eth-cfm eth-cfm mep alarm-notification fng-reset-time
configure port ethernet eth-cfm mep alarm-notification fng-reset-time
configure router interface eth-cfm mep alarm-notification fng-reset-time
configure service epipe sap eth-cfm mep alarm-notification fng-reset-time
configure service epipe spoke-sdp eth-cfm mep alarm-notification fng-reset-time
configure service ies interface sap eth-cfm mep alarm-notification fng-reset-time
configure service ies interface spoke-sdp eth-cfm mep alarm-notification fng-reset-time
configure service ies subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-reset-time
configure service ipipe sap eth-cfm mep alarm-notification fng-reset-time
configure service vpls eth-cfm mep alarm-notification fng-reset-time
configure service vpls mesh-sdp eth-cfm mep alarm-notification fng-reset-time
configure service vpls sap eth-cfm mep alarm-notification fng-reset-time
configure service vpls spoke-sdp eth-cfm mep alarm-notification fng-reset-time
configure service vprn interface sap eth-cfm mep alarm-notification fng-reset-time
configure service vprn interface spoke-sdp eth-cfm mep alarm-notification fng-reset-time
configure service vprn sap eth-cfm mep alarm-notification fng-reset-time
configure service vprn subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-reset-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Fault Notification Generation time values to reset the CCM defect alarm. This timer is used for network management processes and is not tied into delaying the notification to the fault management system on the network element. This timer does not affect fault propagation mechanisms.

Parameters *time* — Specifies the time, in centiseconds (10ms intervals), that a defect condition at or above the **low-priority-defect** must be cleared before resetting the alarm.

Values 0, 250, 500, 1000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-reset-time
- configure service ies subscriber-interface group-interface sap eth-cfm mep alarm-notification fng-reset-time

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep alarm-notification fng-reset-time
- configure service epipe sap eth-cfm mep alarm-notification fng-reset-time
- configure service ies interface sap eth-cfm mep alarm-notification fng-reset-time
- configure service vpls eth-cfm mep alarm-notification fng-reset-time
- configure service vprn interface sap eth-cfm mep alarm-notification fng-reset-time
- configure service vprn interface spoke-sdp eth-cfm mep alarm-notification fng-reset-time
- configure service vpls mesh-sdp eth-cfm mep alarm-notification fng-reset-time
- configure service ipipe sap eth-cfm mep alarm-notification fng-reset-time
- configure service epipe spoke-sdp eth-cfm mep alarm-notification fng-reset-time
- configure port ethernet eth-cfm mep alarm-notification fng-reset-time
- configure service vpls sap eth-cfm mep alarm-notification fng-reset-time
- configure router interface eth-cfm mep alarm-notification fng-reset-time
- configure service vpls spoke-sdp eth-cfm mep alarm-notification fng-reset-time

fng-reset-time

Syntax **fng-reset-time** *time*

Context **[Tree]** (config>router>if>eth-cfm>mep fng-reset-time)

Full Context configure router interface eth-cfm mep fng-reset-time

Description This command configures the FNG reset time.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *time* — The length of time, in centiseconds, that must expire before a defect is reset.

Values 0, 250, 500, 1000

Default 0

10.100 follow

follow

Syntax **follow router** *router-instance* **pool** *name*
no follow

Context **[Tree]** (config>service>vprn>nat>outside>pool>redundancy follow)
[Tree] (config>router>nat>outside>pool>redundancy follow)

Full Context configure router nat outside pool redundancy follow
configure service vprn nat outside pool redundancy follow

Description This command implicitly enables Pool Fate-Sharing Group (PFSG) which is required in case of multiple NAT policies per inside routing context. A NAT pool configured with this command will not advertise or monitor any route in order to change its (activity) state but instead it will directly follow the state of the lead pool in the PFSG. Once the lead pool changes its (activity) state, all the remaining pools following the lead pool will change their state accordingly.

Default no follow

Parameters **router** *router-instance* — Specifies the routing instance where the lead pool resides.

Values <router-name> | <service-id>
router-name - Base
service-id - 1 to 2147483647

pool *name* — Specifies the pool whose activity state is being shared up to 32 characters in length.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.101 force-auth

force-auth

Syntax **force-auth** [**cid-change**] [**rid-change**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

force-auth disabled
no force-auth

Context [Tree] (config>service>ies>sub-if>grp-if>ipoe-session force-auth)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session force-auth)

Full Context configure service ies subscriber-interface group-interface ipoe-session force-auth
configure service vprn subscriber-interface group-interface ipoe-session force-auth

Description By default, if the circuit-id/interface-id or remote-id in the IPoE session re-authentication trigger packet (such as a DHCP renewal) is not empty and different from the circuit-id/ interface-id or remote-id stored in the IPoE session data, a forced re-authentication is performed, ignoring the configured **min-auth-interval**. This default behavior can be changed with this command.

The **no** form of this command reverts to the default behavior.

Default force-auth cid-change rid-change force-auth disabled on wlan-gw group interfaces

Parameters **cid-change** — Perform a forced re-authentication upon a circuit-id/interface-id change. An empty circuit-id/interface-id is not considered a change.

rid-change — Perform a forced re-authentication upon a remote-id change. an empty remote-id is not considered a change. For DHCPv6, the enterprise number is excluded from the comparison.

disabled — Specifies that the **min-auth-interval** never is ignored. The system does not perform a forced re-authentication upon a circuit-id or interface-id or remote-id change.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.102 force-ipv6cp

force-ipv6cp

Syntax [**no**] **force-ipv6cp**

Context [Tree] (config>subscr-mgmt>loc-user-db>ppp>host force-ipv6cp)

Full Context configure subscriber-mgmt local-user-db ppp host force-ipv6cp

Description This command specifies if the IPv6 control protocol should be negotiated after PPP reaches the Network-Layer Protocol phase.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.103 force-l2pt-boundary

force-l2pt-boundary

Syntax **force-l2pt-boundary** [**cdp**] [**dtp**] [**pagp**] [**stp**] [**udld**] [**vtp**]
no force-l2pt-boundary

Context **[Tree]** (config>service>vpls>sap force-l2pt-boundary)

Full Context configure service vpls sap force-l2pt-boundary

Description Enabling force-l2pt-boundary will force all SAPs managed by the specified m-vpls instance on the corresponding port to have l2pt-termination enabled. This command is applicable only to SAPs created under m-vpls regardless of the flavor of STP currently active. It is not applicable to spoke-SDPs.

The execution of this command will fail as soon as at least one of the currently managed SAPs (all SAPs falling within the specified managed-vlan-range) does not have l2pt-termination enabled regardless of its admin/operational status.

If force-l2pt-boundary is enabled on a specified m-vpls SAP, all newly created SAPs falling into the specified managed-vlan-range will have l2pt-termination enabled per default.

Extending or adding new range into a managed-vlan-range declaration will fail as soon as there is at least one SAPs falling into the specified vlan-range does not have l2pt-termination enabled.

Disabling l2pt-termination on currently managed SAPs will fail as soon as the force-l2pt-boundary is enabled under corresponding m-vpls SAP.

Parameters **cdp** — Specifies the Cisco discovery protocol

dtp — Specifies the dynamic trunking protocol

pagp — Specifies the port aggregation protocol

stp — Specifies all spanning tree protocols: stp, rstp, mstp, pvst (default)

udld — Specifies unidirectional link detection

vtp — Specifies the virtual trunk protocol

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.104 force-mcast

force-mcast

Syntax **force-mcast** [**ip**] [**mac**]
no force-mcast

Context **[Tree]** (config>subscr-mgmt>rtr-adv-plcy force-mcast)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv force-mcast)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 force-mcast)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv force-mcast)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 force-mcast)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv force-mcast)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv force-mcast)

Full Context configure service ies subscriber-interface group-interface ipv6 force-mcast
configure service ies subscriber-interface group-interface ipv6 router-advertisements force-mcast
configure service ies subscriber-interface ipv6 router-advertisements force-mcast
configure service vprn subscriber-interface group-interface ipv6 force-mcast
configure service vprn subscriber-interface group-interface ipv6 router-advertisements force-mcast
configure service vprn subscriber-interface ipv6 router-advertisements force-mcast
configure subscriber-mgmt router-advertisement-policy force-mcast

Description This command configures the protocols with forced multicast, either IP or MAC.

The **no** form of this command returns the command to the default setting.

Parameters **ip** — Specifies that IP for multicast is forced.

mac — Specifies that MAC for multicast is forced.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.105 force-ppp-mtu-gt-1492

force-ppp-mtu-gt-1492

Syntax [**no**] **force-ppp-mtu-gt-1492**

Context **[Tree]** (config>subscr-mgmt>ppp-policy force-ppp-mtu-gt-1492)

Full Context configure subscriber-mgmt ppp-policy force-ppp-mtu-gt-1492

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables PPPoE Maximum-Receive-Unit (MRU) negotiations greater than 1492 bytes without the need to receive a “PPP-Max-Payload” tag in PADI/PADR from the client as defined in RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*.

The MRU send in the initial LCP Config Request is determined by the **port mtu** and **ppp-policy ppp-mtu** parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.106 force-qinq-vc-forwarding

force-qinq-vc-forwarding

Syntax **force-qinq-vc-forwarding** [{**c-tag-c-tag** | **s-tag-c-tag**}]
no force-qinq-vc-forwarding

Context **[Tree]** (config>service>epipe>spoke-sdp force-qinq-vc-forwarding)
[Tree] (config>service>vpls>mesh-sdp force-qinq-vc-forwarding)
[Tree] (config>service>vpls>spoke-sdp force-qinq-vc-forwarding)
[Tree] (config>service>pw-template force-qinq-vc-forwarding)
[Tree] (config>service>epipe>bgp-evpn>mpls force-qinq-vc-forwarding)

Full Context configure service epipe bgp-evpn mpls force-qinq-vc-forwarding
configure service epipe spoke-sdp force-qinq-vc-forwarding
configure service pw-template force-qinq-vc-forwarding
configure service vpls mesh-sdp force-qinq-vc-forwarding
configure service vpls spoke-sdp force-qinq-vc-forwarding

Description This command forces the data path to push two VLAN tags at network egress when sending traffic on SDP bindings or EVPN-MPLS destinations. The VLAN tag values are derived from the service-delimiting tags at the ingress, depending on the configured parameter. At network ingress this command, configured on EVPN-MPLS or the SDP-binding, pops two VLAN tags at most.

The **no** version of this command does not make the data path to push any VLAN tags in SDP bindings or EVPN-MPLS, or pop two VLAN tags.

Default no force-qinq-vc-forwarding

Parameters **c-tag-c-tag** — Pushes two tags with the same value derived from the inner service delimiting tag. At network ingress, two VLAN tags are extracted at most and the c-tag and s-tag p/de bits are propagated to the egress SAPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

s-tag-c-tag — Pushes two tags that are copied from the QinQ service-delimiting VLAN values and may be different. At network ingress, two VLAN tags are extracted at most and the p/de bits are propagated to the egress SAP service-delimiting s-tag and c-tag respectively.

Platforms All

10.107 force-qtag-forwarding

force-qtag-forwarding

Syntax [**no**] **force-qtag-forwarding**

Context **[Tree]** (config>service>vpls>pbb force-qtag-forwarding)

Full Context configure service vpls pbb force-qtag-forwarding

Description This command forces the addition of a IEEE 802.1q tag after the Customer MAC (C-MAC) addresses when the PBB header is built, as it egresses a related BVPLS.

It is used to preserve the dot1q and DE bits from the customer domain when the service delimiting qtags are stripped when the packet is ingressing a PBB Epipe or an IVPLS. The VLAN value of the service delimiting qtag if one exists is used for the corresponding inserted dot1q field. If a service delimiting qtag does not exist, then the value of zero is used for all the inserted qtag bits.

The **no** form of this command sets default behavior.

Default no force-qtag-forwarding

Platforms All

force-qtag-forwarding

Syntax [**no**] **force-qtag-forwarding**

Context **[Tree]** (config>service>epipe>pbb force-qtag-forwarding)

Full Context configure service epipe pbb force-qtag-forwarding

Description This command forces the addition of a IEEE 802.1q tag after the Customer MAC (C-MAC) addresses when the PBB header is built, as it egresses a related BVPLS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

It is used to preserve the dot1q and DE bits from the customer domain when the service delimiting qtags are stripped when the packet is ingressing a PBB Epipe or an IVPLS. The VLAN value of the service delimiting qtag if one exists is used for the corresponding inserted dot1q field. If a service delimiting qtag does not exist, then the value of zero is used for all the inserted qtag bits.

The **no** form of this command sets default behavior.

Default no force-qtag-forwarding

Platforms All

10.108 force-reference

force-reference

Syntax **force-reference** {**ref1** | **ref2** | **bits** | **bits1** | **bits2** | **bitsa** | **bitsb** | **ptp**}
no force-reference

Context **[Tree]** (debug>sync-if-timing force-reference)

Full Context debug sync-if-timing force-reference

Description This command allows an operator to force the system synchronous timing output to use a specific reference.

The **debug sync-if-timing force-reference** command should only be used to test and debug problems. Network synchronization problems may appear if network elements are left with this manual override setting. Once the system timing reference input has been forced, it may be cleared using the **no force-reference** command.

This command also clears the Wait-to-Restore state of the reference so that the reference can be selected.

The CPM clock can be forced to use a specific input reference using the force-reference command.

When the command is executed, the CPM clock on the active CPM immediately switches its input reference to that specified by the command. If the specified input is not available (shutdown), or in a disqualified state, the CPM clock shall use the next qualified input reference based on the selection rules.

This command also affects the BITS output port on the active CPM. If the BITS output port selection is set to line-reference and the reference being forced is not the BITS input port, then the system uses the forced reference to generate the signal out the BITS output port. If the BITS output port selection is set to internal-clock, then the system uses the output of the CPM clock to generate the signal for the BITS output port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

On a CPM activity switch, the force command is cleared and normal reference selection is determined.

Debug configurations are not saved between reboots.

Parameters **ref1** — Specifies that the clock will use the first timing reference.

ref2 — Specifies that the clock will use the second timing reference.

bits — Specifies that the clock will use the external network interface on the active CPM to be the highest priority input.

bitsa — Specifies that the clock will use the bitsa timing reference.

bitsb — Specifies that the clock will use the bitsb timing reference.

ptp — Specifies that the clock will use the PTP slave as the timing reference (applies to the 7450 ESS and 7750 SR).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.109 force-renews

force-renews

Syntax [**no**] **force-renews**

Context **[Tree]** (config>router>dhcp>server force-renews)
[Tree] (config>service>vprn>server force-renews)

Full Context configure router dhcp local-dhcp-server force-renews
configure service vprn server force-renews

Description This command enables the sending of sending FORCERENEW messages for DHCP.

The **no** form of this command disables the sending of FORCERENEW messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.110 force-switchover

force-switchover

Syntax **force-switchover** [**now**] [**ignore-status**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (admin>redundancy force-switchover)

Full Context admin redundancy force-switchover

Description This command forces a switchover to the standby CPM card. The primary CPM reloads its software image and becomes the secondary CPM.

Parameters **now** — Forces the switchover to the redundant CPM card immediately.

ignore-status — Forces a switchover despite any diagnostics or conditions on the standby. This is true even if the standby cannot reach the extension CPMs on the extension chassis of a 7950 XRS-40 via its local CPM interconnect ports.

This option is supported on 7950 XRS-20 and 7950 XRS-40 platforms only.

Platforms All

10.111 force-vlan-vc-forwarding

force-vlan-vc-forwarding

Syntax [**no**] **force-vlan-vc-forwarding**

Context [Tree] (config>service>epipe>bgp-evpn>mpls force-vlan-vc-forwarding)
[Tree] (config>service>vpls>bgp-evpn>srv6 force-vlan-vc-forwarding)
[Tree] (config>service>vpls>bgp-evpn>mpls force-vlan-vc-forwarding)

Full Context configure service epipe bgp-evpn mpls force-vlan-vc-forwarding
configure service vpls bgp-evpn mpls force-vlan-vc-forwarding
configure service epipe bgp-evpn segment-routing-v6 force-vlan-vc-forwarding

Description This command enables the system to preserve the VLAN ID and 802.1p bits of the service-delimiting qtag in a new tag, which is sent in the customer frame to the EVPN destinations.

If this configuration is used in conjunction with the **sap ingress vlan-translation** command, the configured translated VLAN ID is the VLAN ID sent to the EVPN destinations, instead of the service-delimiting tag VLAN ID. If the ingress SAP or SDP binding is null-encapsulated, the output VLAN ID and p-bits are zero.

The **no** form of this command does not preserve the VLAN ID and 802.1p bits of the service-delimiting qtag.

Default no force-vlan-vc-forwarding

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service epipe bgp-evpn segment-routing-v6 force-vlan-vc-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service epipe bgp-evpn mpls force-vlan-vc-forwarding
- configure service vpls bgp-evpn mpls force-vlan-vc-forwarding

force-vlan-vc-forwarding

Syntax [**no**] **force-vlan-vc-forwarding**

Context **[Tree]** (config>service>epipe>spoke-sdp force-vlan-vc-forwarding)
[Tree] (config>service>vpls>mesh-sdp force-vlan-vc-forwarding)
[Tree] (config>service>vpls>spoke-sdp force-vlan-vc-forwarding)

Full Context configure service epipe spoke-sdp force-vlan-vc-forwarding
configure service vpls mesh-sdp force-vlan-vc-forwarding
configure service vpls spoke-sdp force-vlan-vc-forwarding

Description This command forces vc-vlan-type forwarding in the datapath for spoke and mesh SDPs which have either vc-type. This command is not allowed on vlan-vc-type SDPs.

The **no** version of this command sets default behavior.

Default no force-vlan-vc-forwarding

Platforms All

10.112 foreign-ip

foreign-ip

Syntax **foreign-ip** *ip-address*[*/mask*]
no foreign-ip

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>match foreign-ip)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry match foreign-ip

Description This command configures the foreign IP address or subnet in the match criterion for this entry. The foreign IP or subnet implies a matching destination IP for upstream traffic and a source IP for downstream traffic.

The **no** form of this command removes the IP address or subnet from the match criterion in the entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address/mask* — Specifies the IPv4 address and mask.

Values ip-address a.b.c.d
mask 0 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

foreign-ip

Syntax [**no**] **foreign-ip**

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>include foreign-ip)

Full Context configure service nat syslog syslog-export-policy include foreign-ip

Description This command includes the foreign IP address in the flow log. A foreign IP address is the original IP address toward the destination node and in DNAT it is replaced by the destination IP.

If DNAT is not used, the foreign IP address (the IP address of the destination node) is the same on both sides of NAT.

The **no** form of the command disables the feature.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

foreign-ip

Syntax **foreign-ip** *ip-address*
no foreign-ip

Context **[Tree]** (config>service>nat>nat-classifier>entry>match foreign-ip)

Full Context configure service nat nat-classifier entry match foreign-ip

Description This command specifies matching on a foreign IP, that is the destination IP address of the NAT inside service before translation.

Default no foreign-ip

Parameters *ip-address* — Specifies the foreign IP address.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.113 foreign-port

foreign-port

Syntax **foreign-port** *port*
no foreign-port

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>match foreign-port)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry match foreign-port

Description This command configures the foreign TCP/UDP port to match in this entry of the VAS filter.

The **no** form of this command

Parameters *port* — Specifies the foreign IP port to match.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

foreign-port

Syntax [**no**] **foreign-port**

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>include foreign-port)

Full Context configure service nat syslog syslog-export-policy include foreign-port

Description This command includes the foreign port address in the flow log. A foreign port is the port towards the destination node and this port is not translated by any form of NAT.

A foreign port (the port towards the destination node) is the same on both sides of NAT.

The **no** form of the command disables the feature.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.114 format

format

Syntax **format** [*cflash-id*] [**reliable**]

Context **[Tree]** (file format)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context file format

Description This command formats the compact flash. The compact flash must be shut down before starting the format.

Parameters *cflash-id* — Specifies the compact flash type.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

reliable — Enables the reliance file system and disables the default DoS file system. This option is valid only on compact flashes 1 and 2.

Platforms All

10.115 forward

forward

Syntax **forward**
forward sf-ip *ip-address* | *ipv6-address* **svc** *service-id* [**esi** *esi*]
no forward

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action forward)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action forward

Description This command configures the forward action.

The **no** form of this command removes the parameters from the configuration..

Parameters *ip-address* — Specifies forwarding the SF IPv4 address for the action in a VAS filter entry.

ipv6-address — Specifies forwarding the SF IPv6 address for the action in a VAS filter entry.

service-id — Specifies the service ID.

Values 1 to 2147483647

esi — Specifies the ESI for the action in a VAS filter entry.

Values 10-byte Ethernet Segment Identifier:
00-11-22-33-44-55-66-77-88-99 with any of these separators ('-',':',' ')

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

forward

Syntax **forward**
forward bonding-connection *connection-id*
IPv4: forward esi *esi* **sf-ip** *ip-address* **vas-interface** *interface-name* **router** *router-instance*
IPv6: forward esi *esi* **sf-ip** *ipv6-address* **vas-interface** *interface-name* **router** *router-instance*
IPv4: forward esi *esi* **sf-ip** *ip-address* **vas-interface** *interface-name* **router service-name** *service-name*
IPv6: forward esi *esi* **sf-ip** *ipv6-address* **vas-interface** *interface-name* **router service-name** *service-name*
forward esi *esi* **service-id** *vpls-service-id*
forward gre-tunnel *gre-tunnel-name*
forward lsp *lsp-name*
IPv4: forward mpls-policy *ip-address*
IPv6: forward mpls-policy *ipv6-address*
IPv4: forward next-hop *ip-address*
IPv6: forward next-hop *ipv6-address*
IPv4: forward next-hop *ip-address* **router** *router-instance*
IPv6: forward next-hop *ipv6-address* **router** *router-instance*
IPv4: forward next-hop *ip-address* **router service-name** *service-name*
IPv6: forward next-hop *ipv6-address* **router service-name** *service-name*
IPv4: forward next-hop indirect *ip-address*
IPv6: forward next-hop indirect *ipv6-address*
IPv4: forward next-hop indirect *ip-address* **router** *router-instance*
IPv6: forward next-hop indirect *ipv6-address* **router** *router-instance*
IPv4: forward next-hop indirect *ip-address* **router service-name** *service-name*
IPv6: forward next-hop indirect *ipv6-address* **router service-name** *service-name*
forward next-hop interface *ip-int-name*
forward redirect-policy *policy-name*
forward router *router-instance*
forward router service-name *service-name*
forward sap *sap-id*
forward sdp *sdp-id:vc-id*
IPv4: forward srte-policy *ip-address* **color** *color-id*
IPv6: forward srte-policy *ipv6-address* **color** *color-id*
IPv4: forward vprn-target bgp-nh *ip-address* **router** *router-instance* [**adv-prefix** *ip-address/mask*] [**lsp** *lsp-name*]
IPv6: forward vprn-target bgp-nh *ip-address* **router** *router-instance* [**adv-prefix** *ipv6-address/prefix-length*] [**lsp** *lsp-name*]
IPv4: forward vprn-target bgp-nh *ip-address* **router service-name** *service-name* [**adv-prefix** *ip-address/mask*] [**lsp** *lsp-name*]
IPv6: forward vprn-target bgp-nh *ip-address* **router service-name** *service-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[**adv-prefix** *ipv6-address/prefix-length*] [**lsp** *lsp-name*]

Context [Tree] (config>filter>ip-filter>entry>action forward)
[Tree] (config>filter>ipv6-filter>entry>action forward)

Full Context configure filter ip-filter entry action forward
configure filter ipv6-filter entry action forward

Description This command sets the context for specific forward commands to be performed.

Parameters *connection-id* — Specifies that the packet should be forwarded over the specified connection (specified by the connection ID under the bonding group interface), if that connect is available. Outside of a bonding egress context, the behavior of this filter is undefined.

Values 1, 2

esi service-id — Specifies that the packet matching the entry is forwarded to an ESI-identified first appliance in Nuage service chain using EVPN-resolved VXLAN tunnel in the specified VPLS service.

esi sf-ip vas-interface router — Specifies that the packet matching the entry is forwarded to ESI/SF-IP identified first appliance in Nuage service chain using EVPN-resolved VXLAN tunnel over the configured VAS interface in the specified VPRN service.

gre-tunnel-name — Specifies the GRE tunnel name up to 32 characters.

lsp — Specifies that the packet matching the entry is forwarded using the specified lsp.

mpls-policy — Specifies the redirection of the traffic to the programed instance of the MPLS FP specified by its endpoint IPv4 or IPv6 address. The behavior results in a simple forward if no policy exists, if no instance is programmed, and if the policy or instance is administratively down.

next-hop — Specifies that the packet matching the entry is forwarded in the routing context of the incoming interface using direct or indirect IPv4 address in the routing lookup.

next-hop router — Specifies that the packet matching the entry is forwarded in the configured routing context using direct or indirect IPv4 address in the routing lookup.

next-hop interface — Specifies that the packet matching the entry is forwarded using the configured local interface.

redirect-policy — Specifies that the packet matching the entry is forwarded using forward next-hop or forward next hop router and the IP address of destination selected by the configured redirect policy. If no destination is selected, packets are subject to action forward.

router — Specifies that the packet matching the entry is routed in the configured routing instance and not in the incoming interface routing instance.

sap — Specifies that the packet matching the entry is forwarded using the configured SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sdp — Specifies that the packet matching the entry is forwarded using the configured SDP.

srte-policy — Specifies the redirection of the traffic to the programed instance of the SR-TE policy specified by its endpoint IPv4 address or IPv6 address and color. The behavior results in a simple forward if no policy exists, if no instance is programmed, and if the policy or instance is administratively down.

color-id — Specifies the color identifier of the specified SR-TE policy.

Values 0 to 4294967295

vprn-target — Specifies that the packet matching the entry is redirected towards a designated BGP next-hop (**bgp-nh**). The user may specify an LSP (**lsp** *lsp-name*) to use towards that next-hop. If no LSP is specified, the system will automatically select one. The user must specify the routing context (**router** {*router-instance* | **service-name** *service-name*}) in which the system will perform the lookups in order to derive the proper VPRN service label. The user may specify an advertised prefix route (**adv-prefix** *ip-address/prefix-length*). This is needed in case label per VRF is not the label allocation method configured at the BGP peer.

esi — Specifies a 10-byte Ethernet Segment Identifier.

ip-address/mask — Specifies an IPv4 advertised route in the CIDR notation. The IPv4 address is in dotted decimal notation.

Values ip-address a.b.c.d (host bits must be 0)
mask: 0 to 32

ipv6-address/prefix-length — Specifies an IPv6 advertised route in the CIDR notation.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d, where “x” is [0..FFFF]H, and “d” is [0..255]

prefix-length: 0 to 128

bgp-nh *ip-address* — Specifies the IPv4 address (in dotted decimal notation) of the target BGP next-hop.

Values ip-address d.d.d.d

ip-address — Specifies the IPv4 address of a direct or indirect next hop to which to forward matching packets.

ipv6-address — Specifies the IPv6 address of a direct or indirect next hop to which to forward matching packets.

ip-int-name — Specifies the name of an egress IP interface where matching packets will be forwarded from. This parameter is only valid for unnumbered point-to-point interfaces. If the string contains special characters (such as #, $, spaces), the entire string must be enclosed within double quotes.

interface-name — Specifies the (maximum 32-character) name of an egress R-VPLS IP interface used to forward the packets using ESI redirect for VPRN/IES service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsp-name — Specifies an existing RSVP-TE, MPLS-TP, or SR-TE LSP that supports LSP redirect.

policy-name — Specifies an IPv4 redirect policy configured in the config>filter>redirect-policy context.

sap-id — Specifies an existing VPLS Ethernet SAP.

sdp-id:vc-id — Specifies an existing VPLS SDP.

router-instance — Specifies “Base” or an existing VPRN service ID. For the **forward vprn-target bgp-nh** command, *router-instance* must specify an existing VPRN service ID.

service-name — Specifies an existing VPRN service name.

vpls-service-id — Specifies an existing VPLS service ID or service name.

Platforms All

forward

Syntax **forward**
forward esi *esi* **service-id** *vpls-service-id*
forward sap *sap-id*
forward sdp *sdp-id:vc-id*

Context **[Tree]** (config>filter>mac-filter>entry>action forward)

Full Context configure filter mac-filter entry action forward

Description This command sets the context for specific forward commands to be performed.

Parameters *esi* — Specifies a 10-byte Ethernet Segment Identifier.

service-id — Specifies that a packet matching the entry is forwarded to an ESI-identified first appliance in the Nuage service chain using an EVPN-resolved VXLAN tunnel in the specified VPLS service.

vpls-service-id — Specifies an existing VPLS service ID or service name.

sap — Specifies that the packet matching the entry is forwarded using the configured SAP.

sap-id — Specifies an existing VPLS Ethernet SAP.

sdp — Specifies that the packet matching the entry is forwarded using the configured SDP.

sdp-id:vc-id — Specifies an existing VPLS SDP.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.116 forward-6in4

forward-6in4

Syntax [**no**] **forward-6in4**

Context **[Tree]** (config>system>ip forward-6in4)

Full Context configure system ip forward-6in4

Description This command enables forwarding of IPv6 traffic encapsulated in an IPv4 transport sent to the system IP address.

The **no** form of this command disables this option and returns the system to the default behavior.

Default no forward-6in4

Platforms All

10.117 forward-delay

forward-delay

Syntax **forward-delay** *forward-delay*
no forward-delay [*forward-delay*]

Context **[Tree]** (config>service>vpls>stp forward-delay)
[Tree] (config>service>template>vpls-template>stp forward-delay)

Full Context configure service template vpls-template stp forward-delay
configure service vpls stp forward-delay

Description RSTP, as defined in the IEEE 802.1D-2004 standards, will normally transition to the forwarding state via a handshaking mechanism (rapid transition), without any waiting times. If handshaking fails (e.g. on shared links, see below), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two nodes (for example, a shared 10/100BaseT segment). The port-type command is used to configure a link as point-to-point or shared.

For timer-based transitions, the 802.1D-2004 standard defines an internal variable forward-delay, which is used in calculating the default number of seconds that a SAP or spoke-SDP spends in the discarding and learning states when transitioning to the forwarding state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The value of the forward-delay variable depends on the STP operating mode of the VPLS instance:

- in rstp or mstp mode, but only when the SAP or spoke-SDP has not fallen back to legacy STP operation, the value configured by the hello-time command is used;
- in all other situations, the value configured by the forward-delay command is used.

Default forward-delay 15

Parameters *seconds* — The forward delay timer for the STP instance in seconds

Values 4 to 30

Platforms All

10.118 forward-entries

forward-entries

Syntax **forward-entries**

Context **[Tree]** (config>subscr-mgmt>http-rdr-plcy forward-entries)

Full Context configure subscriber-mgmt http-redirect-policy forward-entries

Description Enters the context to configure entries that need to be forwarded.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.119 forward-ip-over-gre

forward-ip-over-gre

Syntax [**no**] **forward-ip-over-gre**

Context **[Tree]** (config>system>ip forward-ip-over-gre)

Full Context configure system ip forward-ip-over-gre

Description This command enables forwarding of IP traffic encapsulated in a GRE over IPv4 transport sent to the system IP address.

The **no** form of this command disables this option and returns the system to the default behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no forward-ip-over-gre

Platforms All

10.120 forward-ipv4-multicast-to-ip-int

forward-ipv4-multicast-to-ip-int

Syntax [**no**] **forward-ipv4-multicast-to-ip-int**

Context **[Tree]** (config>service>vpls>allow-ip-int-bind forward-ipv4-multicast-to-ip-int)

Full Context configure service vpls allow-ip-int-bind forward-ipv4-multicast-to-ip-int

Description This command enables support for forwarding IPv4 multicast traffic from sources connected to the VPLS service of a routed VPLS to the IP interface of the routed VPLS service. It can only be enabled after the routed VPLS service has been bound to an IP interface.

Default no forward-ipv4-multicast-to-ip-int

Platforms All

10.121 forward-ipv4-packets

forward-ipv4-packets

Syntax [**no**] **forward-ipv4-packets**

Context **[Tree]** (config>service>vprn>if>ipv6 forward-ipv4-packets)

Full Context configure service vprn interface ipv6 forward-ipv4-packets

Description This command allows an IPv6-only interface (with no configured IPv4 addresses) to be used for forwarding transit and locally originating and terminating IPv4 packets.

The interface will report that its IPv4 oper-state is up if its IPv6 oper-state is up. Be aware that not all protocols will observe the interface as up from an IPv4 perspective. This command is mostly intended to support BGP routing use cases. Refer to RFC 5549, Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop, for further information.

The **no** form of this command restores the default behavior and prevents the interface from forwarding IPv4 packets if it has no configured IPv4 subnets.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

forward-ipv4-packets

Syntax [**no**] **forward-ipv4-packets**

Context **[Tree]** (config>router>if>ipv6 forward-ipv4-packets)

Full Context configure router interface ipv6 forward-ipv4-packets

Description This command allows an IPv6-only interface (with no configured IPv4 addresses) to be used for forwarding transit and locally originating and terminating IPv4 packets.

The interface reports that its IPv4 operational state is up if its IPv6 operational state is up. Be aware that not all protocols observe the interface as up from an IPv4 perspective. This command is mostly intended to support BGP routing use cases. Refer to RFC 5549, Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop, for further information.

The **no** form of this command restores the default behavior and prevents the interface from forwarding IPv4 packets if it has no configured IPv4 subnets.

Default no forward-ipv4-packets

Platforms All

10.122 forward-ipv6-multicast-to-ip-int

forward-ipv6-multicast-to-ip-int

Syntax [**no**] **forward-ipv6-multicast-to-ip-int**

Context **[Tree]** (config>service>vpls>allow-ip-int-bind forward-ipv6-multicast-to-ip-int)

Full Context configure service vpls allow-ip-int-bind forward-ipv6-multicast-to-ip-int

Description This command enables support for forwarding IPv6 multicast traffic from sources connected to the VPLS service of a routed VPLS to the IP interface of the routed VPLS service. It can only be enabled after the routed VPLS service has been bound to an IP interface.

Default no forward-ipv6-multicast-to-ip-int

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.123 forward-path

forward-path

Syntax [**no**] **forward-path**

Context **[Tree]** (config>router>mpls>mpls-tp>transit-path forward-path)

Full Context configure router mpls mpls-tp transit-path forward-path

Description This command enables the forward path of an MPLS-TP transit path to be created or edited.

The forward path must be created before the reverse path.

The **no** form of this command removes the forward path. The forward path cannot be removed if a reverse exists.

Default no forward-path

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.124 forward-when

forward-when

Syntax **forward-when pattern expression** *expression* **mask** *mask* **offset-type** *offset-type* **offset-value** *offset-value*

Context **[Tree]** (config>filter>ip-filter>entry>action forward-when)
[Tree] (config>filter>ipv6-filter>entry>action forward-when)

Full Context configure filter ip-filter entry action forward-when
configure filter ipv6-filter entry action forward-when

Description This command configures the forward-when action for the traffic that matches this filter entry.

Parameters **pattern** — Specifies the traffic that can be forwarded based on a pattern found in the packet header or data payload.

expression — Specifies the hexadecimal pattern to match, up to eight bytes.

Values 0x0000000000000000 to 0xffffffffffffffff

mask — Specifies the mask for the pattern expression, up to eight bytes.

Values 0x0000000000000000 to 0xffffffffffffffff

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

offset-type — Specifies the starting point reference for the offset-value of this pattern.

Values layer-3, layer-4, data, dns-qtype

offset-value — Specifies the offset value for the pattern expression.

Values 0 to 255

Platforms All

10.125 forwarding

forwarding

Syntax **forwarding** *limit*
no forwarding

Context **[Tree]** (config>service>nat>nat-policy>port-limits forwarding)
[Tree] (config>service>nat>firewall-policy>port-limits forwarding)

Full Context configure service nat firewall-policy port-limits forwarding
configure service nat nat-policy port-limits forwarding

Description This command configures the maximum number of port forwarding entries.

Default no forwarding

Parameters *limit* — Specifies the maximum number of port forwarding entries per subscriber.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy port-limits forwarding

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy port-limits forwarding

forwarding

Syntax **forwarding** {**next-hop** *ip-address* | **interface** *interface-name* | **bypass-routing**}
no forwarding

Context **[Tree]** (config>oam-pm>session>ip forwarding)

Full Context configure oam-pm session ip forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command influences the forwarding decision of the TWAMP Light packet. When this command is used, only one of the forwarding options can be enabled at any time.

The **no** form of this command removes the options and enables the default forwarding logic.

Parameters *ip-address* — Specifies the IP address of the next hop on the path.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

interface-name — Specifies the name, up to 32 characters, to refer to the interface from which the packet is sent. The name must already exist in the **config>router>interface** context or within the appropriate **config>service** context.

bypass-routing — Specifies to send the packet to a host on a directly attached network, bypassing the routing table.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.126 forwarding-bits-set

forwarding-bits-set

Syntax **forwarding-bits-set** {**all** | **non-fwd**}
no forwarding-bits-set

Context **[Tree]** (config>service>vprn>bgp>graceful-restart>long-lived forwarding-bits-set)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived forwarding-bits-set)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived forwarding-bits-set)

Full Context configure service vprn bgp graceful-restart long-lived forwarding-bits-set
configure service vprn bgp group graceful-restart long-lived forwarding-bits-set
configure service vprn bgp group neighbor graceful-restart long-lived forwarding-bits-set

Description This command determines the setting of the F bits in the GR and LLGR capabilities advertised by the router. When the F bit is set for an AFI/SAFI, it indicates that the advertising router was able to preserve forwarding state for the routes of that AFI/SAFI across the last restart. If a router restarts and does not set F=1, then when the session with a peer is re-established, the peer immediately deletes all LLGR stale routes it was preserving on behalf of the restarting router for the corresponding AFI/SAFI.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command allows the F bits for all advertised AFI/SAFI to be set to 1, or only the F bits for non-forwarding AFI/SAFI to be set to 1. Non-forwarding AFI/SAFI are the following configuration-related address families: L2-VPN, route-target, flow-IPv4, and flow-IPv6.

Default no forwarding-bits-set

Parameters **all** — Specifies that the F bit for all AFI/SAFI should be set to 1.

non-fwd — Specifies that the F bit for only non-forwarding AFI/SAFI should be set to 1. These AFI/SAFI correspond to the following families: L2-VPN, route-target, flow-IPv4, and flow-IPv6.

Platforms All

forwarding-bits-set

Syntax **forwarding-bits-set** {**all** | **non-fwd**}
no forwarding-bits-set

Context **[Tree]** (config>router>bgp>graceful-restart>long-lived forwarding-bits-set)
[Tree] (config>router>bgp>group>graceful-restart>long-lived forwarding-bits-set)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived forwarding-bits-set)

Full Context configure router bgp graceful-restart long-lived forwarding-bits-set
configure router bgp group graceful-restart long-lived forwarding-bits-set
configure router bgp group neighbor graceful-restart long-lived forwarding-bits-set

Description This command determines the setting of the F bits in the GR and LLGR capabilities advertised by the router. When the F bit is set for an AFI/SAFI, it indicates that the advertising router was able to preserve forwarding state for the routes of that AFI/SAFI across the last restart. If a router restarts and does not set F=1, then when the session with a peer re-establishes the peer immediately deletes all LLGR stale routes it was preserving on behalf of the restarting router for the corresponding AFI/SAFI.

This command allows the F bits for all advertised AFI/SAFI to be set to 1, or only the F bits for non-forwarding AFI/SAFI to be set to 1. Non-forwarding AFI/SAFI are the following configuration-related address families: L2-VPN, route-target, flow-IPv4, and flow-IPv6.

Default no forwarding-bits-set

Parameters **all** — Specifies that the F bit for all AFI/SAFI should be set to 1.

non-fwd — Specifies that the F bit for only non-forwarding AFI/SAFI should be set to 1. These AFI/SAFI correspond to the following families: L2-VPN, route-target, flow-IPv4, and flow-IPv6.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.127 forwarding-class

forwarding-class

Syntax **forwarding-class** {*be* | *l2* | *af* | *l1* | *h2* | *ef* | *h1* | *nc*}
no forwarding-class [{*be* | *l2* | *af* | *l1* | *h2* | *ef* | *h1* | *nc*}]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect forwarding-class)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel forwarding-class)
[Tree] (config>service>vprn>static-route-entry>next-hop forwarding-class)

Full Context configure service vprn static-route-entry indirect forwarding-class
configure service vprn static-route-entry ipsec-tunnel forwarding-class
configure service vprn static-route-entry next-hop forwarding-class

Description This command specifies the enqueuing forwarding class that should be associated with traffic matching the associate static route. If this parameter is not specified, the packet will use the forwarding-class association based on default classification or other QoS Policy associations.

Default no forwarding-class

Parameters *Forwarding class* — The forwarding class must be one of the pre-defined system forwarding classes.

Values be, l2, af, l1, h2, ef, h1, nc

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

forwarding-class

Syntax **forwarding-class** {**be** | **l2** | **af** | **l1** | **h2** | **ef** | **h1** | **nc**}
no forwarding-class [{**be** | **l2** | **af** | **l1** | **h2** | **ef** | **h1** | **nc**}]

Context **[Tree]** (config>router>static-route-entry>indirect forwarding-class)
[Tree] (config>router>static-route-entry>next-hop forwarding-class)

Full Context configure router static-route-entry indirect forwarding-class
configure router static-route-entry next-hop forwarding-class

Description This command specifies the enqueuing forwarding class that should be associated with traffic matching the associate static route. If this parameter is not specified, the packet will use the forwarding-class association based on default classification or other QoS Policy associations.

Default no forwarding-class

Parameters **be | l2 | af | l1 | h2 | ef | h1 | nc** — Specifies the forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

forwarding-class

Syntax [**no**] **forwarding-class**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr forwarding-class)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr forwarding-class)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters forwarding-class
configure log accounting-policy custom-record aa-specific to-aa-sub-counters forwarding-class

Description This command enables the collection of a Forwarding Class bitmap information added to the XML aa-sub and router level accounting records, and only applies to the 7750 SR.

Default no forwarding-class

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.128 forwarding-policies

forwarding-policies

Syntax [**no**] **forwarding-policies**

Context **[Tree]** (config>router>mpls forwarding-policies)

Full Context configure router mpls forwarding-policies

Description Commands in this context configure an MPLS forwarding policy.

The **no** form of this command deletes all policies from the forwarding policy database.

Platforms All

10.129 forwarding-policy

forwarding-policy

Syntax [**no**] **forwarding-policy** *name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>mpls>fwd-policies forwarding-policy)

Full Context configure router mpls forwarding-policies forwarding-policy

Description This command creates an MPLS forwarding policy.

There are two types of MPLS forwarding policy:

- endpoint policy
- label-binding policy

The endpoint policy allows the user to forward unlabeled packets over a set of user-defined direct (with option to push a label stack) or indirect next hops. Routes are bound to an endpoint policy when their next hop matches the endpoint address of the policy.

The label-binding policy provides the same capability for labeled packets. In this case, labeled packets matching the ILM of the policy binding label are forwarded over the set of next hops of the policy.

The data model of a forwarding policy represents each pair of {primary next hop, backup next hop} as a group and models the ECMP set as the set of Next-Hop Groups (NHGs). Flows of prefixes can be switched on a per-NHG basis from the primary next hop, when it fails, to the backup next hop without disturbing the flows forwarded over the other NHGs of the policy. The same can be performed when reverting back from a backup next hop to the restored primary next hop of the same NHG.

The MPLS forwarding policy supports two types of NHGs on a per policy basis:

- An NHG of resolution type indirect supported with the label-binding policy and in which forwarding over the primary/backup next hop is modeled as a swap operation from the binding label to an implicit-null label over multiple outgoing interfaces (multiple NHLFEs) corresponding to the resolved next hops of the indirect route.

  Within a given NHG, the primary next hop is the preferred active path in the absence of any failure of the NHG of resolution type indirect.

  The forwarding database tracks the primary or backup next hop in the routing table. A **route delete** of the primary indirect next hop causes CPM to program the backup indirect next hop in the data path.

  A **route modify** to the indirect primary or backup next hop causes CPM to update the its resolved next hops and to update the data path if it is the active indirect next hop.

  When the primary indirect next hop is restored and is added back into the routing table, CPM waits for an amount of time equal to the user-programmed revert timer before updating the data path. However, if the backup indirect next hop fails while the timer is running, CPM updates the data path immediately.
- An NHG of resolution type direct is modeled as follows:
  - For a label-binding policy, forwarding over the primary or backup next hop is modeled as a swap operation from the binding label to the configured label stack or to an implicit-null label (if the **pushed-labels** command not configured) over a single outgoing interface to the next hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- For an endpoint policy, forwarding over the primary or backup next hop is modeled as a push operation from the binding label to the configured label stack or to an implicit-null label (if the **pushed-labels** command not configured) over a single outgoing interface to the next hop.
- The labels configured by the **pushed-labels** command are not validated.

Within a given NHG, the primary next hop is the preferred active path in the absence of any failure of the NHG of resolution type direct.

The NHG supports uniform failover. The forwarding policy database assigns a Protect-Group ID (PG-ID) to each of the primary next hop and the backup next hop and programs both of them in data path. A failure of the active path switches traffic to the other path following the uniform failover procedures.

The forwarding database tracks the primary or backup next hop in the routing table. A **route delete** of the primary/backup direct next hop causes CPM to send the corresponding PG-ID switch to the data path.

A **route modify** to the direct primary or backup next hop causes CPM to update the MPLS forwarding database and to update the data path since both next hops are programmed.

When the primary direct next hop is restored and is added back into the routing table, CPM waits for an amount of time equal to the user programmed revert timer before activating it and updating the data path. However, if the backup direct next hop fails while the timer is running, CPM activates it and updates the data path immediately. The latter failover to the restored primary next hop is performed using the uniform failover procedure.

The forwarding policy database activates the best endpoint policy among the named policies sharing the same value of the endpoint parameter by selecting the lowest preference value policy. This policy is then programmed into the TTM and into the tunnel table in data path. If this policy goes down, then the forwarding policy database performs a re-evaluation and activates the named policy with the next lowest preference value for the same endpoint value. If a more preferred policy comes back up, the forwarding policy database reverts to it and activates it.

The forwarding policy database similarly activates the best label-binding policy among the named policies sharing the same binding label by selecting the lowest preference value policy. This policy is then programmed into the label FIB table in data path. If this policy goes down, then the forwarding policy database performs a re-evaluation and activates the names policy with the next lowest preference value for the same binding label value. If a more preferred policy comes back up, the forwarding policy database reverts to it and activates it.

Ingress statistics can be enabled as is associated with binding label, that is the ILM of the forwarding policy, and provides aggregate packet and byte counters for packets matching the binding label.

The **no** form of the command deletes the named MPLS forwarding policy.

Parameters *name* — Specifies the name of the MPLS forwarding policy, up to 64 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.130 forwarding-set

forwarding-set

Syntax **forwarding-set policy** *policy-name* **set** *set-id*
no forwarding-set

Context **[Tree]**
(config>router>mpls>lsp>class-forwarding>config>router>mpls>lsp-template>class-forwarding forwarding-set)

Full Context configure router mpls lsp class-forwarding config router mpls lsp-template class-forwarding forwarding-set

Description This command configures the mapping of a class-forwarding policy and forwarding set ID to an LSP (RSVP-TE or SR-TE) or an LSP template.

An MPLS LSP can only map to one single class forwarding policy and forwarding set. Multiple LSPs can map to the same policy and set. If the LSPs form part of an ECMP set of next-hops for an IPv4 or IPv6 prefix resolved to IGP shortcuts, the prefix packets with a matching FC are mapped to this set and are sprayed over these LSPs. This behavior is based on a modulo operation of the output of the hash routine on the packet's headers and the number of LSPs in the set.

Parameters *policy-name* — Specifies the name of the class forwarding policy, to a maximum of 32 characters.

set-id — Specifies the class forwarding set.

Values 1 to 4 (in system profile None/A)
1 to 6 (in system profile B)

10.131 forwarding-tree-topology

forwarding-tree-topology

Syntax **forwarding-tree-topology unicast** [**st** | **spf**]

Context **[Tree]** (config>service>vpls>spb>level forwarding-tree-topology)

Full Context configure service vpls spb level forwarding-tree-topology

Description This command sets the unicast forwarding to follow the shortest path tree defined by the ECT algorithm shortest path forwarding (spf) or to follow a single tree. (st). Shortest path trees make use of more link resources.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Multicast traffic is defaulted to follow the single tree topology. A single tree unicast would make Multicast and unicast follow the same path.

Default forwarding-tree-topology unicast spf

Parameters **spf** — Follows the shortest path tree.

st — Follows a single tree.

Platforms All

10.132 fp

fp

Syntax **fp** [*fp-number*]

Context **[Tree]** (config>card fp)

Full Context configure card fp

Description This command enables access to the configuration of the forwarding planes on a card.

The default forwarding plane is 1. When entering the FP node, if the forwarding plane number is omitted, the system will assume forwarding plane number 1.

Commands can only be configured under **card>fp** if the hardware that the FP resides on (either a card or an XMA) is provisioned. Conversely, all commands under **card>fp** of the corresponding FPs are automatically removed when that hardware is unprovisioned.

Parameters *fp-number* — Specifies that the FP number parameter is optional following the **fp** command.

Values 1 to 8

Default fp 1

Platforms All

10.133 fp-redirect-group

fp-redirect-group

Syntax **fp-redirect-group** *policer-type policer-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no fp-redirect-group *policer-type*

Context [Tree] (config>qos>network>ingress>fc fp-redirect-group)

Full Context configure qos network ingress fc fp-redirect-group

Description This command is used to redirect the FC of a broadcast packet received in a VPLS service over a PW or network IP interface to an ingress forwarding plane queue-group.

It defines the mapping of an FC to a policer-id and redirects the lookup of the policer of the same ID in some ingress forwarding plane queue-group instance. However, the queue-group name and instance are explicitly provided only at the time the network QoS policy is applied to the ingress context of a spoke or mesh SDP or a network IP interface.

The broadcast-policer statement is ignored when the network QoS policy is applied to any object other than a VPLS spoke or mesh SDP or a network IP interface.

The **no** form of this command removes the redirection of the FC.

Parameters *policer-type* — The policer type to be used. The *policer-type* is ignored when the network QoS policy is applied to any object other than a VPLS spoke or mesh SDP or a network IP interface.

Values broadcast-policer | mcast-policer | policer | unknown-policer

policer-id — The specified *policer-id* must exist within the queue-group template applied to the ingress context of the forwarding plane.

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

10.134 fp-resource-policy

fp-resource-policy

Syntax **fp-resource-policy** *name*
no fp-resource-policy

Context [Tree] (config>card>fp fp-resource-policy)

Full Context configure card fp fp-resource-policy

Description This command configures the FP resource policy for the specified FP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the allocation configured within the FP resources policy is not achievable with the current ingress or egress queue consumption, the command fails. The configuration within the newly applied FP resource policy takes effect on the FP on which the FP resources policy is applied, and that includes removing an applied user created FP resource policy to return to the default policy, and causes the router to immediately reset the associated cards, XIOMs, and MDAs, except on the 7750 SR-1 where the configuration must be saved, and the router rebooted, immediately after committing the configuration transaction.

The **no** form of this command reverts to the default value by applying the default **fp-resource-policy** to the FP.

Default no fp-resource-policy

Parameters *name* — Specifies the FP resource policy name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

fp-resource-policy

Syntax **fp-resource-policy** *policy-name* [**create**]
no fp-resource-policy *policy-name*

Context **[Tree]** (config>qos fp-resource-policy)

Full Context configure qos fp-resource-policy

Description This command configures an FP resource policy that is used to manage resources on an FP4 forwarding plane.

A default policy is created by the system and applied to all FP4 FPs by default. If an FP resource policy is removed from an FP, the system automatically applies the default policy to that FP. The system prevents the modification or deletion of the default policy, and the deletion of any user created policy that is applied to an FP. The system supports a maximum of 15 FP resource policies.

The **no** form of this command deletes the FP resources policy from the system.

Parameters *policy-name* — Specifies the FP resource policy, up to 64 characters.

create — Creates the FP resource policy entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.135 fpe

fpe

Syntax **fpe** *fpe-id*
no fpe

Context **[Tree]** (config>service>vprn>sub-if>grp-if>bonding-parameters fpe)
[Tree] (config>service>ies>sub-if>grp-if>bonding-parameters fpe)

Full Context configure service ies subscriber-interface group-interface bonding-parameters fpe
configure service vprn subscriber-interface group-interface bonding-parameters fpe

Description This command specifies which FPE is used to provision bonding functionality. The FPE cannot be changed when there are active bonded subscribers.

The **no** form of this command disables the FPE for bonding functionality under this group interface.

fpe

Syntax **fpe** *fpe-id*
no fpe

Context **[Tree]** (config>service>vprn>sub-if>grp-if>gtp-parameters fpe)
[Tree] (config>service>ies>sub-if>grp-if>gtp-parameters fpe)

Full Context configure service ies subscriber-interface group-interface gtp-parameters fpe
configure service vprn subscriber-interface group-interface gtp-parameters fpe

Description This command configures the FPE to be used by a group interface for extended ESM functionality such as GTP termination or bonding.

The FPE must be configured in mode sub-mgmt-extension and must be provisioned before the extended functionality becomes active.

The **no** form of this command disables the FPE for GTP functionality under this group interface.

fpe

Syntax **fpe** *fpe-id* [**create**]
no fpe *fpe-id*

Context **[Tree]** (config>fwd-path-ext fpe)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure fwd-path-ext fpe

Description This command configures an FPE object which associates the application with a PXC (paired set of PXC sub-ports or a paired set of PXC based LAGs).

The **no** form of this command disables the FPE object association.

Parameters *fpe-id* — Specifies the FPE ID.

Values 1 to 64

create — Keyword used to associate the queue group. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

10.136 fpipe

fpipe

Syntax **fpipe** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**vc-type** *fr-dlci*] [**vc-switching**] [**name** *name*]
no fpipe *service-id*

Context **[Tree]** (config>service fpipe)

Full Context configure service fpipe

Description This command configures an Fpipe service. An Fpipe provides a point-to-point L2 VPN connection to a remote SAP or to another local SAP. An Fpipe connects only Frame Relay endpoints either locally or over a PSN to a remote endpoint of the same type.

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7750 SR on which this service is defined.

Values *service-id*: 1 to 2147483647
svc-name: up to 64 characters

customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

Values 1 to 2147483647

Default null (0)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vc-type — Specifies a 15 bit value that defines the type of the VC signaled to the peer. Its values are defined in *draft-ietf-pwe3-iana-allocation* and it defines both the signaled VC type as well as the resulting data path encapsulation over the Apipe.

Values fr-dlci

vc-switching — Specifies if the pseudowire switching signaling is used for the spoke SDPs configured in this service.

name *name* — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Values *name*: up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.137 fqdn

fqdn

Syntax **fqdn** *fully-qualified-domain-name*
no fqdn

Context **[Tree]** (config>app-assure>group>url-filter>web-service fqdn)

Full Context configure application-assurance group url-filter web-service fqdn

Description This command configures the host name of the web-service.

The **no** form of this command removes the host name configuration.

Default no fqdn

Parameters *fully-qualified-domain-name* — Specifies the host name of the web service, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.138 frag-required

frag-required

Syntax [**no**] **frag-required**

Context **[Tree]** (config>ipsec>tnl-temp>icmp-generation frag-required)
[Tree] (config>router>if>ipsec>ipsec-tunnel>icmp-generation frag-required)
[Tree] (config>router>if>ipsec>ipsec-tunnel>icmp-generation frag-required)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>icmp-generation frag-required)
[Tree] (config>service>ies>if>sap>ip-tunnel>icmp-generation frag-required)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>icmp-generation frag-required)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel>icmp-generation frag-required)
[Tree] (config>service>vprn>if>sap>ip-tunnel>icmp-generation frag-required)

Full Context configure ipsec tunnel-template icmp-generation frag-required
configure router interface ipsec ipsec-tunnel icmp-generation frag-required
configure service ies interface ipsec ipsec-tunnel icmp-generation frag-required
configure service ies interface sap ip-tunnel icmp-generation frag-required
configure service vprn interface ipsec ipsec-tunnel icmp-generation frag-required
configure service vprn interface sap ip-tunnel icmp-generation frag-required
configure service vprn interface sap ipsec-tunnel icmp-generation frag-required

Description Commands in this context configure ICMP Fragmentation Required parameters.

The **no** form of this command disables sending the ICMP messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel icmp-generation frag-required
- configure service vprn interface sap ip-tunnel icmp-generation frag-required
- configure service ies interface sap ip-tunnel icmp-generation frag-required
- configure ipsec tunnel-template icmp-generation frag-required

VSR

- configure service ies interface ipsec ipsec-tunnel icmp-generation frag-required
- configure service vprn interface ipsec ipsec-tunnel icmp-generation frag-required
- configure router interface ipsec ipsec-tunnel icmp-generation frag-required

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.139 fragment

fragment

Syntax **fragment** {**true** | **false**}

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match fragment)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match fragment)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match fragment
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match fragment

Description This command configures the fragmentation match condition.

The **no** form of this command reverts to the default.

Parameters **true** — Enables fragmentation matching.

false — Disables fragmentation matching.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

fragment

Syntax **fragment** {**true** | **false**}
no fragment

Context **[Tree]** (config>li>li-filter>li-ip-filter>entry>match fragment)

Full Context configure li li-filter li-ip-filter entry match fragment

Description This command specifies match criterion for fragmented packets.

The **no** form of this command removes the match criterion.

Default no fragment

Parameters **true** — Specifies to match on all fragmented IP packets.

false — Specifies to match on all non-fragmented IP packets.

Platforms All

fragment

Syntax **fragment** {**true** | **false**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no fragment

Context [Tree] (config>qos>sap-ingress>ip-criteria>entry>match fragment)
[Tree] (config>qos>sap-egress>ip-criteria>entry>match fragment)

Full Context configure qos sap-egress ip-criteria entry match fragment
configure qos sap-ingress ip-criteria entry match fragment

Description This command configures fragmented or non-fragmented IP packets as a SAP QoS policy match criterion.

The **no** form of this command removes the match criterion and matches all packets regardless of whether they are fragmented or not.

Default no fragment

Parameters **true** — Configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.

false — Configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.

Platforms All

fragment

Syntax **fragment** {**true** | **false** | **first-only** | **non-first-only**}
no fragment

Context [Tree] (config>qos>sap-ingress>ipv6-criteria>entry>match fragment)

Full Context configure qos sap-ingress ipv6-criteria entry match fragment

Description This command configures fragmented or non-fragmented IPv6 packets as a SAP ingress QoS policy match criterion.

The **no** form of this command removes the match criterion and matches all packets regardless of whether they are fragmented or not.

Default no fragment

Parameters **true** — Specifies to match on all fragmented IPv6 packets. A match will occur for all packets that contain an IPv6 Fragmentation Extension Header.

false — Specifies to match on all non-fragmented IP packets. Non-fragmented IPv6 packets are packets that do not contain an IPv6 Fragmentation Extension Header.

first-only — Matches if a packet is an initial fragment of the fragmented IPv6 packet.

non-first-only — Matches if a packet is a non-initial fragment of the fragmented IPv6 packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

fragment

Syntax **fragment** {**true** | **false**}
no fragment

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry>match fragment)
[Tree] (config>qos>network>egress>ip-criteria>entry>match fragment)

Full Context configure qos network egress ip-criteria entry match fragment
configure qos network ingress ip-criteria entry match fragment

Description This command configures fragmented or non-fragmented IP packets as a network QoS policy match criterion.

The **no** form of this command removes the match criterion and matches all packets regardless of whether they are fragmented or not.

Parameters **true** — Configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.

false — Configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.

Platforms All

fragment

Syntax **fragment** {**true** | **false** | **first-only** | **non-first-only**}
no fragment

Context **[Tree]** (config>qos>network>ingress>ipv6-criteria>entry>match fragment)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match fragment)

Full Context configure qos network egress ipv6-criteria entry match fragment
configure qos network ingress ipv6-criteria entry match fragment

Description This command configures fragmented or non-fragmented IPv6 packets as a network QoS policy match criterion.

The **no** form of this command removes the match criterion and matches all packets regardless of whether they are fragmented or not.

Parameters **true** — Specifies to match on all fragmented IPv6 packets. A match will occur for all packets that contain an IPv6 Fragmentation Extension Header.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

false — Specifies to match on all non-fragmented IP packets. Non-fragmented IPv6 packets are packets that do not contain an IPv6 Fragmentation Extension Header.

first-only — Matches if a packet is an initial fragment of the fragmented IPv6 packet.

non-first-only — Matches if a packet is a non-initial fragment of the fragmented IPv6 packet.

Platforms All

fragment

Syntax **fragment** {**true** | **false** | **first-only** | **non-first-only**}
no fragment

Context **[Tree]** (config>filter>ip-filter>entry>match fragment)
[Tree] (config>filter>ipv6-filter>entry>match fragment)

Full Context configure filter ip-filter entry match fragment
configure filter ipv6-filter entry match fragment

Description This command specifies match criterion for fragmented packets.

Matches can be based on the presence of a fragmented packet (or otherwise) on the ingress or egress interface.

Matches can also be based on the presence of the first fragment of a packet, or on the presence of a fragment that is not the first fragment on the ingress interface.

The **no** form of the command removes the match criterion.

Default no fragment

Parameters **true** — Specifies to match on all fragmented packets.

false — Specifies to match on all non-fragmented packets.

first-only — Matches if a packet is an initial fragment of a fragmented packet.

non-first-only — Matches if a packet is a non-initial fragment of a fragmented packet.

Platforms All

fragment

Syntax **fragment** {**true** | **false**}
no fragment

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match fragment)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match fragment)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security cpm-filter ip-filter entry match fragment
configure system security cpm-filter ipv6-filter entry match fragment

Description This command specifies fragmented or non-fragmented IP packets as an IP filter match criterion.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The **no** version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

The **no** form of this command removes the match criterion.

This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The **no** version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default no fragment

Parameters **true** — Specifies to match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value. For IPv6, packet matches if it contains IPv6 Fragmentation Extension Header.

false — Specifies to match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero. For IPv6, packet matches if it does not contain IPv6 Fragmentation Extension Header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.140 fragment-drop

fragment-drop

Syntax **fragment-drop** {**all** | **out-of-order**} [**event-log** *event-log-name*]
no fragment-drop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>policy>aqp>entry>action fragment-drop)

Full Context configure application-assurance group policy app-qos-policy entry action fragment-drop

Description This command specifies the action to apply to fragments.

Default no fragment-drop

Parameters **all** — All the fragments will be dropped.

out-of-order — All out of order fragments will be dropped.

event-log-name — Specifies if the dropping of fragments should be logged to the specified event log name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.141 fragment-drop-all

fragment-drop-all

Syntax **fragment-drop-all** *direction* [**create**]
no fragment-drop-all *direction*

Context [Tree] (config>app-assure>group>statistics>tca fragment-drop-all)

Full Context configure application-assurance group statistics threshold-crossing-alert fragment-drop-all

Description This command configures a TCA for the counter capturing drops due to the fragment-drop-all AQP command. A fragment-drop-all TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a fragment-drop-all TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.142 fragment-drop-out-of-order

fragment-drop-out-of-order

Syntax **fragment-drop-out-of-order** *direction* [**create**]
no fragment-drop-out-of-order *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca fragment-drop-out-of-order)

Full Context configure application-assurance group statistics threshold-crossing-alert fragment-drop-out-of-order

Description This command configures a TCA for the counter capturing drops due to the fragment-drop-out-of-order AQP command. A fragment-drop-out-of-order TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a fragment-drop-out-of-order TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.143 fragment-threshold

fragment-threshold

Syntax **fragment-threshold** *fragment-threshold*
fragment-threshold unlimited
no fragment-threshold

Context **[Tree]** (config>port>multilink-bundle fragment-threshold)

Full Context configure port multilink-bundle fragment-threshold

Description This command sets the maximum length in bytes of a fragment transmitted across a multilink bundle.

The **no** form of this command resets the fragment threshold back to the default value.

Default fragment-threshold 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *fragment-threshold* — Specify the maximum fragment length, in bytes, to be transmitted across a multilink bundle. Note that the value range is dependent on the MDA type. For example: channelized MDAs, such as the m1-choc12-sfp, m4-choc3-sfp, m12-chds3, and m4-chds3, support values of 128, 256, 512; ASAP channelized MDAs support any value in the valid range.

Values 128 to 512 bytes inclusive for MLPPP and MLFR bundles 128 bytes for IMA bundles

unlimited — This keyword disables fragmentation (MLPPP and MLFR only).

Platforms 7450 ESS, 7750 SR-7/12/12e

fragment-threshold

Syntax **fragment-threshold** *fragment-threshold*
no fragment-threshold

Context **[Tree]** (config>port>tdm>ds1>channel-group>frame-relay>frf-12 fragment-threshold)
[Tree] (config>port>tdm>e1>channel-group>frame-relay>frf-12 fragment-threshold)
[Tree] (config>port>tdm>ds3>frame-relay>frf-12 fragment-threshold)
[Tree] (config>port>tdm>e3>frame-relay>frf-12 fragment-threshold)
[Tree] (config>port>sonet-sdh>path>frame-relay>frf-12 fragment-threshold)

Full Context configure port sonet-sdh path frame-relay frf-12 fragment-threshold
configure port tdm ds1 channel-group frame-relay frf-12 fragment-threshold
configure port tdm ds3 frame-relay frf-12 fragment-threshold
configure port tdm e1 channel-group frame-relay frf-12 fragment-threshold
configure port tdm e3 frame-relay frf-12 fragment-threshold

Description This command sets the maximum length in bytes of a fragment transmitted across a frame relay port with the FRF.12 UNI/NNI fragmentation enabled.

The **no** form of this command resets the fragment threshold back to the default value.

Default fragment-threshold 128

Parameters *fragment-threshold* — Specifies the maximum fragment length, in bytes, to be transmitted across the FRF.12 port.

Values 128 to 512 bytes

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay frf-12 fragment-threshold

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 frame-relay frf-12 fragment-threshold
- configure port tdm e3 frame-relay frf-12 fragment-threshold
- configure port tdm e1 channel-group frame-relay frf-12 fragment-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port tdm ds1 channel-group frame-relay frf-12 fragment-threshold

10.144 frame-based-accounting

frame-based-accounting

Syntax [**no**] **frame-based-accounting**

Context **[Tree]** (config>qos>scheduler-policy frame-based-accounting)

Full Context configure qos scheduler-policy frame-based-accounting

Description The frame-based-accounting command is used to enable frame-based accounting for both the children queues parented to the scheduling policy and for the schedulers within the scheduler policy.

When frame-based accounting is enabled on the policy, all queues associated with the scheduler (through the parent command on each queue) will have their rate and CIR values interpreted as frame-based values. When shaping, the queues will include the 12-byte Inter-Frame Gap (IFG) and 8 byte preamble for each packet scheduled out the queue. The profiling CIR threshold will also include the 20-byte frame encapsulation overhead. Statistics associated with the queue do not include the frame encapsulation overhead.

The scheduler policy's scheduler rate and CIR values will be interpreted as frame-based values.

The configuration of **parent-location** and **frame-based-accounting** in a scheduler policy is mutually exclusive to ensure consistency between the different scheduling levels. Packet byte offset settings are not included in the applied rate when frame-based accounting is configured; however, the offsets are applied to the statistics.

The **no** form of this command is used to return all schedulers within the policy and queues associated with the policy to the default packet-based accounting mode. If **frame-based-accounting** is not currently enabled for the scheduling policy, the **no frame-based-accounting** command has no effect.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.145 frame-counters

frame-counters

Syntax [**no**] **frame-counters**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes frame-counters)

Full Context configure aaa isa-radius-policy acct-include-attributes frame-counters

Description This command includes the frame-counters attribute.

The **no** form of the command excludes frame-counters attribute.

Default no frame-counters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.146 frame-relay

frame-relay

Syntax **frame-relay**

Context **[Tree]** (config>port>ml-bundle>mlfr frame-relay)

Full Context configure port multilink-bundle mlfr frame-relay

Description This command configures the Frame Relay parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e

frame-relay

Syntax **frame-relay**

Context **[Tree]** (config>port>sonet-sdh>path frame-relay)
[Tree] (config>port>tdm>ds1>channel-group frame-relay)
[Tree] (config>port>tdm>ds3 frame-relay)
[Tree] (config>port>tdm>e1>channel-group frame-relay)
[Tree] (config>port>tdm>e3 frame-relay)

Full Context configure port sonet-sdh path frame-relay
configure port tdm ds1 channel-group frame-relay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port tdm ds3 frame-relay
configure port tdm e1 channel-group frame-relay
configure port tdm e3 frame-relay

Description This command allows access to the context to configure the Frame Relay Local Management Interface (LMI) operational parameters for a SONET/SDH PoS link, a DS-0 channel group, or a DS-3/E-3 port or channel.

The port's **mode** must be set to **access** in **config>port>sonet-sdh>path>mode access** context.

The port's encapsulation type must be set to **frame-relay** in the **config>port>sonet-sdh>path>encap-type frame-relay** context.

The **no** form of this command removes the Frame Relay LMI operational parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 frame-relay
- configure port tdm ds1 channel-group frame-relay
- configure port tdm e1 channel-group frame-relay
- configure port tdm e3 frame-relay

frame-relay

Syntax [**no**] **frame-relay**

Context **[Tree]** (debug frame-relay)

Full Context debug frame-relay

Description This command enables, disables and configures debugging for frame relay.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

frame-relay

Syntax **frame-relay**

Context **[Tree]** (config>service>apipe>sap frame-relay)
[Tree] (config>service>epipe>sap frame-relay)
[Tree] (config>service>fpipe>sap frame-relay)
[Tree] (config>service>ipipe>sap frame-relay)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service apipe sap frame-relay
configure service epipe sap frame-relay
configure service fpipe sap frame-relay
configure service ipipe sap frame-relay

Description Commands in this context configure Frame Relay parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ipipe sap frame-relay
- configure service fpipe sap frame-relay
- configure service epipe sap frame-relay

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap frame-relay

frame-relay

Syntax **frame-relay**

Context **[Tree]** (config>service>vpls>sap frame-relay)

Full Context configure service vpls sap frame-relay

Description Commands in this context configure frame-relay parameters.

Platforms All

frame-relay

Syntax **frame-relay**

Context **[Tree]** (config>service>ies>if>sap frame-relay)

Full Context configure service ies interface sap frame-relay

Description This command allows access to the context to configure the Frame Relay Local Management Interface (LMI) operational parameters for a SONET/SDH PoS link, a DS-0 channel group, or a DS-3/E-3 port or channel.

The port's **mode** must be set to **access** in **config>port>sonet-sdh>path>mode access** context.

The port's encapsulation type must be set to **frame-relay** in the **config>port>sonet-sdh>path>encap-type frame-relay** context.

The **no** form of this command removes the Frame Relay LMI operational parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

frame-relay

Syntax **frame-relay**

Context **[Tree]** (config>service>vprn>if>sap frame-relay)

Full Context configure service vprn interface sap frame-relay

Description Commands in this context configure Frame Relay parameters on the SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.147 framed-interface-id

framed-interface-id

Syntax [**no**] **framed-interface-id**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute framed-interface-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-interface-id

Description This command enables the generation of the **framed-interface-id** RADIUS attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.148 framed-ip-addr

framed-ip-addr

Syntax [**no**] **framed-ip-addr**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute framed-ip-addr)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-ip-addr

Description This command enables the inclusion of the **framed-ip-addr** attribute.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

framed-ip-addr

Syntax [**no**] **framed-ip-addr**

Context **[Tree]** (config>ipsec>rad-acct-plcy>include framed-ip-addr)

Full Context configure ipsec radius-accounting-policy include-radius-attribute framed-ip-addr

Description This command enables the inclusion of the **framed-ip-addr** attribute.

Default no framed-ip-addr

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

framed-ip-addr

Syntax [**no**] **framed-ip-addr**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes framed-ip-addr)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes framed-ip-addr)

Full Context configure aaa isa-radius-policy acct-include-attributes framed-ip-addr
configure aaa isa-radius-policy auth-include-attributes framed-ip-addr

Description This command enables the inclusion of the framed-ip-addr attribute.

The **no** form of the command excludes called framed-ip-addr attributes.

Default no framed-ip-addr

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.149 framed-ip-netmask

framed-ip-netmask

Syntax [**no**] **framed-ip-netmask**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute framed-ip-netmask)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-ip-netmask

Description This command enables the inclusion of the **framed-ip-netmask** attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

framed-ip-netmask

Syntax [**no**] **framed-ip-netmask**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes framed-ip-netmask)

Full Context configure aaa isa-radius-policy acct-include-attributes framed-ip-netmask

Description This command enables the inclusion of the framed-ip-netmask attribute.

The **no** form of the command disables the inclusion.

Default no framed-ip-netmask

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.150 framed-ipv6-prefix

framed-ipv6-prefix

Syntax [**no**] **framed-ipv6-prefix**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute framed-ipv6-prefix)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-ipv6-prefix

Description This command enables the generation of the **framed-ipv6-prefix** RADIUS attribute.

The **no** form of this command disables the generation of the **framed-ipv6-prefix** RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

framed-ipv6-prefix

Syntax [**no**] **framed-ipv6-prefix**

Context **[Tree]** (config>ipsec>rad-acct-plcy>include framed-ipv6-prefix)

Full Context configure ipsec radius-accounting-policy include-radius-attribute framed-ipv6-prefix

Description This command enables the inclusion of the **framed-ipv6-prefix** attribute.

Default no framed-ipv6-prefix

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

framed-ipv6-prefix

Syntax [**no**] **framed-ipv6-prefix**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes framed-ipv6-prefix)

Full Context configure aaa isa-radius-policy acct-include-attributes framed-ipv6-prefix

Description If an active SLAAC lease exists, this attribute defines if the SLAAC prefix of the UE is present in accounting.

Default no framed-ipv6-prefix

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.151 framed-ipv6-route

framed-ipv6-route

Syntax [**no**] **framed-ipv6-route**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute framed-ipv6-route)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-ipv6-route

Description When enabled, all valid [99] Framed-IPv6-Route attributes as received in the RADIUS authentication phase and associated with an instantiated IPv6 wan host is included in the RADIUS accounting request messages. The state of the Framed-IPv6-Route (installed, shadowed, hostInactive, and so on) is not considered for reporting in the accounting request messages.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.152 framed-route

framed-route

Syntax [**no**] **framed-route**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute framed-route)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute framed-route

Description When enabled, all valid [22] Framed-Route attributes as received in the RADIUS authentication phase and associated with an instantiated IPv4 host is included in the RADIUS accounting request messages. The state of the Framed-Route (installed, shadowed, hostInactive, and so on) is not considered for reporting in the accounting request messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

10.153 framing

framing

Syntax **framing** {**sonet** | **sdh**}

Context **[Tree]** (config>port>sonet-sdh framing)

Full Context configure port sonet-sdh framing

Description This command specifies SONET/SDH framing to be either SONET or SDH.

This command is supported by TDM satellite.

Default framing sonet

Parameters **sonet** — Configures the port for SONET framing.

sdh — Configures the port for SDH framing.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

framing

Syntax **framing** {**esf** | **sf** | **unframed-ds1**}

Context **[Tree]** (config>port>tdm>ds1 framing)

Full Context configure port tdm ds1 framing

Description This command specifies the DS-1 framing to be used with the associated channel.

Default framing esf

Parameters **esf** — Configures the DS-1 port for extended super frame framing.

sf — Configures the DS-1 port for super frame framing.

unframed-ds1 — Specifies ds-1 unframed (G.703) mode for DS-1 interfaces. This parameter allows the configuration of an unstructured DS-1 channel on a CES MDA. In G.704, timeslot 0 is used to carry timing information by a service provider, thus, only 31 slots are made available to the end user. In G.703, all 32 time slots are available to the end user. Timing is provided by the end user. When an e1-unframed channel is shutdown, it sends the AIS pattern to the far-end DS-1 which does not react. The operational status remains up and no alarms are generated while the near-end (shutdown) is operationally down. This is normal behavior since the G.703 option does not have framing. G.703 framing is only applicable for FR, PPP, and cHDLC encapsulations.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

framing

Syntax **framing** {**no-crc-g704** | **g704** | **e1-unframed**}

Context **[Tree]** (config>port>tdm>e1 framing)

Full Context configure port tdm e1 framing

Description This command specifies the E-1 framing to be used with the associated channel.

Default framing g704

Parameters **g704** — Configures the E-1 port for G.704 framing.

no-crc-g70 — Configures the E-1 for G.704 with no CRC4.

e1-unframed — Specifies E-1 unframed (G.703) mode for E-1 interfaces. This parameter also allows the configuration of an unstructured E-1 channel on an ASAP or CES MDA. In G.704, timeslot 0 is used to carry timing information by a service provider, thus, only 31 slots are made available to the end user. In G.703, all 32 time slots are available to the end user. Timing is provided by the end user. When an

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

e1-unframed channel is shutdown, it sends the AIS pattern to the far-end E-1 which does not react. The operational status remains up and no alarms are generated while the near-end (shutdown) is operationally down. This is normal behavior since the G.703 option does not have framing. G.703 framing is only applicable for FR, PPP, and cHDLC and CEM encapsulations.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

framing

Syntax **framing** {**c-bit** | **m23** | **unframed-ds3**}

Context **[Tree]** (config>port>tdm>ds3 framing)

Full Context configure port tdm ds3 framing

Description This command specifies DS-3 framing for the associated DS-3 port or channel.

Default framing c-bit

Parameters **c-bit** — Configures the DS-3 port/channels for C-Bit framing.

m23 — Configures the DS-3 port/channel for M23 framing.

unframed-ds3 — Specifies ds-3 unframed mode for DS-3 interfaces. This parameter allows the configuration of an unstructured DS-3 channel on a CES MDA.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

framing

Syntax **framing** {**g751** | **g832** | **unframed-e3**}

Context **[Tree]** (config>port>tdm>e3 framing)

Full Context configure port tdm e3 framing

Description This command specifies E-3 framing for the associated E-3 port or channel.

Default for E-3 non-ATM: framing g751 and cannot be changed. for E-3 ATM: framing g832 and cannot be changed.

Parameters **g751** — Configures the E-3 port/channel for g751 framing.

g832 — Configures the E-3 port/channel for g832 framing.

unframed-e3 — Specifies e-3 unframed mode for E-3 interfaces. This parameter allows the configuration of an unstructured E-3 channel on a CES MDA.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.154 frequency

frequency

Syntax **frequency** *frequency*
no frequency

Context **[Tree]** (config>port>dwdm frequency)

Full Context configure port dwdm frequency

Description This command configures the center frequency to use for a tunable DWDM optical interface. It replaces the **configure**>**port**>**dwdm**>**channel** command (used prior to Release 22.2.R1). The **frequency** command supports any frequency in the C band, but the actual operating frequency is dependent on the installed optic module.

Provisioning rules

The provisioned MDA type must have DWDM tunable optics (for example, p1-100g-tun-b) or the MDA must support the option of tunable DWDM optic modules. The following provisioning rules apply:

- The DWDM frequency must set to a non-zero value before the port is set to **no shutdown**.
- The port must be **shutdown** before changing the DWDM frequency.
- The port must be a physical port to set the DWDM frequency.

Default frequency 0

Parameters *frequency* — Specifies the frequency in MHz.

Values 0, 191100000 to 196150000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.155 frf-12

frf-12

Syntax [**no**] **frf-12**

Context **[Tree]** (config>port>tdm>ds1>channel-group>frame-relay frf-12)
[Tree] (config>port>tdm>ds3>frame-relay frf-12)
[Tree] (config>port>tdm>e1>channel-group>frame-relay frf-12)
[Tree] (config>port>tdm>e3>frame-relay frf-12)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>port>sonet-sdh>path>frame-relay frf-12)

Full Context configure port sonet-sdh path frame-relay frf-12
configure port tdm ds1 channel-group frame-relay frf-12
configure port tdm ds3 frame-relay frf-12
configure port tdm e1 channel-group frame-relay frf-12
configure port tdm e3 frame-relay frf-12

Description This command defines the context to configure the parameters of FRF.12 Frame Relay fragmentation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay frf-12

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 frame-relay frf-12
- configure port tdm e3 frame-relay frf-12
- configure port tdm e1 channel-group frame-relay frf-12
- configure port tdm ds1 channel-group frame-relay frf-12

frf-12

Syntax [**no**] **frf-12**

Context **[Tree]** (config>service>epipe>sap>frame-relay frf-12)
[Tree] (config>service>ipipe>sap>frame-relay frf-12)

Full Context configure service epipe sap frame-relay frf-12
configure service ipipe sap frame-relay frf-12

Description This command enables the use of FRF12 headers.

The **no** form of this command disables the use of FRF12 headers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

frf-12

Syntax [**no**] **frf-12**

Context **[Tree]** (config>service>vpls>sap>fr frf-12)

Full Context configure service vpls sap frame-relay frf-12

Description This command enables FRF12 headers. This must be set to disabled for this entry to be added to an MLFR bundle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables FRF12 headers.

Platforms All

frf-12

Syntax [**no**] **frf-12**

Context **[Tree]** (config>service>ies>if>sap>frame-relay frf-12)
[Tree] (config>service>vprn>if>sap>frame-relay frf-12)

Full Context configure service ies interface sap frame-relay frf-12
configure service vprn interface sap frame-relay frf-12

Description This command defines the context to configure the parameters of FRF.12 Frame Relay fragmentation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

frf-12

Syntax [**no**] **frf-12**

Context **[Tree]** (config>service>vprn>if>sap frf-12)

Full Context configure service vprn interface sap frf-12

Description This command enables the use of FRF12 headers.

The **no** form of this command disables the use of FRF12 headers.

10.156 frf16

frf16

Syntax [**no**] **frf16** *port-id*

Context **[Tree]** (debug>frame-relay frf16)

Full Context debug frame-relay frf16

Description This command enables tracing of all FRF16 compliant MLFR link integrity protocol messages in both the receive and transmit directions on a specific member link of an MLFR bundle. The **no** form of this command turns off MLFR debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id* — Specifies the port ID of the FRF16 bundle member link.

port-id	*slot*/*mda*/*port* [.*channel*]	
bundle-id	bundle-*type*-slot/mda.*bundle-num*	
	bundle	keyword
	type	fr
	bundle-num	1 to 336

Output The following output is an example of frame relay FRF16 information.

Sample Output

```
1 2009/02/18 10:39:42.74 UTC MINOR: DEBUG #2001 Base MLFR
"MLFR: [_LIP_ParseRxFrame]
RxMsg <bundle-fr-1/1.1:1/1/1.0x56> <state-0: Up>
<MsgType-5:HelloAck>
     <ie-03:      MagicNum>,<len 06>, <27002>
     <ie-05:     TimeStamp>,<len 06>, <0x4b1c4558>"

2 2009/02/18 10:39:43.73 UTC MINOR: DEBUG #2001 Base MLFR
"MLFR: [_LIP_TxFrame]
TxMsg <bundle-fr-1/1.1:1/1/1.0x56> <state-0: Up>
<MsgType-4:Hello>
     <ie-03:      MagicNum>,<len 06>, <31104>
     <ie-05:     TimeStamp>,<len 06>, <0x5d804569>"

3 2009/02/18 10:39:43.73 UTC MINOR: DEBUG #2001 Base MLFR
"MLFR: [_LIP_ParseRxFrame]
RxMsg <bundle-fr-1/1.1:1/1/1.0x56> <state-0: Up>
<MsgType-5:HelloAck>
     <ie-03:      MagicNum>,<len 06>, <27002>
     <ie-05:     TimeStamp>,<len 06>, <0x5d804569>"
```

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

10.157 from

from

Syntax **from** [**main**] [**security**] [**change**] [**debug-trace**]
no from

Context **[Tree]** (config>service>vprn>log>log-id from)

Full Context configure service vprn log log-id from

Description This command selects the source stream to be sent to a log destination.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

One or more source streams must be specified. The source of the data stream must be identified using the **from** command before you can configure the destination using the **to** command. The **from** command can identify multiple source streams in a single statement (for example: **from main change debug-trace**).

Only one **from** command may be entered for a single *log-id*. If multiple **from** commands are configured, then the last command entered overwrites the previous **from** command.

The **no** form of this command removes all previously configured source streams.

Default No source stream is configured.

Parameters **main** — Instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the **filter** command.

security — Instructs all events in the security event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The security event stream contains all events that pertain to attempts to breach system security. To limit the events forwarded to the destination, configure filters using the **filter** command.

change — Instructs all events in the user activity stream to be sent to the destination configured in the **to** command for this destination *log-id*. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the filter command.

debug-trace — Instructs all events in the debug-trace event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The debug-trace event stream contains all events that pertain to trace or other debugging information. To limit the events forwarded to the destination, configure filters using the **filter** command.

Platforms All

from

Syntax **from** *ip-address*

Context **[Tree]** (config>router>mpls>lsp from)
[Tree] (config>router>mpls>lsp-template from)

Full Context configure router mpls lsp from
configure router mpls lsp-template from

Description This optional command specifies the IP address of the ingress router for the LSP. When this command is not specified, the system IP address is used. IP addresses that are not defined in the system are allowed. If an invalid IP address is entered, LSP bring-up fails and an error is logged.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If an interface IP address is specified as the **from** address, and the egress interface of the LSP nexthop IP address is a different interface, the LSP is not signaled. As the egress interface changes due to changes in the routing topology, it is recommended to set the **from** IP address to the system IP address or to the address of a loopback interface to ensure the LSP recovers.

Only one **from** address can be configured.

Default The system IP address

Parameters *ip-address* — Specifies the IP address of the ingress router. This can be either the interface, the system or a loopback interface IP address. If the IP address is local, the LSP must egress through that local interface which ensures local strictness. When the LSP type is **sr-te**, then an IPv6 address can be used.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — 0 to FFFF (hexadecimal)
d — 0 to 255 (decimal)

Platforms All

from

Syntax **from li**
no from

Context **[Tree]** (config>li>log>log-id from)

Full Context configure li log log-id from

Description This command configures a bit mask that specifies the log event source stream(s) to be forwarded to the destination specified in the log destination (memory, session, SNMP). Events from more than one source can be forwarded to the log destination.

Parameters **li** — Specifies the **li** event stream that contains all events configured for Lawful Intercept activities.

If the requester does not have access to the **li** context, the event stream will fail.

Platforms All

from

Syntax **from** *ipv4-address*
no from

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>oam-pm>session>mpls>lsp>rsvp-auto from)

Full Context configure oam-pm session mpls lsp rsvp-auto from

Description One of three mandatory configuration statements that are required to identify automatically create RSVP LSPs, created using **config>router>mpls>lsp-template**. The **config>router>mpls>auto-lsp** *lsp-template* links three distinct functions. The **config>router>policy-options>prefix-list**, **config>router>policy-options>policy-statement>entry>from** and config>router>mpls> lsp-template. The from address under the test context is the same as the config>router>mpls>lsp-template>from address.

The three required identifiers are from, lsp-template and to, all under this container.

The **no** form of this command deletes the IP address from the configuration.

Parameters *ipv4-address* — Specifies the IPv4 address.

Values a.b.c.d.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

from

Syntax **from** {[**main**] [**security**] [**change**] [**debug-trace**]}
no from

Context [Tree] (config>log>log-id from)

Full Context configure log log-id from

Description This command selects the source stream to be sent to a log destination.

One or more source streams must be specified. The source of the data stream must be identified using the **from** command before you can configure the destination using the **to** command. The **from** command can identify multiple source streams in a single statement (for example: **from main change debug-trace**).

Only one **from** command may be entered for a single *log-id*. If multiple **from** commands are configured, then the last command entered overwrites the previous **from** command.

The **no** form of this command removes all previously configured source streams.

Parameters **main** — Instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the **filter** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

security — Instructs all events in the security event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. To limit the events forwarded to the destination, configure filters using the **filter** command.

change — Instructs all events in the user activity stream to be sent to the destination configured in the **to** command for this destination *log-id*. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the **filter** command.

debug-trace — Instructs all debug-trace messages in the debug stream to be sent to the destination configured in the **to** command for this destination *log-id*. Filters applied to debug messages are limited to application and subject.

Platforms All

from

Syntax [**no**] **from**

Context **[Tree]** (config>router>policy-options>policy-statement>entry from)

Full Context configure router policy-options policy-statement entry from

Description This command creates the context to configure policy match criteria based on a route's source or the protocol from which the route is received.

If no condition is specified, all route sources are considered to match.

The **no** form of this command deletes the source match criteria for the route policy statement entry.

Platforms All

10.158 from-aa-sub-counters

from-aa-sub-counters

Syntax [**no**] **from-aa-sub-counters** [**all**]

Context **[Tree]** (config>log>acct-policy>cr>aa from-aa-sub-counters)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure Application Assurance “from subscriber” counter parameters. This command only applies to the 7750 SR.

The **no** form of this command excludes the “from subscriber” count.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.159 from-subscriber

from-subscriber

Syntax **from-subscriber**

Context **[Tree]** (config>isa>aa-grp>qos>egress from-subscriber)

Full Context configure isa application-assurance-group qos egress from-subscriber

Description Commands in this context configure Quality of Service for this application assurance group from-subscriber logical port, traffic entering the system from AA subscribers and entering an application assurance engine.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.160 from-vpls

from-vpls

Syntax **from-vpls** *service-id*
no from-vpls

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mvr from-vpls)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mvr from-vpls

Description This command configures the VPLS from which multicast traffic is copied upon receipt of an IGMP join request.

IGMP snooping must be enabled on the MVR VPLS.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — Specifies the MVR VPLS from which multicast channels be copied into an MSAP.

Values
service-id: 1 to 2147483647
service-name: up to 64 characters (applies only to the 7750 SR)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

from-vpls

Syntax **from-vpls** *vpls-id*
no from-vpls

Context **[Tree]** (config>service>vpls>sap>igmp-snooping>mvr from-vpls)
[Tree] (config>service>vpls>sap>mld-snooping>mvr from-vpls)

Full Context configure service vpls sap igmp-snooping mvr from-vpls
configure service vpls sap mld-snooping mvr from-vpls

Description This command configures the VPLS from which multicast traffic is copied upon receipt of an IGMP join request. IGMP snooping must be enabled on the MVR VPLS.

Default no from-vpls

Parameters *vpls-id* — Specifies the MVR VPLS from which multicast channels should be copied into this SAP

Values *service-id*:1 to 2147483648

Platforms All

10.161 frr

frr

Syntax **frr** [**detail**]
no frr

Context **[Tree]** (debug>router>mpls>event frr)

Full Context debug router mpls event frr

Description This command debugs fast re-route events.

The **no** form of the command disables the debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **detail** — Displays detailed information about re-route events.

Platforms All

10.162 frr-object

frr-object

Syntax [**no**] **frr-object**

Context **[Tree]** (config>router>mpls frr-object)

Full Context configure router mpls frr-object

Description This command specifies whether fast reroute for LSPs using the **facility** bypass method is signaled with or without the fast reroute object using the **one-to-one** keyword. The value is ignored if fast reroute is disabled for the LSP or if the LSP is using one-to-one Backup.

Default frr-object — Specifies the value is by default inherited by all LSPs.

Platforms All

10.163 fsm-state-changes

fsm-state-changes

Syntax [**no**] **fsm-state-changes**

Context **[Tree]** (debug>service>id>stp fsm-state-changes)

Full Context debug service id stp fsm-state-changes

Description This command enables STP debugging for FSM state changes.

The **no** form of the command disables debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

10.164 fsm-timers

fsm-timers

Syntax [**no**] **fsm-timers**

Context **[Tree]** (debug>service>id>stp fsm-timers)

Full Context debug service id stp fsm-timers

Description This command enables STP debugging for FSM timer changes.

The **no** form of the command disables debugging.

Platforms All

10.165 ftp

ftp

Syntax [**no**] **ftp**

Context **[Tree]** (config>service>nat>nat-policy>alg ftp)
[Tree] (config>service>nat>firewall-policy>alg ftp)
[Tree] (config>service>nat>up-nat-policy>alg ftp)

Full Context configure service nat firewall-policy alg ftp
configure service nat nat-policy alg ftp
configure service nat up-nat-policy alg ftp

Description This command enables FTP ALG.

The **no** form of the command disables FTP ALG.

Default ftp

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy alg ftp
- configure service nat up-nat-policy alg ftp

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy alg ftp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ftp

Syntax **ftp**

Context **[Tree]** (config>system>login-control ftp)

Full Context configure system login-control ftp

Description This command creates the context to configure FTP login control parameters.

Platforms All

10.166 ftp-server

ftp-server

Syntax [**no**] **ftp-server**

Context **[Tree]** (config>system>security ftp-server)

Full Context configure system security ftp-server

Description This command enables FTP servers running on the system.

FTP servers are disabled by default. At system startup, only SSH servers are enabled.

The **no** form of this command disables FTP servers running on the system.

Platforms All

10.167 function

function

Syntax **function**

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc function)
[Tree] (config>service>vprn>srv6>locator function)
[Tree] (config>service>epipe>srv6>locator function)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function
configure service epipe segment-routing-v6 locator function
configure service vprn segment-routing-v6 locator function

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure SRv6 SID function values and parameters for the locator.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

10.168 function-length

function-length

Syntax **function-length** *function-length*
no function-length

Context **[Tree]** (config>router>segment-routing>srv6>locator function-length)

Full Context configure router segment-routing segment-routing-v6 locator function-length

Description This command configures the length of the function field of an SRv6 locator.

The sum of the function length and the locator prefix length must not exceed 128 bits. This is enforced by CLI validation.

The **no** form of this command reverts to the default value.

Default function-length 20

Parameters *function-length* — Specifies the function length, in bits.

Values 20 to 96

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

10.169 fwd-inside-router

fwd-inside-router

Syntax **fwd-inside-router** *router-instance*
fwd-inside-router service-name *service-name*
no fwd-inside-router

Context **[Tree]** (config>router>pcp-server>server fwd-inside-router)

Full Context configure router pcp-server server fwd-inside-router

Description This command configures the PCP forwarding inside virtual router instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default no fwd-inside-router

Parameters *router-instance* — Specifies the router name or the VPRN service ID.

Values
router-instance: *router name* | *vprn-svc-id*

router-name	Base
vprn-svc-id	1 to 2147483647

service-name — Specifies the service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

10.170 fwd-path-ext

fwd-path-ext

Syntax **fwd-path-ext**

Context **[Tree]** (config fwd-path-ext)

Full Context configure fwd-path-ext

Description This command provides context for configuring Forwarding Path Extensions (FPE). FPE is utilized by certain applications that rely on PXC functionality. Its purpose is to simplify configuration of such applications.

Platforms All

10.171 fwd-wholesale

fwd-wholesale

Syntax **fwd-wholesale**

Context **[Tree]** (config>service>vprn>if>sap fwd-wholesale)
[Tree] (config>service>vprn>sub-if>grp-if>sap fwd-wholesale)

Full Context configure service vprn interface sap fwd-wholesale
configure service vprn subscriber-interface group-interface sap fwd-wholesale

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context select specific protocols ingressing on the SAP to be redirected to another service. The command is applicable to static SAPs as well as PW-SAPs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

fwd-wholesale

Syntax **fwd-wholesale**

Context **[Tree]** (config>service>ies>if>sap fwd-wholesale)

Full Context configure service ies interface sap fwd-wholesale

Description Commands in this context select specific protocols ingressing on the SAP to be redirected to another service. The command is applicable to static SAPs as well as PW-SAPs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

fwd-wholesale

Syntax [**no**] **fwd-wholesale**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap fwd-wholesale)

Full Context configure service ies subscriber-interface group-interface sap fwd-wholesale

Description Commands in this context select specific protocols ingressing on the SAP to be redirected to another service. The command is applicable to static SAPs as well as PW-SAPs.

The **no** form of this command removes the redirection.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11 g Commands

11.1 garp-flood-evpn

garp-flood-evpn

Syntax [**no**] **garp-flood-evpn**

Context **[Tree]** (config>service>vpls>proxy-arp garp-flood-evpn)

Full Context configure service vpls proxy-arp garp-flood-evpn

Description This command controls whether the system floods GARP-requests and GARP-replies to the EVPN. The GARPs impacted by this command are identified by the sender's IP being equal to the target's IP and the MAC DA being broadcast.

The **no** form of the command only floods to local SAPs or binds but not to EVPN destinations.

Disabling this command is only recommended in networks where CEs are routers that are directly connected to the PEs. Networks using aggregation switches between the host/routers and the PEs should flood GARP messages in the EVPN to ensure that the remote caches are updated and the BGP does not miss the advertisement of these entries.

Default garp-flood-evpn

Platforms All

11.2 gateway

gateway

Syntax **gateway name** *name* **tunnel** *ip-address*[**:***port*] [**nat-ip** *nat-ip*[**:***port*]] [**detail**] [**no-dpd-debug**] [**display-keys**]
no gateway name *name* **tunnel** *ip-address*[**:***port*] [**nat-ip** *nat-ip*[**:***port*]
gateway name *name* **tunnel-subnet** *ip-prefix/ip-prefix-length* [**port** *port*] [**detail**] [**no-dpd-debug**] [**display-keys**]
no gateway name *name* **tunnel-subnet** *ip-prefix/ip-prefix-length*

Context **[Tree]** (debug>ipsec gateway)

Full Context debug ipsec gateway

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for dynamic IPsec tunnels that terminate on the specified IPsec gateway.

The tunnel to be debugged can be specified by either its source address or source subnet. If a subnet is specified, the system will enable debugging for all tunnels with source addresses in the specified subnet.

Parameters *name* — Specifies the name of the IPsec gateway up to 32 characters.

ip-address:port — Specifies the tunnel IP address of the remote peer and, optionally, the remote UDP port of IKE.

nat-ip:port — Specifies the inside IP address of the NAT tunnel and, optionally, the port.

detail — Specifies to display detailed debug information.

no-dpd-debug — Specifies to stop logging IKEv1 and IKEv2 DPD events during debug in order to produce less noise.

ip-prefix/ip-prefix-length — Specifies the subnet of the peer's tunnel address.

display-keys — Specifies the IKE-SA and CHILD-SA keys for inclusion in the debug output.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gateway

Syntax **gateway** [**create**]
no gateway

Context **[Tree]** (config>mirror>mirror-dest>encap>layer-3-encap gateway)

Full Context configure mirror mirror-dest encap layer-3-encap gateway

Description This command configures the parameters to send the mirrored packets to a remote destination gateway. Once a gateway is created, no changes to the **layer-3-encap** type, router or direction-bit are allowed.

Platforms All

11.3 gateway-ip

gateway-ip

Syntax **gateway-ip** *ip-address*
no gateway-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>video-interface gateway-ip)

Full Context configure service vpls video-interface gateway-ip

Description This command assigns a gateway IP address for the video interface within the VPLS service. Because VPLS is a Layer 2 service and the video interface is modeled like a host within the service, the video interface needs a gateway IP to send requests to devices outside of the VPLS subnet.

The **no** form of the command deletes the gateway IP address from the VPLS video interface.

Default none

Parameters *ip-address* — Specifies the gateway IP address of the VPLS video interface.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

11.4 gen-keypair

gen-keypair

Syntax **gen-keypair** *url-string* **curve** {**secp256r1** | **secp384r1** | **secp521r1**}
gen-keypair *url-string* [**size** *key-size*] [**type** {**rsa** | **dsa**}]

Context [Tree] (admin>certificate gen-keypair)

Full Context admin certificate gen-keypair

Description This command generates RSA, DSA, or ECDSA private key or public key pairs at the specified location.

Parameters *url-string* — Specifies the path of the key file.

Values

url-string	<local-url> [up to 99 characters]
local-url	<cflash-id>/<file-path>
cflash-id	cf1: | cf2: | cf3:

curve — Generates an ECDSA key with a specified curve.

Values secp256r1, secp384r1, secp521r1

key-size — Specifies the key size in bits.

The minimum key-size is 1024 when running in FIPS-140-2 mode.

Values 512 to 8192

Default 2048

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type — Specifies the type of key.

Values rsa, dsa

Default rsa

Platforms All

11.5 gen-local-cert-req

gen-local-cert-req

Syntax **gen-local-cert-req keypair** *url-string* **subject-dn** *subject-dn* [**domain-name** *name*] [**ip-addr** *ip-address*] **file** *cert-req-file-url* [**hash-alg hash-algorithm**]

Context **[Tree]** (admin>certificate gen-local-cert-req)

Full Context admin certificate gen-local-cert-req

Description This command generates a PKCS#10 formatted certificate request by using a local existing key pair file.

Parameters *url-string* — Specifies the name of the keyfile in cf3:\system-pki\key that is used to generate a certificate request.

Values

url-string	<local-url> [up to 99 characters]
local-url	<cflash-id>/<file-path>
cflash-id	cf1: | cf2: | cf3:

subject-dn — Specifies the distinguish name that is used as the subject in a certificate request, including:

- C-Country
- ST-State
- O-Organization name
- OU-Organization Unit name
- CN-common name

This parameter is formatted as a text string including any of the above attributes. The attribute and its value is linked by using “=”, and “,” is used to separate different attributes.

For example: C=US,ST=CA,O=ALU,CN=SR12

Values attr1=val1,attr2=val2... where: attrN={C| ST| O| OU| CN}, 256 chars max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

domain-name — Specifies a domain name string can be specified and included as the dNSName in the Subject Alternative Name extension of the certificate request.

ip-address — Specifies an IPv4 address string can be specified and included as the ipAddress in the Subject Alternative Name extension of the certificate request.

cert-req-file-url — Specifies the certificate URL. This URL could be either a local CF card path and filename to save the certificate request; or an FTP URL to upload the certificate request.

hash-algorithm — Specifies the hash algorithm to be used in a certificate request.

Values sha1, sha224, sha256, sha384, sha512

Platforms All

11.6 general-port

general-port

Syntax **general-port** *port-number*
no general-port

Context **[Tree]** (config>system>snmp general-port)

Full Context configure system snmp general-port

Description This command configures the port number used by this node to receive SNMP request messages and to send replies. SNMP notifications generated by the agent are sent from the port specified in the **config>log>snmp-trap-group>trap-target** CLI command.

The **no** form of the command reverts to the default value.

Default general-port 161

Parameters *port-number* — Specifies the port number used to send SNMP traffic other than traps.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.7 generalized-pid

generalized-pid

Syntax **generalized-pid** *generalized-pid*
no generalized-pid

Context **[Tree]** (config>router>gmpls>lsp generalized-pid)

Full Context configure router gmpls lsp generalized-pid

Description This command configures the type of payload carried by the gLSP. Standard ethertype values are used for packet and Ethernet LSPs (see RFC 3471).

Default generalized-pid ethernet

Parameters *generalized-pid* — Specifies the name of the generalized-pid.

Values ethernet

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.8 generate-basic-fec-only

generate-basic-fec-only

Syntax [**no**] **generate-basic-fec-only**

Context **[Tree]** (config>router>ldp generate-basic-fec-only)

Full Context configure router ldp generate-basic-fec-only

Description This command enables mLDP to generate a basic FEC despite the actual root node being resolved using BGP. This functionality is useful if a connected router does not support the mLDP recursive FEC type.

This command only operates with recursive opaque type 7 FECs and non-recursive type 1 FECs.

The **no** form of the command causes mLDP to generate a recursive FEC if the actual root node is resolved using BGP.

Default no generate-basic-fec-only

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.9 generate-icmp

generate-icmp

Syntax [**no**] **generate-icmp**

Context **[Tree]** (config>service>vprn>static-route-entry>black-hole generate-icmp)

Full Context configure service vprn static-route-entry black-hole generate-icmp

Description This optional command causes the ICMP unreachable messages to be sent when received packets match the associated static route. By default, the ICMP unreachable messages for those types of static routes are not generated.

This command can only be associated with a static route that has a black-hole next-hop

The **no** form of this command removes the black-hole next-hop from static route configuration.

Default no generate-icmp

Platforms All

generate-icmp

Syntax [**no**] **generate-icmp**

Context **[Tree]** (config>router>static-route-entry>black-hole generate-icmp)

Full Context configure router static-route-entry black-hole generate-icmp

Description This optional command causes the ICMP unreachable messages to be sent when received packets match the associated static route. By default, the ICMP unreachable messages for those types of static routes are not generated.

This command can only be associated with a static route that has a blackhole next-hop

The **no** form of this command removes the black-hole nexthop from the static route configuration.

Default no generate-icmp

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.10 generate-traps

generate-traps

Syntax [**no**] **generate-traps**

Context **[Tree]** (config>system>network-element-discovery generate-traps)

Full Context configure system network-element-discovery generate-traps

Description This command configures whether traps are generated every time a node is updated, added, or removed from the OSPF opaque database (using LSA type 10 opaque update).

The **no** form of causes traps to not be generated for database changes.

Platforms All

11.11 get

get

Syntax [**no**] **get**

Context **[Tree]** (config>service>nat>pcp-server-policy>opcode get)

Full Context configure service nat pcp-server-policy opcode get

Description This command enables/disables support for the **get** opcode.

Default no get

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

get

Syntax [**no**] **get**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization get)

Full Context configure system security profile netconf base-op-authorization get

Description This command enables the NETCONF get operation.

The **no** form of this command disables the operation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no get

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

11.12 get-config

get-config

Syntax [**no**] **get-config**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization get-config)

Full Context configure system security profile netconf base-op-authorization get-config

Description This command enables the NETCONF get-config operation.

The **no** form of this command disables the operation.

Default no get-config

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

11.13 get-data

get-data

Syntax [**no**] **get-data**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization get-data)

Full Context configure system security profile netconf base-op-authorization get-data

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the NETCONF get-data operation.

The **no** form of this command disables the operation.

Default no get-data

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

11.14 get-schema

get-schema

Syntax [**no**] **get-schema**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization get-schema)

Full Context configure system security profile netconf base-op-authorization get-schema

Description This command enables the NETCONF get-schema operation.

The **no** form of this command disables the operation.

Default no get-schema

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

11.15 ggsn

ggsn

Syntax **ggsn**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>gtp>peer-profile ggsn)

Full Context configure subscriber-mgmt gtp peer-profile ggsn

Description Commands in this context configure communication with a GGSN Mobile Gateway.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.16 ggsn-address

ggsn-address

Syntax **ggsn-address** {**ipv4** | **ipv6**}
no ggsn-address

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gy>avp ggsn-address)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp ggsn-address

Description The command includes the GGSN-Address AVP value in all Diameter DCCA CCR messages. The value is either the local IPv4 address or local IPv6 address used to set up the diameter peer.

The **no** form of this command removes the GGSN-Address AVP from the Diameter DCCA CCR messages.

Parameters **ipv4** | **ipv6** — Specifies to include either the IPv4 or IPv6 address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.17 gi-address

gi-address

Syntax **gi-address** *ip-address*
no gi-address

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host gi-address)

Full Context configure subscriber-mgmt local-user-db ipoe host gi-address

Description This command allows selection of GI addresses based on the host entry in LUDB.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The gi-address must be a valid address (associated with an interface) within the routing context that received the DHCP message on the access side.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IPv4 gi-address.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

gi-address

Syntax **gi-address** *ip-address* [**src-ip-address**]
no gi-address

Context **[Tree]** (config>service>ies>if>dhcp gi-address)
[Tree] (config>service>vprn>if>dhcp gi-address)
[Tree] (config>service>vprn>sub-if>dhcp gi-address)
[Tree] (config>service>ies>sub-if>grp-if>dhcp gi-address)
[Tree] (config>service>ies>sub-if>dhcp gi-address)

Full Context configure service ies interface dhcp gi-address
configure service ies subscriber-interface dhcp gi-address
configure service ies subscriber-interface group-interface dhcp gi-address
configure service vprn interface dhcp gi-address
configure service vprn subscriber-interface dhcp gi-address

Description This command configures the gateway interface address for the DHCP relay. A subscriber interface can include multiple group interfaces with multiple SAPs. The GI address is needed, when the router functions as a DHCP relay, to distinguish between the different subscriber interfaces and potentially between the group interfaces defined.

By default, the GI address used in the relayed DHCP packet is the primary IP address of a normal IES interface. Specifying the GI address allows the user to choose a secondary address. For group interfaces a GI address must be specified under the group interface DHCP context or subscriber-interface DHCP context in order for DHCP to function.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the host IP address to be used for DHCP relay packets.

Values a.b.c.d

src-ip-address — Specifies that this GI address is to be the source IP address for DHCP relay packets. This parameter is not applicable for PPPoE DHCP client messages (**dhcp client-applications ppp**).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface dhcp gi-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn subscriber-interface dhcp gi-address
- configure service ies subscriber-interface group-interface dhcp gi-address

All

- configure service vprn interface dhcp gi-address
- configure service ies interface dhcp gi-address

gi-address

Syntax **gi-address** *ip-address*
no gi-address

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>dhcp gi-address)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp gi-address)

Full Context configure service ies interface sap ipsec-gw dhcp gi-address
configure service vprn interface sap ipsec-gw dhcp gi-address

Description This command specifies the gateway IP address of the DHCPv4 packets sent by the system. IPsec DHCP Relay uses only the **gi-address** configuration found under the IPsec gateway and does not take into account **gi-address** with **src-ip-addr** configuration below other interfaces.

Default no gi-address

Parameters *ip-address* — Specifies the host IP address to be used for DHCP relay packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gi-address

Syntax **gi-address** *ip-address* [**src-ip-addr**]
no gi-address

Context **[Tree]** (config>router>if>dhcp gi-address)

Full Context configure router interface dhcp gi-address

Description This command configures the gateway interface address for the DHCP relay. The GI address is needed, when the router functions as a DHCP relay, to distinguish between the different subscriber interfaces and potentially between the group interfaces defined.

Default no gi-address

Parameters *ip-address* — Specifies the host IP address to be used for DHCP relay packets.

src-ip-addr — Uses the GI address as the source IP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

11.18 global

global

Syntax **global** *file-url*
no global

Context **[Tree]** (config>system>login-control>login-scripts global)

Full Context configure system login-control login-scripts global

Description This command enables an operator to define a common CLI script that executes when any user logs into a CLI session. This login exec script is executed when any user (authenticated by any means including local user database, TACACS+, or RADIUS) opens a CLI session. This allows a user, for example, to define a common set of CLI aliases that are made available on the router for all users. This global login exec script is executed before any user-specific login exec files that may be configured.

This CLI script executes in the context of the user who opens the CLI session. Any commands in the script that the user is not authorized to execute will fail.

The **no** form of this command disables the execution of a global login-script.

Default no global

Parameters *file-url* — The path or directory name.

Platforms All

11.19 global-id

global-id

Syntax **global-id** *global-id*
no global-id

Context **[Tree]** (config>router>mpls>mpls-tp global-id)

Full Context configure router mpls mpls-tp global-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the MPLS-TP Global ID for the node. This is used as the 'from' Global ID used by MPLS-TP LSPs originating at this node. If a value is not entered, the Global ID is taken to be Zero. This is used if the global-id is not configured. If an operator expects that inter-domain LSPs will be configured, then it is recommended that the global ID should be set to the local ASN of the node, as configured under **config**>**system**. If two-byte ASNs are used, then the most significant two bytes of the global-id are padded with zeros.

In order to change the value of the **global-id**, **config**>**router**>**mpls**>**mpls-tp** must be in the shutdown state. This will bring down all of the MPLS-TP LSPs on the node. New values a propagated to the system when a no shutdown is performed.

Default no global-id

Parameters *global-id* — Specifies the global ID for the node.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.20 global-timeouts

global-timeouts

Syntax **global-timeouts**

Context **[Tree]** (config>system>management-interface>ops global-timeouts)

Full Context configure system management-interface operations global-timeouts

Description Commands in this context configure system timeout parameters for operational commands.

Timeout parameters provide default system-level control for various types of operational commands in model-driven interfaces. The timeout values are used when specific execution and retention timeouts are not requested for a specific operation.

Platforms All

11.21 global-variables

global-variables

Syntax **global-variables**
no global-variables

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>policy-options global-variables)

Full Context configure router policy-options global-variables

Description This command enables the **global-variables** configuration context.

The **no** form of this command removes all global variables.

Platforms All

11.22 glsp

glsp

Syntax [**no**] **glsp session-name** *name*

Context [Tree] (config>gmpls-tun-grp>member glsp)

Full Context configure gmpls-tun-grp member glsp

Description This command binds a GMPLS LSP as a member of the GMPLS tunnel group. The session name is used to identify the GMPLS LSP. This is the LSP name of the GMPLS LSP.

The **no** form of this command removes the member.

Parameters **session-name name** — Specifies the session name of the GMPLS LSP, up to 80 characters.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.23 gmpls

gmpls

Syntax [**no**] **gmpls**

Context [Tree] (config>router gmpls)

Full Context configure router gmpls

Description Commands in this context configure GMPLS parameters. GMPLS is not enabled by default and must be explicitly enabled using **no shutdown**. The **shutdown** command administratively disables GMPLS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes this GMPLS protocol instance; this will remove all configuration parameters for this GMPLS instance.

GMPLS must be shut down before the GMPLS instance can be deleted. If GMPLS is not shut down when the **no gmpls** command is executed, a warning message on the console indicates that GMPLS is still administratively up.

Default no gmpls

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

gmpls

Syntax **gmpls** [**lsp** *lsp-name*] [**sender** *sender-address*] [**endpoint** *endpoint-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**peer** *peer-node-id*]
no gmpls

Context **[Tree]** (debug>router gmpls)

Full Context debug router gmpls

Description This command enables and configures debugging for GMPLS.

The **no** form of the command disables debugging for GMPLS.

Parameters *lsp-name* — Debug all GMPLS instances that contain the specified LSP. 80 characters max.

sender-address — Debug all GMPLS instances that contain the specified sender IP address, in dotted decimal notation.

Values a.b.c.d

endpoint-address — Debug all GMPLS instances that contain the specified endpoint IP address, in dotted decimal notation.

Values a.b.c.d

tunnel-id — Debug all GMPLS instances that contain the specified identifier of a tunnel.

Values 0 to 4294967295

lsp-id — Debug all GMPLS instances that contain the specified identifier of an LSP.

Values 1 to 65535

peer-node-id — Debug all GMPLS instances that contain the specified identifier or IP address of a peer node.

Values 1 to 4294967295 | a.b.c.d

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.24 gmpls-loopback-address

gmpls-loopback-address

Syntax **gmpls-loopback-address** *ip-address*
no gmpls-loopback-address

Context **[Tree]** (config>router>lmp gmpls-loopback-address)

Full Context configure router lmp gmpls-loopback-address

Description This command specifies the GMPLS Loopback Address to be used by LMP. A corresponding **gmpls-loopback** interface must have been configured for LMP to be enabled.

Default no gmpls-loopback-address

Parameters *ip-address* — Specifies an IPv4 address.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

gmpls-loopback-address

Syntax **gmpls-loopback-address** *ipv4-address*
no gmpls-loopback-address

Context **[Tree]** (config>router>lmp>peer>control-channel-router gmpls-loopback-address)

Full Context configure router lmp peer control-channel-router gmpls-loopback-address

Description This command configures a loopback address to refer to the GMPLS loopback IP interface configured within the control channel router.

The **no** form of the command removes the configured loopback address.

Default no gmpls-loopback-address

Parameters *ipv4-address* — Specifies an IPv4 address.

Values a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.25 gmpls-tun-grp

gmpls-tun-grp

Syntax [**no**] **gmpls-tun-grp** *gmpls-tunnel-group-id*

Context **[Tree]** (config gmpls-tun-grp)

Full Context configure gmpls-tun-grp

Description This command configures a GMPLS tunnel group. A GMPLS tunnel group is a bundle of GMPLS LSPs providing an abstraction of the data bearers that are intended to be associated to one IP interface. This object allows, for example, end-to-end load balancing across the set of data bearers corresponding to a set of gLSPs. A gLSP is bound to an overlay tunnel group by a gLSP tunnel name at both the head end and the tail end UNI-C nodes of a gLSP. A sender-address may be optionally configured for the tail end of a gLSP in case overlapping GMPLS LSP tunnel names are used by different head end nodes.

The **no** form of this command removes the tunnel group. All members of a GMPLS tunnel group must be removed and the tunnel group shutdown before the tunnel group can be deleted.

Default no gmpls-tun-grp

Parameters *gmpls-tunnel-group-id* — Specifies the identifier of the GMPLS tunnel group.

Values 1 to 1024

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.26 gnmi

gnmi

Syntax **gnmi**

Context **[Tree]** (config>system>grpc gnmi)

Full Context configure system grpc gnmi

Description Commands in this context configure a gNMI service on gRPC.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.27 gnmi-capabilities

gnmi-capabilities

Syntax **gnmi-capabilities** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnmi-capabilities)

Full Context configure system security profile grpc rpc-authorization gnmi-capabilities

Description This command permits the use of Capability RPC for a user associated with the given format.

The **no** form of this command reverts to the default value.

Default gnmi-capabilities permit

Parameters **permit** — Specifies that the use of the Capability RPC is permitted.

deny — Specifies that the use of the Capability RPC is denied.

Platforms All

11.28 gnmi-get

gnmi-get

Syntax **gnmi-get** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnmi-get)

Full Context configure system security profile grpc rpc-authorization gnmi-get

Description This command permits the use of Get RPC.

The **no** form of this command reverts to the default value.

Default gnmi-get permit

Parameters **permit** — Specifies that the use of the Get RPC is permitted.

deny — Specifies that the use of the Get RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.29 gnmi-set

gnmi-set

Syntax **gnmi-set** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnmi-set)

Full Context configure system security profile grpc rpc-authorization gnmi-set

Description This command permits the use of Set RPC.

The **no** form of this command reverts to the default value.

Default gnmi-set permit

Parameters **permit** — Specifies that the use of the Set RPC is permitted.

deny — Specifies that the use of the Set RPC is denied.

Platforms All

11.30 gnmi-subscribe

gnmi-subscribe

Syntax **gnmi-subscribe** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnmi-subscribe)

Full Context configure system security profile grpc rpc-authorization gnmi-subscribe

Description This command permits the use of Subscribe RPC.

The **no** form of this command reverts to the default value.

Default gnmi-subscribe permit

Parameters **permit** — Specifies that the use of the Subscribe RPC is permitted.

deny — Specifies that the use of the Subscribe RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.31 gnoi-cert-mgmt-cangenerate

gnoi-cert-mgmt-cangenerate

Syntax **gnoi-cert-mgmt-cangenerate** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-cert-mgmt-cangenerate)

Full Context configure system security profile grpc rpc-authorization gnoi-cert-mgmt-cangenerate

Description This command permits the use of gNOI CanGenerateCSR RPCs for the user profile.

The **no** form of this command reverts to the default value.

Default gnoi-cert-mgmt-cangenerate deny

Parameters **permit** — Specifies that the use of the gNOI CanGenerateCSR RPCs for the user profile is permitted.

deny — Specifies that the use of the gNOI CanGenerateCSR RPCs for the user profile is denied.

Platforms All

11.32 gnoi-cert-mgmt-getcert

gnoi-cert-mgmt-getcert

Syntax **gnoi-cert-mgmt-getcert** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-cert-mgmt-getcert)

Full Context configure system security profile grpc rpc-authorization gnoi-cert-mgmt-getcert

Description This command permits the use of gNOI GetCertificate RPCs for the user profile.

The **no** form of this command reverts to the default value.

Default gnoi-cert-mgmt-getcert deny

Parameters **permit** — Specifies that the use of the gNOI GetCertificate RPCs for the user profile is permitted.

deny — Specifies that the use of the gNOI GetCertificate RPCs for the user profile is denied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

11.33 gnoi-cert-mgmt-install

gnoi-cert-mgmt-install

Syntax **gnoi-cert-mgmt-install** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-cert-mgmt-install)

Full Context configure system security profile grpc rpc-authorization gnoi-cert-mgmt-install

Description This command permits the use of gNOI Install RPCs for the user profile.

The **no** form of this command reverts to the default value.

Default gnoi-cert-mgmt-install deny

Parameters **permit** — Specifies that the use of the gNOI Install RPCs for the user profile is permitted.

deny — Specifies that the use of the gNOI Install RPCs for the user profile is denied.

Platforms All

11.34 gnoi-cert-mgmt-revoke

gnoi-cert-mgmt-revoke

Syntax **gnoi-cert-mgmt-revoke** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-cert-mgmt-revoke)

Full Context configure system security profile grpc rpc-authorization gnoi-cert-mgmt-revoke

Description This command permits or denies the use of gNOI RevokeCertificates RPCs for the user profile.

The **no** form of this command reverts to the default value.

Default gnoi-cert-mgmt-revoke deny

Parameters **permit** — Specifies that the use of gNOI RevokeCertificates RPCs for the user profile is permitted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

deny — Specifies that the use of gNOI RevokeCertificates RPCs for the user profile is denied.

Platforms All

11.35 gnoi-cert-mgmt-rotate

gnoi-cert-mgmt-rotate

Syntax **gnoi-cert-mgmt-rotate** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-cert-mgmt-rotate)

Full Context configure system security profile grpc rpc-authorization gnoi-cert-mgmt-rotate

Description This command permits the use of gNOI Rotate RPCs for the user profile.

Default gnoi-cert-mgmt-rotate deny

Parameters **permit** — Specifies that the use of the gNOI Rotate RPCs for the user profile is permitted.

deny — Specifies that the use of the gNOI Rotate RPCs for the user profile is denied.

Platforms All

11.36 gnoi-file-get

gnoi-file-get

Syntax **gnoi-file-get** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-file-get)

Full Context configure system security profile grpc rpc-authorization gnoi-file-get

Description This command permits the use of gNOI File Get RPC for a file from a target location.

Default gnoi-file-get permit

Parameters **permit** — Specifies that the use of the gNOI File Get RPC is permitted.

deny — Specifies that the use of the gNOI File Get RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.37 gnoi-file-put

gnoi-file-put

Syntax **gnoi-file-put** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-file-put)

Full Context configure system security profile grpc rpc-authorization gnoi-file-put

Description This command permits the use of gNOI File Put RPC to write to a file on a target location.

Default gnoi-file-put permit

Parameters **permit** — Specifies that the use of the gNOI File Put RPC is permitted.

deny — Specifies that the use of the gNOI File Put RPC is denied.

Platforms All

11.38 gnoi-file-remove

gnoi-file-remove

Syntax **gnoi-file-remove** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-file-remove)

Full Context configure system security profile grpc rpc-authorization gnoi-file-remove

Description This command permits the use of gNOI File Remove RPC to remove a file from the specified target location.

Default gnoi-file-remove permit

Parameters **permit** — Specifies that the use of the gNOI File Remove RPC is permitted.

deny — Specifies that the use of the gNOI File Remove RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.39 gnoi-file-stat

gnoi-file-stat

Syntax **gnoi-file-stat** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-file-stat)

Full Context configure system security profile grpc rpc-authorization gnoi-file-stat

Description This command permits the use of gNOI File Stat RPC to retrieve metadata for a file from the specified target location.

Default gnoi-file-stat permit

Parameters **permit** — Specifies that the use of the gNOI File Stat RPC is permitted.

deny — Specifies that the use of the gNOI File Stat RPC is denied.

Platforms All

11.40 gnoi-file-transfertoremote

gnoi-file-transfertoremote

Syntax **gnoi-file-transfertoremote** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-file-transfertoremote)

Full Context configure system security profile grpc rpc-authorization gnoi-file-transfertoremote

Description This command permits the use of the gNOI File TransferToRemote RPC to transfer the file from the target node to a specified remote location.

Default gnoi-file-transfertoremote permit

Parameters **permit** — Specifies that the use of the gNOI File TransferToRemote RPC is permitted.

deny — Specifies that the use of the gNOI File TransferToRemote RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.41 gnoi-system-cancelreboot

gnoi-system-cancelreboot

Syntax **gnoi-system-cancelreboot** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-cancelreboot)

Full Context configure system security profile grpc rpc-authorization gnoi-system-cancelreboot

Description This command permits the use of gNOI System CancelReboot RPC for a user-given profile.

Default gnoi-system-cancelreboot deny

Parameters **permit** — Specifies that the use of gNOI System CancelReboot RPC is permitted.

deny — Specifies that the use of gNOI System CancelReboot RPC is denied.

Platforms All

11.42 gnoi-system-ping

gnoi-system-ping

Syntax **gnoi-system-ping** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-ping)

Full Context configure system security profile grpc rpc-authorization gnoi-system-ping

Description This command permits the use of the gNOI Ping RPC to execute the ping command on the target node and stream back the results.

Default gnoi-system-ping permit

Parameters **permit** — Specifies that the use of the gNOI Ping RPC is permitted.

deny — Specifies that the use of the gNOI Ping RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.43 gnoi-system-reboot

gnoi-system-reboot

Syntax **gnoi-system-reboot** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-reboot)

Full Context configure system security profile grpc rpc-authorization gnoi-system-reboot

Description This command permits the use of gNOI System Reboot RPC for a user-given profile.

The **no** form of this command reverts to the default value.

Default gnoi-system-reboot deny

Parameters **permit** — Specifies that the use of gNOI System Reboot RPC is permitted.

deny — Specifies that the use of gNOI System Reboot RPC is denied.

Platforms All

11.44 gnoi-system-rebootstatus

gnoi-system-rebootstatus

Syntax **gnoi-system-rebootstatus** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-rebootstatus)

Full Context configure system security profile grpc rpc-authorization gnoi-system-rebootstatus

Description This command permits the use of gNOI System RebootStatus RPC for a user-given profile.

The **no** form of this command reverts to the default value.

Default gnoi-system-rebootstatus deny

Parameters **permit** — Specifies that the use of gNOI System RebootStatus RPC is permitted for a user-given profile.

deny — Specifies that the use of gNOI System RebootStatus RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.45 gnoi-system-setpackage

gnoi-system-setpackage

Syntax **gnoi-system-setpackage** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-setpackage)

Full Context configure system security profile grpc rpc-authorization gnoi-system-setpackage

Description This command permits the use of gNOI System SetPackage RPC for a user-given profile.

The **no** form of this command reverts to the default value.

Default gnoi-system-setpackage deny

Parameters **deny** — Specifies that the use of gNOI System SetPackage RPC is denied.

permit — Specifies that the use of gNOI System SetPackage RPC is permitted.

Platforms All

11.46 gnoi-system-switchcontrolprocessor

gnoi-system-switchcontrolprocessor

Syntax **gnoi-system-switchcontrolprocessor** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-switchcontrolprocessor)

Full Context configure system security profile grpc rpc-authorization gnoi-system-switchcontrolprocessor

Description This command permits the use of gNOI System SwitchControlProcessor RPC for a user-given profile.

The **no** form of this command reverts to the default value.

Default gnoi-system-switchcontrolprocessor deny

Parameters **deny** — Specifies that the use of gNOI System SwitchControlProcessor RPC is denied.

permit — Specifies that the use of gNOI System SwitchControlProcessor RPC is permitted.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.47 gnoi-system-time

gnoi-system-time

Syntax **gnoi-system-time** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-time)

Full Context configure system security profile grpc rpc-authorization gnoi-system-time

Description This command permits the use of the gNOI Time RPC to return the current time on the target node.

Default gnoi-system-time permit

Parameters **permit** — Specifies that the use of the gNOI Time RPC is permitted.

deny — Specifies that the use of the gNOI Time RPC is denied.

Platforms All

11.48 gnoi-system-traceroute

gnoi-system-traceroute

Syntax **gnoi-system-traceroute** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization gnoi-system-traceroute)

Full Context configure system security profile grpc rpc-authorization gnoi-system-traceroute

Description This command permits the use of the gNOI Traceroute RPC to execute the traceroute command on the target node and stream back the results.

Default gnoi-system-traceroute permit

Parameters **permit** — Specifies that the use of the gNOI Traceroute RPC is permitted.

deny — Specifies that the use of the gNOI Traceroute RPC is denied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.49 goto

goto

Syntax **goto** *line*

Context **[Tree]** (candidate goto)

Full Context candidate goto

Description This command changes the edit point of the candidate configuration. The edit point is the point after which new commands are inserted into the candidate configuration as an operator navigates the CLI and issues commands in edit-cfg mode.

Parameters **line** — Indicates which line to change starting at the point indicated by the following options.

Values

line, offset, **first**, **edit-point**, **last**

line	absolute line number
offset	relative line number to current edit point. Prefixed with '+' or '-'
first	keyword - first line
edit-point	keyword - current edit point
last	keyword - last line that is not 'exit'

11.50 gprs-negotiated-qos-profile

gprs-negotiated-qos-profile

Syntax [**no**] **gprs-negotiated-qos-profile**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute gprs-negotiated-qos-profile)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute gprs-negotiated-qos-profile

Description This command enables the inclusion of the 3GPP QoS specification in AAA protocols as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.51 gr-helper

gr-helper

Syntax **gr-helper** [**enable** | **disable**]

Context **[Tree]** (config>router>rsvp>if gr-helper)

Full Context configure router rsvp interface gr-helper

Description This command enables the RSVP Graceful Restart Helper feature.

The RSVP-TE Graceful Restart helper mode allows the SR OS based system (the helper node) to provide another router that has requested it (the restarting node) a grace period, during which the system will continue to use RSVP sessions to neighbors requesting the grace period. This is typically used when another router is rebooting its control plane but its forwarding plane is expected to continue to forward traffic based on the previously available Path and Resv states.

The user can enable Graceful Restart helper on each RSVP interface separately. When the GR helper feature is enabled on an RSVP interface, the node starts inserting a new Restart_Cap Object in the Hello packets to its neighbor. The restarting node does the same and indicates to the helper node the desired Restart Time and Recovery Time.

The GR Restart helper consists of a couple of phases. Once it loses Hello communication with its neighbor, the helper node enters the Restart phase. During this phase, it preserves the state of all RSVP sessions to its neighbor and waits for a new Hello message.

Once the Hello message is received indicating the restarting node preserved state, the helper node enters the recovery phase in which it starts refreshing all the sessions that were preserved. The restarting node will activate all the stale sessions that are refreshed by the helper node. Any Path state which did not get a Resv message from the restarting node once the Recovery Phase time is over is considered to have expired and is deleted by the helper node causing the proper Path Tear generation downstream.

The duration of the restart phase (recovery phase) is equal to the minimum of the neighbor's advertised Restart Time (Recovery Time) in its last Hello message and the locally configured value of the max-restart (max-recovery) parameter.

When GR helper is enabled on an RSVP interface, its procedures apply to the state of both P2P and P2MP RSVP LSP to a neighbor over this interface.

Default disable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.52 gr-helper-time

gr-helper-time

Syntax **gr-helper-time max-recovery** *recovery-interval* **max-restart** *restart-interval*
no gr-helper-time

Context **[Tree]** (config>router>gmpls gr-helper-time)

Full Context configure router gmpls gr-helper-time

Description This command configures the local values for the max-recovery and the max-restart intervals used in the RSVP Graceful Restart Helper feature when applied to a GMPLS UNI.

The values are configured globally in GMPLS.

The **no** version of this command re-instates the default value for the delay timer.

Default gr-helper-time max-recovery 300 max-restart 180

Parameters *recovery-interval* — Specifies the maximum recovery interval value, in s.

Values 1 to 1800

restart-interval — Specifies the maximum restart interval value, in s.

Values 1 to 300

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

gr-helper-time

Syntax **gr-helper-time max-recovery** *recovery-interval* **max-restart** *restart-interval*
no gr-helper-time

Context **[Tree]** (config>router>rsvp gr-helper-time)

Full Context configure router rsvp gr-helper-time

Description This command configures the local values for the max-recovery and the max-restart intervals used in the RSVP Graceful Restart Helper feature.

The values are configured globally in RSVP but separate instances of the timers are applied to each RSVP interface that has the RSVP Graceful Restart Helper enabled.

The **no** version of this command re-instates the default value for the delay timer.

Default gr-helper-time max-recovery 300 max-restart 120

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *recovery-interval* — Specifies the max recovery interval value in seconds.

Values 1 to 1800

restart-interval — Specifies the max restart interval value in seconds.

Values 1 to 300

Platforms All

11.53 grace

grace

Syntax **grace**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep grace)
[Tree] (config>eth-tunnel>path>eth-cfm>mep grace)
[Tree] (config>lag>eth-cfm>mep grace)
[Tree] (config>port>ethernet>eth-cfm>mep grace)

Full Context configure eth-ring path eth-cfm mep grace
configure eth-tunnel path eth-cfm mep grace
configure lag eth-cfm mep grace
configure port ethernet eth-cfm mep grace

Description Commands in this context configure Nokia ETH-CFM Grace and ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

grace

Syntax **grace**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep grace)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep grace)
[Tree] (config>service>ipipe>sap>eth-cfm>mep grace)

Full Context configure service epipe sap eth-cfm mep grace
configure service epipe spoke-sdp eth-cfm mep grace
configure service ipipe sap eth-cfm mep grace

Description Commands in this context configure Nokia ETH-CFM Grace and ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

grace

Syntax **grace**

Context **[Tree]** (config>service>vpls>eth-cfm>mep grace)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep grace)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep grace)
[Tree] (config>service>vpls>sap>eth-cfm>mep grace)

Full Context configure service vpls eth-cfm mep grace
configure service vpls mesh-sdp eth-cfm mep grace
configure service vpls sap eth-cfm mep grace
configure service vpls spoke-sdp eth-cfm mep grace

Description Commands in this context configure Nokia ETH-CFM Grace and ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

grace

Syntax **grace**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep grace)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep grace)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep grace)

Full Context configure service ies interface sap eth-cfm mep grace
configure service ies interface spoke-sdp eth-cfm mep grace
configure service ies subscriber-interface group-interface sap eth-cfm mep grace

Description Commands in this context configure Nokia ETH-CFM Grace and ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep grace
- configure service ies interface sap eth-cfm mep grace

grace

Syntax **grace**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep grace)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep grace)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep grace)

Full Context configure service vprn interface sap eth-cfm mep grace
configure service vprn interface spoke-sdp eth-cfm mep grace
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace

Description Commands in this context configure Nokia ETH-CFM Grace and ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm mep grace
- configure service vprn interface spoke-sdp eth-cfm mep grace

grace

Syntax **grace**

Context [Tree] (config>router>if>eth-cfm>mep grace)

Full Context configure router interface eth-cfm mep grace

Description Commands in this context configure Nokia ETH-CFM Grace and ITU-T Y.1731 ETH-ED expected defect functional parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.54 grace-tx-enable

grace-tx-enable

Syntax [**no**] **grace-tx-enable**

Context [Tree] (config>system>ethernet>efm-oam grace-tx-enable)
[Tree] (config>port>ethernet>efm-oam grace-tx-enable)

Full Context configure port ethernet efm-oam grace-tx-enable
configure system ethernet efm-oam grace-tx-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Enables the sending of grace for all the enabled EFM-OAM sessions on the node. Disabled by default at the system level and enabled by default at the port level. The combination of the system level and port level configuration will determine if the grace function is enabled on the individual ports. Both the system level and the port level must be enabled in order to support grace on a specific port. If either level is disabled, grace is not enabled on those ports. Enabling grace during an active ISSU or soft reset does not invoke the grace function for the active event.

When both **grace-tx-enable** and **config>system>ethernet>efm-oam dying-gasp-tx-on-reset**, **config>port>ethernet>efm-oam dying-gasp-tx-on-reset** are active on the same port, **grace-tx-enable** takes precedence when a soft reset is invoked if the Peer Vendor OUI being received is 00:16:4d (ALU) or the configured **config>port>ethernet>efm-oam grace-vendor-oui** value. The **grace-tx-enable** command should not be configured if the Nokia Vendor Specific Grace TLV is not supported on the remote peer.

The **no** form of this command disables the sending of the Nokia Vendor Specific Grace TLV.

Default config>system>ethernet>efm-oam>no grace-tx-enable

config>port>ethernet>efm-oam>grace-tx-enable

Platforms All

grace-tx-enable

Syntax [**no**] **grace-tx-enable**

Context **[Tree]** (config>eth-cfm>system grace-tx-enable)

Full Context configure eth-cfm system grace-tx-enable

Description This command enables ETH-CFM grace transmission at the system level when a soft reset message is received and processed by the ETH-CFM module. Individual MEP configuration determines which of the two supported grace functions, ETH-VSM or ETH-ED, is used to announce grace.

This command controls the overall capability to transmit grace and does not control which grace announcement to use. This command also has no impact on the reception and processing of grace-style PDUs.

The **no** form of this command disables ETH-CFM grace transmission at the system level.

Default grace-tx-enable

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.55 grace-vendor-oui

grace-vendor-oui

Syntax **grace-vendor-oui** *oui*
no grace-vendor-oui

Context **[Tree]** (config>port>ethernet>efm-oam grace-vendor-oui)

Full Context configure port ethernet efm-oam grace-vendor-oui

Description This optional command configures an additional peer vendor OUI which indicates support for the Vendor Specific EFM-OAM Grace functionality, allowing grace to be preferred over dying gasp when both are configured. This is in addition to the Nokia Vendor OUI 00:16:4d.

When both **grace-tx-enable (config>system>ethernet>efm-oam grace-tx-enable**, **config>port>ethernet>efm-oam grace-tx-enable)** and **dying-gasp-tx-on-reset (config>system>ethernet>efm-oam dying-gasp-tx-on-reset**, **config>port>ethernet>efm-oam dying-gasp-tx-on-reset)** are active on the same port, **grace-tx-enable** takes precedence when a soft reset is invoked if the Peer Vendor OUI being received is 00:16:4d (ALU) or the configured **grace-vendor-oui** value. The **grace-tx-enable** command should not be configured if the Nokia Vendor Specific Grace TLV is not supported on the remote peer, including Nokia 7750 SR equipment prior to release 11.0 R4.

The **no** form of this command removes the additional Vendor OUI but does not remove the Nokia 00:16:4d value.

Default no grace-vendor-oui

Parameters *oui* — Hex value in the range 00:00:00 to FF:FF:FF.

Platforms All

11.56 graceful-restart

graceful-restart

Syntax [**no**] **graceful-restart**

Context **[Tree]** (config>service>vprn>bgp graceful-restart)
[Tree] (config>service>vprn>bgp>group graceful-restart)
[Tree] (config>service>vprn>bgp>group>neighbor graceful-restart)

Full Context configure service vprn bgp graceful-restart
configure service vprn bgp group graceful-restart

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group neighbor graceful-restart

Description This command enables BGP graceful restart helper procedures (the “receiving router” role defined in the standard) for address families included in the GR capabilities of both peers. In a VPRN, SR OS can support GR helper functionality for IPv4, IPv6, label-ipv4, flow-ipv4 (IPv4 FlowSpec) and flow-ipv6 (IPv6 FlowSpec) routes.

When a neighbor covered by the GR helper mode restarts its control plane, forwarding can continue uninterrupted while the session is re-established and routes are re-learned.

The **no** form of this command disables graceful restart.

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context **[Tree]** (config>service>vprn>isis graceful-restart)

Full Context configure service vprn isis graceful-restart

Description This command enables IS-IS graceful restart (GR) to minimize service interruption. When the control plane of a GR-capable router fails or restarts, the neighboring routers (GR helpers) temporarily preserve IS-IS forwarding information. Traffic continues to be forwarded to the restarting router using the last known forwarding tables. If the control plane of the restarting router becomes operationally and administratively up within the grace period, the restarting router resumes normal IS-IS operation. If the grace period expires, then the restarting router is presumed inactive and the IS-IS topology is recalculated to route traffic around the failure.

The **no** form of this command disables graceful restart and removes the graceful restart configuration from the IS-IS instance.

Default no graceful-restart

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context **[Tree]** (config>service>vprn>ospf graceful-restart)
[Tree] (config>service>vprn>ospf3 graceful-restart)

Full Context configure service vprn ospf graceful-restart
configure service vprn ospf3 graceful-restart

Description This command enables OSPF graceful restart (GR) to minimize service interruption.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the control plane of a GR-capable router fails or restarts, the neighboring routers (GR helpers) temporarily preserve OSPF forwarding information. Traffic continues to be forwarded to the restarting router using the last known forwarding tables. If the control plane of the restarting router becomes operationally and administratively up within the grace period, the restarting router resumes normal OSPF operation. If the grace period expires, the restarting router is presumed inactive and the OSPF topology is recalculated to route traffic around the failure.

The **no** form of this command disables GR and removes the GR configuration from the OSPF instance.

Default no graceful-restart

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context **[Tree]** (config>router>ldp graceful-restart)

Full Context configure router ldp graceful-restart

Description This command enables graceful restart helper.

The **no** form of this command disables graceful restart.

Graceful restart helper configuration changes, enable/disable, or change of a parameter will cause the LDP session to bounce.

Default no graceful-restart (disabled) — Graceful-restart must be explicitly enabled.

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context **[Tree]** (config>router>bgp graceful-restart)
[Tree] (config>router>bgp>group graceful-restart)
[Tree] (config>router>bgp>group>neighbor graceful-restart)

Full Context configure router bgp graceful-restart
configure router bgp group graceful-restart
configure router bgp group neighbor graceful-restart

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables BGP graceful restart helper procedures (the “receiving router” role defined in the standard) for address families included in the GR capabilities of both peers. SR OS can support GR helper functionality for IPv4, IPv6, VPN-IPv4, VPN-IPv6, Label-IPv4, Label-IPv6, L2-VPN, Route-Target (RTC), Flow-IPv4 (IPv4 FlowSpec) and Flow-IPv6 (IPv6 FlowSpec) routes.

If a neighbor covered by the GR helper mode restarts its control plane, forwarding can continue uninterrupted while the session is re-established and routes are re-learned.

The **no** form of this command disables graceful restart.

Default no graceful-restart

Platforms All

graceful-restart

Syntax **graceful-restart** [**neighbor** *ip-address* | **group** *name*]
no graceful-restart

Context **[Tree]** (debug>router>bgp graceful-restart)

Full Context debug router bgp graceful-restart

Description This command enables debugging for BGP graceful restart.

The **no** form of this command disables the debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis graceful-restart)

Full Context configure router isis graceful-restart

Description This command enables IS-IS graceful restart (GR) to minimize service interruption. When the control plane of a GR-capable router fails or restarts, the neighboring routers (GR helpers) temporarily preserve IS-IS forwarding information. Traffic continues to be forwarded to the restarting router using the last known forwarding tables. If the control plane of the restarting router becomes operationally and administratively up within the grace period, the restarting router resumes normal IS-IS operation. If the grace period expires, then the restarting router is presumed inactive and the IS-IS topology is recalculated to route traffic around the failure.

The **no** form of this command disables graceful restart and removes the graceful restart configuration from the IS-IS instance.

Default no graceful-restart

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context [Tree] (debug>router>isis graceful-restart)

Full Context debug router isis graceful-restart

Description This command enables debugging for IS-IS graceful-restart.

The **no** form of the command disables debugging.

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context [Tree] (config>router>ospf graceful-restart)
[Tree] (config>router>ospf3 graceful-restart)

Full Context configure router ospf graceful-restart
configure router ospf3 graceful-restart

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables OSPF graceful restart (GR) to minimize service disruption. When the control plane of a GR-capable router fails or restarts, the neighboring routers (GR helpers) temporarily preserve OSPF forwarding information. Traffic continues to be forwarded to the restarting router using the last known forwarding tables. If the control plane of the restarting router comes back up within the grace period, the restarting router resumes normal OSPF operation. If the grace period expires, then the restarting router is presumed inactive and the OSPF topology is recalculated to route traffic around the failure.

The **no** form of this command disables graceful restart and removes the graceful restart configuration from the OSPF instance.

Default no graceful-restart

Platforms All

graceful-restart

Syntax [**no**] **graceful-restart**

Context **[Tree]** (debug>router>ospf graceful-restart)
[Tree] (debug>router>ospf3 graceful-restart)

Full Context debug router ospf graceful-restart
debug router ospf3 graceful-restart

Description This command enables debugging for OSPF and OSPF3 graceful restart.

Platforms All

11.57 graceful-shutdown

graceful-shutdown

Syntax [**no**] **graceful-shutdown**

Context **[Tree]** (config>router>rsvp graceful-shutdown)
[Tree] (config>router>rsvp>interface graceful-shutdown)

Full Context configure router rsvp graceful-shutdown
configure router rsvp interface graceful-shutdown

Description This command initiates a graceful shutdown of the specified RSVP interface or all RSVP interfaces on the node if applied at the RSVP level. These are referred to as maintenance interface and maintenance node, respectively.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To initiate a graceful shutdown the maintenance node generates a PathErr message with a specific error sub-code of Local Maintenance on TE Link required for each LSP that is exiting the maintenance interface.

The node performs a single make-before-break attempt for all adaptive CSPF LSPs it originates and LSP paths using the maintenance interfaces. If an alternative path for an affected LSP is not found, then the LSP is maintained on its current path. The maintenance node also tears down and re-signals any detour LSP path using listed maintenance interfaces as soon as they are not active.

The maintenance node floods an IGP TE LSA/LSP containing Link TLV for the links under graceful shutdown with TE metric set to 0xffffffff and Unreserved Bandwidth parameter set to zero (0).

A head-end LER node, upon receipt of the PathErr message performs a single make-before-break attempt on the affected adaptive CSPF LSP. If an alternative path is not found, then the LSP is maintained on its current path.

A node does not take any action on the paths of the following originating LSPs after receiving the PathErr message:

a. An adaptive CSPF LSP for which the PathErr indicates a node address in the address list and the node corresponds to the destination of the LSP. In this case, there are no alternative paths which can be found.

b. An adaptive CSPF LSP whose path has explicit hops defined using the listed maintenance interface(s)/node(s).

c. A CSPF LSP with the adaptive option disabled and which current path is over the listed maintenance interfaces in the PathErr message. These are not subject to make-before-break.

d. A non CSPF LSP which current path is over the listed maintenance interfaces in the PathErr message.

The head-end LER node upon receipt of the updates IPG TE LSA/LSP for the maintenance interfaces updates the TE database. This information will be used at the next scheduled CSPF computation for any LSP which path may traverse any of the maintenance interfaces.

The **no** form of this command disables the graceful shutdown operation at the RSVP interface level or at the RSVP level. The configured TE parameters of the maintenance links are restored and the maintenance node floods the links.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.58 grafts

grafts

Syntax **grafts** [**source** *ip-address*] [**group** *grp-ip-address*] [**detail**]
no grafts

Context **[Tree]** (debug>router>pim grafts)

Full Context debug router pim grafts

Description This command enables debugging for PIM grafts.

The **no** form of this command disables PIM graft debugging.

Parameters *ip-address* — Debugs graft information associated with the specified source.

Values source address (ipv4, ipv6)

grp-ip-address — Debugs graft information associated with the specified group.

Values multicast group address (ipv4, ipv6)

detail — Debugs detailed graft information.

11.59 granularity

granularity

Syntax **granularity** {**percent** *percent-of-admin-pir* | **rate** *rate-in-kilobits-per-second*}
no granularity

Context **[Tree]** (config>qos>adv-config-policy>child-control>bandwidth-distribution granularity)

Full Context configure qos adv-config-policy child-control bandwidth-distribution granularity

Description This command is used to create a step-like behavior where the operational PIR will round up to the nearest increment of the specified granularity before being applied to the child. The only exception is when the distributed bandwidth is less than 1% above a lower step value, in which case the lower step value is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This step-like behavior may be useful when the bandwidth used by an active child is well known. While the **above-offered-cap** command automatically adds a specified amount to the operational PIR of a child, the **granularity** command only increments the operational PIR to the next step value. While not expected to be used in conjunction, the **above-offered-cap** and **granularity** commands may be used simultaneously, in which case the above-offered-cap increase will be applied first, followed by the granularity rounding to the next step value.

If the **granularity** command is used with a percent-based value, the rounding up function of the configured PIR value on the policer or queue is based on the child's administrative PIR. In this case, care should be taken that the child is either configured with an explicit PIR rate (other than max) or the child's administrative PIR is defined using the percent-rate command with the local parameter enabled if an explicit value is not desired. When a maximum PIR is in use on the child, the system attempts to interpret the maximum child forwarding rate. This rate could be very large if the child is associated with multiple ingress or egress ports.

If the child's administrative PIR is modified while a percent-based granularity is in effect, the system automatically uses the new relative rounding value the next time the child's operational PIR is determined.

When this command is not specified or removed, the system makes no attempt to round up the child's determined operational PIR.

The **no** form of this command is used to remove the operational PIR rounding behavior from all child policers and queues associated with the policy.

Parameters *percent-of-admin-pir* — When the percent qualifier is used, the following percent-of-admin-pir parameter specifies the percentage of the child's administrative PIR that should be used as the rounding step value. If a value of 0 or 0.00 is used, the system will interpret this equivalent to no granularity.

Values 0.00 to 100.00

rate-in-kilobits-per-second — When the rate qualifier is used, the following rate-in-kilobits-per-second parameter specifies an explicit rate, in kb/s, that should be used as the child's rounding step value. If a rate step of 0 is specified, the system interprets this equivalent to no granularity.

Values 0 to 100,000,000

Platforms All

granularity

Syntax **granularity** {**percent** *percent-of-admin-pir* | **rate** *rate-in-kilobits-per-second*}
no granularity

Context **[Tree]** (config>qos>adv-config-policy>child-control>offered-measurement granularity)

Full Context configure qos adv-config-policy child-control offered-measurement granularity

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to adjust the sensitivity of the virtual scheduler to changes in the child offered rate. As the child offered rate is determined, it is compared to the previous offered rate. If the delta does not exceed the sensitivity threshold determined for the current offered rate, the change in offered rate is ignored for that iteration.

While it is assumed that changing the offered rate change sensitivity will be a rare occurrence, it may be prudent to react to smaller changes in the offered rate of a particular child policer or queue. Another possible reason for changing the sensitivity is that it may be desired to lower the impact of changes in offered rate on the virtual scheduler for a particular child by raising the granularity.

A side effect of higher sensitivity (lower granularity) is that the virtual scheduler may need to adjust the distributed bandwidth between all children more often, resulting in the possibility of lowering resources available to other virtual scheduler instances on the slot.

A side effect of lower sensitivity (higher granularity) is that the parent virtual scheduler may distribute insufficient bandwidth to the child resulting in dropped packets.

If the granularity command is used with a percent-based value, the sensitivity is a function of the configured PIR value on the policer or queue. In this case, care should be taken that the child is either configured with an explicit PIR rate (other than max) or the child's administrative PIR is defined using the percent-rate command with the local parameter enabled if an explicit value is not desired. When a maximum PIR is in use on the child, the system attempts to interpret the maximum child forwarding rate. This rate could be very large if the child is associated with multiple ingress or egress ports.

Except for the overall cap on the offered input into the virtual scheduler, the child's administrative PIR has no effect on the calculated sensitivity if an explicit rate is specified.

If the child's administrative PIR is modified while a percent-based granularity is in effect, the system automatically uses the new relative sensitivity value the next time the child's offered rate is determined.

The **no** form of this command is used to restore the default offered rate sensitivity behavior to all child policers and queues associated with the policy.

Parameters *percent-of-admin-pir* — When the percent qualifier is used, this parameter specifies the percentage of the child's administrative PIR that are used as the threshold sensitivity to offered rate change. If a value of 0 or 0.00 is used, the system will interpret this equivalent to no granularity.

Values 1.00 to 100.00

rate-in-kilobits-per-second — When the rate qualifier is used, this parameter specifies an explicit rate, in kb/s, that are used as the child's offered rate change sensitivity value. If a rate sensitivity of 0 is specified, the system interprets this equivalent to no granularity.

Values 0 to 100,000,000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.60 gratuitous-arp

gratuitous-arp

Syntax **gratuitous-arp {one-per-sap| one-per-outer-tag}**

Context **[Tree]** (config>subscr-mgmt>up-resiliency>fsg-template gratuitous-arp)

Full Context configure subscriber-mgmt up-resiliency fate-sharing-group-template gratuitous-arp

Description This command configures the granularity with which Gratuitous ARP packets are sent upon switchover events.

Parameters **one-per-sap** — Specifies to send a single GARP per SAP. The Sender Protocol Address is any subnet associated with the SAP. If no subnet is available, the system IP is used.

one-per-outer-tag — Specifies to send a single GARP for all q-in-q SAPs sharing the same outer tag. For dot1q SAPs this behaves the same as **one-per-sap**. The Sender Protocol Address is any subnet associated with the SAP. If no subnet is available, the system IP is used.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.61 gratuitous-rtr-adv

gratuitous-rtr-adv

Syntax [**no**] **gratuitous-rtr-adv**

Context **[Tree]** (config>service>ies>sub-if>ipoe-linking gratuitous-rtr-adv)
[Tree] (config>service>vprn>sub-if>ipoe-linking gratuitous-rtr-adv)
[Tree] (config>service>ies>sub-if>grp-if>ipoe-linking gratuitous-rtr-adv)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-linking gratuitous-rtr-adv)

Full Context configure service ies subscriber-interface group-interface ipoe-linking gratuitous-rtr-adv
configure service ies subscriber-interface ipoe-linking gratuitous-rtr-adv
configure service vprn subscriber-interface group-interface ipoe-linking gratuitous-rtr-adv
configure service vprn subscriber-interface ipoe-linking gratuitous-rtr-adv

Description This command enables the generation of unsolicited Router-advertisement on creation of v4 host.

The **no** form of this command disables **gratuitous-rtr-adv.**

Default gratuitous-rtr-adv

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.62 gre

gre

Syntax [**no**] **gre**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>type gre)

Full Context configure subscriber-mgmt wlan-gw tunnel-query type gre

Description This command enables matching on GRE tunnels.

The **no** form of this command disables matching on GRE tunnels, unless no other tunnel type specifier is configured.

Default no gre

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gre

Syntax [**no**] **gre**

Context **[Tree]** (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter gre)

Full Context configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter gre

Description This command enables setting the tunnel type for the auto bind tunnel.

The **gre** encapsulation of the MPLS service packet uses the base 4-byte header as per RFC 2890. The optional fields Checksum (plus Reserved field), Key, and Sequence Number are not inserted.

The **no** form of this command disables the setting the tunnel type for the auto bind tunnel.

Default no gre

Platforms All

gre

Syntax **gre**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>test-oam>build-packet>header gre)

Full Context configure test-oam build-packet header gre

Description This command creates a GRE header for inclusion in test OAM build packet instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.63 gre-eth-bridged

gre-eth-bridged

Syntax **gre-eth-bridged**

Context [Tree] (config>service>system gre-eth-bridged)

Full Context configure service system gre-eth-bridged

Description Commands in this context configure parameters related to termination of a GRE tunnel carrying Ethernet payload onto a PW port by using Forwarding Path Extensions (FPE).

Platforms All

11.64 gre-header

gre-header

Syntax **gre-header send-key** *send-key* **receive-key** *receive-key*
no gre-header

Context [Tree] (config>service>ies>if>sap>ip-tunnel gre-header)
[Tree] (config>service>vprn>if>sap>ip-tunnel gre-header)

Full Context configure service ies interface sap ip-tunnel gre-header
configure service vprn interface sap ip-tunnel gre-header

Description This command configures the type of the IP tunnel. If the **gre-header** command is configured then the tunnel is a GRE tunnel with a GRE header inserted between the outer and inner IP headers. If the **no** form of this command is configured then the tunnel is a simple IP-IP tunnel.

Default no gre-header

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **send-key** *send-key* — Specifies a 32-bit unsigned integer.

Values 0 to 4294967295

receive-key *receive-key* — Specifies a 32-bit unsigned integer.

Values 0 to 4294967295

Platforms All

11.65 gre-key

gre-key

Syntax **gre-key if-index**
no gre-key

Context **[Tree]** (config>filter>gre-tun-tmp>ipv4 gre-key)

Full Context configure filter gre-tunnel-template ipv4 gre-key

Description This command enables the population of the GRE key field in the GRE header sent with the encapsulated IP packet.

The **no** form of this command disables the population of the optional GRE key field when the matching IP packet is sent encapsulated in a GRE tunnel.

Parameters **if-index** — Causes the GRE key field to be populated with the ifIndex of the ingress interface on which the matching IP packet was received.

Platforms All

11.66 gre-termination

gre-termination

Syntax [**no**] **gre-termination**

Context **[Tree]** (config>router>if gre-termination)

Full Context configure router interface gre-termination

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the termination of MPLS-over-GRE and IP-over-GRE packets on destination IP addresses from a user-defined subnet. The user defines a subnet for the termination of GRE packets by applying the **gre-termination** command to a numbered network IP interface, including a loopback interface.

For more information, refer to “IP-over-GRE and MPLS-over-GRE Termination on a User-Configured Subnet” in the 7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide.

The **no** form of this command disables the termination of MPLS-over-GRE and IP-over-GRE packets on the subnet of the interface. Packets are dropped.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.67 gre-tunnel-template

gre-tunnel-template

Syntax **gre-tunnel-template** *name* [**create**]
no gre-tunnel-template *name*

Context **[Tree]** (config>filter gre-tunnel-template)

Full Context configure filter gre-tunnel-template

Description Commands in this context configure a GRE tunnel template parameters to be used to tunnel associated traffic.

The **no** form of this command removes the GRE tunnel template from the configuration.

Parameters *name* — Specifies a GRE tunnel template name up to 32 characters.

create — This keyword is required to create the configuration context. Once it is created, the context can be enabled with or without the **create** keyword.

Platforms All

11.68 group

group

Syntax **group** *name* [**create**]
no group *name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>hw-agg-shap-sched-plcy group)

Full Context configure qos hw-agg-shaper-scheduler-policy group

Description This command creates a group within a hardware aggregate shaper scheduler policy.

The **no** form of this command removes the group from the policy.

Parameters *name* — Specifies a group name, up to 32 characters.

Platforms 7750 SR-1, 7750 SR-s

group

Syntax **group** *tunnel-group-name* [**service-id** *service-id*]
no group

Context [Tree] (config>subscr-mgmt>loc-user-db>ppp>host>l2tp group)

Full Context configure subscriber-mgmt local-user-db ppp host l2tp group

Description This command configures the L2TP tunnel group. The tunnel-group-name is configured in the **config>router>l2tp** context. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*.

Parameters *tunnel-group-name* — Specifies an existing tunnel L2TP group, up to 63 characters.

service-id *service-id* — Specifies an existing service ID or service name.

Values *service-id*: 1 to 214748364
service-name: up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group

Syntax **group** *tunnel-group-name* [**create**]
group *tunnel-group-name* [**create**] [**protocol** *protocol*]
no group *tunnel-group-name*

Context [Tree] (config>router>l2tp group)
[Tree] (config>service>vprn>l2tp group)

Full Context configure router l2tp group
configure service vprn l2tp group

Description This command configures an L2TP tunnel group.

The **no** form of this command reverts removes the tunnel group name from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *tunnel-group-name* — Specifies a name string to identify a L2TP group up to 63 characters in length.

create — This keyword is mandatory when creating a tunnel group name. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

protocol — Specifies the l2tp protocol for use.

Values v2, v3, v3draft

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group

Syntax **group** *tunnel-group-name*

Context **[Tree]** (debug>router>l2tp group)

Full Context debug router l2tp group

Description This command enables and configures debugging for an L2TP group.

Parameters *tunnel-group-name* — Specifies the tunnel group name, up to 63 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group

Syntax **group** *name* [**create**]
no group *name*

Context **[Tree]** (config>service>vpls>gsmp group)
[Tree] (config>service>vprn>gsmp group)

Full Context configure service vpls gsmp group
configure service vprn gsmp group

Description This command specifies a GSMP name. A GSMP group name is unique only within the scope of the service in which it is defined.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies a GSMP name up to 32 characters.

create — Keyword used to create the GSMP group name. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group

Syntax [**no**] **group** *ip-address*

Context **[Tree]** (config>subscr-mgmt>igmp-policy>static group)

Full Context configure subscriber-mgmt igmp-policy static group

Description This command adds or removes a static multicast group.

The **no** form of this command reverts to the default value.

Parameters *ip-address* — Specifies the multicast group IP address.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group

Syntax [**no**] **group** *grp-ipv6-address*

Context **[Tree]** (config>subscr-mgmt>mld-policy>static group)

Full Context configure subscriber-mgmt mld-policy static group

Description This command configures a static multicast group.

The **no** form of this command reverts to the default.

Parameters *grp-ipv6-address* — Specifies the IPv6 address.

Values ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D
- multicast group IPv6 address

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group

Syntax [**no**] **group** *group-name*

Context **[Tree]** (config>service>vprn>rip group)
[Tree] (config>service>ies>rip group)

Full Context configure service ies rip group
configure service vprn rip group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a context for configuring a RIP group of neighbors. RIP groups are a way of logically associating RIP neighbor interfaces to facilitate a common configuration for RIP interfaces.

The **no** form of this command deletes the RIP neighbor interface group. Deleting the group also removes the RIP configuration of all the neighbor interfaces currently assigned to this group.

Default no group

Parameters *group-name* — The RIP group name. Allowed values are any string, up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

group

Syntax **group** *group-id* **rate** *rate*
no group *group-id*

Context **[Tree]** (config>port>ethernet>egress>hs-sched-ovr group)

Full Context configure port ethernet egress hs-scheduler-overrides group

Description This command overrides a group rate configured in the HS scheduler policy applied to the port egress.

The **no** form of this command removes the rate override from the port egress configuration.

Parameters *group-id* — Specifies the group ID.

Values 1

rate — Specifies the maximum rate in megabits per second. When the **max** keyword follows the **rate** keyword, the bandwidth limitation is removed from the group. The **max** keyword is mutually exclusive to the **rate** parameter. Either the **max** keyword or a rate value must follow the **rate** keyword.

Values 1 to 100000, max

Platforms 7750 SR-7/12/12e

group

Syntax **group** *sonet-sdh-index* **payload** {**tu3** | **vt2** | **vt15**}

Context **[Tree]** (config>port>sonet-sdh group)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port sonet-sdh group

Description This command configures payload of the SONET/SDH group.

This command is supported by TDM satellite, however the **tu3** parameter is not.

For example:

config>port>sonet-sdh#

group tug3-1.1 payload tu3 group tug3-1.2 payload vt2 group tug3-1.3 payload vt2 group tug3-2.1 payload vt15 group tug3-2.2 payload vt15 group tug3-2.3 payload tu3 group tug3-3.1 payload tu3 group tug3-3.2 payload tu3 group tug3-3.3 payload tu3

Parameters *sonet-sdh-index* — Specifies the components making up the specified SONET/SDH path. Depending on the type of SONET/SDH port the *sonet-sdh-index* must specify more path indexes to specify the payload location of the path.

tu3 — Specifies the Tributary Unit Group (TUG3) on a path. Configures the port or channel for transport network use.

vt2 — Configures the path as a virtual tributary group of type vt2.

vt15 — Configures the path as a virtual tributary group of type vt15.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

group

Syntax [**no**] **group** *name*

Context **[Tree]** (config>router>bgp group)

Full Context configure router bgp group

Description Commands in this context configure a BGP peer group.

The **no** form of this command deletes the specified peer group and all configurations associated with the peer group. The group must be shut down before it can be deleted.

Default no group

Parameters *name* — Specifies the peer group name. Allowed values are any string, up to 64 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group

Syntax [**no**] **group** *grp-ip-address*
[**no**] **group** *grp-ipv6-address*

Context **[Tree]** (config>service>vpls>igmp-snooping>static group)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping>static group)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping>static group)
[Tree] (config>service>vpls>sap>igmp-snooping>static group)
[Tree] (config>service>vpls>sap>mld-snooping>static group)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping>static group)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping>static group)

Full Context configure service vpls igmp-snooping static group
configure service vpls mesh-sdp igmp-snooping static group
configure service vpls mesh-sdp mld-snooping static group
configure service vpls sap igmp-snooping static group
configure service vpls sap mld-snooping static group
configure service vpls spoke-sdp igmp-snooping static group
configure service vpls spoke-sdp mld-snooping static group

Description Commands in this context add a static multicast group as a (*, G) or as one or more (S,G) records. When a static MLD or IGMP group is added, multicast data for that (*,G) or (S,G) is forwarded to the specific SAP or SDP without receiving any membership report from a host.

Parameters *grp-ip-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

grp-ipv6-address — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

group

Syntax **group** *name* [**esm-dynamic-peer**]
no group *name*

Context **[Tree]** (config>service>vprn>bgp group)

Full Context configure service vprn bgp group

Description This command creates a context to configure a BGP peer group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the specified peer group and all configurations associated with the peer group. The group must be shut down before it can be deleted.

Parameters *name* — Specifies the peer group name. Allowed values is a string up to 64 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

esm-dynamic-peer — Specifies that the given BGP group is used by BGP peers created dynamically based on subscriber-hosts pointing to corresponding BGP peering policy. There can be only one BGP group with this flag set in any given VPRN. No BGP neighbors can be manually configured in a BGP group with this flag set.

Default disabled

Platforms All

group

Syntax [**no**] **group** *grp-ip-address*
[**no**] **group start** *grp-ip-address* **end** *grp-ip-address* [**step** *ip-address*]

Context **[Tree]** (config>service>vprn>igmp>if>static group)

Full Context configure service vprn igmp interface static group

Description This command adds a static multicast group either as a (*,G) or one or more (S,G) records. Use IGMP static group memberships to test multicast forwarding without a receiver host. When IGMP static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP.

Parameters *grp-ip-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group. The address must be in dotted decimal notation.

start *grp-ip-address* — Specifies the start multicast group address.

end *grp-ip-address* — Specifies the end multicast group address.

step *ip-address* — Specifies the step increment.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group

Syntax [**no**] **group** *grp-ipv6-address*
[**no**] **group start** *grp-ipv6-address* **end** *grp-ipv6-address* [**step** *ipv6-address*]

Context **[Tree]** (config>service>vprn>mld>if>static group)

Full Context configure service vprn mld interface static group

Description Commands in this context add a static multicast group either as a (*,G) or one or more (S,G) records. Use MLD static group memberships to test multicast forwarding without a receiver host. When MLD static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static MLD group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static MLD group entries do not generate join messages toward the RP.

The **no** form of this command removes the IPv6 address from the configuration.

Parameters *grp-ipv6-address* — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

start *grp-ipv6-address* — Specifies the start multicast group address.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

end *grp-ipv6-address* — Specifies the end multicast group address.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

step *ipv6-address* — Specifies the step increment.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group

Syntax [**no**] **group** *group-name*

Context **[Tree]** (config>service>vprn>msdp group)

Full Context configure service vprn msdp group

Description This command enables access to the context to create or modify a Multicast Source Discovery Protocol (MSDP) group. To configure multiple MSDP groups, include multiple group statements.

By default, the group's options are inherited from the global MSDP options. To override these global options, group-specific options within the group statement can be configured.

If the group name provided is already configured then this command only provides the context to configure the options pertaining to this group.

If the group name provided is not already configured, then the group name must be created and the context to configure the parameters pertaining to the group should be provided. In this case, the $ prompt to indicate that a new entity (group) is being created should be used.

For a group to be of use, at least one peer must be configured.

Default no group

Parameters *group-name* — Specifies a unique name for the MSDP group.

Platforms All

group

Syntax [**no**] **group** *ip-address* [/*mask*]

Context **[Tree]** (config>service>vprn>mvpn>pt>selective>multistream-spmsi group)

Full Context configure service vprn mvpn provider-tunnel selective multistream-spmsi group

Description This command creates group prefixes that map to the multicast stream. At least one source must be specified for the policy to be active.

Parameters *Ip-address/mask* — Specifies the IP address.

Values

ipv4-prefix	a.b.c.d	
	ipv4-prefix-le	[0..32]
ipv6-prefix		x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
	x	[0..FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

d	[0..255]D
ipv6-prefix-le	[0..128]

Platforms All

group

Syntax **group** *aa-group-id*[**:***partition-id* [**create**]
no group *aa-group-id*:*partition-id*

Context **[Tree]** (config>app-assure group)

Full Context configure application-assurance group

Description This command configures and enables the context to configure an application assurance group and partition parameters.

Parameters *aa-group-id* — Specifies a group of ISA MDAs.

Values 1 to 255

partition-id — Specifies a partition within a group.

Values 1 to 65535

create — Keyword used to create the partition in the group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

group

Syntax **group** *aa-group-id*

Context **[Tree]** (admin>app-assure group)

Full Context admin application-assurance group

Description This commands performs a group-specific upgrade.

Parameters *aa-group-id* — Specifies the AA group identifier.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

group

Syntax **group** *aa-group-id*[**:***partition-id*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>app-assure group)

Full Context debug application-assurance group

Description This command configures application-assurance within a group/partition debugging.

Parameters *aa-group-id[:partition-id]* — Specifies the existing application assurance group and partition id.

Values

*aa-group-id:parti** : *aa-group-id*[:*partition-id]*	
aa-group-id	[1..255]
partition-id	[1..65535]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

group

Syntax [**no**] **group** *grp-ip-address*
[**no**] **group start** *grp-ip-address* **end** *grp-ip-address* [**step** *ip-address*]

Context [Tree] (config>router>igmp>if>static group)

Full Context configure router igmp interface static group

Description Commands in this context add a static multicast group either as a (*,G) or one or more (S,G) records. Use IGMP static group memberships to test multicast forwarding without a receiver host. When IGMP static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP.

Parameters *ip-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

start *grp-ip-address* — Specifies the start multicast group address.

end *grp-ip-address* — Specifies the end multicast group address.

step *ip-address* — Specifies the step increment.

Platforms All

group

Syntax [**no**] **group** *grp-ip-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>igmp>tunnel-interface>static group)

Full Context configure router igmp tunnel-interface static group

Description Commands in this context add a static multicast group either as a (*,G) or one or more (S,G) records.

The user can assign static multicast group joins to a tunnel interface associated with an RSVP P2MP LSP.

A given (*,G) or (S,G) can only be associated with a single tunnel interface.

A multicast packet which is received on an interface and which succeeds the RPF check for the source address will be replicated and forwarded to all OIFs which correspond to the branches of the P2MP LSP. The packet is sent on each OIF with the label stack indicated in the NHLFE of this OIF. The packets will also be replicated and forwarded natively on all OIFs which have received IGMP or PIM joins for this (S,G).

The multicast packet can be received over a PIM or IGMP interface which can be an IES interface, a spoke SDP terminated IES interface, or a network interface.

Parameters *grp-ip-address* — Specifies a multicast group address that receives data on a tunnel interface. The IP address must be unique for each static group.

Platforms All

group

Syntax [**no**] **group** *grp-ipv6-address*
[**no**] **group start** *grp-ipv6-address* **end** *grp-ipv6-address* [**step** *ipv6-address*]

Context [Tree] (config>router>mld>if>static group)

Full Context configure router mld interface static group

Description Commands in this context add a static multicast group either as a (*,G) or one or more (S,G) records. Use MLD static group memberships to test multicast forwarding without a receiver host. When MLD static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static MLD group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static MLD group entries do not generate join messages toward the RP.

The **no** form of this command removes the IPv6 address from the configuration.

Parameters *grp-ipv6-address* — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

start *grp-ipv6-address* — Specifies the start multicast group address.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

end *grp-ipv6-address* — Specifies the end multicast group address.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

step *ipv6-address* — Specifies the step increment.

Platforms All

group

Syntax [**no**] **group** *group-name*

Context **[Tree]** (config>router>msdp group)

Full Context configure router msdp group

Description This command enables access to the context to create or modify a Multicast Source Discovery Protocol (MSDP) group. To configure multiple MSDP groups, include multiple group statements.

By default, the group's options are inherited from the global MSDP options. To override these global options, group-specific options within the group statement can be configured.

If the group name provided is already configured then this command only provides the context to configure the options pertaining to this group.

If the group name provided is not already configured, then the group name must be created and the context to configure the parameters pertaining to the group should be provided. In this case, the $ prompt to indicate that a new entity (group) is being created should be used.

For a group to be of use, at least one peer must be configured.

The **no** form of this command removes the *group-name* from the MSDP configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no group

Parameters *group-name* — Species a MSDP group name, up to 32 characters.

Platforms All

group

Syntax **group** *group-id* **rate** *rate*
no group *group-id*

Context **[Tree]** (config>qos>hs-scheduler-policy group)

Full Context configure qos hs-scheduler-policy group

Description This command defines the maximum rate allowed for the scheduling classes mapped to the specified *group-id*. A group is a scheduling component used to combine up to six consecutive scheduling classes into a single strict priority level. Each scheduling class within the group has an associated weight. When the scheduler is servicing the strict level associated with the group, the ratio of bandwidth allocated to each scheduling class within the group during congestion is relative to the ratio of the weight of each active member.

The **no** form of the command reverts to the default.

Default group 1 rate max

Parameters *group-id* — Specifies the group ID. The group always exists and does not need to be created prior to defining group membership.

Values 1

rate — Specifies the maximum rate in megabits per second. When the **max** keyword follows the rate keyword, the bandwidth limitation is removed from the group. The **max** keyword and the *rate* parameter are mutually exclusive. Either **max** or a rate value must follow the **rate** keyword.

Values 1 to 100000, max

Platforms 7750 SR-7/12/12e

group

Syntax **group** *name* [**create**]
no group *name*

Context **[Tree]** (config>qos>port-scheduler-policy group)

Full Context configure qos port-scheduler-policy group

Description This command defines a weighted scheduler group within a port scheduler policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The port scheduler policy defines a set of eight priority levels. The weighted scheduler group allows for the application of a scheduling weight to groups of child queues competing at the same priority level of the port scheduler policy applied to a Vport defined in the context of the egress of an Ethernet port or applied to the egress of an Ethernet port.

Up to eight groups can be defined within each port scheduler policy. One or more levels can map to the same group. A group has a rate and, optionally, a cir-rate, and inherits the highest scheduling priority of its member levels. A group receives bandwidth from the port or from the Vport and distributes it within the member levels of the group according to the weight of each level within the group.

Each priority level will compete for bandwidth within the group based on its weight under a congestion situation. If there is no congestion, a priority level can achieve up to its rate (cir-rate) worth of bandwidth.

CLI will enforce that mapping of levels to a group are contiguous. A user would not be able to add a priority level to a group unless the resulting set of priority levels is contiguous.

The **no** form of this command removes the group from the port scheduler policy.

Parameters *name* — Specifies the name of the weighted scheduler group and can be up to 32 ASCII characters.

create — This keyword is mandatory when creating the specified group.

Platforms All

group

Syntax **group** *aa-group-id*

Context **[Tree]** (admin>application-assurance group)

Full Context admin application-assurance group

Description Commands in this context perform a group-specific upgrade.

Parameters *aa-group-id* — Specifies an AA ISA group ID.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

group

Syntax **group** *group-name*
no group

Context **[Tree]** (config>system>security>user>snmp group)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security user snmp group

Description This command associates (or links) a user to a group name. The group name must be configured with the **config>system>security>user >snmp>group** command. The **config>system>security>user access** command links the group with one or more views, security model (s), security level (s), and read, write, and notify permissions.

Parameters *group-name* — Enter the group name (between 1 and 32 alphanumeric characters) that is associated with this user. A user can be associated with one group-name per security model.

Platforms All

group

Syntax [**no**] **group** *group-name*

Context **[Tree]** (config>router>rip group)
[Tree] (config>router>ripng group)

Full Context configure router rip group
configure router ripng group

Description This command creates a context for configuring a RIP group of neighbor interfaces.

RIP groups are a way of logically associating RIP neighbor interfaces to facilitate a common configuration for RIP interfaces.

The **no** form of the command deletes the RIP neighbor interface group. Deleting the group will also remove the RIP configuration of all the neighbor interfaces currently assigned to this group.

Default no group

Parameters *group-name* — Specifies the RIP group name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

group

Syntax [**no**] **group** *ip-address* [/*mask*]

Context **[Tree]** (config>service>vprn>mvpn>pt>selective>umh-rm group)

Full Context configure service vprn mvpn provider-tunnel selective umh-rate-monitoring group

Description This command configures UMH bandwidth monitoring for the specified <S,G>.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes UMH bandwidth monitoring from the specified <S,G>.

Parameters *ip-address/mask* — Specifies the IP address.

Values

ipv4-prefix	a.b.c.d	
	ipv4-prefix-le	[0..32]
ipv6-prefix		x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
	x	[0..FFFF]H
	d	[0..255]D
	ipv6-prefix-le	[0..128]

Platforms All

11.69 group down

group down

Syntax **group down** *time* | **no group down**

Context **[Tree]** (config>service>oper-group>hold-time group down)

Full Context configure service oper-group hold-time group down

Description This command configures the number of seconds to wait before notifying clients monitoring this group when its operational status transitions from up to down.

The **no** form of the command sets the values back to the default.

Default group down 0

11.70 group up

group up

Syntax **group up** *time* | **no group up**

Context **[Tree]** (config>service>oper-group>hold-time group up)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service oper-group hold-time group up

Description This command configures the number of seconds to wait before notifying clients monitoring this group when its operational status transitions from down to up. A value of zero indicates that transitions are reported immediately to monitoring clients. The up time option is a must to achieve fast convergence: when the group comes up, the monitoring MH site which tracks the group status may wait without impacting the overall convergence; there is usually a pair MH site that is already handling the traffic.

The **no** form of the command reverts to the default.

Default group-up 4

Parameters *time* — Specifies the group up time value.

Values 0 to 3600

11.71 group-address

group-address

Syntax **group-address** *prefix-list-name*
no group-address

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from group-address)

Full Context configure router policy-options policy-statement entry from group-address

Description This command specifies the multicast group-address prefix list containing multicast group-addresses that are embedded in the join or prune packet as a filter criterion. The prefix list must be configured prior to entering this command. Prefix lists are configured in the **config>router>policy-options>prefix-list** context.

The **no** form of this command removes the criterion from the configuration.

Default no group-address

Parameters *prefix-list-name* — Specifies the prefix-list name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The *prefix-list-name* is defined in the **config>router>policy-options>prefix-list** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.72 group-encryption

group-encryption

Syntax **group-encryption**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw group-encryption)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw group-encryption)

Full Context configure service ies subscriber-interface group-interface wlan-gw group-encryption
configure service vprn subscriber-interface group-interface wlan-gw group-encryption

Description This command configures group encryption for the WLAN-GW group interface.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

group-encryption

Syntax [**no**] **group-encryption**

Context **[Tree]** (config>router>interface group-encryption)

Full Context configure router interface group-encryption

Description This command enables NGE on the router interface. When NGE is enabled on the interface, all received Layer 3 packets that have the protocol ID configured as ESP are considered to be NGE packets and must be encrypted using a valid set of keys from any preconfigured key group on the system.

The **no** form of this command disables NGE on the interface. NGE cannot be disabled unless all key groups and IP exception filters are removed.

Default no group-encryption

Platforms VSR

group-encryption

Syntax **group-encryption**

Context **[Tree]** (config group-encryption)

Full Context configure group-encryption

Description Commands in this context configure group encryption parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.73 group-encryption-label

group-encryption-label

Syntax **group-encryption-label** *encryption-label*
no group-encryption-label

Context **[Tree]** (config>grp-encryp group-encryption-label)

Full Context configure group-encryption group-encryption-label

Description This command configures the group encryption label used to identify when an MPLS payload is encrypted. This label must be unique network-wide and must be configured consistently on all nodes participating in a network group encryption domain. The label cannot be changed or deleted when there are any key groups configured on the node.

The **no** form of the command reverts to the default setting.

Parameters *encryption-label* — The network-wide, unique reserved MPLS label for group encryption.

Values 32 to 2047

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.74 group-inserted-entries

group-inserted-entries

Syntax **group-inserted-entries application** *application* **location** *location*

Context **[Tree]** (config>filter>ip-filter group-inserted-entries)
[Tree] (config>filter>ipv6-filter group-inserted-entries)

Full Context configure filter ip-filter group-inserted-entries
configure filter ipv6-filter group-inserted-entries

Description This command groups automatically-inserted entries.

Parameters *application* — Specifies the application for which the group entries are inserted.

Values radius, credit-control

location — Specifies the location in the entry list in which the group entries are inserted.

Values top, bottom

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.75 group-interface

group-interface

Syntax **group-interface** *ip-int-name* [**prefix** {*port-id*}] [**suffix** {*port-id*}]
no group-interface

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>msap-defaults group-interface)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>msap-defaults group-interface)

Full Context configure subscriber-mgmt local-user-db ipoe host msap-defaults group-interface
configure subscriber-mgmt local-user-db ppp host msap-defaults group-interface

Description This command configures the group interface.

The **no** form of this command removes the group interface parameters from the configuration.

Parameters *ip-int-name* — Specifies the IP interface name, up to 32 characters.

prefix *port-id* — Specifies the port ID as the prefix to the specified IP interface name.

suffix *port-id* — Specifies the port ID as the suffix to the specified IP interface name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group-interface

Syntax **group-interface** *ip-int-name* [**create**] [**type**]
no group-interface *ip-int-name*

Context **[Tree]** (config>service>ies>sub-if group-interface)
[Tree] (config>service>vprn>sub-if group-interface)

Full Context configure service ies subscriber-interface group-interface
configure service vprn subscriber-interface group-interface

Description This command creates a group interface. This interface is designed for triple play services where multiple SAPs are part of the same subnet. A group interface may contain one or more SAPs.

The **no** form of this command removes the group interface from the subscriber interface.

Default no group-interface

Parameters *ip-int-name* — Specifies the interface name of a group interface. If the string contains special characters (#, $, spaces, and so on.), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type — Specifies the interface type.

Values bonding — Specifies to use connection bonding.
gtp — Specifies to use GTP.
lns — Specifies to use LNS.
wlangw — Specifies to use WLANGW.

create — Keyword used to create the group interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group-interface

Syntax **group-interface** *interface-name* **svc-id** *service-id*
no group-interface

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn>defaults group-interface)

Full Context configure subscriber-mgmt gtp apn-policy apn defaults group-interface

Description This command configures the default group interface where the hosts of the GTP connection is enabled. The group interface must be of type **gtp**.

The **no** form of this command removes the default group interface. In this case, a group interface must be specified using authentication.

Default no group-interface

Parameters *interface-name* — Specifies the name of the group interface, up to 32 characters.

service-id — Specifies the ID of the service where the group interface resides.

Values
service-id: 1 to 2147483647
svc-name: up to 64 characters

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

group-interface

Syntax [**no**] **group-interface** *ip-int-name*
[**no**] **group-interface fwd-service** *service-id ip-int-name*

Context **[Tree]** (config>service>vprn>igmp group-interface)

Full Context configure service vprn igmp group-interface

Description This command configures IGMP group interfaces.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *ip-int-name* — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

fwd-service *service-id* — Specifies the service ID. This is only configured in the retailer VRF. This construct references the wholesaler service under which the group-interface (and the subscriber) is actually defined.

Values 1 to 2147483650, svc-name up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group-interface

Syntax [**no**] **group-interface** [**fwd-service** *service-id*] [*ip-int-name*]

Context **[Tree]** (debug>router>igmp group-interface)

Full Context debug router igmp group-interface

Description This command enables debugging for IGMP group-interface.

The **no** form of the command disables debugging.

Parameters *service-id* — Debugs information associated with the service ID.

Values service-id: 1 to 2148278386
svc-name: up to 64 characters.

ip-int-name — Debugs information associated with the specified IP interface name.

Values IP interface address

Platforms All

group-interface

Syntax [**no**] **group-interface** *ip-int-name*

Context **[Tree]** (config>router>igmp group-interface)
[Tree] (config>router>igmp>if group-interface)

Full Context configure router igmp group-interface
configure router igmp interface group-interface

Description This command enables IGMP on a group-interface in a VRF context. Activating IGMP under the group-interface is a prerequisite for subscriber replication. The group-interface is also needed so that MCAC can be applied and various IGMP parameters defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command can be used in a regular, wholesaler or retailer type of VRF. The retailer VRF does not have the concept of group-interfaces under the subscriber-interface hierarchy. In the case that this command is applied to a retailer VRF instance, the optional **fwd-service** command must be configured. The **fwd-service** command is referencing the wholesaler VRF in which the traffic is ultimately replicated. Redirection in the retailer VRF is supported.

This command enables IGMP on a group-interface in the Global Routing Table (GRT). The group-interface in GRT is defined under the IES service. Activating IGMP under the group-interface is a prerequisite for subscriber replication. The group-interface is also needed so that MCAC can be applied and various IGMP parameters defined.

Parameters *ip-int-name* — Specifies the name of the group interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

group-interface

Syntax [**no**] **group-interface** *ip-int-name*

Context **[Tree]** (config>router>mld group-interface)

Full Context configure router mld group-interface

Description This command creates and enables the context to configure MLD group interface parameters.

The **no** form of this command removes the interface name from the MLD configuration.

Parameters *ip-int-name* — Specifies the IP group interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.76 group-interface-statistics

group-interface-statistics

Syntax **group-interface-statistics**

Context **[Tree]** (config>subscr-mgmt group-interface-statistics)

Full Context configure subscriber-mgmt group-interface-statistics

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context enable or disable the collection of group interface statistics.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.77 group-interface-template

group-interface-template

Syntax **group-interface-template** *name* [**create**]
no group-interface-template *name*

Context **[Tree]** (config>subscr-mgmt group-interface-template)

Full Context configure subscriber-mgmt group-interface-template

Description This command creates a template for specifying parameters for automatically generated group interfaces, for example, the creation of CUPS sessions. When no specific name is specified, a template named “default” is used, if it has been manually provisioned.

Parameters *name* — Specifies the name of the group interface, up to 32 characters.

create — Keyword used to create the group interface template.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.78 group-name

group-name

Syntax **group-name** *group-name* **value** *group-value*
no group-name *group-name*

Context **[Tree]** (config>service>sdp-group group-name)

Full Context configure service sdp-group group-name

Description This command defines SDP administrative groups, referred to as SDP admin groups.

SDP admin groups provide a way for services using a pseudowire template to automatically include or exclude specific provisioned SDPs. SDPs sharing a specific characteristic or attribute can be made members of the same admin group. When users configure a pseudowire template, they can include and/or exclude one or more admin groups. When the service is bound to the pseudowire template, the SDP selection rules will enforce the admin group constraints specified in the **sdp-include** and **sdp-exclude** commands.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A maximum of 32 admin groups can be created. The group value ranges from zero (0) to 31. It is uniquely associated with the group name at creation time. If the user attempts to configure another group name for a group value that is already assigned to an existing group name, the SDP admin group creation is failed. The same happens if the user attempts to configure an SDP admin group with a new name but associates it to a group value already assigned to an existing group name.

The **no** option of this command deletes the SDP admin group but is only allowed if the group-name is not referenced in a PW template or SDP.

Parameters *group-name* — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.

group-value — Specifies the group value associated with this SDP admin group. This value is unique within the system.

Values 0 to 31

Platforms All

11.79 group-policy

group-policy

Syntax **group-policy** *policy-name*
no group-policy

Context **[Tree]** (config>service>vpls>pim-snooping group-policy)
[Tree] (config>service>vpls>sap>igmp-snooping>mvr group-policy)
[Tree] (config>service>vpls>mld-snooping>mvr group-policy)
[Tree] (config>service>vpls>igmp-snp>mvr group-policy)

Full Context configure service vpls igmp-snooping mvr group-policy
configure service vpls mld-snooping mvr group-policy
configure service vpls pim-snooping group-policy
configure service vpls sap igmp-snooping mvr group-policy

Description This command identifies filter policy of multicast groups to be applied to this VPLS entity. The sources of the multicast traffic must be a member of the VPLS.

The **no** form of this command removes the policy association from the VPLS configuration.

Default no group-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the group policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the config>router>policy-options context. The router policy must be defined before it can be imported.

Platforms All

11.80 group-prefix

group-prefix

Syntax **group-prefix** *ip-address/mask* [*ip-address/mask*] [**starg**]
no group-prefix *ip-address/mask*

Context **[Tree]** (config>service>vprn>mvpn>rpf-select>core-mvpn group-prefix)

Full Context configure service vprn mvpn rpf-select core-mvpn group-prefix

Description This command configures multicast group IPv4 prefixes for the MVPN with per-group mapping extranet functionality. Multiple lines are allowed. Duplicate prefixes are ignored.

When the starg option is specified, extranet functionality is enabled for PIM ASM as for the specified group. When the option is not specified (not recommended with PIM ASM), the PIM ASM join will be mapped and data plane will be established, but the control plane will not be updated on SPT switchover, unless the switchover is driven by a CPE router on a receiver side.

The **no** form of this command deletes specified prefix from the list, or removes mapping of all prefixes if group-prefix any was specified.

Parameters *ip-address/mask* — Specifies the IPv4 multicast address prefix with mask. Up to 8 addresses can be specified in a single statement.

Platforms All

group-prefix

Syntax **group-prefix** *ip-address*/*mask* [*ip-address*/*mask*...(up to 8 max)] [**starg**]
group-prefix any
no group-prefix *ip-address/mask*
no group-prefix any

Context **[Tree]** (config>service>vprn>pim>rpf-select>grt-extranet group-prefix)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn pim rpf-select grt-extranet group-prefix

Description This command configures multicast group IPv4 prefixes for the multicast GRT/VRF with per group mapping extranet functionality. Multiple lines are allowed. Duplicate prefixes are ignored. Operator can either configure specific groups for extranet or specify all groups by using key-word any. The two options are mutually exclusive in configuration.

When the starg option is specified, extranet functionality is enabled for PIM ASM as for the specified group. When the option is not specified (not recommended with PIM ASM), the PIM ASM join will be mapped and data plane will be established, but the control plane will not be updated on SPT switchover, unless the switchover is driven by a CPE router on a receiver side.

The **no** form of this command deletes specified prefix from the list, or removes mapping of all prefixes if group-prefix any was specified.

Parameters *ip-address/mask* — Specifies the IPv4 multicast address prefix with mask.

group-prefix

Syntax [**no**] **group-prefix grp-ipv6-address/prefix-length**

Context **[Tree]** (config>service>vprn>pim>rp>ipv6>static group-prefix)

Full Context configure service vprn pim rp ipv6 static group-prefix

Description The group-prefix for a static-rp defines a range of multicast-ip-addresses for which this static RP is applicable.

The **no** form of this command removes the criterion.

Parameters *grp-ipv6-address* — Specifies the multicast IPv6 address.

prefix-length — Specifies the address prefix length.

Values

grp-ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D
prefix-length	[8 to 128]

group-prefix

Syntax [**no**] **group-prefix** {*grp-ip-address*/*mask* | *grp-ip-address netmask*}

Context **[Tree]** (config>service>vprn>pim>rp>static group-prefix)

Full Context configure service vprn pim rp static group-prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **group-prefix** for a static-rp defines a range of multicast-ip-addresses for which a certain RP is applicable.

The **no** form of this command removes the criterion.

Parameters *grp-ip-address* — Specifies the multicast IP address.

mask — Defines the mask of the multicast-ip-address.

Values 4 to 32

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

group-prefix

Syntax [**no**] **group-prefix** *grp-ipv6-address*/*prefix-length*

Context **[Tree]** (config>router>pim>rp>static>address group-prefix)
[Tree] (config>router>pim>rp>ipv6>static>address group-prefix)

Full Context configure router pim rp ipv6 static address group-prefix
configure router pim rp static address group-prefix

Description This command specifies the range of multicast group addresses which should be used by the router as the Rendezvous Point (RP). The **config**>**router**>**pim**>**rp**>**static**>**address** *a.b.c.d* implicitly defaults to deny all for all multicast groups (224.0.0.0/4). A group-prefix must be specified for that static address. This command does not apply to the whole group range.

The **no** form of this command removes the group-prefix from the configuration.

Parameters *grp-ipv6-address* — Specifies the multicast group IPv6 address expressed in dotted decimal notation.

Values grp-ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0..255]D

prefix-length — Specifies the prefix length of the IPv6 address.

Values 8 to 128

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.81 group-range

group-range

Syntax [**no**] **group-range** {*ipv6-address*/*prefix-length*}

Context **[Tree]** (config>service>vprn>pim>rp>ipv6>embedded-rp group-range)
[Tree] (config>service>vprn>pim>rp>ipv6>rp-candidate group-range)

Full Context configure service vprn pim rp ipv6 embedded-rp group-range
configure service vprn pim rp ipv6 rp-candidate group-range

Description This command configures the group address or range of group addresses for which this router can be the rendezvous point (RP).

The **no** form of this command removes the group address or range of group addresses for which this router can be the RP from the configuration.

Parameters *ipv6-address* — Specifies the addresses or address ranges that this router can be an RP.

prefix-length — Specifies the address prefix length.

Values

ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D
prefix-length	[8 to 128] // for embedded-rp
prefix-length	[16 to 128] // for rp-candidate

Platforms All

group-range

Syntax [**no**] **group-range** {*ip-prefix*/*mask* | *ip-prefix netmask*}

Context **[Tree]** (config>service>vprn>pim>rp>rp-candidate group-range)
[Tree] (config>service>vprn>pim>ssm group-range)

Full Context configure service vprn pim rp rp-candidate group-range
configure service vprn pim ssm-groups group-range

Description This command configures the group address or range of group addresses for which this router can be the rendezvous point (RP).

Use the **no** form of this command to remove the group address or range of group addresses for which this router can be the RP from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix* — Specifies the addresses or address ranges that this router can be an RP.

Values ipv4-prefix - a.b.c.d ipv4-prefix-le - [0 to 32] ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0 to FFFF]H d - [0 to 255]D ipv6-prefix-le - [0 to 128]

mask — Specifies the address mask with the address to define a range of addresses.

netmask — Specifies the subnet mask in dotted decimal notation.

Values :a.b.c.d (network bits all 1 and host bits all 0)

Platforms All

group-range

Syntax [**no**] **group-range** *ipv6-address/prefix-length*

Context **[Tree]** (config>router>pim>rp>ipv6>embedded-rp group-range)
[Tree] (config>router>pim>rp>ipv6>rp-candidate group-range)

Full Context configure router pim rp ipv6 embedded-rp group-range
configure router pim rp ipv6 rp-candidate group-range

Description This command defines which multicast groups can embed RP address information besides FF70::/12. Embedded RP information is only used when the multicast group is in FF70::/12 or the configured group range.

The **no** form of this command removes the parameter from the

Parameters *ipv6-address/prefix-length* — Specifies the group range for embedded RP.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

prefix-length: 16 to 128

Platforms All

group-range

Syntax [**no**] **group-range** {*grp-ip-address/mask* | *grp-ip-address netmask*}

Context **[Tree]** (config>router>pim>rp>rp-candidate group-range)

Full Context configure router pim rp rp-candidate group-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the address ranges of the multicast groups for which this router can be an RP.

The **no** form of this commands removes the parameter from the configuration.

Parameters *grp-ip-address* — Specifies the multicast group IP address expressed in dotted decimal notation.

Values 224.0.0.0 to 239.255.255.255

mask — Specifies the mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example, /16 for a sixteen-bit mask. The mask can also be entered in dotted decimal notation (255.255.0.0).

Values 4 to 32

netmask — Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

Platforms All

group-range

Syntax [**no**] **group-range** {*ip-prefix/mask* | *ip-prefix netmask*}

Context **[Tree]** (config>router>pim>ssm-groups group-range)

Full Context configure router pim ssm-groups group-range

Description This command configures the address ranges of the multicast groups for this router. When there are parameters present, the command configures the SSM group ranges for IPv6 addresses and netmasks.

The **no** form of this command removes the parameter from the configuration.

Parameters *ip-prefix/mask* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area ipv6-prefix.

Values ipv4-prefix:

- a.b.c.d

ipv4-prefix-le: 0 to 32

ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

ipv6-prefix-le: 0 to 128

Values 0 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

netmask — Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

Platforms All

11.82 group-session-limit

group-session-limit

Syntax **group-session-limit** *session-limit*
group-session-limit unlimited
no group-session-limit

Context **[Tree]** (config>router>l2tp group-session-limit)
[Tree] (config>service>vprn>l2tp group-session-limit)

Full Context configure router l2tp group-session-limit
configure service vprn l2tp group-session-limit

Description This command configures the session limit. The value controls how many L2TP session will be allowed within a given context (system, group, tunnel).

The **no** form of this command removes the session limit value from the configuration.

Default no group-session-limit

Parameters *session-limit* — Specifies the allowed number of sessions within the given context.

Values 1 to 250000

unlimited — Specifies to use the maximum number of sessions available.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.83 grp-if-query-src-ip

grp-if-query-src-ip

Syntax **grp-if-query-src-ip** *ip-address*
no grp-if-query-src-ip

Context **[Tree]** (config>service>vprn>igmp grp-if-query-src-ip)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn igmp grp-if-query-src-ip

Description This command configures the query source IP address for all group interfaces.

The **no** form of this command removes the IP address.

Platforms All

grp-if-query-src-ip

Syntax **grp-if-query-src-ip** *ip-address*
no grp-if-query-src-ip

Context **[Tree]** (config>router>igmp grp-if-query-src-ip)

Full Context configure router igmp grp-if-query-src-ip

Description This command configures the query source IP address for all group interfaces.

The **no** form of the command removes the IP address.

Parameters *ip-address* — Sets the query source IP address.

Platforms All

grp-if-query-src-ip

Syntax **grp-if-query-src-ip** *ipv6-address*
no grp-if-query-src-ip

Context **[Tree]** (config>router>mld grp-if-query-src-ip)

Full Context configure router mld grp-if-query-src-ip

Description This command configures the query source IPv6 address for all group interfaces.

The **no** form of this command removes the IP address.

Parameters *ipv6-address* — Sets the source IPv6 address for all group interfaces. The address can be up to 64 characters. The source address should be link local.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.84 grp-range

grp-range

Syntax [**no**] **grp-range** *start end*

Context **[Tree]** (config>service>vprn>igmp>ssm-translate grp-range)

Full Context configure service vprn igmp ssm-translate grp-range

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

Platforms All

grp-range

Syntax [**no**] **grp-range** *start end*

Context **[Tree]** (config>service>vprn>mld>ssm-translate grp-range)

Full Context configure service vprn mld ssm-translate grp-range

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

Platforms All

grp-range

Syntax [**no**] **grp-range** *start end*

Context **[Tree]** (config>router>igmp>if>ssm-translate grp-range)
[Tree] (config>router>igmp>ssm-translate grp-range)

Full Context configure router igmp interface ssm-translate grp-range
configure router igmp ssm-translate grp-range

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

Platforms All

grp-range

Syntax [**no**] **grp-range** *start end*

Context **[Tree]** (config>router>mld>ssm-translate grp-range)
[Tree] (config>router>mld>if>ssm-translate grp-range)

Full Context configure router mld interface ssm-translate grp-range
configure router mld ssm-translate grp-range

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

The **no** form of this command removes the start and end ranges from the configuration.

Parameters *start* — Specifies an IP address for the start of the group range.

end — Specifies an IP address for the end of the group range. This value should always be greater than or equal to the value of the *start* value.

Platforms All

11.85 grpc

grpc

Syntax [**no**] **grpc**

Context **[Tree]** (debug>system grpc)

Full Context debug system grpc

Description This command enables the debug context for gRPC.

The **no** form of this command removes any debug activation within the gRPC context.

Platforms All

grpc

Syntax **grpc**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>system>security>management-interface grpc)

Full Context configure system security management-interface grpc

Description Commands in this context configure hash-control for the gRPC interface.

Platforms All

grpc

Syntax **grpc**

Context **[Tree]** (config>system>security>profile grpc)

Full Context configure system security profile grpc

Description Commands in this context configure a specific gRPC security profile.

Platforms All

grpc

Syntax **grpc**

Context **[Tree]** (config>system grpc)
[Tree] (config>router>sgt-qos>application grpc)
[Tree] (admin>system>telemetry grpc)

Full Context admin system telemetry grpc
configure router sgt-qos application grpc
configure system grpc

Description Commands in this context configure gRPC parameters.

Platforms All

11.86 grpc-tunnel

grpc-tunnel

Syntax **grpc-tunnel**

Context **[Tree]** (config>system grpc-tunnel)

Full Context configure system grpc-tunnel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the GRPC tunnel.

Platforms All

11.87 grt

grt

Syntax [**no**] **grt**

Context **[Tree]** (config>service>vprn>static-route-entry grt)

Full Context configure service vprn static-route-entry grt

Description This command creates a static route in a VPRN service context that points to the global routing context (base router). This is primarily used to allow traffic that ingress through a VPRN service to be routed out of the global routing context.

This next-hop type cannot be used in conjunction with any other next-hop types.

Default no grt

Platforms All

11.88 grt-extranet

grt-extranet

Syntax [**no**] **grt-extranet**

Context **[Tree]** (config>service>vprn>pim grt-extranet)

Full Context configure service vprn pim grt-extranet

Description Commands in this context configure GRT/VRF extranet for this MVPN instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.89 grt-lookup

grt-lookup

Syntax **grt-lookup**

Context **[Tree]** (config>service>vprn grt-lookup)

Full Context configure service vprn grt-lookup

Description Commands in this context configure all Global Route Table (GRT) leaking commands. If all the supporting commands in the context are removed, this command is also removed.

Platforms All

11.90 gsmp

gsmp

Syntax **gsmp**

Context **[Tree]** (config>service>vpls gsmp)
[Tree] (config>service>vprn gsmp)

Full Context configure service vpls gsmp
configure service vprn gsmp

Description Commands in this context configure General Switch Management Protocol (GSMP) connections maintained in this service.

Platforms All

11.91 gtm

gtm

Syntax **gtm**

Context **[Tree]** (config>router gtm)

Full Context configure router gtm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure GTM parameters.

Platforms All

gtm

Syntax **gtm**

Context **[Tree]** (config>router>pim gtm)

Full Context configure router pim gtm

Description Commands in this context configure GTM parameters.

Platforms All

gtm

Syntax **gtm**

Context **[Tree]** (config>router>pim gtm)

Full Context configure router pim gtm

Description Commands in this context configure GTM parameters.

Platforms All

11.92 gtp

gtp

Syntax **gtp**

Context **[Tree]** (config>router gtp)
[Tree] (config>service>vprn gtp)

Full Context configure router gtp
configure service vprn gtp

Description Commands in this context configure GTP parameters for the routing context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gtp

Syntax **gtp**

Context **[Tree]** (config>subscr-mgmt gtp)

Full Context configure subscriber-mgmt gtp

Description Commands in this context configure box-wide GTP parameters and profiles.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gtp

Syntax **gtp**

Context **[Tree]** (debug gtp)

Full Context debug gtp

Description Commands in this context configure debugging for GTP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gtp

Syntax [**no**] **gtp**

Context **[Tree]** (config>service>vprn>wlan-gw gtp)

Full Context configure service vprn wlan-gw gtp

Description Commands in this context configure distributed GTP parameters.

gtp

Syntax **gtp**

Context **[Tree]** (config>app-assure>group gtp)

Full Context configure application-assurance group gtp

Description Commands in this context configure GTP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gtp

Syntax [**no**] **gtp**

Context **[Tree]** (config>sys>security>cpu-protection>ip>included-protocols gtp)

Full Context configure system security cpu-protection ip-src-monitoring included-protocols gtp

Description This command includes the extracted IPV4 GTP packets for ip-src-monitoring. IPv4 GTP packets will be subject to the per-source-rate of CPU protection policies.

Default no gtp

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

11.93 gtp-authorized

gtp-authorized

Syntax [**no**] **gtp-authorized**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state gtp-authorized)

Full Context configure subscriber-mgmt wlan-gw ue-query state gtp-authorized

Description This command enables matching on UEs in a GTP-authorized state.

The **no** form of this command disables matching on UEs in a GTP-authorized state, unless all state matching is disabled.

Default no gtp-authorized

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.94 gtp-filter

gtp-filter

Syntax **gtp-filter** *gtp-filter-name*
no gtp-filter

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action gtp-filter)

Full Context configure application-assurance group policy app-qos-policy entry action gtp-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command assigns an existing GTP filter as an action on flows matching this AQP entry.

The **no** form of this command removes this GTP filter from actions on flows matching this AQP entry.

Default no gtp-filter

Parameters *gtp-filter-name* — Specifies the name of an existing GTP filter for this application assurance profile. The *gtp-filter-name* is configured in the **config>app-assure>group[:partition]>gtp>gtp-filter** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gtp-filter

Syntax **gtp-filter** *filter-name*

Context **[Tree]** (config>app-assure>group>statistics>tca gtp-filter)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter

Description This command configures TCA generation for a GTP filter.

Parameters *filter-name* — Specifies the name of the GTP filter, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gtp-filter

Syntax **gtp-filter** *gtp-filter-name* [**create**]
no gtp-filter *gtp-filter-name*

Context **[Tree]** (config>app-assure>group>gtp gtp-filter)

Full Context configure application-assurance group gtp gtp-filter

Description This command allows AA to treat traffic on UDP port number 2152 as GTP-u. Without further specifying any other parameters within this GTP context, AA performs basic GTP-u header sanity checks and discards packets that are malformed. This GTP context allows the operator to configure various GTP filters (maximum of 128 GTP filters).

Parameters *gtp-filter-name* — Specifies a GTP filter name, up to 32 characters.

create — Keyword used to create the GTP filter name and parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.95 gtp-filter-stats

gtp-filter-stats

Syntax [**no**] **gtp-filter-stats**

Context **[Tree]** (config>app-assure>group>statistics>aa-admit-deny gtp-filter-stats)

Full Context configure application-assurance group statistics aa-admit-deny gtp-filter-stats

Description This command configures whether to include or exclude GTP filter admit-deny statistics in accounting records.

Default no gtp-filter-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.96 gtp-in-gtp

gtp-in-gtp

Syntax **gtp-in-gtp direction** *direction* [**create**]
no gtp-in-gtp direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter gtp-in-gtp)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter gtp-in-gtp

Description This command configures a TCA for the counter capturing drops due to the GTP filter GTP-in-GTP packet check. A gtp-in-gtp drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a gtp-in-gtp TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gtp-in-gtp

Syntax **gtp-in-gtp**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>gtp>gtp-fltr gtp-in-gtp)

Full Context configure application-assurance group gtp gtp-filter gtp-in-gtp

Description This command configures GTP-in-GTP packet filtering.

Default gtp-in gtp permit

Parameters **permit | deny** — Specifies the action to take for GTP packets that are encapsulated in GTP (GTP-in-GTP).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.97 gtp-local-breakout

gtp-local-breakout

Syntax **gtp-local-breakout**

Context [Tree] (config>filter>ip-filter>entry>action gtp-local-breakout)

Full Context configure filter ip-filter entry action gtp-local-breakout

Description This command specifies the filter entry action to gtp-local-breakout.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.98 gtp-mobility

gtp-mobility

Syntax [**no**] **gtp-mobility**

Context [Tree] (config>subscr-mgmt>acct-plcy>triggered-updates gtp-mobility)

Full Context configure subscriber-mgmt radius-accounting-policy triggered-updates gtp-mobility

Description This command, when enabled causes an interim update to be sent whenever a mobility event for ESM over GTP is detected. Mobility events include X2 mobility, service re-activation after idling, notification changes and any detected change of ULI or RAT-Type.

The **no** version of this command disables generating mobility related events.

Default no gtp-mobility

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.99 gtp-parameters

gtp-parameters

Syntax **gtp-parameters**

Context **[Tree]** (config>service>vprn>sub-if>grp-if gtp-parameters)
[Tree] (config>service>ies>sub-if>grp-if gtp-parameters)

Full Context configure service ies subscriber-interface group-interface gtp-parameters
configure service vprn subscriber-interface group-interface gtp-parameters

Description Commands in this context configure GTP parameters. The configuration of parameters under this context is only allowed when the group interface is created with the GTP parameter specified.

11.100 gtp-peer-clear-timeout

gtp-peer-clear-timeout

Syntax **gtp-peer-clear-timeout** *seconds*
no gtp-peer-clear-timeout

Context **[Tree]** (config>service>vprn>wlan-gw>dsm gtp-peer-clear-timeout)

Full Context configure service vprn wlan-gw dsm gtp-peer-clear-timeout

Description This command configures a GTP peer cleanup timeout to terminate a handover wait state.

Parameters *seconds* — Specifies a GTP peer cleanup timeout, in seconds, to terminate a handover wait state.

Values 0 to 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.101 gtp-ping

gtp-ping

Syntax **gtp-ping** *gtp-interface* [**router** *router-instance*] [**source** *ip-address*] **destination** *ip-address* **udp-port** *port-number* [**retry-count** *count*] [**time-out** *timeout*]

Context **[Tree]** (oam gtp-ping)

Full Context oam gtp-ping

Description This command verifies whether a GTPv2 peer is reachable and correctly responds to GTPv2-C Echo Request messages. This command can be executed if no peering exists for the specified peer.

Parameters *gtp-interface* — Specifies the GTP interface where the echo is sent.

Values s11, s1u, gnc, gnu, s2bc, s2bu, s2ac, s2au

router-instance — Specifies the router or VRF in which the GTP echo is sent.

Values *router-name* — Base, management
vprn-svc-id — 1 to 2147483647

Default Base

source *ip-address* — Specifies the source IP address to be used in the GTP ping.

Values a.b.c.d

destination *ip-address* — Specifies the destination IP address to be used in the GTP ping.

Values a.b.c.d

port-number — Specifies the port number to be used. Suggested port numbers are 2123 (GTP-C) or 2152 (GTP-U).

Values 1 to 65535

count — Specifies the number of echo message requests before the peer is considered unreachable.

Values 1 to 100

Default 1

timeout — Specifies the timeout, in seconds, of a single echo message.

Values 1 to 10

Default 5

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.102 gtp-sanity-drop

gtp-sanity-drop

Syntax **gtp-sanity-drop direction** *direction* [**create**]
no gtp-sanity-drop direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca gtp-sanity-drop)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-sanity-drop

Description This command configures a TCA for the counter capturing drops due to basic GTP header sanity checks, such as validating that the GTP-U version is 1 and that the protocol bit is set to 1 for UDP traffic destined to port 2152. A GTP sanity drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a default action TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.103 gtp-traffic

gtp-traffic

Syntax [**no**] **gtp-traffic**

Context **[Tree]** (config>app-assure>group>policer gtp-traffic)

Full Context configure application-assurance group policer gtp-traffic

Description This command provides a mechanism to configure a policer to function at the GTP tunnel level. GTP tunnels are defined by a TEID and destination IP address as oppose to normal flows that are defined by IP 5 tuple values. By setting this value, the policer then can be used to limit GTP traffic (SeGW GTP firewall application).

The **no** form of this command resets policer behavior to act at the normal 5 tuple flow level and not at the GTP tunnel level.

Default no gtp-traffic

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.104 gtp-tunnel-database

gtp-tunnel-database

Syntax **gtp-tunnel-database**

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr gtp-tunnel-database)

Full Context configure application-assurance group gtp gtp-filter gtp-tunnel-database

Description Commands in this context configure GTP advanced firewall functions (such as validating GTP tunnels, sequence numbers, source IP addresses).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

gtp-tunnel-database

Syntax **gtp-tunnel-database** *size*

Context **[Tree]** (config>isa>aa-grp>shr-res-pool gtp-tunnel-database)

Full Context configure isa application-assurance-group shared-resources gtp-tunnel-database

Description This command configures the allocation of memory resources required for stateful GTP firewall deployment on 3GPP S5/S8/Gn/Gp interfaces.

Default gtp-tunnel-database 0

Parameters *size* — Specifies the percentage of allocated memory resources.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.105 gtp-user

gtp-user

Syntax **gtp-user**

Context **[Tree]** (config>test-oam>build-packet>header gtp-user)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (debug>oam>build-packet>packet>field-override>header gtp-user)

Full Context configure test-oam build-packet header gtp-user
debug oam build-packet packet field-override header gtp-user

Description This command causes the associated header to be defined as a GTP user header template and enables the context to define the GTP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.106 gtp-user-name

gtp-user-name

Syntax **gtp-user-name** {**imsi** | **imsi-apn** | **msisdn** | **msisdn-apn**}
no gtp-user-name

Context **[Tree]** (config>subscr-mgmt>auth-plcy gtp-user-name)

Full Context configure subscriber-mgmt authentication-policy gtp-user-name

Description This command configures the username used to authenticate an FWA session. If a PAP message is present in the PCO IE of the Create Session request, the system uses that for authentication instead of the format specified for this command. If you specify a format that includes APN, the separator is an @ character; for example, msisdn@apn.

The **no** form of this command reverts to the default.

Default gtp-user-name imsi

Parameters **imsi** — Specifies to use IMSI as the username.

imsi-apn — Specifies to use IMSI and APN as the username; for example, imsi@apn.

msisdn — Specifies to use MSISDN as the username.

msisdn-apn — Specifies to use MSISDN and APN as the username; for example, msisdn@apn.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.107 gtpc-inspection

gtpc-inspection

Syntax [**no**] **gtpc-inspection**

Context **[Tree]** (config>app-assure>group>gtp gtpc-inspection)

Full Context configure application-assurance group gtp gtpc-inspection

Description This command configures the inspection of GTP-C packets. This is relevant only when AA GTP FW is deployed on S8/S5/Gp/Gn interfaces. The **gtpc-inspection** command must be enabled before configuring related features, such as APN filtering, GTP tunnel validation, message-type-v2 filtering, sequence number validation, SRC IP validation.

The **no** form of this command disables GTP-C packet inspection.

Default no gtpc-inspection

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.108 gtpv1-c

gtpv1-c

Syntax **gtpv1-c** *type* **direction** {**ingress** | **egress**} **script** [*script*]
no gtpv1-c *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy gtpv1-c)

Full Context configure python python-policy gtpv1-c

Description This command configures a Python script for the specified GTPv1-C message type in the specified direction.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type.

Values echo-request, echo-response, version-not-supported, create-pdp-context-request, create-pdp-context-response, delete-pdp-context-request, delete-pdp-context-response, error-indication

direction {**ingress** | **egress**} — Specifies if the message is incoming or outgoing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

script — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

11.109 gtpv2-c

gtpv2-c

Syntax **gtpv2-c** *type* **direction** {**ingress** | **egress**} **script** [*script*]
no gtpv2-c *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy gtpv2-c)

Full Context configure python python-policy gtpv2-c

Description This command configures a Python script for the specified GTPv2-C message type in the specified direction.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type

Values echo-request, echo-response, version-not-supported, create-session-request, create-session-response, delete-session-request, delete-session-response, delete-bearer-request, delete-bearer-response, modify-bearer-request, modify-bearer-response, release-access-bearers-request, release-access-bearers-response, downlink-data-notification, downlink-data-notification-ack, change-notification-request, change-notification-response, stop-paging-indication

direction {**ingress** | **egress**} — Specifies if the message is incoming or outgoing.

script — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

11.110 guard-time

guard-time

Syntax **guard-time** *time*
no guard-time

Context **[Tree]** (config>eth-ring guard-time)

Full Context configure eth-ring guard-time

Description This command configures the guard time for an Eth-Ring. The guard timer is standard and is configurable from “x” ms to 2 seconds.

The **no** form of this command restores the default guard-time.

Default no guard-time

Parameters *value* — Specifies the guard-time, in deciseconds.

Values 1 to 20

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

11.111 gw-address-range

gw-address-range

Syntax **gw-address-range start** *start* **end** *end*
no gw-address-range

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>evpn>export gw-address-range)

Full Context configure subscriber-mgmt isa-service-chaining evpn export gw-address-range

Description This command specifies the address range to be used for the gateway IP address field in EVPN type-5 routes that are advertised for configured NAT pools, to the peer for service-chaining. The system allocates one address for each ISA in the NAT group out of the specified range.

The **no** form of this command removes the values from the configuration..

Parameters *start* — Specifies the starting gateway address range (V4) for this EVPN service.

Values ipv4-address: a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

end — Specifies the ending gateway address range (V4) for this EVPN service.

Values ipv4-address: a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.112 gw-addresses

gw-addresses

Syntax **gw-addresses**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw gw-addresses)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw gw-addresses)

Full Context configure service ies subscriber-interface group-interface wlan-gw gw-addresses
configure service vprn subscriber-interface group-interface wlan-gw gw-addresses

Description This command specifies gateway endpoint address for the wlan-gw tunnel.

The **no** form of this command removes the gateway ipv4 or IPv6 endpoint address for the wlan-gw tunnel.

Parameters *ip-address* — Specifies the IP address of the wlan-gw tunnels on this group interface.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

11.113 gw-mac

gw-mac

Syntax **gw-mac** *mac-address*
no gw-mac

Context **[Tree]** (config>service>vprn>sub-if>grp-if>srrp gw-mac)

Full Context configure service vprn subscriber-interface group-interface srrp gw-mac

Description This command overrides the default SRRP gateway MAC address used by the SRRP instance. Unless specified, the system uses the same base MAC address for all SRRP instances with the last octet overridden by the lower 8 bits of the SRRP instance ID. The same SRRP gateway MAC address should be in-use by both the local and remote routers participating in the same SRRP context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

One reason to change the default SRRP gateway MAC address is if two SRRP instances sharing the same broadcast domain are using the same SRRP gateway MAC. The system will use the SRRP instance ID to separate the SRRP messages (by ignoring the messages that does not match the local instance ID), but a unique SRRP gateway MAC is essential to separate the routed packets for each gateway IP address.

The **no** form of this command removes the explicit SRRP gateway MAC address from the SRRP instance. The SRRP gateway MAC address can only be changed or removed when the SRRP instance is shutdown.

Parameters *mac-address* — Specifies a MAC address that is used to override the default SRRP base MAC address.

Values Any MAC address except all zeros, broadcast or multicast addresses. The offset is expressed in normal Ethernet MAC address notation. The defined gw-mac cannot be 00:00:00:00:00:00, ff:ff:ff:ff:ff:ff or any multicast address.

If not specified, the system uses the default SRRP gateway MAC address with the last octet set to the 8 least significant bits of the SRRP instance ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

gw-mac

Syntax **gw-mac** *mac-address*
no gw-mac

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp gw-mac)

Full Context configure service ies subscriber-interface group-interface srrp gw-mac

Description This command overrides the default SRRP gateway MAC address used by the SRRP instance. Unless specified, the system uses the same base MAC address for all SRRP instances with the last octet overridden by the lower 8 bits of the SRRP instance ID. The same SRRP gateway MAC address should be in-use by both the local and remote routers participating in the same SRRP context.

One reason to change the default SRRP gateway MAC address is if two SRRP instances sharing the same broadcast domain are using the same SRRP gateway MAC. The system will use the SRRP instance ID to separate the SRRP messages (by ignoring the messages that does not match the local instance ID), but a unique SRRP gateway MAC is essential to separate the routed packets for each gateway IP address.

The **no** form of this command removes the explicit SRRP gateway MAC address from the SRRP instance. The SRRP gateway MAC address can only be changed or removed when the SRRP instance is shutdown.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac-address* — Specifies a MAC address that is used to override the default SRRP base MAC address.

Values Any MAC address except all zeros, broadcast or multicast addresses. The offset is expressed in normal Ethernet MAC address notation. The defined gw-mac cannot be 00:00:00:00:00:00, ff:ff:ff:ff:ff:ff or any multicast address.

If not specified, the system uses the default SRRP gateway MAC address with the last octet set to the 8 least significant bits of the SRRP instance ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.114 gx

gx

Syntax **gx**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy gx)

Full Context configure subscriber-mgmt diameter-application-policy gx

Description Commands in this context configure Gx parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.115 gx-session-level-usage

gx-session-level-usage

Syntax [**no**] **gx-session-level-usage**

Context **[Tree]** (config>subscr-mgmt>cat-map gx-session-level-usage)

Full Context configure subscriber-mgmt category-map gx-session-level-usage

Description This command controls the instantiation of an internal category required for Diameter Gx session level Usage Monitoring (per IP-CAN session).

When configured, Gx session level Usage Monitoring can be enabled for sessions associated with this category map.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The internal category for Gx session level Usage Monitoring is counted against the maximum of sixteen categories that can be configured.

When not configured (default), then no internal category is instantiated and Gx session level Usage Monitoring cannot be enabled for sessions associated with this category map.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

11.116 gy

gy

Syntax **gy**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy gy)

Full Context configure subscriber-mgmt diameter-application-policy gy

Description Commands in this context configure Diameter Credit Control Application or Gy-specific options.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12 h Commands

12.1 half-life

half-life

Syntax **half-life** *half-life* **max-suppress-time** *max-time*

Context **[Tree]** (config>port>ethernet>dampening half-life)

Full Context configure port ethernet dampening half-life

Description This command configures the half-life decay time and the maximum period of time for which the port up state can be suppressed.

The *half-life* and *max-time* values must be set at the same time; the ratio of *max-time*/*half-life* must be less than or equal to 49 and greater than or equal to 1.

Parameters *half-life* — Specifies the required elapsed time, in seconds, before penalties decay to one-half the initial amount.

Values 1 to 2000

Default 5

max-time — Specifies the maximum suppression time, in seconds, which is the time it can take after the physical link comes up before the worst case accumulated penalties have decayed to the reuse threshold. The maximum penalty is derived from the maximum suppression time, half-life, and reuse threshold, using the following equation:

maximum penalty = (reuse threshold) × 2 expo:(max-time/half-life)

Values 1 to 43200

Default 20

Platforms All

half-life

Syntax **half-life** *minutes*
no half-life

Context **[Tree]** (config>router>policy-options>damping half-life)

Full Context configure router policy-options damping half-life

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the **half-life** parameter for the route damping profile.

The half-life value is the time, expressed in minutes, required for a route to remain stable in order for the Figure of Merit (FoM) value to be reduced by one half; for example, if the half-life value is 6 (minutes) and the route remains stable for 6 minutes, then the new FoM value is 3 (minutes). After another 3 minutes pass and the route remains stable, the new FoM value is 1.5 (minutes).

When the FoM value falls below the **config>router>policy-options>damping reuse** threshold, the route is once again considered valid and can be reused or included in route advertisements.

The **no** form of this command removes the half life parameter from the damping profile.

Default no half-life

Parameters *minutes* — Specifies the half-life in minutes expressed as a decimal integer.

Values 1 to 45

Platforms All

12.2 handler

handler

Syntax [**no**] **handler** *event-handler-name*

Context **[Tree]** (config>log>event-handling handler)

Full Context configure log event-handling handler

Description This command configures an EHS handler.

The **no** form of this command removes the specified EHS handler.

Parameters *event-handler-name* — Specifies the name of the EHS handler, up to 32 characters maximum.

Platforms All

handler

Syntax **handler** *name* **[create]**
no handler *name*

Context **[Tree]** (config>system>grpc-tunnel>tunnel handler)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system grpc-tunnel tunnel handler

Description Commands in this context configure tunnel handler parameters. There can be multiple handlers created for any tunnel.

The **no** form of this command removes the specified tunnel handler.

Parameters *name* — Specifies the handler name, up to 32 characters.

create — Keyword used to create a tunnel.

Platforms All

12.3 hardware-timestamp

hardware-timestamp

Syntax [**no**] **hardware-timestamp**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes hardware-timestamp)

Full Context configure aaa isa-radius-policy acct-include-attributes hardware-timestamp

Description This command enables the inclusion of the hardware timestamp attributes.

The **no** form of the command excludes the hardware timestamp attributes.

Default no hardware-timestamp

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.4 hash-algorithm

hash-algorithm

Syntax **hash-algorithm** {**hash** | **hash2** | **custom**| **cleartext**}
no hash-algorithm

Context **[Tree]** (config>system>security>management-interface>grpc hash-algorithm)
[Tree] (config>system>security>management-interface>md-cli hash-algorithm)
[Tree] (config>system>security>management-interface>netconf hash-algorithm)

Full Context configure system security management-interface grpc hash-algorithm
configure system security management-interface md-cli hash-algorithm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system security management-interface netconf hash-algorithm

Description This command specifies the format of the input and output for encrypted configuration secrets.

The **no** form of this command reverts to the default value.

Default hash-algorithm hash2

Parameters **hash** — Specifies hash. Use this option to transport a phrase between modules and nodes.

hash2 — Specifies hash2 which is module-specific.

custom — Specifies the custom encryption to management interface.

cleartext — Specifies that the phrase is displayed as clear text everywhere.

Platforms All

12.5 hash-label

hash-label

Syntax **hash-label**
hash-label [**signal-capability**]
no hash-label

Context **[Tree]** (config>service>epipe>spoke-sdp hash-label)
[Tree] (config>service>fpipe>spoke-sdp hash-label)
[Tree] (config>service>ipipe>spoke-sdp hash-label)
[Tree] (config>service>pw-template hash-label)

Full Context configure service epipe spoke-sdp hash-label
configure service fpipe spoke-sdp hash-label
configure service ipipe spoke-sdp hash-label
configure service pw-template hash-label

Description This command enables the use of the hash label on a VLL, VPRN or VPLS service bound to any MPLS type encapsulated SDP, as well as to a VPRN service that is using the **auto-bind-tunnel** with the **resolution-filter** set to any MPLS tunnel type. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option. This feature is also not supported on multicast packets forwarded using RSVP P2MP LSP or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance. It is, however, supported when forwarding multicast packets using an IES/VPRN spoke-interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

To allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note, however, that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh SDP, or an IES/VPRN spoke interface by adding the **signal-capability** option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The local PE will insert the flow label interface parameters sub-TLV with F=1 in the PW ID FEC element in the label mapping message for that spoke SDP or mesh SDP.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the **hash-label** option or the **signal-capability** option), then the local PE establishes the PW but must not insert the hash label in the user and control packets over that spoke SDP or mesh SDP. If the remote PE does not support the **signal-capability** option, then there are a couple of possible outcomes:
  - If the **hash-label** option was enabled on the local configuration of the spoke SDP or mesh SDP at the remote PE, the PW packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.
  - If the **hash-label** option is not supported or was not enabled on the local configuration of the spoke SDP or mesh SDP at the remote PE, the PW received by the local PE will not have the hash label included.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The user can enable or disable the signal-capability option in CLI as needed. When doing so, the 7450 ESS or 7750 SR must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

The **no** form of this command disables the use of the hash label.

Default no hash-label

Parameters **signal-capability** — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The **signal-capability** option is not supported on a VPRN spoke-sdp.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp hash-label

All

- configure service ipipe spoke-sdp hash-label
- configure service pw-template hash-label
- configure service epipe spoke-sdp hash-label

hash-label

Syntax **hash-label signal-capability**
hash-label
no hash-label

Context **[Tree]** (config>service>vpls>spoke-sdp hash-label)
[Tree] (config>service>vpls>mesh-sdp hash-label)

Full Context configure service vpls mesh-sdp hash-label
configure service vpls spoke-sdp hash-label

Description This command enables the use of the hash label on a VLL, VPRN, or VPLS service bound to any MPLS type encapsulated SDP, as well as to a VPRN service using the **auto-bind-tunnel** with the **resolution-filter** set to any MPLS tunnel type. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option. This feature is also not supported on multicast packets forwarded using RSVP P2MP LSP or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance. It is, however, supported when forwarding multicast packets using an IES/VPRN spoke-interface.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note, however, that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the **signal-capability** option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The 7450 ESS, 7750 SR, and 7950 XRS local PE will insert the flow label interface parameters sub-TLV with F=1 in the pseudowire ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the **hash-label** option or the **signal-capability** option), then the local PE establishes the pseudowire but must not insert the hash label in the user and control packets over that spoke-sdp or mesh-sdp. If the remote PE does not support the **signal-capability** option, then there are a couple of possible outcomes:
  - If the **hash-label** option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.
  - If the **hash-label** option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire received by the local PE will not have the hash label included.
- The user can enable or disable the signal-capability option in CLI as needed. When doing so, the 7450 ESS, 7750 SR, and 7950 XRS must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the pseudowire ID FEC element.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the use of the hash label.

Default no hash-label

Parameters **signal-capability** — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The **signal-capability** option is not supported on a VPRN spoke-sdp.

Platforms All

hash-label

Syntax **hash-label** [**signal-capability**]
no hash-label

Context **[Tree]** (config>service>ies>if>spoke-sdp hash-label)

Full Context configure service ies interface spoke-sdp hash-label

Description This command enables the use of the hash label on a VLL, VPLS, or VPRN service bound to any MPLS-type encapsulated SDP, as well as to a VPRN service using **auto-bind-tunnel** with the **resolution-filter** configures as any MPLS tunnel type. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to 1 to indicate that.

In order to allow for applications whereby the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the hash label. This means that the value of the hash label will always be in the range [524,288 to 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. For VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets that are generated in CPM and forwarded labeled within the context of a service (for example, OAM packets) must also include a hash label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the **signal-capability** option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The local PE will insert the flow label interface parameters sub-TLV with F=1 in the PW ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the **hash-label** option or the **signal-capability** option), then the local PE establishes the PW but must not insert the hash label in the user and control packets over that spoke-sdp or mesh-sdp. If the remote PE does not support the **signal-capability** option, then there are a couple of possible outcomes:
  - If the **hash-label** option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.
  - If the **hash-label** option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW received by the local PE will not have the hash label included.
- The user can enable or disable the signal-capability option in CLI as needed. When doing so, the router must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

The **no** form of this command disables the use of the hash label.

Default no hash-label

Parameters **signal-capability** — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The **signal-capability** option is not supported on a VPRN spoke-sdp.

Platforms All

hash-label

Syntax **hash-label**
hash-label signal-capability
no hash-label

Context **[Tree]** (config>service>vprn hash-label)
[Tree] (config>service>vprn>spoke-sdp hash-label)
[Tree] (config>service>vprn>if>spoke-sdp hash-label)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn hash-label
configure service vprn interface spoke-sdp hash-label
configure service vprn spoke-sdp hash-label

Description This command enables the use of the hash label on a VLL, VPLS, or VPRN service bound to any MPLS-type encapsulated SDP as well as to a VPRN service using **auto-bind-tunnel** with the **resolution-filter** configured as any MPLS tunnel type. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to 1 to indicate that.

In order to allow for applications whereby the egress LER infers the presence of the Hash Label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. For VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets that are generated in CPM and forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The **no** form of this command disables the use of the hash label.

Default no hash-label

Parameters **signal-capability** — Specifies whether the service should send the Stack Capability and check whether the capability is received from the peer via LDP interface parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.6 hash-mask-len

hash-mask-len

Syntax **hash-mask-len** *hash-mask-length*
no hash-mask-len

Context **[Tree]** (config>service>vprn>pim>rp>bsr-candidate hash-mask-len)

Full Context configure service vprn pim rp bsr-candidate hash-mask-len

Description This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Default hash-mask-len 30

Parameters *hash-mask-length* — The hash mask length.

Values 0 to 32

Platforms All

hash-mask-len

Syntax **hash-mask-len** *hash-mask-length*
no hash-mask-len

Context **[Tree]** (config>service>vprn>pim>rp>ipv6>bsr-candidate hash-mask-len)

Full Context configure service vprn pim rp ipv6 bsr-candidate hash-mask-len

Description This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Default hash-mask-len 126

Parameters *hash-mask-length* — The hash mask length.

Values 0 to 128

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash-mask-len

Syntax **hash-mask-len** *hash-mask-length*
no hash-mask-len

Context [Tree] (config>router>pim>rp>bsr-candidate hash-mask-len)
[Tree] (config>router>pim>rp>ipv6>bsr-candidate hash-mask-len)

Full Context configure router pim rp bsr-candidate hash-mask-len
configure router pim rp ipv6 bsr-candidate hash-mask-len

Description This command configures the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

The **no** form of this command reverts to the default value.

Default hash-mask-len 30 — for **config**>**router**>**pim**>**rp**>**bsr-candidate**

hash-mask-len 126 — for **config**>**router**>**pim**>**rp**>**ipv6**>**bsr-candidate**

Parameters *hash-mask-length* — Specifies the hash mask length.

Values 0 to 32 (v4)
0 to 128 (v6)

Platforms All

12.7 hash-weight-threshold

hash-weight-threshold

Syntax **hash-weight-threshold** *weight* [**action** *action*] [**cost** *static-cost*]
no hash-weight-threshold

Context [Tree] (config>lag hash-weight-threshold)

Full Context configure lag hash-weight-threshold

Description This command controls the operational status of the LAG or the IGP cost based on the sum of the **hash-weight** values for the active links in the LAG.

The **no** form of this command disables the hash weight threshold.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *weight* — Specifies the value for the sum of all the active LAG ports **hash-weight** at or below which the configured action is invoked. If the sum of **hash-weight** for operational LAG links exceeds the **hash-weight-threshold** value, then no action is taken.

Values 1 to 6400000

action — Specifies the action to take if the sum of the **hash-weight** for active links in the LAG is equal or below the threshold value.

Values
down — Specifies that the LAG is operationally DOWN. The LAG is only considered as UP once the number of **hash-weight** for the active links exceeds the configured threshold value.

dynamic-cost — Specifies that dynamic cost is activated. The LAG remains operationally UP with a link cost relative to the number of operational links. The link is only considered as operationally DOWN when all links in the LAG are down.

static-cost — Specifies that static cost is activated. The LAG remains operationally UP with the configured cost, regardless of the number of operational links. The link is only considered as operationally DOWN when all links in the LAG are down. If this parameter is used with an IGP, its **reference-bandwidth** must also be configured.

static-cost — Specifies the decimal integer static cost of the LAG.

Values 1 to 16777215

Platforms All

12.8 hashing

hashing

Syntax **hashing** {**bcrypt** | **sha2-pbkdf2**| **sha3-pbkdf2**}

Context **[Tree]** (config>system>security>password hashing)

Full Context configure system security password hashing

Description This command configures the password hashing algorithm.

Default hashing bcrypt

Parameters **bcrypt** — Keyword to indicate that the command configures the bcrypt algorithm.

sha2-pbkdf2 — Keyword to indicate that the command configures the PBKDF2 algorithm hashed via SHA2.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sha3-pbkdf2 — Keyword to indicate that the command configures the PBKDF2 algorithm hashed via SHA3.

Platforms All

12.9 hd

hd

Syntax **hd**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if hd)

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd

Description This command configures properties relating to requests received by the video interface for High Definition (HD) channel requests.

Default none

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

12.10 head-end

head-end

Syntax **head-end local**
head-end *ipv4-address*
no head-end

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy head-end)

Full Context configure router segment-routing sr-policies static-policy head-end

Description This command associates a head-end location with a statically-defined segment-routing policy. The head-end identifies the router that is the target to install the policy. This is a mandatory parameter and configuration command for enabling the segment-routing policy; if the head-end parameter value is not configured, the execution of the **no shutdown** command on the static segment routing policy fails.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To associate a static policy with the local router as head-end, the keyword **local** must be specified. The static policy is associated with another (non-local) router, if the head-end parameter is set to any IPv4 address. When a non-local, static segment routing policy that originates as a BGP route is imported into BGP, the configured head-end address is converted to an IPv4-address specific route-target extended community that is automatically added to the route.

The **no** form of this command removes the head-end association.

Default no head-end

Parameters **local** — Keyword indicating that the policy is intended to be used by the local router and not advertised to other BGP routers.

ipv4-address — Specifies the IP address of the target head-end router.

Values
ipv4-address: a.b.c.d

Platforms All

12.11 header

header

Syntax **header** *header-number* [**create**]
no header *header-number*

Context **[Tree]** (config>test-oam>build-packet header)
[Tree] (debug>oam>build-packet>packet>field-override header)

Full Context configure test-oam build-packet header
debug oam build-packet packet field-override header

Description Commands in this context configure header parameters.

The **no** form of this command deletes the associated header.

Parameters *header-number* — Specifies the ID for the header being defined or referenced.

Values 1 to 65535

create — Creates a header instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.12 header-sanity

header-sanity

Syntax **header-sanity direction** *direction* [**create**]
no header-sanity direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-fltr>msg header-sanity)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type header-sanity

Description This command configures a TCA for the counter capturing hits for the GTP filter header sanity. A GTP filter header-sanity TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.13 header-sequence

header-sequence

Syntax **header-sequence** *header-sequence*
no header-sequence

Context **[Tree]** (debug>oam>build-packet>packet header-sequence)

Full Context debug oam build-packet packet header-sequence

Description This command configures the sequence of headers for a packet to be launched by the OAM **find-egress** tool.

Parameters *header-sequence* — Specifies the sequence of headers, such as "h7/h255/h32", where h7 is the header for the lowest level protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.14 health-check

health-check

Syntax **health-check**

Context **[Tree]** (config>aaa>radius-server-policy>servers health-check)

Full Context configure aaa radius-server-policy servers health-check

Description Commands in this context configure health check parameters for the RADIUS server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

health-check

Syntax [**no**] **health-check** [**interval** *interval*]

Context **[Tree]** (config>system>security>password health-check)

Full Context configure system security password health-check

Description This command specifies that RADIUS, TACACS+, and LDAP servers are monitored for 3 seconds each at 30 second intervals. Servers that are not configured will have 3 seconds of idle time. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, a trap will be sent based on the type of the server.

The **no** form of this command disables the periodic monitoring of the RADIUS, TACACS+, and LDAP servers. In this case, the operational status for the active server will be up if the last access was successful.

Default health-check interval 30

Parameters *interval* — Specifies the polling interval for RADIUS, TACACS+, and LDAP servers.

Values 6 to 1500

Default 30

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.15 heartbeat

heartbeat

Syntax **heartbeat**

Context **[Tree]** (config>subscr-mgmt>pfcp-association heartbeat)

Full Context configure subscriber-mgmt pfcp-association heartbeat

Description Commands in this context configure parameters for transmitting PFCP Heartbeat Request messages to a PFCP peer.

Default heartbeat

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

12.16 hello

hello

Syntax **hello** [**interval** *hello-interval*] **dead-interval** *hello-dead-interval*
hello interval *hello-interval* [**dead-interval** *hello-dead-interval*]

Context **[Tree]** (config>router>lmp>peer>control-channel hello)

Full Context configure router lmp peer control-channel hello

Description This command configures the transmission interval for LMP Hello packets. The **dead-interval** specifies the period after which the IPCC is declared down if no Hello packets are received from the LMP peer.

Default hello interval 1000 dead-interval 4000

Parameters *hello-interval* — The interval at which LMP Hello packets are sent on an IP control channel.

Values 1000 to 65535 ms

hello-dead-interval — The interval after which the IPCC is declared down if no Hello packets are received from the LMP peer.

Values 3000 to 65535 ms

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hello

Syntax **hello** [**detail**]
no hello

Context **[Tree]** (debug>router>gmpls>packet hello)

Full Context debug router gmpls packet hello

Description This command enables debugging for GMPLS Hello packets.

The **no** form of the command disables debugging for GMPLS Hello packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

hello

Syntax **hello** *timeout factor*
no hello

Context **[Tree]** (config>router>ldp>if-params>if>ipv4 hello)
[Tree] (config>router>ldp>if-params>if>ipv6 hello)
[Tree] (config>router>ldp>if-params>ipv4 hello)
[Tree] (config>router>ldp>if-params>ipv6 hello)
[Tree] (config>router>ldp>targ-session>ipv4 hello)
[Tree] (config>router>ldp>targ-session>ipv6 hello)
[Tree] (config>router>ldp>targ-session>peer hello)
[Tree] (config>router>ldp>targ-session>peer-template hello)

Full Context configure router ldp interface-parameters interface ipv4 hello
configure router ldp interface-parameters interface ipv6 hello
configure router ldp interface-parameters ipv4 hello
configure router ldp interface-parameters ipv6 hello
configure router ldp targeted-session ipv4 hello
configure router ldp targeted-session ipv6 hello
configure router ldp targeted-session peer hello
configure router ldp targeted-session peer-template hello

Description This command configures the time interval to wait before declaring a neighbor down. The **factor** parameter derives the Hello interval.

The **config**>**router**>**ldp**>**if-params**>**ipv6**>**hello** and **config**>**router**>**ldp**>**targ-session**>**ipv6**>**hello** commands are not supported on the 7450 ESS.

Hold time is local to the system and sent in the Hello messages to the neighbor. Hold time cannot be less than three times the Hello interval. The hold time can be configured globally (applies to all LDP interfaces) or per interface. The most specific value is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When LDP session is being set up, the hold down time is negotiated to the lower of the two peers. Once an operational value is agreed upon, the Hello factor is used to derive the value of the Hello interval.

The **no** form of the command at the interface-parameters and targeted-session level sets the **hello timeout** and the **hello factor** to the default values.

The **no** form of the command, at the interface level, sets the **hello timeout** and the **hello factor** to the value defined under the interface-parameters level.

The **no** form of this command, at the peer level, sets the **hello timeout** and the **hello factor** to the value defined under the targeted-session level.

The session must be flapped for the new settings to operate.

Default Table 61 lists the default values.

Table 61 **Hello Timeout Factors**

Context	Timeout	Factor
config>router>ldp>if-params	15	3
config>router>ldp>targ-session	45	3
config>router>ldp>if-params>if	Inherits values from interface-parameters context.	
config>router>ldp>targ-session>peer	Inherits values from targeted-session context.	

Parameters *timeout* — Configures the time interval, in seconds, that LDP waits before a neighbor down.

Values 1 to 65535

factor — Specifies the number of keepalive messages that should be sent on an idle LDP session in the Hello timeout interval.

Values 1 to 255

Platforms All

hello

Syntax **hello** [**detail**]
no hello

Context **[Tree]** (debug>router>ldp>if>packet hello)
[Tree] (debug>router>ldp>peer>packet hello)

Full Context debug router ldp interface packet hello

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router ldp peer packet hello

Description This command enables debugging for LDP Hello packets.

The **no** form of the command disables the debugging output.

Parameters **detail** — Displays detailed information.

Platforms All

hello

Syntax **hello** [**detail**]
no hello

Context **[Tree]** (debug>router>rsvp>packet hello)

Full Context debug router rsvp packet hello

Description This command debugs Hello packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about Hello packets.

Platforms All

12.17 hello-auth-keychain

hello-auth-keychain

Syntax **hello-auth-keychain** *name*

Context **[Tree]** (config>router>isis hello-auth-keychain)
[Tree] (config>router>isis>level hello-auth-keychain)

[Tree] (config>service>vprn>isis>interface hello-auth-keychain)
[Tree] (config>service>vprn>isis>interface>level hello-auth-keychain)

Full Context configure router isis hello-auth-keychain
configure router isis level hello-auth-keychain
configure service vprn isis interface hello-auth-keychain
configure service vprn isis interface level hello-auth-keychain

Description This command configures an authentication keychain to use for the protocol interface. The keychain allows the rollover of authentication keys during the lifetime of a session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no hello-auth-keychain

Parameters *name* — Specifies the name of the keychain, up to 32 characters, to use for the specified protocol session or sessions.

Platforms All

12.18 hello-authentication

hello-authentication

Syntax [**no**] **hello-authentication**

Context **[Tree]** (config>service>vprn>isis hello-authentication)
[Tree] (config>service>vprn>isis>if hello-authentication)
[Tree] (config>service>vprn>isis>level hello-authentication)

Full Context configure service vprn isis hello-authentication
configure service vprn isis interface hello-authentication
configure service vprn isis level hello-authentication

Description This command enables authentication of individual IS-IS Hello packets for the VPRN instance.

The **no** form of this command suppresses authentication of Hello packets.

Platforms All

hello-authentication

Syntax [**no**] **hello-authentication**

Context **[Tree]** (config>router>isis hello-authentication)
[Tree] (config>router>isis>interface hello-authentication)
[Tree] (config>router>isis>level hello-authentication)

Full Context configure router isis hello-authentication
configure router isis interface hello-authentication
configure router isis level hello-authentication

Description This command enables authentication of individual IS-IS packets of HELLO type.

The **no** form of this command suppresses authentication of HELLO packets.

Default hello-authentication

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.19 hello-authentication-key

hello-authentication-key

Syntax **hello-authentication-key** {*authentication-key* | *hash-key*} [**hash** | **hash2** | **custom**]
no hello-authentication-key

Context **[Tree]** (config>service>vprn>isis>if hello-authentication-key)
[Tree] (config>service>vprn>isis>if>level hello-authentication-key)

Full Context configure service vprn isis interface hello-authentication-key
configure service vprn isis interface level hello-authentication-key

Description This command configures the authentication key (password) for Hello PDUs. Neighboring routers use the password to verify the authenticity of Hello PDUs sent from this interface. Both the Hello authentication key and the Hello authentication type on a segment must match. The **hello-authentication-type** must be specified.

To configure the Hello authentication key in the interface context use the **hello-authentication-key** in the **config>router>isis>if** context.

To configure or override the Hello authentication key for a specific level, configure the **hello-authentication-key** in the **config>router>isis>if>level** context.

If both IS-IS and hello-authentication are configured, Hello messages are validated using Hello authentication. If only IS-IS authentication is configured, it will be used to authenticate all IS-IS (including Hello) protocol PDUs.

When the Hello authentication key is configured in the **config>router>isis>if** context, it applies to all levels configured for the interface.

The **no** form of this command removes the authentication-key from the configuration.

Default no hello-authentication-key — No Hello authentication key is configured.

Parameters *authentication-key* — The Hello authentication key (password). The key can be any combination of ASCII characters up to 254 characters in length (un-encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

hello-authentication-key

Syntax **hello-authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2** | **custom**]
no hello-authentication-key

Context **[Tree]** (config>router>isis>interface hello-authentication-key)
[Tree] (config>router>isis>if>level hello-authentication-key)

Full Context configure router isis interface level hello-authentication-key
configure router isis interface hello-authentication-key

Description This command configures the authentication key (password) for Hello PDUs. Neighboring routers use the password to verify the authenticity of Hello PDUs sent from this interface. Both the Hello authentication key and the Hello authentication type on a segment must match. The **hello-authentication-type** must be specified.

To configure the Hello authentication key in the interface context, use the **hello-authentication-key** in the **config>router>isis>interface** context.

To configure or override the Hello authentication key for a specific level, configure the **hello-authentication-key** in the **config>router>isis>interface>level** context.

If both IS-IS and hello-authentication are configured, Hello messages are validated using Hello authentication. If only IS-IS authentication is configured, it will be used to authenticate all IS-IS (including Hello) protocol PDUs.

When the Hello authentication key is configured in the **config>router>isis>interface** context, it applies to all levels configured for the interface.

The **no** form of this command removes the authentication-key from the configuration.

Parameters *authentication-key* — Specifies the Hello authentication key (password). The key can be any combination of ASCII characters, up to 254 characters (un-encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — Specifies the hash key. The key can be any combination of ASCII characters, up to 342 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

12.20 hello-authentication-type

hello-authentication-type

Syntax **hello-authentication-type** {**password** | **message-digest**}
no hello-authentication-type

Context **[Tree]** (config>service>vprn>isis>if hello-authentication-type)
[Tree] (config>service>vprn>isis>if>level hello-authentication-type)

Full Context configure service vprn isis interface hello-authentication-type
configure service vprn isis interface level hello-authentication-type

Description This command enables Hello authentication at either the interface or level context. Both the Hello authentication key and the Hello authentication type on a segment must match. The hello **authentication-key** statement must also be included.

To configure the Hello authentication type at the interface context, use **hello-authentication-type** in the **config>router>isis>if** context.

To configure or override the Hello authentication setting for a given level, configure the **hello-authentication-type** in the **config>router>isis>if>level** context.

The **no** form of this command disables Hello authentication.

Default no hello-authentication-type — Hello authentication is disabled

Parameters **password** — Specifies simple password (plain text) authentication is required.

message-digest — Specifies MD5 authentication in accordance with RFC2104 (HMAC: Keyed-Hashing for Message Authentication) is required.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hello-authentication-type

Syntax **hello-authentication-type** {**password** | **message-digest**}
no hello-authentication-type

Context **[Tree]** (config>router>isis>interface hello-authentication-type)
[Tree] (config>router>isis>if>level hello-authentication-type)

Full Context configure router isis interface level hello-authentication-type
configure router isis interface hello-authentication-type

Description This command enables Hello authentication at either the interface or level context. Both the Hello authentication key and the Hello authentication type on a segment must match. The hello **authentication-key** statement must also be included.

To configure the Hello authentication type at the interface context, use **hello-authentication-type** in the **config>router>isis>interface** context.

To configure or override the Hello authentication setting for a given level, configure the **hello-authentication-type** in the **config>router>isis>interface>level** context.

The **no** form of this command disables Hello authentication.

Parameters **password** — Specifies simple password (plain text) authentication is required.

message-digest — Specifies MD5 authentication in accordance with RFC 2104 (HMAC: Keyed-Hashing for Message Authentication) is required.

Platforms All

12.21 hello-interval

hello-interval

Syntax **hello-interval** *hello-interval*
hello-interval infinite
no hello-interval

Context **[Tree]** (config>router>l2tp hello-interval)
[Tree] (config>router>l2tp>group hello-interval)
[Tree] (config>router>l2tp>group>tunnel hello-interval)
[Tree] (config>service>vprn>l2tp hello-interval)
[Tree] (config>service>vprn>l2tp>group hello-interval)
[Tree] (config>service>vprn>l2tp>group>tunnel hello-interval)

Full Context configure router l2tp group hello-interval
configure router l2tp group tunnel hello-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router l2tp hello-interval
configure service vprn l2tp group hello-interval
configure service vprn l2tp group tunnel hello-interval
configure service vprn l2tp hello-interval

Description This command configures the time interval between two consecutive tunnel Hello messages. The Hello message is an L2TP control message sent by either peer of a LAC-LNS control connection. This control message is used as a keepalive for the tunnel.

The **no** form of this command removes the interval from the configuration.

Default hello-interval 300

Parameters *hello-interval* — Specifies the time interval, in seconds, between two consecutive tunnel Hello messages.

Default no hello-interval

Values 10 to 3600

infinite — Specifies that no Hello interval messages are sent.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

hello-interval

Syntax **hello-interval** *timer*
no hello-interval

Context **[Tree]** (config>port>multilink-bundle>mlfr hello-interval)

Full Context configure port multilink-bundle mlfr hello-interval

Description This command specifies the value of the MLFR bundle T_HELLO timer. The timer controls the rate that Hello messages are sent. Following a period of T_HELLO duration, a Hello message is transmitted onto the bundle link.

Note that T_HELLO timer is also used during the bundle link add process as an additional delay before resending an ADD_LINK message to the peer bundle link when the peer bundle link does not answer as expected.

Default hello-interval 10

Parameters *timer* — Specifies the amount of time between HELLO messages in seconds.

Values 1 to 180

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hello-interval

Syntax **hello-interval** *seconds*
no hello-interval

Context **[Tree]** (config>service>vpls>sap>spb>level hello-interval)
[Tree] (config>service>vpls>spoke-sdp>spb>level hello-interval)

Full Context configure service vpls sap spb level hello-interval
configure service vpls spoke-sdp spb level hello-interval

Description This command configures the interval in seconds between Hello messages issued on this interface at this level. This command is valid only for interfaces on control B-VPLS.

The no form of this command to reverts to the default value.

Default hello-interval 3 — Hello interval default for the designated inter-system.

hello-interval 9 — Hello interval default for non-designated inter-systems.

Parameters *seconds* — The Hello interval in seconds expressed as a decimal integer.

Values 1 to 20000

Platforms All

hello-interval

Syntax **hello-interval** *seconds*
no hello-interval

Context **[Tree]** (config>router>isis>if>level hello-interval)
[Tree] (config>service>vprn>isis>if>level hello-interval)

Full Context configure router isis interface level hello-interval
configure service vprn isis interface level hello-interval

Description This command configures the interval between IS-IS Hello PDUs issued on the interface at this level. The **hello-interval**, along with the **hello-multiplier**, is used to calculate a hold time, which is communicated to a neighbor in a Hello PDU.

Note: The neighbor hold time is (hello multiplier × hello interval) on non-designated intermediate system broadcast interfaces and point-to-point interfaces and is (hello multiplier × hello interval / 3) on designated intermediate system broadcast interfaces. Hello values can be adjusted for faster convergence, but the hold time should always be > 3 to reduce routing instability.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default 3 – for designated intermediate system interfaces

9 – for non-designated intermediate system interfaces and point-to-point interfaces

Parameters *seconds* — The Hello interval in seconds expressed as a decimal integer.

Values 1 to 20000

Platforms All

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>pim hello-interval)

Full Context configure service vprn mvpn provider-tunnel inclusive pim hello-interval

Description This command configures the frequency at which PIM Hello messages are transmitted on this interface.

The **no** form of this command resets the configuration to the default value.

Default hello-interval 30

Parameters *hello-interval* — Specifies the Hello interval in seconds. A 0 (zero) value disables the sending of Hello messages (the PIM neighbor will never timeout the adjacency).

Values 0 to 255 seconds

Platforms All

hello-interval

Syntax **hello-interval** *seconds*
no hello-interval

Context **[Tree]** (config>service>vprn>ospf>area>if hello-interval)
[Tree] (config>service>vprn>ospf3>area>if hello-interval)
[Tree] (config>service>vprn>ospf>area>virtual-link hello-interval)
[Tree] (config>service>vprn>ospf3>area>virtual-link hello-interval)
[Tree] (config>service>vprn>ospf>area>sham-link hello-interval)

Full Context configure service vprn ospf area interface hello-interval
configure service vprn ospf area sham-link hello-interval
configure service vprn ospf area virtual-link hello-interval
configure service vprn ospf3 area interface hello-interval
configure service vprn ospf3 area virtual-link hello-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the interval between OSPF Hello messages issued on the interface, virtual link, or sham-link.

The Hello interval, in combination with the dead-interval, is used to establish and maintain the adjacency. Use this parameter to edit the frequency that Hello packets are sent.

Reducing the interval, in combination with an appropriate reduction in the associated **dead-interval**, allows for faster detection of link and/or router failures at the cost of higher processing costs.

The **no** form of this command reverts to the default value.

Default hello-interval 10 — a 10-second Hello interval

Special Cases **OSPF Interface —** If the configured **hello-interval** applies to an interface, then all nodes on the subnet must have the same Hello interval.

Virtual Link — If the configured **hello-interval** applies to a virtual link, then the interval on both termination points of the virtual link must have the same Hello interval.

Sham Link — If the configured **hello-interval** applies to a sham-link, then the interval on both endpoints of the sham-link must have the same Hello interval.

Parameters *seconds* — The Hello interval in seconds expressed as a decimal integer.

Values 1 to 65535

Platforms All

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context **[Tree]** (config>service>vprn>pim>if hello-interval)

Full Context configure service vprn pim interface hello-interval

Description This command configures the frequency at which PIM Hello messages are transmitted on this interface.

The **no** form of this command resets the configuration to the default value.

Default hello-interval 30

Parameters *hello-interval* — Specifies the Hello interval in seconds. A 0 (zero) value disables the sending of Hello messages (the PIM neighbor will never timeout the adjacency).

Values 0 to 255 seconds

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hello-interval

Syntax [**no**] **hello-interval** *hello-interval*

Context **[Tree]** (config>router>gmpls>peer hello-interval)

Full Context configure router gmpls peer hello-interval

Description This command configures the RSVP Hello packet interval (in ms), towards the peer UNI-N node.

The **no** form of this command sets the **hello-interval** to the default value. A value of 0 disables RSVP Hellos.

Default hello-interval 3000

Parameters *hello-interval* — Specifies the RSVP Hello packet interval, in milliseconds.

Values 0 to 60000

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

hello-interval

Syntax **hello-interval** *milli-seconds*
no hello-interval

Context **[Tree]** (config>router>rsvp>interface hello-interval)

Full Context configure router rsvp interface hello-interval

Description This command configures the time interval between RSVP Hello messages.

RSVP Hello packets are used to detect loss of RSVP connectivity with the neighboring node. Hello packets detect the loss of neighbor far quicker than it would take for the RSVP session to time out based on the refresh interval. After the loss of the of number keep-multiplier consecutive Hello packets, the neighbor is declared to be in a down state.

The **no** form of this command reverts to the default value of the hello-interval. To disable sending hello messages, set the value to zero.

Default hello-interval 3000

Parameters *milli-seconds* — Specifies the RSVP Hello interval (in ms), in multiples of 1000. A 0 (zero) value disables the sending of RSVP Hello messages.

Values 0 to 60000 ms (in multiples of 1000)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context **[Tree]** (config>router>pim>interface hello-interval)

Full Context configure router pim interface hello-interval

Description This command configures the frequency at which PIM Hello messages are transmitted on this interface.

The **no** form of this command resets the configuration to the default value.

Default hello-interval 30

Parameters *hello-interval* — Specifies the Hello interval in seconds. A 0 (zero) value disables the sending of Hello messages (the PIM neighbor will never timeout the adjacency).

Values 0 to 255 seconds

Platforms All

hello-interval

Syntax **hello-interval** *seconds*
no hello-interval

Context **[Tree]** (config>router>ospf>area>interface hello-interval)
[Tree] (config>router>ospf>area>virtual-link hello-interval)
[Tree] (config>router>ospf3>area>interface hello-interval)
[Tree] (config>router>ospf3>area>virtual-link hello-interval)

Full Context configure router ospf area interface hello-interval
configure router ospf area virtual-link hello-interval
configure router ospf3 area interface hello-interval
configure router ospf3 area virtual-link hello-interval

Description This command configures the interval between OSPF Hellos issued on the interface or virtual link.

The Hello interval, in combination with the dead-interval, is used to establish and maintain the adjacency. Use this parameter to edit the frequency that Hello packets are sent.

Reducing the interval, in combination with an appropriate reduction in the associated **dead-interval,** allows for faster detection of link and/or router failures at the cost of higher processing costs.

The **no** form of this command reverts to the default value.

Default hello-interval 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Special Cases **OSPF Interface —** If the **hello-interval** configured applies to an interface, then all nodes on the subnet must have the same Hello interval.

Virtual Link — If the **hello-interval** configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same Hello interval.

Parameters *seconds* — Specifies the Hello interval, in seconds, expressed as a decimal integer.

Values 1 to 65535

Platforms All

hello-interval

Syntax **hello-interval** *number*
no hello-interval

Context **[Tree]** (config>system>management-interface>remote-management hello-interval)

Full Context configure system management-interface remote-management hello-interval

Description This command configures the time interval between Hello messages sent from the SR OS node to the remote manager.

Default hello-interval 10

Parameters *number* — Specifies the Hello interval, in minutes.

Values 10 to 3600

Platforms All

12.22 hello-multiplier

hello-multiplier

Syntax **hello-multiplier** *multiplier*
no hello-multiplier

Context **[Tree]** (config>service>vpls>sap>spb>level hello-multiplier)
[Tree] (config>service>vpls>spoke-sdp>spb>level hello-multiplier)

Full Context configure service vpls sap spb level hello-multiplier
configure service vpls spoke-sdp spb level hello-multiplier

Description This command configures the number of missing Hello PDUs from a neighbor SPB declares the adjacency down. This command is valid only for interfaces on control B-VPLS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The no form of this command reverts to the default value.

Default hello-interval 3 — SPB can miss up to 3 Hello messages before declaring the adjacency down.

Parameters *multiplier* — The multiplier for the Hello interval expressed as a decimal integer.

Values 2 to 100

Platforms All

hello-multiplier

Syntax **hello-multiplier** *multiplier*
no hello-multiplier

Context **[Tree]** (config>router>isis>if>level>level-number hello-multiplier)
[Tree] (config>service>vprn>isis>if>level hello-multiplier)

Full Context configure router isis interface level level-number hello-multiplier
configure service vprn isis interface level hello-multiplier

Description This command configures the number of missing Hello messages from a neighbor before the router declares the adjacency down.

Note: The neighbor hold time is (hello multiplier × hello interval) on point-to-point interfaces, and (hello multiplier × hello interval / 3) on broadcast interfaces. Hello values can be adjusted for faster convergence, but the hold-time should always be > 3 to reduce routing instability.

The **no** form of this command reverts to the default value.

Default hello-multiplier 3

Parameters *multiplier* — The multiplier for the Hello interval expressed as a decimal integer.

Values 2 to 100

Platforms All

hello-multiplier

Syntax **hello-multiplier** *deci-units*
no hello-multiplier

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>pim hello-multiplier)

Full Context configure service vprn mvpn provider-tunnel inclusive pim hello-multiplier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the multiplier to determine the hold time for a PIM neighbor on this interface.

The **hello-multiplier** in conjunction with the **hello-interval** determines the holdtime for a PIM neighbor.

Parameters *deci-units* — Specify the value, specified in multiples of 0.1, for the formula used to calculate the holdtime based on the **hello-multiplier**:

(**hello-interval** × **hello-multiplier**) / 10

This allows the PIMv2 default **hello-multiplier** of 3.5 and the default timeout of 105 seconds to be supported.

Values 20 to 100

Default 35

Platforms All

hello-multiplier

Syntax **hello-multiplier** *deci-units*
no hello-multiplier

Context **[Tree]** (config>service>vprn>pim>if hello-multiplier)

Full Context configure service vprn pim interface hello-multiplier

Description This command configures the multiplier to determine the hold time for a PIM neighbor on this interface.

The **hello-multiplier** in conjunction with the **hello-interval** determines the holdtime for a PIM neighbor.

Default hello-multiplier 35

Parameters *deci-units* — Specify the value, specified in multiples of 0.1, for the formula used to calculate the holdtime based on the **hello-multiplier**:

(**hello-interval** × **hello-multiplier**) / 10

This allows the PIMv2 default **hello-multiplier** of 3.5 and the default timeout of 105 seconds to be supported.

Values 20 to 100

Platforms All

hello-multiplier

Syntax **hello-multiplier** *deci-units*
no hello-multiplier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>pim>interface hello-multiplier)

Full Context configure router pim interface hello-multiplier

Description This command configures the multiplier to determine the holdtime for a PIM neighbor on this interface.

The **hello-multiplier** in conjunction with the **hello-interval** determines the holdtime for a PIM neighbor.

The **no** form of this command reverts to the default value.

Default hello-multiplier 35

Parameters *deci-units* — Specifies the value, in multiples of 0.1, for the formula used to calculate the holdtime based on the **hello-multiplier**:

(**hello-interval** × **hello-multiplier**) / 10

This allows the PIMv2 default **hello-multiplier** of 3.5 and the default timeout of 105 seconds to be supported.

Values 20 to 100

Default 35

Platforms All

hello-multiplier

Syntax **hello-multiplier** *multiplier*
no hello-multiplier

Context [Tree] (config>router>isis>if>level hello-multiplier)

Full Context configure router isis interface level hello-multiplier

Description This command configures a Hello multiplier. The **hello-multiplier**, along with the **hello-interval**, is used to calculate a hold time, which is communicated to a neighbor in a Hello PDU.

The hold time is the time in which the neighbor expects to receive the next Hello PDU. If the neighbor receives a Hello within this time, the hold time is reset. If the neighbor does not receive a Hello within the hold time, it brings the adjacency down.

Note: The neighbor hold time is (hello multiplier × hello interval) on non-designated intermediate system broadcast interfaces and point-to-point interfaces and is (hello multiplier × hello interval / 3) on designated intermediate system broadcast interfaces. Hello values can be adjusted for faster convergence, but the hold time should always be > 3 to reduce routing instability.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default hello-multiplier 3

Parameters *multiplier* — Specifies the multiplier for the Hello interval expressed as a decimal integer.

Values 2 to 100

Platforms All

12.23 hello-padding

hello-padding

Syntax **hello-padding** {**none** | **adaptive** | **loose** | **strict**}
no hello-padding

Context **[Tree]** (config>service>vprn>isis hello-padding)
[Tree] (config>service>vprn>isis>level hello-padding)
[Tree] (config>service>vprn>isis>if hello-padding)
[Tree] (config>service>vprn>isis>if>level hello-padding)

Full Context configure service vprn isis hello-padding
configure service vprn isis interface hello-padding
configure service vprn isis interface level hello-padding
configure service vprn isis level hello-padding

Description This command enables the IS-IS Hello (IIH) message padding to ensure that IS-IS LSPs can traverse the link. When this option is enabled, IS-IS Hello messages are padded to the maximum LSP MTU value, which can be set with the **lsp-mtu-size** command. If link MTU is greater than the maximum LSP MTU value, padding to the link MTU is applied.

The **no** form of this command disables IS-IS Hello message padding at this level. However, the router may still perform Hello padding if it was set at a higher level in the configuration. To ensure that Hello message padding is disabled, set all levels of configuration to **no hello-padding**.

Default no hello-padding

Parameters **adaptive** — Specifies the adaptive padding option; this option is able to detect MTU asymmetry from one side of the connection but uses more overhead than loose padding.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- point-to-point interface—Hello PDUs are padded until the sender declares an adjacency on the link to be in the state up. If the implementation supports RFC 3373/5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*, then this is when the three-way state is up. If the implementation uses the “classic” algorithm described in ISO 10589, this is when the adjacency state is up. If the neighbor does not support the adjacency state TLV, then padding continues.
- broadcast interface—Padding starts until at least one adjacency is up on the interface.

loose — Specifies the loose padding option; the loose padding may not be able to detect certain conditions such as asymmetrical MTUs between the routing devices.

- point-to-point interface—the Hello packet is padded from the initial detection of a new neighbor until the adjacency transitions to the INIT state
- broadcast interface—padding starts until at least one adjacency (broadcast only has up/down) is up on the interface

none — Specifies that the Hello message padding is not enabled at this level, even if it is configured at one of the parent levels.

strict — Specifies the strict padding option.

- point-to-point interface—padding is done for all adjacency states, and is continuous. Strict padding has the most overhead but detects MTU issues on both sides of a link
- broadcast interface—padding is done for all adjacency states, and is continuous. Strict padding has the most overhead but detects MTU issues on both sides of a link

Platforms All

hello-padding

Syntax [**no**] **hello-padding** {**none** | **adaptive** | **loose** | **strict**}

Context **[Tree]** (config>router>isis hello-padding)
[Tree] (config>router>isis>level hello-padding)
[Tree] (config>router>isis>interface hello-padding)
[Tree] (config>router>isis>interface>level hello-padding)

Full Context configure router isis hello-padding
configure router isis interface hello-padding
configure router isis interface level hello-padding
configure router isis level hello-padding

Description This command enables IS-IS Hello (IIH) message padding to ensure that IS-IS LSPs can traverse the link. When this option is enabled, IS-IS Hello messages are padded to the maximum LSP MTU value, which can be set with the **lsp-mtu-size** command. If link MTU is greater than the maximum LSP MTU value, padding to the link MTU is applied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables IS-IS Hello padding at this level. However, the router may still perform Hello padding if it was set at a higher level in the configuration. To ensure that Hello message padding is disabled, set all levels of configuration to **no hello-padding**.

Default no hello-padding

Parameters **none** — Specifies that the Hello message padding is not enabled at this level, even if it is configured at one of the parent levels.

adaptive — Specifies the adaptive padding option; this option is able to detect LSP MTU asymmetry from one side of the connection but uses more overhead than loose padding.

1. point-to-point interface—Hello PDUs are padded until the sender declares an adjacency on the link to be in state up. If the implementation supports RFC 3373/5303, “Three-Way Handshake for IS-IS Point-to- Point Adjacencies” then this is when the three-way state is Up. If the implementation use the “classic” algorithm described in ISO 10589, this is when adjacency state is Up. If the neighbor does not support the adjacency state TLV, then padding continues.
2. broadcast interface—Padding starts until at least one adjacency is up on the interface.

loose — Specifies the loose padding option; the loose padding may not be able to detect certain situations such as asymmetrical LSP MTUs between the routing devices.

1. point-to-point interface—The Hello packet is padded from the initial detection of a new neighbor until the adjacency transitions to the INIT state.
2. broadcast interface—Padding starts until there is at least one adjacency (broadcast only has up/down) is up on the interface.

strict — Specifies the strict padding option; this option is the most overhead-intensive but detects LSP MTU issues on both sides of a link.

1. point-to-point interface—Padding is done for all adjacency states, and is continuous.
2. broadcast interface—Padding is done for all adjacency states, and is continuous.

Platforms All

12.24 hello-reduction

hello-reduction

Syntax **hello-reduction** {**enable** *factor* | **disable**}
no hello-reduction

Context **[Tree]** (config>router>ldp>targ-session>ipv4 hello-reduction)
[Tree] (config>router>ldp>targ-session>ipv6 hello-reduction)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ldp>targ-session>peer hello-reduction)
[Tree] (config>router>ldp>targ-session>peer-template hello-reduction)

Full Context

configure router ldp targeted-session ipv4 hello-reduction
configure router ldp targeted-session ipv6 hello-reduction
configure router ldp targeted-session peer hello-reduction
configure router ldp targeted-session peer-template hello-reduction

Description

This command enables the suppression of periodic targeted Hello messages between LDP peers once the targeted LDP session is brought up.

The **config**>**router**>**ldp**>**targ-session**>**ipv6**>**hello-reduction** command is not supported on the 7450 ESS.

When this feature is enabled, the target Hello adjacency is brought up by advertising the Hold-Time value the user configured in the "**hello** timeout" parameter for the targeted session. The LSR node will then start advertising an exponentially increasing Hold-Time value in the Hello message as soon as the targeted LDP session to the peer is up. Each new incremented Hold-Time value is sent in a number of Hello messages equal to the value of the argument *factor*, which represents the dampening factor, before the next exponential value is advertised. This provides time for the two peers to settle on the new value. When the Hold-Time reaches the maximum value of 0xffff (binary 65535), the two peers will send Hello messages at a frequency of every [(65535-1)/local helloFactor] seconds for the lifetime of the targeted-LDP session (for example, if the local Hello Factor is three (3), then Hello messages will be sent every 21844 seconds.

The LSR node continues to compute the frequency of sending the Hello messages based on the minimum of its local Hold-time value and the one advertised by its peer as in RFC 5036. Thus for the targeted LDP session to suppress the periodic Hello messages, both peers must bring their advertised Hold-Time to the maximum value. If one of the LDP peers does not, the frequency of the Hello messages sent by both peers will continue to be governed by the smaller of the two Hold-Time values.

When the user enables the Hello reduction option on the LSR node while the targeted LDP session to the peer is operationally up, the change will take effect immediately. In other words, the LSR node will start advertising an exponentially increasing Hold-Time value in the Hello message, starting with the current configured Hold-Time value.

When the user disables the Hello reduction option while the targeted LDP session to the peer is operationally up, the change in the Hold-Time from 0xffff (binary 65535) to the user configured value for this peer will take effect immediately. The local LSR will immediately advertise the value of the user configured Hold-Time value and will not wait until the next scheduled time to send a Hello to make sure the peer adjusts its local hold timeout value immediately.

In general, any configuration change to the parameters of the T-LDP Hello adjacency (modifying the Hello adjacency Hello Timeout or factor, enabling/disabling Hello reduction, or modifying Hello reduction factor) will cause the LSR node to trigger immediately an updated Hello message with the updated Hold Time value without waiting for the next scheduled time to send a Hello.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the Hello reduction feature.

Default no hello-reduction

Parameters *factor* — Specifies the integer that specifies the Hello reduction dampening factor.

Values 3 to20

Platforms All

12.25 hello-time

hello-time

Syntax **hello-time** *hello-time*
no hello-time [*hello-time*]

Context **[Tree]** (config>service>vpls>stp hello-time)
[Tree] (config>service>template>vpls-template>stp hello-time)

Full Context configure service template vpls-template stp hello-time
configure service vpls stp hello-time

Description This command configures the Spanning Tree Protocol (STP) Hello time for the Virtual Private LAN Service (VPLS) STP instance.

The Hello time parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active Hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode, then the Hello time is always taken from the locally configured parameter).

The configured **hello-time** can also be used to calculate the forward delay. See **auto-edge** (**config>service>vpls>sap>stp auto-edge, config>service>template>vpls-sap-template>stp auto-edge, config>service>vpls>spoke-sdp>stp auto-edge**).

The **no** form of this command returns the Hello time to the default value.

Default hello-time 2

Parameters *hello-time* — The Hello time for the STP instance in seconds.

Values 1 to 10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hello-time

Syntax [**no**] **hello-time** *seconds*

Context **[Tree]** (config>service>sdp>keep-alive hello-time)

Full Context configure service sdp keep-alive hello-time

Description This command configures the time period between SDP keepalive messages on the SDP-ID for the SDP connectivity monitoring messages.

The **no** form of this command reverts the **hello-time** *seconds* value to the default setting.

Default hello-time 10

Parameters *seconds* — Specifies the time period in seconds between SDP keepalive messages, expressed as a decimal integer.

Values 1 to 3600

Platforms All

12.26 help

help

Syntax **help**
help edit
help global
help special-characters

Context **[Tree]** (global help)

Full Context global help

Description This command provides a brief description of the help system. The following information is shown:

```
Help may be requested at any point by hitting a question mark '?'.
In case of an executable node, the syntax for that node will be displayed with an
explanation of all parameters.
In case of sub-commands, a brief description is provided.
Global Commands:
Help on global commands can be observed by issuing "help globals" at any time.
Editing Commands:
Help on editing commands can be observed by issuing "help edit" at any time.
```

Parameters **help** — Displays a brief description of the help system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

edit — Displays help on editing.

Available editing keystrokes:

```
Delete current character.....................Ctrl-d
Delete text up to cursor.....................Ctrl-u
Delete text after cursor.....................Ctrl-k
Move to beginning of line....................Ctrl-a
Move to end of line..........................Ctrl-e
Get prior command from history...............Ctrl-p
Get next command from history................Ctrl-n
Move cursor left.............................Ctrl-b
Move cursor right............................Ctrl-f
Move back one word...........................Esc-b
Move forward one word........................Esc-f
Convert rest of word to uppercase............Esc-c
Convert rest of word to lowercase............Esc-l
Delete remainder of word.....................Esc-d
Delete word up to cursor.....................Ctrl-w
Transpose current and previous character.....Ctrl-t
Enter command and return to root prompt......Ctrl-z
Refresh input line...........................Ctrl-l
```

global — Displays help on global commands.

Available global commands:

```
back            - Go back a level in the command tree
echo            - Echo the text that is typed in
exec            - Execute a file - use -echo to show the commands and
                  prompts on the screen
exit            - Exit to intermediate mode - use option all to exit to
                  root prompt
help            - Display help
history         - Show command history
info            - Display configuration for the present node
logout          - Log off this system
oam             + OAM Test Suite
ping            - Verify the reachability of a remote host
pwc             - Show the present working context
sleep           - Sleep for specified number of seconds
ssh             - SSH to a host
telnet          - Telnet to a host
traceroute      - Determine the route to a destination address
tree            - Display command tree structure from the context of
                  execution
write           - Write text to another user
```

special-characters — Displays help on special characters.

Use the following CLI commands to display more information about commands and command syntax:

? — Lists all commands in the current context.

string? — Lists all commands available in the current context that start with the string.

command ? — Displays command's syntax and associated keywords.

string<Tab> or **string<Space>** — Completes a partial command name (auto-completion) or lists available commands that match the string.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.27 helper-disable

helper-disable

Syntax [**no**] **helper-disable**

Context **[Tree]** (config>service>vprn>isis>graceful-restart helper-disable)

Full Context configure service vprn isis graceful-restart helper-disable

Description This command disables helper support for IS-IS graceful restart (GR).

When **graceful-restart** is enabled, the router can be a helper (that is, the router is helping a neighbor to restart), a restarting router, or both. The router only supports helper mode. It will not act as a restarting router, because the high availability feature set already preserves IS-IS forwarding information such that this functionality is not needed. This command is a historical command and should not be disabled. Configuring **helper-disable** has the effect of disabling graceful restart, because the router only supports helper mode.

The **no helper-disable** command enables helper support and is the default when graceful restart is enabled.

Default no helper-disable

Platforms All

helper-disable

Syntax [**no**] **helper-disable**

Context **[Tree]** (config>service>vprn>ospf>graceful-restart helper-disable)
[Tree] (config>service>vprn>ospf3>graceful-restart helper-disable)

Full Context configure service vprn ospf graceful-restart helper-disable
configure service vprn ospf3 graceful-restart helper-disable

Description This command disables helper support for OSPF graceful restart (GR).

When **graceful-restart** is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart), a restarting router, or both. The router only supports helper mode. It will not act as a restarting router, because the high availability feature set already preserves OSPF forwarding information such that this functionality is not needed. This command is a historical command and should not be disabled. Configuring **helper-disable** has the effect of disabling graceful restart, because the router only supports helper mode.

The **no helper-disable** command enables helper support and is the default when graceful restart is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no helper-disable

Platforms All

helper-disable

Syntax [**no**] **helper-disable**

Context **[Tree]** (config>router>isis>graceful-restart helper-disable)

Full Context configure router isis graceful-restart helper-disable

Description This command disables helper support for IS-IS graceful restart (GR).

When **graceful-restart** is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart), a restarting router, or both. The router only supports helper mode. It will not act as a restarting router, because the high availability feature set already preserves IS-IS forwarding information so that this functionality is not needed. This command is a historical command and should not be disabled. Configuring **helper-disable** has the effect of disabling graceful restart, because the router only supports helper mode.

The **no** form of this command enables helper support and is the default when graceful restart is enabled.

Platforms All

helper-disable

Syntax [**no**] **helper-disable**

Context **[Tree]** (config>router>ospf>graceful-restart helper-disable)
[Tree] (config>router>ospf3>graceful-restart helper-disable)

Full Context configure router ospf graceful-restart helper-disable
configure router ospf3 graceful-restart helper-disable

Description This command disables helper support for OSPF graceful restart (GR).

When **graceful-restart** is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart), a restarting router, or both. The router only supports helper mode. It will not act as a restarting router because the high availability feature set already preserves OSPF forwarding information so that this functionality is not needed. This command is a historical command and should not be disabled. Configuring **helper-disable** has the effect of disabling graceful restart because the router only supports helper mode.

The **no** form of this command enables helper support and is the default when **graceful-restart** is enabled.

Default no helper-disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

12.28 helper-override-restart-time

helper-override-restart-time

Syntax **helper-override-restart-time** *seconds*
no helper-override-restart-time

Context [Tree] (config>service>vprn>bgp>graceful-restart>long-lived helper-override-restart-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived helper-override-restart-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived helper-override-restart-time)

Full Context configure service vprn bgp graceful-restart long-lived helper-override-restart-time
configure service vprn bgp group graceful-restart long-lived helper-override-restart-time
configure service vprn bgp group neighbor graceful-restart long-lived helper-override-restart-time

Description This command overrides the restart-time advertised by a peer (in its GR capability) with a locally-configured value. This override applies only to AFI/SAFI that were included in the GR capability of the peer. The restart-time is always zero for AFI/SAFI not included in the GR capability. This command is useful if the local router wants to force LLGR phase to begin after a set time for all protected AFI/SAFI.

By default, the restart time for all AFI/SAFI in the GR capability is the value signaled by the peer.

Default no helper-override-restart-time

Parameters *seconds* — The locally-imposed restart time for all AFI/SAFI included in the peer's GR capability.

Values 0 to 4095

Platforms All

helper-override-restart-time

Syntax **helper-override-restart-time** *seconds*
no helper-override-restart-time

Context [Tree] (config>router>bgp>graceful-restart>long-lived helper-override-restart-time)
[Tree] (config>router>bgp>group>graceful-restart>long-lived helper-override-restart-time)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived helper-override-restart-time)

Full Context configure router bgp graceful-restart long-lived helper-override-restart-time
configure router bgp group graceful-restart long-lived helper-override-restart-time
configure router bgp group neighbor graceful-restart long-lived helper-override-restart-time

Description This command overrides the restart-time advertised by a peer (in its GR capability) with a locally-configured value. This override applies only to AFI/SAFI that were included in the GR capability of the peer. The restart-time is always zero for AFI/SAFI not included in the GR capability. This command is useful if the local router wants to force LLGR phase to begin after a set time for all protected AFI/SAFI.

By default, the restart time for all AFI/SAFI in the GR capability is the value signaled by the peer.

Default no helper-override-restart-time

Parameters *seconds* — The locally-imposed restart time for all AFI/SAFI included in the peer's GR capability.

Values 0 to 4095

Platforms All

12.29 helper-override-stale-time

helper-override-stale-time

Syntax **helper-override-stale-time** *seconds*
no helper-override-stale-time

Context [Tree] (config>service>vprn>bgp>graceful-restart>long-lived helper-override-stale-time)
[Tree] (config>service>vprn>bgp>graceful-restart>long-lived>family helper-override-stale-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived helper-override-stale-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart>long-lived>family helper-override-stale-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived helper-override-stale-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart>long-lived>family helper-override-stale-time)

Full Context configure service vprn bgp graceful-restart long-lived family helper-override-stale-time
configure service vprn bgp graceful-restart long-lived helper-override-stale-time
configure service vprn bgp group graceful-restart long-lived family helper-override-stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group graceful-restart long-lived helper-override-stale-time
configure service vprn bgp group neighbor graceful-restart long-lived family helper-override-stale-time
configure service vprn bgp group neighbor graceful-restart long-lived helper-override-stale-time

Description This command overrides the LLGR stale-time advertised by a peer (in its LLGR capability) with a locally-configured value. When configured in the long-lived configuration context, **helper-override-stale-time** applies to all AFI/SAFI in the advertised LLGR capability except for any AFI/SAFI with a family-specific override. A family-specific override is configured with the **helper-override-stale-time** command in a family context.

By default, the LLGR stale-time for an AFI/SAFI is the value signaled by the peer in the corresponding AFI/SAFI part of the LLGR capability.

Default no helper-override-stale-time

Parameters *seconds* — Specifies the locally imposed LLGR stale time in seconds.

Values 0 to 16777215

Platforms All

helper-override-stale-time

Syntax **helper-override-stale-time** *seconds*
no helper-override-stale-time

Context **[Tree]** (config>router>bgp>graceful-restart>long-lived helper-override-stale-time)
[Tree] (config>router>bgp>graceful-restart>long-lived>family helper-override-stale-time)
[Tree] (config>router>bgp>group>graceful-restart>long-lived helper-override-stale-time)
[Tree] (config>router>bgp>group>graceful-restart>long-lived>family helper-override-stale-time)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived helper-override-stale-time)
[Tree] (config>router>bgp>group>neighbor>graceful-restart>long-lived>family helper-override-stale-time)

Full Context configure router bgp graceful-restart long-lived family helper-override-stale-time
configure router bgp graceful-restart long-lived helper-override-stale-time
configure router bgp group graceful-restart long-lived family helper-override-stale-time
configure router bgp group graceful-restart long-lived helper-override-stale-time
configure router bgp group neighbor graceful-restart long-lived family helper-override-stale-time
configure router bgp group neighbor graceful-restart long-lived helper-override-stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command overrides the LLGR stale-time advertised by a peer (in its LLGR capability) with a locally-configured value. When configured in the **long-lived** configuration context, **helper-override-stale-time** applies to all AFI/SAFI in the advertised LLGR capability except for any AFI/SAFI with a family-specific override. A family-specific override is configured with the **helper-override-stale-time** command in a family context.

By default, the LLGR stale-time for an AFI/SAFI is the value signaled by the peer in the corresponding AFI/SAFI part of the LLGR capability.

Default no helper-override-stale-time

Parameters *seconds* — Specifies the locally imposed LLGR stale time in seconds.

Values 0 to 16777215

Platforms All

12.30 hi-bw-mcast-src

hi-bw-mcast-src

Syntax **hi-bw-mcast-src** [**alarm**] [**group** *group-id*] [**default-paths-only**]
no hi-bw-mcast-src

Context **[Tree]** (config>card>fp hi-bw-mcast-src)

Full Context configure card fp hi-bw-mcast-src

Description This command designates the forwarding plane as a high-bandwidth IP multicast source, expecting the ingress traffic to include high-bandwidth IP multicast traffic. When configured, the system attempts to allocate a dedicated multicast switch fabric plane (MSFP) to the forwarding plane. If a group is specified, all FPs in the group will share the same MSFP. If the alarm parameter is specified and the system cannot allocate a dedicated MSFP to the new group or FP, the FPs will be brought online and generate an event (SYSTEM: 2052 - tmnxChassisHiBwMulticastAlarm). Similarly, if during normal operation there is a failure or removal of resources, an event will be generated if the system cannot maintain separation of MSFPs for the MDAs.

The **no** form of this command removes the high-bandwidth IP multicast source designation from the forwarding plane.

Default no hi-bw-mcast-src

Parameters **alarm** — Enables event generation if the MDA is required to share an MSFP with another MDA that is in a different group. MDAs within the same group sharing an MSFP will not cause this alarm.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group-id — Specifies the logical MSFP group for the MDA. MDAs configured with the same *group-id* will be placed on the same MSFP.

Values 0 to 32 (A value of 0 removes the MDA from the group).

Default By default, “none” is used, and the system will attempt to assign a unique MSFP to the MDA.

default-paths-only — When this parameter is specified the system will only attempt to allocate the two default paths (one high priority and one low priority) to dedicated MSFPs.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS

12.31 high

high

Syntax **high**

Context **[Tree]** (config>qos>sap-egress>queue>drop-tail high)

Full Context configure qos sap-egress queue drop-tail high

Description Commands in this context configure the queue high drop tail parameters. The high drop tail defines the queue depth beyond which in-profile packets will not be accepted into the queue and will be discarded.

Platforms All

high

Syntax **high**

Context **[Tree]** (cfg>qos>qgrps>egr>qgrp>queue>drop-tail high)

Full Context configure qos queue-group-templates egress queue-group queue drop-tail high

Description Commands in this context configure the queue high drop-tail parameters. The high drop tail defines the queue depth beyond which in-profile packets will not be accepted into the queue and will be discarded.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.32 high-availability

high-availability

Syntax **high-availability** *seconds*
no high-availability

Context **[Tree]** (config>python>py-pol>cache>minimum-lifetimes high-availability)

Full Context configure python python-policy cache minimum-lifetimes high-availability

Description This command specifies the minimum lifetime of an entry that it could be synced across CPM.

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the minimal lifetime in seconds.

Values 1 to 600

Platforms All

12.33 high-octets-discarded-count

high-octets-discarded-count

Syntax [**no**] **high-octets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters high-octets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters high-octets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters high-octets-discarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters high-octets-discarded-count

Description This command includes the high octets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv4 octets discarded count instead.

The **no** form of this command excludes the high octets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

high-octets-discarded-count

Syntax [**no**] **high-octets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters high-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters high-octets-discarded-count)

Full Context configure log accounting-policy custom-record queue i-counters high-octets-discarded-count
configure log accounting-policy custom-record ref-queue i-counters high-octets-discarded-count

Description This command includes the high octets discarded count.

The **no** form of this command excludes the high octets discarded count.

Default no high-octets-discarded-count

Platforms All

12.34 high-octets-offered-count

high-octets-offered-count

Syntax [**no**] **high-octets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters high-octets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters high-octets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters high-octets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters high-octets-offered-count

Description This command includes the high octets offered count.

The **no** form of this command excludes the high octets offered count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

high-octets-offered-count

Syntax [**no**] **high-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters high-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters high-octets-offered-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log accounting-policy custom-record queue i-counters high-octets-offered-count
configure log accounting-policy custom-record ref-queue i-counters high-octets-offered-count

Description This command includes the high octets offered count.

The **no** form of this command excludes the high octets offered count.

Default no high-octets-offered-count

Platforms All

12.35 high-packets-discarded-count

high-packets-discarded-count

Syntax [**no**] **high-packets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-count high-packets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-count high-packets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters high-packets-discarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters high-packets-discarded-count

Description This command includes the high packets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv4 packets discarded count instead.

The **no** form of this command excludes the high packets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

high-packets-discarded-count

Syntax [**no**] **high-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters high-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters high-packets-discarded-count)

Full Context configure log accounting-policy custom-record queue i-counters high-packets-discarded-count
configure log accounting-policy custom-record ref-queue i-counters high-packets-discarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command includes the high packets discarded count.

The **no** form of this command excludes the high packets discarded count.

Default no high-packets-discarded-count

Platforms All

12.36 high-packets-offered-count

high-packets-offered-count

Syntax [**no**] **high-packets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters high-packets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters high-packets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters high-packets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters high-packets-offered-count

Description This command includes the high packets offered count.

The **no** form of this command excludes the high packets offered count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

high-packets-offered-count

Syntax [**no**] **high-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters high-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters high-packets-offered-count)

Full Context configure log accounting-policy custom-record queue i-counters high-packets-offered-count
configure log accounting-policy custom-record ref-queue i-counters high-packets-offered-count

Description This command includes the high packets offered count.

The **no** form of this command excludes the high packets offered count.

Default no high-packets-offered-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.37 high-prio-only

high-prio-only

Syntax **high-prio-only** *percent*
no high-prio-only

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue high-prio-only)
[Tree] (config>subscr-mgmt>sla-prof>ingress>qos>queue high-prio-only)

Full Context configure subscriber-mgmt sla-profile egress qos queue high-prio-only
configure subscriber-mgmt sla-profile ingress qos queue high-prio-only

Description This command configures the value of the percentage of buffer space for the queue, used exclusively by high priority packets. The specified value overrides the default value for the context.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The **high-prio-only** parameter is used to override the default value derived from the **network-queue** command.

The defined **high-prio-only** value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the **high-prio-only** value larger than the current MBS size will also result in an error and fail execution.

The **no** form of this command returns high-prio-only to the size as configured in the QoS policy.

Parameters *percent* — The *percent* parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue is reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.

Values 0 to 100, default

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

high-prio-only

Syntax **high-prio-only** *percent-of-mbs*
no high-prio-only

Context **[Tree]** (config>qos>sap-egress>policer high-prio-only)
[Tree] (config>qos>sap-ingress>policer high-prio-only)

Full Context configure qos sap-egress policer high-prio-only
configure qos sap-ingress policer high-prio-only

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to configure the percentage of the policer's PIR leaky bucket's MBS (maximum burst size) that is reserved for high-priority traffic. While the **mbs** value defines the policer's high-priority violate threshold, the percentage value defined is applied to the **mbs** value to derive the bucket's low-priority violate threshold. See the **mbs** command details for information about which types of traffic are associated with each violate threshold.

Parameters *percent-of-mbs* — The *percent-of-mbs* parameter is required when specifying **high-prio-only** and is expressed as a percentage.

Values 0 to 100

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

high-prio-only

Syntax **high-prio-only** *percent-of-mbs*
no high-prio-only

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer high-prio-only)
[Tree] (config>qos>qgrps>ing>qgrp>policer high-prio-only)

Full Context configure qos queue-group-templates egress queue-group policer high-prio-only
configure qos queue-group-templates ingress queue-group policer high-prio-only

Description This command is used to configure the percentage of the policer's PIR leaky bucket's MBS (maximum burst size) that is reserved for high-priority traffic. While the **mbs** value defines the policer's high-priority violate threshold, the percentage value defined is applied to the **mbs** value to derive the bucket's low-priority violate threshold. See the **mbs** command details for information on which types of traffic is associated with each violate threshold.

Parameters *percent-of-mbs* — The *percent-of-mbs* parameter is required when specifying **high-prio-only** and is expressed as a percentage.

Values 0 to 100

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

12.38 high-rate-hold-time

high-rate-hold-time

Syntax **high-rate-hold-time** *seconds* [**active-min-only**]
no high-rate-hold-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>adv-config-policy>child-control>offered-measurement high-rate-hold-time)

Full Context configure qos adv-config-policy child-control offered-measurement high-rate-hold-time

Description This command sets a time period that the current offered rate should be maintained for a child policer or queue when it is seen that the offered rate is decreasing. The offered measurement that triggers the hold time is used when the hold timer expires, unless a higher offered rate is seen in the interim. When a higher rate is observed, the hold timer is canceled and the higher offered rate is used immediately.

A possible reason to define a hold timer for an offered rate is to allow a child queue is to dampen the effects of a child with a fluctuating rate on the virtual scheduler. This works similar to the max-decrement in that the child holds on to bandwidth from the virtual scheduler in case it may be needed in the near future.

This parameter has no effect on an increase to the child's offered rate. If the rate increase is above the change sensitivity, the new offered rate is immediately used.

When this command is not specified or removed, the virtual scheduler immediately reacts to measured decreases in offered load.

The **no** form of this command is used to remove any currently configured hold time for all child policers and queues associated with the policy. When the hold time is removed, any current hold timers for child policers are automatically canceled.

Parameters *seconds* — The hold time configured must be specified in seconds. A value of 0 is equivalent to no high-rate-hold-time.

Default 0

Values 0 to 60

active-min-only — When this optional parameter is specified, the **high-rate-hold-time** command will accept the optional **active-min-only** parameter. Attempting to remove the active-min-only parameter from the **add** command, or removing the **add** command itself, will fail while **active-min-only** is enabled on the **high-rate-hold-time** command. When specified, the respective rate or percentage is treated as the minimum offered rate for a queue, only when the queue has an actual non-zero offered rate. This is intended to limit the artificial increase in offered rate to queues that are currently active. When a queue's measured offered rate drops to zero, the system stops enforcing the minimum value.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.39 high-slope

high-slope

Syntax [**no**] **high-slope**

Context **[Tree]** (config>qos>slope-policy high-slope)

Full Context configure qos slope-policy high-slope

Description The **high-slope** context contains the commands and parameters for defining the high Random Early Detection (RED) slope graph. Each buffer pool supports a high RED slope for managing access to the shared portion of the buffer pool for in-profile packets.

The **high-slope** parameters can be changed at any time and the affected buffer pool high RED slopes will be adjusted appropriately.

The **no** form of this command restores the high slope configuration commands to the default values. If the commands within **high-slope** are set to the default parameters, the **high-slope** node will not appear in save config and show config output unless the detail parameter is present.

Platforms All

12.40 high-wmark

high-wmark

Syntax **high-wmark** *percent*

Context **[Tree]** (config>app-assure>group>dns-ip-cache>ip-cache high-wmark)

Full Context configure application-assurance group dns-ip-cache ip-cache high-wmark

Description This command configures the high watermark value for the DNS IP cache. When the number of IP addresses stored in the cache crosses above this threshold, the system will generate a trap.

Default high-wmark 90

Parameters *percent* — Specifies the high watermark value, in percent.

Values 0 to 100

Default 90

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

high-wmark

Syntax **high-wmark** *high-watermark* **low-wmark** *low-watermark*

Context **[Tree]** (config>app-assure>group>statistics>tca>error-drop high-wmark)
[Tree] (config>app-assure>group>statistics>tca>fragment-drop-all high-wmark)
[Tree] (config>app-assure>group>statistics>tca>fragment-drop-out-of-order high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>gtp-in-gtp high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>imsi-apn>default-action high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>imsi-apn>entry high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>max-payload-length high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>missing>mandatory-ie high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg>default-action high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>default-gtp-tunnel-endpoint-limit high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg>entry high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg>header-sanity high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg-gtpv2>default-action high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>msg-gtpv2>entry high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>tunnel-resource-limit high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>validate-gtp-tunnels high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>validate-sequence-number high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-fltr>validate-src-ip-addr high-wmark)
[Tree] (config>app-assure>group>statistics>tca>gtp-sanity-drop high-wmark)
[Tree] (config>app-assure>group>statistics>tca>overload-drop high-wmark)
[Tree] (config>app-assure>group>statistics>tca>policer high-wmark)
[Tree] (config>app-assure>group>statistics>tca>sctp-fltr>packet-sanity high-wmark)
[Tree] (config>app-assure>group>statistics>tca>sctp-fltr>ppid>default-action high-wmark)
[Tree] (config>app-assure>group>statistics>tca>sctp-fltr>ppid>entry high-wmark)
[Tree] (config>app-assure>group>statistics>tca>sctp-fltr>ppid>ppid-range high-wmark)
[Tree] (config>app-assure>group>statistics>tca>sess-fltr>default-action high-wmark)
[Tree] (config>app-assure>group>statistics>tca>sess-fltr>entry high-wmark)
[Tree] (config>app-assure>group>statistics>tca>tcp-validate high-wmark)

Full Context configure application-assurance group statistics threshold-crossing-alert error-drop high-wmark
configure application-assurance group statistics threshold-crossing-alert fragment-drop-all high-wmark
configure application-assurance group statistics threshold-crossing-alert fragment-drop-out-of-order high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter default-gtp-tunnel-endpoint-limit high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter gtp-in-gtp high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter imsi-apn default-action high-wmark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group statistics threshold-crossing-alert gtp-filter imsi-apn entry high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter max-payload-length high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter missing-mandatory-ie high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type default-action high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type entry high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type header-sanity high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type-gtpv2 default-action high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type-gtpv2 entry high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter tunnel-resource-limit high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter validate-gtp-tunnels high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter validate-sequence-number high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-filter validate-src-ip-addr high-wmark
configure application-assurance group statistics threshold-crossing-alert gtp-sanity-drop high-wmark
configure application-assurance group statistics threshold-crossing-alert overload-drop high-wmark
configure application-assurance group statistics threshold-crossing-alert policer high-wmark
configure application-assurance group statistics threshold-crossing-alert sctp-filter packet-sanity high-wmark
configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid default-action high-wmark
configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid entry high-wmark
configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid-range high-wmark
configure application-assurance group statistics threshold-crossing-alert session-filter default-action high-wmark
configure application-assurance group statistics threshold-crossing-alert session-filter entry high-wmark
configure application-assurance group statistics threshold-crossing-alert tcp-validate high-wmark

Description This command configures the high watermark and low watermark thresholds for the specified TCA.

Default high-wmark 4294967295 low-wmark 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *high-watermark* — Specifies the TCA high watermark.

Values 1 to 4294967295

Default 4294967295

low-watermark — Specifies the TCA low watermark.

Values 0 to 4294967294

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.41 highplus

highplus

Syntax **highplus**

Context **[Tree]** (config>qos>sap-egress>queue>drop-tail highplus)

Full Context configure qos sap-egress queue drop-tail highplus

Description Commands in this context configure the queue highplus drop tail parameters. The highplus drop tail defines the queue depth beyond which inplus-profile packets will not be accepted into the queue and will be discarded.

Platforms All

highplus

Syntax **highplus**

Context **[Tree]** (cfg>qos>qgrps>egr>qgrp>queue>drop-tail highplus)

Full Context configure qos queue-group-templates egress queue-group queue drop-tail highplus

Description Commands in this context configure the queue highplus drop-tail parameters. The highplus drop tail defines the queue depth beyond which inplus-profile packets will not be accepted into the queue and will be discarded.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.42 highplus-slope

highplus-slope

Syntax [**no**] **highplus-slope**

Context **[Tree]** (config>qos>slope-policy highplus-slope)

Full Context configure qos slope-policy highplus-slope

Description The **highplus-slope** context contains the commands and parameters for defining the highplus Random Early Detection (RED) slope graph. Each buffer pool supports a highplus RED slope for managing access to the shared portion of the buffer pool for inplus-profile packets.

The **highplus-slope** parameters can be changed at any time and the affected buffer pool highplus RED slopes will be adjusted appropriately.

The **no** form of this command restores the highplus slope configuration commands to the default values. If the commands within **highplus-slope** are set to the default parameters, the **highplus-slope** node will not appear in save config and show config output unless the detail parameter is present.

Platforms All

12.43 history

history

Syntax **history**

Context **[Tree]** (global history)

Full Context global history

Description This command lists the last 30 commands entered in this session.

Re-execute a command in the history with the **!n** command, where **n** is the line number associated with the command in the history output.

Example:

```
A:ALA-1# history
  68 info
  69 exit
  70 info
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
  71 filter
  72 exit all
  73 configure
  74 router
  75 info
  76 interface "test"
  77 exit
  78 reduced-prompt
  79 info
  80 interface "test"
  81 icmp unreachables exit all
  82 exit all
  83 reduced-prompt
  84 configure router
  85 interface
  86 info
  87 interface "test"
  88 info
  89 reduced-prompt
  90 exit all
  91 configure
  92 card 1
  93 card-type
  94 exit
  95 router
  96 exit
  97 history
A:ALA-1# !91
A:ALA-1# configure
A:ALA-1>config#
```

12.44 history-size

history-size

Syntax **history-size** *size*
no history-size

Context **[Tree]** (config>system>security>password history-size)

Full Context configure system security password history-size

Description Configure how many previous passwords a new password is matched against.

Default history-size 0

Parameters *size* — Specifies how many previous passwords a new password is matched against.

Values 0 to 20

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.45 hli-event

hli-event

Syntax **hli-event** {**forward** | **backward** | **aggregate**} **threshold** *raise-threshold* [**clear** *clear-threshold*]
no hli-event {**forward** | **backward** | **aggregate**}

Context **[Tree]** (config>oam-pm>session>ethernet>slm>loss-events hli-event)
[Tree] (config>oam-pm>session>ethernet>lmm>loss-events hli-event)
[Tree] (config>oam-pm>session>ip>twamp-light>loss-events hli-event)

Full Context configure oam-pm session ethernet lmm loss-events hli-event
configure oam-pm session ethernet slm loss-events hli-event
configure oam-pm session ip twamp-light loss-events hli-event

Description This command sets the high loss interval (HLI) threshold to be monitored and the associated thresholds using the counter of the specified direction. The aggregate is a function of summing forward and backward. This value is only used as a threshold mechanism and is not part of the stored statistics. If the optional **clear** *clear-threshold* parameter is not specified, the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and regardless of any previous window. Each unique event can only be raised once within measurement interval. If the optional **clear** *clear-threshold* parameter is specified, the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is carried forward to following measurement intervals. If a threshold crossing event is raised another is raised until a measurement interval completes and the clear threshold has not been exceeded. A clear event is raised under that condition.

The **no** form of this command removes the event threshold for frame loss ratio. The direction must be included with the **no** command.

Default no hli-event forward

no hli-event backward

no hli-event aggregate

Parameters **forward** — Specifies the threshold is applied to the forward direction count.

backward — Specifies the threshold is applied to the backward direction count.

aggregate — Specifies the threshold is applied to the aggregate count (sum of forward and backward).

raise-threshold — Specifies the rising threshold that determines when the event is to be generated, when the percentage of loss value is reached.

Values 1 to 864000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

clear-threshold — Specifies an optional value used for stateful behavior that allows the operator to configure a percentage of loss value lower than the rising percentage to indicate when the clear event should be generated.

Values 0 to 863999

A value of zero means that the HLI counter must be 0.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events hli-event

All

- configure oam-pm session ethernet slm loss-events hli-event
- configure oam-pm session ethernet lmm loss-events hli-event

12.46 hli-force-count

hli-force-count

Syntax [**no**] **hli-force-count**

Context **[Tree]** (config>oam-pm>session>ethernet>lmm>availability hli-force-count)
[Tree] (config>oam-pm>session>ethernet>slm hli-force-count)

Full Context configure oam-pm session ethernet lmm availability hli-force-count
configure oam-pm session ethernet slm hli-force-count

Description This command allows High Loss Interval (HLI) and Consecutive High Loss Interval (CHLI) counters to increment regardless of availability. Without this command, HLI and CHLI counters can only increment during times of availability, which includes undetermined availability. During times of complete packet loss, the forward direction HLI is marked as high loss. The backward direction is not marked as high loss during times of complete packet loss.

The **no** form of this command configures HLI and CHLI counters to increment during times of availability only.

Platforms All

hli-force-count

Syntax [**no**] **hli-force-count**

Context **[Tree]** (config>oam-pm>session>ip>twamp-light>loss hli-force-count)

Full Context configure oam-pm session ip twamp-light loss hli-force-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows High Loss Interval (HLI) and Consecutive High Loss Interval (CHLI) counters to increment regardless of availability. Without this command, HLI and CHLI counters can only increment during times of availability, which includes undetermined availability. During times of complete packet loss, the forward direction HLI is marked as high loss. The backward direction is not marked as high loss during times of complete packet loss.

The **no** form of this command configures HLI and CHLI counters to increment during times of availability only.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

12.47 hold-clear

hold-clear

Syntax **hold-clear** *seconds*
no hold-clear

Context **[Tree]** (config>vrrp>policy>priority-event>host-unreachable hold-clear)
[Tree] (config>vrrp>policy>priority-event>lag-port-down hold-clear)
[Tree] (config>vrrp>policy>priority-event>mc-ipsec-non-forwarding hold-clear)
[Tree] (config>vrrp>policy>priority-event>port-down hold-clear)
[Tree] (config>vrrp>policy>priority-event>route-unknown hold-clear)

Full Context configure vrrp policy priority-event host-unreachable hold-clear
configure vrrp policy priority-event lag-port-down hold-clear
configure vrrp policy priority-event mc-ipsec-non-forwarding hold-clear
configure vrrp policy priority-event port-down hold-clear
configure vrrp policy priority-event route-unknown hold-clear

Description This command configures the hold clear time for the event. The *seconds* parameter specifies the hold-clear time, the amount of time in seconds by which the effect of a cleared event on the associated virtual router instance is delayed.

The hold-clear time is used to prevent black hole conditions when a virtual router instance advertises itself as a master before other conditions associated with the cleared event have had a chance to enter a forwarding state.

Default no hold-clear

Parameters *seconds* — Specifies the amount of time in seconds by which the effect of a cleared event on the associated virtual router instance is delayed.

Values 0 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure vrrp policy priority-event mc-ipsec-non-forwarding hold-clear

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure vrrp policy priority-event route-unknown hold-clear
- configure vrrp policy priority-event lag-port-down hold-clear
- configure vrrp policy priority-event host-unreachable hold-clear
- configure vrrp policy priority-event port-down hold-clear

12.48 hold-count

hold-count

Syntax **hold-count** *BPDU tx hold count*
no hold-count

Context **[Tree]** (config>service>vpls>stp hold-count)
[Tree] (config>service>template>vpls-template>stp hold-count)

Full Context configure service template vpls-template stp hold-count
configure service vpls stp hold-count

Description This command configures the peak number of BPDUs that can be transmitted in a period of one second.

The **no** form of this command returns the hold count to the default value

Default hold-count 6

Parameters *BPDU tx hold count* — The hold count for the STP instance in seconds

Values 1 to 10

Platforms All

12.49 hold-down-time

hold-down-time

Syntax **hold-down-time** *seconds*
no hold-down-time

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server hold-down-time)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt authentication-policy radius-authentication-server hold-down-time

Description This command determines the interval during which no new communication attempts is made to a RADIUS server that is marked **down** to prevent immediately overloading the server when it is starting up. The only exception is when all servers in the authentication policy are marked **down**; in that case they will all be used again to prevent failures on new client connections.

The **no** form of this command reverts to the default.

Default hold-down-time 30

Parameters *seconds* — Specifies the hold time before re-using a RADIUS server that was down.

Values 30 to 900

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

hold-down-time

Syntax **hold-down-time** [**sec** *seconds*] [**min** *minutes*] [**hrs** *hours*] [**days** *days*]
no hold-down-time

Context **[Tree]** (config>aaa>radius-srv-plcy>servers hold-down-time)

Full Context configure aaa radius-server-policy servers hold-down-time

Description This command determines the interval during which no new communication attempts are made to a RADIUS server that is marked down to prevent immediately overloading the server when it is starting up. The only exception is when all servers in the authentication policy are marked down; in that case, they will all be used again to prevent failures on new client connections.

The **no** form of this command reverts to the default.

Default hold-down-time sec 30

Parameters *days* — Specifies the hold time in days before re-using a RADIUS server that was down.

Values 1 to 1

hours — Specifies the hold time in hours before re-using a RADIUS server that was down.

Values 1 to 23

minutes — Specifies the hold time in minutes before re-using a RADIUS server that was down.

Values 1 to 59

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

seconds — Specifies the hold time in seconds before re-using a RADIUS server that was down.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

hold-down-time

Syntax **hold-down-time** *seconds*
no hold-down-time

Context **[Tree]** (config>service>sdp>keep-alive hold-down-time)

Full Context configure service sdp keep-alive hold-down-time

Description This command configures the minimum time period the SDP will remain in the operationally down state in response to SDP keepalive monitoring.

This parameter can be used to prevent the SDP operational state from “flapping” by rapidly transitioning between the operationally up and operationally down states based on keepalive messages.

When an SDP keepalive response is received that indicates an error condition or the **max-drop-count** keepalive messages receive no reply, the *sdp-id* will immediately be brought operationally down. If a keepalive response is received that indicates the error has cleared, the *sdp-id* will be eligible to be put into the operationally up state only after the **hold-down-time** interval has expired.

The **no** form of this command reverts the **hold-down-time seconds** *value* to the default setting.

Default hold-down-time 10

Parameters *seconds* — Specifies time, in seconds, expressed as a decimal integer. The SDP ID will remain in the operationally down state before it is eligible to enter the operationally up state. A value of 0 indicates that no **hold-down-time** will be enforced for SDP ID.

Values 0 to 3600

Platforms All

12.50 hold-down-timer

hold-down-timer

Syntax **hold-down-timer** *hold-down-timer*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no hold-down-timer

Context [Tree] (config>router>segment-routing>maintenance-policy hold-down-timer)

Full Context configure router segment-routing maintenance-policy hold-down-timer

Description This command configures the hold down timer for SR policy candidate paths.

This command is intended to prevent bouncing of the SR policy path state if one or more S-BFD sessions associated with segment lists flap and therefore cause the threshold to be repeatedly crossed in a short period of time. It is started when the number of up S-BFD sessions drops below the threshold. The SR policy path is not considered to be up again until the hold down timer has expired and the number of up S-BFD sessions equals or exceeds the threshold and the internal hold timer is not running.

Note: If the revert timer is also configured, the revert timer is not started until after the number of S-BFD sessions that are up ≥ threshold and the hold down timer for the primary candidate path has expired.

The **no** form of this command reverts to the default.

Default hold-down-timer 0

Parameters *hold-down-timer* — Specifies the hold-down timer, in deciseconds, in 10ms steps.

Values 0 to 5000

Platforms All

12.51 hold-multiplier

hold-multiplier

Syntax **hold-multiplier** *multiplier*
no hold-multiplier

Context [Tree] (config>service>vpls>gsmp hold-multiplier)
[Tree] (config>service>vprn>gsmp hold-multiplier)

Full Context configure service vpls gsmp hold-multiplier
configure service vprn gsmp hold-multiplier

Description This command configures the hold-multiplier for the GSMP connections in this group.

The **no** form of this command removes the multiplier value from the GSMP configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *multiplier* — Specifies the GSMP hold multiplier value.

Values 1 to 100

hold-multiplier

Syntax **hold-multiplier** *multiplier*
no hold-multiplier

Context **[Tree]** (config>service>vpls>gsmp>group hold-multiplier)

Full Context configure service vpls gsmp group hold-multiplier

Description This command configures the hold-multiplier for the GSMP connections in this group.

Parameters *multiplier* — Specifies the GSMP hold multiplier value

Values 1 to 100

Platforms All

hold-multiplier

Syntax **hold-multiplier** *multiplier*
no hold-multiplier

Context **[Tree]** (config>service>vprn>gsmp>group hold-multiplier)

Full Context configure service vprn gsmp group hold-multiplier

Description This command configures the hold-multiplier for the GSMP connections in this group.

The **no** form of this command removes the multiplier value from the configuration

Default no hold-multiplier

Parameters *multiplier* — Specifies the GSMP hold multiplier value.

Values 1 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.52 hold-on-neighbor-failure

hold-on-neighbor-failure

Syntax **hold-on-neighbor-failure** *multiplier*
no hold-on-neighbor-failure

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-lag hold-on-neighbor-failure)

Full Context configure redundancy multi-chassis peer mc-lag hold-on-neighbor-failure

Description This command specifies the interval that the standby node will wait for packets from the active node before assuming a redundant-neighbor node failure. This delay in switch-over operation is required to accommodate different factors influencing node failure detection rate, such as IGP convergence, or HA switch-over times and to prevent the standby node to act prematurely.

The **no** form of this command reverts to the default.

Default hold-on-neighbor-failure 3

Parameters *multiplier* — Specifies the time interval that the standby node waits for packets from the active node before assuming a redundant-neighbor node failure.

Values 2 to 25

Platforms All

hold-on-neighbor-failure

Syntax **hold-on-neighbor-failure** *multiplier*
no hold-on-neighbor-failure

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ep hold-on-neighbor-failure)

Full Context configure redundancy multi-chassis peer mc-endpoint hold-on-neighbor-failure

Description This command specifies the number of keep-alive intervals that the local node will wait for packets from the MC-EP peer before assuming failure. After this time interval passed the all the mc-endpoints configured under services will revert to single chassis behavior, activating the best local pseudowire.

The **no** form of this command sets the multiplier to default value

Default no hold-on-neighbor-failure

Parameters *multiplier* — Specifies the hold time applied on neighbor failure.

Values 2 to 25

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

hold-on-neighbor-failure

Syntax **hold-on-neighbor-failure** *multiplier*
no hold-on-neighbor-failure

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ipsec hold-on-neighbor-failure)

Full Context configure redundancy multi-chassis peer mc-ipsec hold-on-neighbor-failure

Description This command specifies the number of keep-alive failures before the peer is considered to be down.

The **no** form of this command reverts to the default.

Default hold-on-neighbor-failure 3

Parameters *multiplier* — Specifies the hold time applied on the neighbor failure.

Values 2 to 25

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.53 hold-set

hold-set

Syntax **hold-set** *seconds*
no hold-set

Context **[Tree]** (config>vrrp>policy>priority-event>host-unreachable hold-set)
[Tree] (config>vrrp>policy>priority-event>lag-port-down hold-set)
[Tree] (config>vrrp>policy>priority-event>mc-ipsec-non-forwarding hold-set)
[Tree] (config>vrrp>policy>priority-event>port-down hold-set)
[Tree] (config>vrrp>policy>priority-event>route-unknown hold-set)

Full Context configure vrrp policy priority-event host-unreachable hold-set
configure vrrp policy priority-event lag-port-down hold-set
configure vrrp policy priority-event mc-ipsec-non-forwarding hold-set
configure vrrp policy priority-event port-down hold-set
configure vrrp policy priority-event route-unknown hold-set

Description This command specifies the amount of time that must pass before the set state for a VRRP priority control event can transition to the cleared state to dampen flapping events. A flapping event continually transitions between clear and set.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **hold-set** command is used to dampen the effect of a flapping event. The **hold-set** value is loaded into a hold-set timer that prevents a set event from transitioning to the cleared state until it expires.

Each time an event transitions between cleared and set, the timer is loaded and begins a countdown to zero. When the timer reaches zero, the event is allowed to enter the cleared state. Entering the cleared state is dependent on the object controlling the event, conforming to the requirements defined in the event itself. It is possible, on some event types, to have another set action reload the hold-set timer. This extends the amount of time that must expire before entering the cleared state.

Once the hold-set timer expires and the event meets the cleared state requirements or is set to a lower threshold, the current set effect on the virtual router instances in-use priority can be removed. As with **lag-port-down** events, this may be a decrease in the set effect if the *clearing* amounts to a lower set threshold.

The **hold-set** command can be executed at any time. If the hold-set timer value is configured larger than the new *seconds* setting, the timer is loaded with the new **hold-set** value.

The **no** form of the command disables the hold timer so that event transitions are processed immediately.

Default no hold-set

Parameters *seconds* — The number of seconds that the hold-set timer waits after an event enters a set state or enters a higher threshold set state, depending on the event type.

The value of 0 disables the hold-set timer, preventing any delay in processing lower set thresholds or cleared events.

Values 0 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure vrrp policy priority-event mc-ipsec-non-forwarding hold-set

All

- configure vrrp policy priority-event port-down hold-set
- configure vrrp policy priority-event host-unreachable hold-set
- configure vrrp policy priority-event route-unknown hold-set
- configure vrrp policy priority-event lag-port-down hold-set

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.54 hold-time

hold-time

Syntax **hold-time** *seconds*
no hold-time

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy hold-time)

Full Context configure subscriber-mgmt bgp-peering-policy hold-time

Description This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection.

Even though the router OS implementation allows setting the keepalive time separately, the configured keepalive timer is overridden by the hold-time value under the following circumstances:

If the specified hold-time is less than the configured keepalive time, then the operational keepalive time is set to a third of the hold-time; the configured keepalive time is not changed.

If the hold-time is set to zero, then the operational value of the keepalive time is set to zero; the configured keepalive time is not changed. This means that the connection with the peer is up permanently and no keepalive packets are sent to the peer.

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is up permanently.

Values 0, 3 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

hold-time

Syntax **hold-time** *seconds*
hold-time [**days** *days*] [**hrs** *hrs*] [**min** *min*] [**sec** *sec*]
no hold-time

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile hold-time)

Full Context configure subscriber-mgmt vrgw brg brg-profile hold-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command holds the BRG object for the specified time. This applies when the connectivity verification fails or when the last host is removed and **no connectivity-verification** is enabled. Hold time does not apply to an explicit removal via the **radius** or **clear** commands.

The **no** form of this command disables the hold time.

Parameters *seconds* — Specifies the time, in seconds, to hold on to a BRG after the system considered it down.

Values 30 to 2592000

days — Specifies the hold-time in days.

Values 1 to 30

hrs — Specifies the hold-time in hours.

Values 1 to 23

min — Specifies the hold-time in minutes.

Values 1 to 59

sec — Specifies the hold-time in seconds.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

hold-time

Syntax **hold-time** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no hold-time

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>authentication hold-time)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>authentication hold-time)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication hold-time
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication hold-time

Description This command configures the minimum time that a UE is held down after a failed authentication attempt.

The **no** form of this command reverts to the default.

Default hold-time sec 5

Parameters *hours* — Specifies the minimum time that a user is held down in hours.

Values 1 to 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

minutes — Specifies the minimum time that a user is held down in minutes.

Values 1 to 59

seconds — Specifies the minimum time that a user is held down in seconds.

Values 0 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

hold-time

Syntax **hold-time infinite**
hold-time [**time**]
no hold-time

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>egress hold-time)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>egress hold-time)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress hold-time
configure service vprn subscriber-interface group-interface wlan-gw egress hold-time

Description This command configures the time for which egress shaping resources associated with a wlan-gw tunnel are held after the last subscriber on a tunnel is deleted.

Parameters *time* — Specifies the time, in seconds, for which shaping resources are held in seconds after last subscriber is deleted.

Values infinite to 1 to 86400

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

hold-time

Syntax **hold-time** *time*
no hold-time

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>mobility hold-time)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>mobility hold-time)

Full Context configure service ies subscriber-interface group-interface wlan-gw mobility hold-time
configure service vprn subscriber-interface group-interface wlan-gw mobility hold-time

Description This command configures the minimum time that a UE is held associated with its current Access Point (AP) before being associated with a new AP.

The hold time is used to prevent overwhelming the system with mobility triggers, by limiting the rate at which a UE can move from one AP to another while the system is very busy already.

Default hold-time 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *time* — Specifies a hold-down time, in seconds, for handling of successive mobility triggers for a UE. It is the minimal time a UE stays associated with an AP.

Values 0 to 255

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

hold-time

Syntax **hold-time infinite**
hold-time *seconds*
no hold-time

Context **[Tree]** (config>subscr-mgmt>sap-template hold-time)

Full Context configure subscriber-mgmt sap-template hold-time

Description This command configures the time for which an SAP is retained after the last session has been removed. Such SAPs can be forcefully removed using the **idle-saps** option in the **clear**>**subscriber-mgmt**>**sap-template** context.

The **no** form of this command reverts to the default.

Default hold-time 30

Parameters **infinite** — Keyword specifying to never automatically remove the SAP.

seconds — Specifies the time, in seconds, that the SAP is retained.

Values 30 to 2592000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

hold-time

Syntax **hold-time** *hold-time*
no hold-time

Context **[Tree]** (config>port>aps hold-time)

Full Context configure port aps hold-time

Description This command specifies how much time can pass, in 100s of milliseconds, without receiving an advertise packet from the neighbor before the multi-chassis signaling link is considered not operational.

The **hold-time** is usually 3 times the value of the **advertise-interval**. The value of the **advertise-interval** is valid only for a multi-chassis APS as indicated by the value of neighbor IP address if it is not set to 0.0.0.0.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hold-time* — Specifies how long to wait for an APS advertisement packet before the peer in a Multi-Chassis APS group is considered operationally down.

Values 10 to 650

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

hold-time

Syntax **hold-time** *time-value*
no hold-time

Context **[Tree]** (config>port>ethernet>efm-oam hold-time)

Full Context configure port ethernet efm-oam hold-time

Description This command configures efm-oam operational transition dampening timers which reduce the number of efm-oam state transitions reported to upper layers.

Default no hold-time

Parameters *time-value* — Indicates the number of seconds that the efm-oam protocol will wait before going back to the operational state after leaving the operational state. Note that the hold-time does not apply if efm-oam moved from operational to link-fault.

A hold-time value of zero indicates that there should be no delay in transitioning to the operational state. A non-zero value will cause the efm-oam protocol to attempt to negotiate with a peer if possible, but it will remain in the send-local-remote-ok state until the hold time has expired if negotiation is successful.

If efm-oam is administratively shutdown while it was in the operational state and then re-enabled when a non-zero hold time is configured, efm-oam will attempt transition to the operational state immediately.

The **no** form of this command reverts the value to the default.

Values 0 to 50

Default 0

Platforms All

hold-time

Syntax **hold-time** {[**up** *hold-time-up*] [**down** *hold-time-down*] [**seconds** | **centiseconds**]}
no hold-time

Context **[Tree]** (config>port>ethernet hold-time)

Full Context configure port ethernet hold-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures port link dampening timers which reduce the number of link transitions reported to upper layer protocols. The **hold-time** value dampens interface transitions.

When an interface transitions from an up state to a down state, it is immediately advertised to the rest of the system if the hold-time down interval is zero, but if the hold-time down interval is greater than zero, interface down transitions are not advertised to upper layers until the hold-time down interval has expired. Likewise, an interface is immediately advertised as up to the rest of the system if the hold-time up interval is zero, but if the hold-time up interval is greater than zero, up transitions are not advertised until the hold-time up interval has expired.

For ESM SRRP setup, MCS synchronizes subscriber information between the two chassis. After a chassis recovers from a power reset/down, MCS immediately synchronizes all subscriber information at once. The longer the host list, the longer it will take to synchronize the chassis. In a fully populated chassis, it is recommended to allow at least 45 minutes for MCS synchronization. It is also recommended to hold the port down, facing the subscriber, on the recovering chassis for 45 minutes before it is allowed to forward traffic again.

The **no** form of this command reverts to the default values.

Default down 0 seconds — No port link down dampening is enabled; link down transitions are immediately reported to upper layer protocols.

up 0 seconds — No port link up dampening is enabled; link up transitions are immediately reported to upper layer protocols.

Parameters *hold-time-up* — The delay, in seconds or centiseconds, after which to notify the upper layers when an interface transitions from a down state to an up state.

Values 0 to 36000 seconds, 0 or 10 to 3600000 centiseconds in 5 centisecond increments

The minimum non-zero *hold-time-up* interval on 10G or higher ports is 10 centiseconds with a granularity of 5 centiseconds. The granularity on 1G ports is 1 second. Centiseconds are not supported on 1G ports.

hold-time-down — The delay, in seconds or centiseconds, after which to notify the upper layers when an interface transitions from an up state to a down state.

Values 0 to 36000 seconds, 0 or 10 to 3600000 centiseconds in 5 centisecond increments

The minimum non-zero *hold-time-down* interval on 10G or higher ports is 10 centiseconds with a granularity of 5 centiseconds. The granularity on 1G ports is 1 second. Centiseconds are not supported on 1G ports.

seconds | centiseconds — Specifies the hold time units as **seconds** or **centiseconds**.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hold-time

Syntax **hold-time** {[**up** *hold-time-up*] [**down** *hold-time-down*]}
no hold-time

Context **[Tree]** (config>port>sonet-sdh hold-time)

Full Context configure port sonet-sdh hold-time

Description This command configures SONET link dampening timers in 100s of milliseconds. This guards against reporting excessive interface transitions. This is implemented by not advertising subsequent transitions of the interface to upper layer protocols until the configured timer has expired.

Note: For APS configurations, the **hold-time down** and **up** default values are 100 ms and 500 ms respectively. If there is a large communication delay (time to exchange K1/K2 bytes) between the APS Controllers of the two endpoints of an APS link, it is highly suggested to increase the default hold-time down timer on the APS group port accordingly with the communication delay. See the **config>port aps** command for more information.

This command is supported by TDM satellite.

Default no hold-time

Parameters **up** *hold-time-up* — Configures the hold-timer for link up event dampening. A value of zero (0) indicates that an up transition is reported immediately.

Values 0 to 100

down *hold-time-down* — The hold-timer for link down event dampening. A value of zero (0) indicates that a down transition is reported immediately.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

hold-time

Syntax **hold-time** {[**up** *hold-time-up*] [**down** *hold-time-down*]}
no hold-time

Context **[Tree]** (config>port>tdm hold-time)

Full Context configure port tdm hold-time

Description This command configures link dampening timers in 100s of milliseconds. This guards against reporting excessive interface transitions. This is implemented by not advertising subsequent transitions of the interface to upper layer protocols until the configured timer has expired.

This command is only supported on the m4-chds3-as, m12-chds3-as, and c4-ds3 MDAs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no hold-time

Parameters *hold-time-up* — Configures the hold-timer for link up event dampening. A value of zero (0) indicates that an up transition is reported immediately.

Values 0 to 100 in 100s of milliseconds (default 0)

hold-time-down — The hold-timer for link down event dampening. A value of zero (0) indicates that a down transition is reported immediately.

Values 0 to 100 in 100s of milliseconds (default 5)

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

hold-time

Syntax **hold-time down** *hold-down-time*
no hold-time

Context **[Tree]** (config>lag hold-time)

Full Context configure lag hold-time

Description This command specifies the timer, in tenths of seconds, which controls the delay between detecting that a LAG is down (all active ports are down) and reporting it to the higher levels.

A non-zero value can be configured, for example, when active/standby signaling is used in a 1:1 fashion to avoid informing higher levels during the small time interval between detecting that the LAG is down and the time needed to activate the standby link.

Default no hold-time

Parameters *hold-down-time* — Specifies the hold-time for event reporting.

Values 0 to 2000

Platforms All

hold-time

Syntax **hold-time** *value*
no hold-time

Context **[Tree]** (config>service>vpls>mrp>mvrp hold-time)

Full Context configure service vpls mrp mvrp hold-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the dampening timer and applies to both types of provisioned SAPs – end-station and UNI. When a value is configured for the timer, it controls the delay between detecting that the last provisioned SAP in VPLS goes down and reporting it to the MVRP module. The CPM will wait for the time specified in the value parameter before reporting it to the MVRP module. If the SAP comes up before the hold-timer expires, the event will not be reported to MVRP module.

The non-zero hold-time does not apply for SAP transition from down to up, This kind of transition is reported immediately to MVRP module without waiting for hold-time expiration. Also this parameter applies only to the provisioned SAPs. It does not apply to the SAPs configured with the **vpls-sap-template** command. Also when end-station QinQ SAPs are present only the “no hold-time” configuration is allowed.

The **no** form of this command disables tracking of the operational status for the last active SAP in the VPLS. MVRP will stop declaring the VLAN only when the last provisioned customer (UNI) SAP associated locally with the service is deleted. Also MVRP will declare the associated VLAN attribute as soon as the first provisioned SAP is created in the associated VPLS instance, regardless of the operational state of the SAP.

Default no hold-time

Parameters *value* — Specifies the hold time in minutes

Values 1 to 30

Platforms All

hold-time

Syntax **hold-time** *seconds*
no hold-time

Context **[Tree]** (config>service>vpls>pim-snooping hold-time)

Full Context configure service vpls pim-snooping hold-time

Description This command configures the duration that allows the PIM-snooping switch to snoop all the PIM states in the VPLS. During this duration, multicast traffic is flooded in the VPLS. At the end of this duration, multicast traffic is forwarded using the snooped states.

When PIM snooping is enabled in VPLS, there is a period of time when the PIM snooping switch may not have built complete snooping state. The switch cannot build states until the routers connected to the VPLS refresh their PIM messages.

This parameter is applicable only if PIM snooping is enabled.

Parameters *seconds* — Specifies the PIM snooping hold time, in seconds.

Values 0 to 300

Default 90

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

hold-time

Syntax **hold-time**

Context **[Tree]** (config>router>if hold-time)
[Tree] (config>service>ies>interface hold-time)
[Tree] (config>service>ies>subscriber-interface hold-time)
[Tree] (config>service>ies>redundant-interface hold-time)
[Tree] (config>service>vprn>interface hold-time)
[Tree] (config>service>vprn>network-interface hold-time)
[Tree] (config>service>vprn>subscriber-interface hold-time)
[Tree] (config>service>vprn>redundant-interface hold-time)
[Tree] (config>service>vpls>interface hold-time)

Full Context configure router interface hold-time
configure service ies interface hold-time
configure service ies redundant-interface hold-time
configure service ies subscriber-interface hold-time
configure service vpls interface hold-time
configure service vprn interface hold-time
configure service vprn network-interface hold-time
configure service vprn redundant-interface hold-time
configure service vprn subscriber-interface hold-time

Description This command creates the CLI context to configure interface level hold-up and hold-down timers for the associated IP interface.

The **up** timer controls a delay for the associated IPv4 or IPv6 interface so that the system will delay the deactivation of the associated interface for the specified amount of time.

The **down** timer controls a delay for the associated IPv4 or IPv6 interface so that the system will delay the activation of the associated interface for the specified amount of time

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface hold-time
- configure service ies redundant-interface hold-time
- configure service vprn redundant-interface hold-time
- configure service ies subscriber-interface hold-time

All

- configure service vpls interface hold-time
- configure service ies interface hold-time
- configure router interface hold-time
- configure service vprn interface hold-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn network-interface hold-time

hold-time

Syntax **hold-time** *seconds* [**min** *seconds2*]
no hold-time

Context **[Tree]** (config>service>vprn>bgp hold-time)
[Tree] (config>service>vprn>bgp>group hold-time)
[Tree] (config>service>vprn>bgp>group>neighbor hold-time)

Full Context configure service vprn bgp group hold-time
configure service vprn bgp group neighbor hold-time
configure service vprn bgp hold-time

Description This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Even though the router OS implementation allows setting the **keepalive** (**config>service>vprn>bgp keepalive**, **config>service>vprn>bgp>group keepalive**, **config>service>vprn>bgp>group>neighbor keepalive**) time separately, the configured **keepalive** timer is overridden by the **hold-time** value under the following circumstances:

- If the specified hold-time is less than the configured **keepalive** time, then the operational **keepalive** time is set to a third of the **hold-time**; the configured **keepalive** time is not changed.
- If the **hold-time** is set to zero, then the operational value of the **keepalive** time is set to zero; the configured **keepalive** time is not changed. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default hold-time 90

Parameters *seconds* — Specifies the hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is up permanently.

Values 0, 3 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

seconds2 — Specifies the minimum hold-time that is accepted for the session. If the peer proposes a hold-time lower than this value the session attempt is rejected.

Platforms All

hold-time

Syntax **hold-time**

Context **[Tree]** (config>service>oper-group hold-time)

Full Context configure service oper-group hold-time

Description Commands in this context configure hold time information.

Platforms All

hold-time

Syntax **hold-time** *seconds* [**min** *seconds*]
no hold-time

Context **[Tree]** (config>router>bgp hold-time)
[Tree] (config>router>bgp>group hold-time)
[Tree] (config>router>bgp>group>neighbor hold-time)

Full Context configure router bgp group hold-time
configure router bgp group neighbor hold-time
configure router bgp hold-time

Description This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Even though the implementation allows setting the **keepalive** time separately, the configured **keepalive** timer is overridden by the **hold-time** value under the following circumstances:

- If the specified hold-time is less than the configured **keepalive** time, then the operational **keepalive** time is set to a third of the **hold-time**; the configured **keepalive** time is not changed.
- If the **hold-time** is set to zero, then the operational value of the **keepalive** time is set to zero; the configured **keepalive** time is not changed. This means that the connection with the peer is up permanently and no keepalive packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default hold-time 90

Parameters *seconds* — Specifies the hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is up permanently.

Values 0, 3 to 65535

min *seconds2* — Specifies the minimum hold-time that will be accepted for the session. If the peer proposes a hold-time lower than this value, the session attempt will be rejected.

Platforms All

12.55 hold-time-aps

hold-time-aps

Syntax **hold-time-aps** [**lsignal-failure** *sf-time*] [**lsignal-degrade** *sd-time*]
no hold-time-aps

Context **[Tree]** (config>port>aps hold-time-aps)

Full Context configure port aps hold-time-aps

Description This command configures hold-down timers to debounce signal failure conditions (lais, b2err-sf) and signal degrade conditions (b2err-sd) for Uni 1+1 Sig+Data APS switching mode (switching mode uni-1plus1).

The **no** version of this command resets the hold-down timer to the default value.

Default 0 (disabled)

Parameters *sf-time* — Specifies an integer to define the signal failure hold-down time in milliseconds.

Values 1 to 100

sd-time — Specifies an integer to define the signal degrade hold-down time in milliseconds.

Values 1 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.56 hold-time-down

hold-time-down

Syntax **hold-time-down** *timer*
no hold-time-down

Context **[Tree]** (config>router>mpls>mpls-tp>oam-template hold-time-down)

Full Context configure router mpls mpls-tp oam-template hold-time-down

Description This command configures the hold-down dampening timer. It is equivalent to a hold-off timer.

Default hold-time-down 0

Parameters *interval* — Specifies the hold-down dampening timer interval.

Values 0 to 5000 deciseconds in 10 ms increments

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

12.57 hold-time-up

hold-time-up

Syntax **hold-time-up** *timer*
no hold-time-up

Context **[Tree]** (config>router>mpls>mpls-tp>oam-template hold-time-up)

Full Context configure router mpls mpls-tp oam-template hold-time-up

Description This command configures the hold-up dampening timer. This can be used to provide additional dampening to the state of proactive CC BFD sessions.

Default hold-time-up 20

Parameters *interval* — Specifies the hold-up dampening timer interval.

Values 0 to 500 deciseconds, in 100 ms increments

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.58 hold-timer

hold-timer

Syntax **hold-timer** *seconds*
no hold-timer

Context **[Tree]** (config>router>mpls hold-timer)

Full Context configure router mpls hold-timer

Description This command specifies the amount of time that the ingress node holds before programming its data plane and declaring the LSP up to the service module. This occurs anytime the ingress node brings up an LSP path or switches traffic from a working path to another working path of the same LSP.

The **no** form of this command reverts to the default value.

Default no hold-timer

Parameters *seconds* — Specifies the time (in seconds), for which the ingress node holds before programming its data plane and declaring the LSP up to the service module.

Values 0 to 1000

Default 1

Platforms All

12.59 holddown

holddown

Syntax [**no**] **holddown** [**neighbor** *ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>rip holddown)

Full Context debug router rip holddown

Description This command enables debugging for RIP holddowns.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP holddowns sent on the neighbor IP address or interface.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

holddown

Syntax [**no**] **holddown** [**neighbor** *ip-int-name* | *ipv6-address*]

Context **[Tree]** (debug>router>ripng holddown)

Full Context debug router ripng holddown

Description This command enables debugging for RIPng holddowns.

Parameters *ip-int-name* | *ipv6-address* — Debugs the RIPng holddowns sent on the neighbor IP address or interface.

Platforms All

12.60 holdtime

holdtime

Syntax **holdtime** *holdtime*
no holdtime

Context **[Tree]** (config>service>vprn>pim>rp>rp-candidate holdtime)
[Tree] (config>service>vprn>pim>rp>ipv6>rp-candidate holdtime)

Full Context configure service vprn pim rp ipv6 rp-candidate holdtime
configure service vprn pim rp rp-candidate holdtime

Description This command specifies the length of time a neighbor considers the sending router to be operationally up.

The **no** form of this command reverts to the default value.

Default holdtime 150

Parameters *holdtime* — Specifies the length of time, in seconds, that a neighbor should consider the sending router to be operational.

Values 5 to 255

Platforms All

holdtime

Syntax **holdtime** *holdtime*
no holdtime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>pim>rp>rp-candidate holdtime)
[Tree] (config>router>pim>rp>ipv6>rp-candidate holdtime)

Full Context configure router pim rp ipv6 rp-candidate holdtime
configure router pim rp rp-candidate holdtime

Description This command configures the length of time, in seconds, that neighbors should consider the sending router to be operationally up. A local RP cannot be configured on a logical router.

The **no** form of this command reverts to the default value.

Default holdtime 150

Parameters *holdtime* — Specifies the hold time, in seconds.

Values 5 to 255

Platforms All

12.61 home

home

Syntax **home** *bit* [*bit*]
no home

Context [Tree] (config>subscr-mgmt>gtp>peer-profile>charging home)

Full Context configure subscriber-mgmt gtp peer-profile charging-characteristics home

Description This command configures the charging characteristics for home UE.

Default no home

Parameters *bit* — Specifies up to 16 bits to set in the Charging Characteristics Information Element (IE) for home UE, if not known by other means such as RADIUS.

Values bit0, bit1, bit2, bit3, bit4, bit5, bit6, bit7, bit8, bit9, bit10, bit11, bit12, bit13, bit14, bit15

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.62 home-directory

home-directory

Syntax **home-directory** *url-prefix* [*directory*] [*directoryIdirectory*]
no home-directory

Context **[Tree]** (config>system>security>user home-directory)
[Tree] (config>system>security>user-template home-directory)

Full Context configure system security user home-directory
configure system security user-template home-directory

Description This command configures the local home directory for the user for both console (file commands and '>' redirection) and FTP access.

If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed.

The **no** form of this command removes the configured home directory.

Default no home-directory

Note: If restricted-to-home has been configured no file access is granted and no home-directory is created. If restricted-to-home is not applied then root becomes the user's home-directory.

Parameters *local-url-prefix* [*directory*] [*directory/directory*] — Specifies the user's local home directory URL prefix and directory structure, up to 190 characters.

Platforms All

12.63 hop

hop

Syntax **hop** *hop-index* **node-id** *node-id* [**te-link** *te-link-id*] {**strict** | **loose**}
no hop *hop-index*

Context **[Tree]** (config>router>gmpls>path hop)

Full Context configure router gmpls path hop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the node ID of the hops that the GMPLS LSP should traverse on its way to the egress UNI-C router.

The GMPLS LSP ingress and egress node IDs can be included as the first and the last hop. This is necessary when inter-operating with the Nokia 1830 PSS.

The **no** form of this command deletes hop list entries for the path. All of the GMPLS LSPs currently using the path are affected. Additionally, all services actively using these GMPLS LSPs are affected. The path must be shut down first in order to delete the hop from the hop list. The **no hop** *hop-index* command will not result in any action except a warning message on the console indicating that the path is administratively up.

Parameters *hop-index* — Specifies the order of the hops. The LSP always traverses from the lowest hop index to the highest. The hop index does not need to be sequential.

Values 1 to 1024

node-id — Specified the node ID of the transit GMPLS LSR. This can be an IPv4 address or a 32-bit unsigned integer identifier of the data plane switching node of the adjacent UNI-N.

te-link-id — Specifies the ID of the TE Link.

Values 1 to 4294967295

loose — Specifies that the route taken by the GMPLS LSP from the previous hop to this hop can traverse through other LSRs. Multiple hop entries with the *node-id* are flagged as errors. Either the loose or strict keyword must be specified.

strict — Specifies that the LSP must take a direct path from the previous hop router to this router. No transit routers between the previous router and this router are allowed. If the IP address specified is the interface address, then the LSP must use that interface. If there are direct parallel links between the previous router and this router, and if the system IP address is specified, then any one of the available interfaces can be used by the LSP. The user must ensure that the previous router and this router have a direct link. Multiple hop entries with the same IP address are flagged as errors. Either the loose or strict keyword must be specified.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

hop

Syntax **hop** *hop-index ip-address* {**strict** | **loose**}
hop *hop-index* **sid-label** *sid-value*
no hop *hop-index*

Context **[Tree]** (config>router>mpls>path hop)

Full Context configure router mpls path hop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the hops that the LSP should traverse on its way to the egress router. When specified, the IP address can be the interface IP address, a loopback interface address, or the system IP address. If a loopback interface or the system IP address is specified then the LSP can choose the best available interface.

When an IPv6 hop is specified, the interface IP address must be a global unicast IPv6 address. A link-local address is not allowed and is rejected in the configuration if attempted.

Optionally, the LSP ingress and egress IP address can be included as the first and the last hop. A hop list can include the ingress interface IP address, the system IP address, and the egress IP address of any of the hops being specified.

When the **sid-label** parameter is specified, this command specifies an MPLS label value for a hop in the path of an SR-TE LSP. The label value implied by the SID is only used when the path is used by an SR-TE LSP.

The **no** form of this command deletes hop list entries for the path. All the LSPs currently using this path are affected. Additionally, all services actively using these LSPs are affected. The path must be shutdown first in order to delete the hop from the hop list. The **no hop** *hop-index* command will not result in any action except a warning message on the console indicating that the path is administratively up.

Parameters *hop-index* — Specifies the hop index is used to order the hops specified. The LSP always traverses from the lowest hop index to the highest. The hop index does not need to be sequential.

Values 1 to 1024

ip-address — Specifies a loopback interface, the system or network interface IP address of the transit router. An interface IPv6 address must be a global unicast address.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — 0 to FFFF (hexadecimal)
d — 0 to 255 (decimal)

loose — This keyword specifies that the route taken by the LSP from the previous hop to this hop can traverse through other routers. Multiple hop entries with the same IP address are flagged as errors. Either the **loose** *or* **strict** keyword must be specified.

strict — This keyword specifies that the LSP must take a direct path from the previous hop router to this router. No transit routers between the previous router and this router are allowed. If the IP address specified is the interface address, then that is the interface the LSP must use. If there are direct parallel links between the previous router and this router and if system IP address is specified, then any one of the available interfaces can be used by the LSP. The user must ensure that the previous router and this router have a direct link. Multiple hop entries with the same IP address are flagged as errors. Either the **loose** *or* **strict** keyword must be specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sid-value — Specifies the SID value. The *sid-value* can be any valid MPLS/SR label value. It is not restricted by any locally-defined label ranges since these may be different on the remote node or adjacency for which the SID is defined.

Values 32 to 1048575

Platforms All

hop

Syntax **hop** *hop-index ip-address*
no hop *hop-index*

Context **[Tree]** (config>service>pw-routing>path hop)

Full Context configure service pw-routing path hop

Description This command configures each hop on an explicit path that can be used by one or more dynamic MS-PWs. It specifies the IP addresses of the hops that the MS-PE should traverse. These IP addresses can correspond to the system IP address of each S-PE, or the IP address on which the T-LDP session to a given S-PE terminates.

The **no** form of this command deletes hop list entries for the path. All the MS-PWs currently using this path are unaffected. Additionally, all services actively using these MS-PWs are unaffected. The path must be shutdown first in order to delete the hop from the hop list. The '**no hop hop-index**' command will not result in any action, except for a warning message on the console indicating that the path is administratively up.

Default no hop

Parameters *hop-index* — Specifies a locally significant numeric identifier for the hop. The hop index is used to order the hops specified. The LSP always traverses from the lowest hop index to the highest. The hop index does not need to be sequential.

Values 1 to 1024

ip-address — Specifies the system IP address or terminating IP address for the T-LDP session to the S-PE corresponding to this hop. For a given IP address on a hop, the system will choose the appropriate SDP to use.

Platforms All

12.64 hop-by-hop-opt

hop-by-hop-opt

Syntax **hop-by-hop-opt** {**true** | **false**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no hop-by-hop-opt

Context **[Tree]** (config>filter>ipv6-filter>entry>match hop-by-hop-opt)

Full Context configure filter ipv6-filter entry match hop-by-hop-opt

Description This command enables match on existence of Hop-by-Hop Options Extension Header in the IPv6 filter policy.

The **no** form of this command ignores Hop-by-Hop Options Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default no hop-by-hop-opt

Parameters **true** — Matches a packet with a Hop-by-Hop Options Extension header.

false — Matches a packet without a Hop-by-Hop Options Extension header.

Platforms All

hop-by-hop-opt

Syntax **hop-by-hop-opt** {**true** | **false**}
no hop-by-hop-opt

Context **[Tree]** (cfg>sys>sec>cpm>ipv6-filter>entry>match hop-by-hop-opt)

Full Context configure system security cpm-filter ipv6-filter entry match hop-by-hop-opt

Description This command enables match on existence of Hop-by-Hop Options Extension Header in the IPv6 filter policy. This command applies to the 7750 SR and 7950 XRS.

The **no** form of this command ignores Hop-by-Hop Options Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default no hop-by-hop-opt

Parameters **true** — Match if a packet contains Hop-by-Hop Options Extension Header.

false — Match if a packet does not contain Hop-by-Hop Options Extension Header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

12.65 hop-limit

hop-limit

Syntax **hop-limit** *limit*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no hop-limit

Context [Tree] (config>router>mpls>lsp>fast-reroute hop-limit)
[Tree] (config>router>mpls>lsp-template>fast-reroute hop-limit)

Full Context configure router mpls lsp fast-reroute hop-limit
configure router mpls lsp-template fast-reroute hop-limit

Description For fast reroute, how many more routers a detour is allowed to traverse compared to the LSP itself. For example, if an LSP traverses four routers, any detour for the LSP can be no more than ten router hops, including the ingress and egress routers.

The **no** form of this command reverts to the default value.

Default hop-limit 16

Parameters *limit* — Specify the maximum number of hops.

Values 0 to 255

Platforms All

hop-limit

Syntax **hop-limit** *number*
no hop-limit

Context [Tree] (config>router>mpls>lsp hop-limit)
[Tree] (config>router>mpls>lsp>primary-p2mp-instance hop-limit)

Full Context configure router mpls lsp hop-limit
configure router mpls lsp primary-p2mp-instance hop-limit

Description This command specifies the maximum number of hops that an LSP can traverse, including the ingress and egress routers. An LSP is not set up if the hop limit is exceeded. This value can be changed dynamically for an LSP that is already set up with the following implications.

If the new value is less than the current number of hops of the established LSP, the LSP is brought down. The software then tries to re-establish the LSP within the new **hop-limit** number. If the new value is equal to or greater than the current number hops of the established LSP, the LSP is not affected.

The **config**>**router**>**mpls**>**lsp**>**primary-p2mp-instance**>**hop-limit** command is not supported on the 7450 ESS.

The **no** form of this command returns the parameter to the default value.

Default hop-limit 255

Parameters *number* — Specifies the number of hops the LSP can traverse, expressed as an integer.

Values 2 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

hop-limit

Syntax **hop-limit** *number*
no hop-limit

Context **[Tree]** (config>router>mpls>lsp>primary hop-limit)
[Tree] (config>router>mpls>lsp>secondary hop-limit)

Full Context configure router mpls lsp primary hop-limit
configure router mpls lsp secondary hop-limit

Description This optional command overrides the **config>router>mpls>lsp** *lsp-name***>hop-limit** command. This command specifies the total number of hops that an LSP traverses, including the ingress and egress routers.

This value can be changed dynamically for an LSP that is already set up with the following implications:

If the new value is less than the current hops of the established LSP, the LSP is brought down. MPLS then tries to re-establish the LSP within the new hop-limit number. If the new value is equal or more than the current hops of the established LSP then the LSP will be unaffected.

The **no** form of this command reverts the values defined under the LSP definition using the **config>router>mpls>lsp** *lsp-name***>hop-limit** command.

Default no hop-limit

Parameters *number* — Specifies the number of hops the LSP can traverse, expressed as an integer.

Values 2 to 255

Platforms All

hop-limit

Syntax **hop-limit** {**lt** | **gt** | **eq**} *hop-limit-value*
hop-limit range *hop-limit-value hop-limit-value*
no hop-limit

Context **[Tree]** (config>filter>ipv6-filter>entry>match hop-limit)

Full Context configure filter ipv6-filter entry match hop-limit

Description This command configures the Time To Live (TTL) match criteria.

The **no** form of this command removes the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no hop-limit

Parameters **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

hop-limit-value — Specifies the hop limit value for the rate limit action.

Values 0 to 255

Platforms All

12.66 host

host

Syntax **host** *host-name* [**create**]
no host *host-name*

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe host)
[Tree] (config>subscr-mgmt>loc-user-db>ppp host)

Full Context configure subscriber-mgmt local-user-db ipoe host
configure subscriber-mgmt local-user-db ppp host

Description This command creates an IPoE or PPP host entry in the local user database. A host entry in the local user database is matched based on the specified match-list criteria and an optional mask that is applied to the host-identification parameters.

A default host entry can be created without host-identification parameters which is used when no other host entries match. Note that creating a default host entry also requires a match-list to be specified.

The **no** form of this command removes the host entry from the local user database.

Parameters *host-name* — Specifies a unique host name, up to 32 characters. The *host-name* **default** creates a special match-all host entry that should not have host-identification parameters and is used when no other host entries match.

create — Keyword used to create the host name. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

host

Syntax [**no**] **host** [*ip-address*]
[**no**] **host** [**fwd-service** *service-id*] **group-interface** *ip-int-name*

Context **[Tree]** (debug>router>igmp host)

Full Context debug router igmp host

Description This command enables debugging for the IGMP host.

The **no** form of the command disables debugging.

Parameters *ip-address* — Debugs the information associated with the specified IP address.

service-id — Debugs information associated with the service ID.

Values service-id: 1 to 2148278386
svc-name: up to 64 characters.

group-interface *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IP interface address

Platforms All

12.67 host-accounting

host-accounting

Syntax [**no**] **host-accounting** [**interim-update**]

Context **[Tree]** (config>subscr-mgmt>acct-plcy host-accounting)

Full Context configure subscriber-mgmt radius-accounting-policy host-accounting

Description This command enables per-host accounting. In host accounting mode, the acct-session-id is generated per host. This acct-session-id is uniformly included in all accounting messages (START/INTERIM-UPDATE/STOP) and it can be included in RADIUS Access-Request message.

Accounting counters are based on the queue counters and as such are aggregated for all host sharing the queues within an sla-profile instance. CoA and LI is supported based on the acct-session-id of the host.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **interim-update** — Specifies that no interim-update messages are sent for the related subscriber hosts when the session is deleted. Without this keyword, only START and STOP accounting messages are generated when the host is established or terminated. This is equivalent to a time-based accounting where only the duration of the session is required.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

12.68 host-connectivity-verify

host-connectivity-verify

Syntax **host-connectivity-verify source-ip** *ip-address* [**source-mac** *ieee-address*] [**interval** *interval*] [**action** {**remove** | **alarm**}] [**timeout** *retry-timeout*] [**retry-count** *count*]

Context **[Tree]** (config>service>vpls host-connectivity-verify)
[Tree] (config>service>vpls>sap host-connectivity-verify)

Full Context configure service vpls host-connectivity-verify
configure service vpls sap host-connectivity-verify

Description This command enables subscriber host connectivity verification on a given VPLS SAP or within a VPLS service.

This tool will periodically scan all known hosts (from dhcp-state) and perform a UC ARP request. The subscriber host connectivity verification will maintain state (connected vs. not-connected) for all hosts.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies an unused IP address in the same network for generation of subscriber host connectivity verification packets.

ieee-address — Specifies the source MAC address to be used for generation of subscriber host connectivity verification packets.

interval — The interval, in minutes, which specifies the time interval in which all known sources should be verified. The actual rate is then dependent on number of known hosts and interval.

Values 1 to 6000 Note that a zero value can be used by the SNMP agent to disable host-connectivity-verify.

action {**remove** | **alarm**} — Defines the action taken on a subscriber host connectivity verification failure for a given host. The **remove** keyword raises an alarm and removes the dhcp-state and releases all allocated resources (queues, table entries, and so on). A DHCP release is signaled to corresponding DHCP server. The static host is never removed. The **alarm** keyword raises an alarm indicating that the host is disconnected.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

retry-timeout — Specifies the time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled.

Values 0 to 120

count — Specifies the number of connectivity check retransmissions.

Values 10 to 60 seconds

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-connectivity-verify

Syntax **host-connectivity-verify** [**interval** *interval*] [**action** {**remove** | **alarm**}] [**timeout** *retry-timeout*] [**retry-count** *count*] [**family** *family*]

Context **[Tree]** (config>service>ies>sub-if>grp-if host-connectivity-verify)
[Tree] (config>service>vprn>sub-if>grp-if host-connectivity-verify)

Full Context configure service ies subscriber-interface group-interface host-connectivity-verify
configure service vprn subscriber-interface group-interface host-connectivity-verify

Description This command enables subscriber host connectivity verification on a given SAP within a service. This tool periodically scans all known hosts (from dhcp-state) and perform UC ARP requests. The subscriber host connectivity verification maintains state (connected versus. not-connected) for all hosts.

The **no** form of this command reverts to the default.

Parameters *interval* — Specifies the interval, in minutes, which specifies the time interval which all known sources should be verified. The actual rate is then dependent on the number of known hosts and interval.

Values 1 to 6000

A zero value can be used by the SNMP agent to disable host-connectivity-verify.

action {remove | alarm} — Defines the action taken on a subscriber host connectivity verification failure for a given host. The **remove** keyword raises an alarm and removes dhcp-state and releases all allocated resources (queues, table entries and so on). DHCP-RELEASE is signaled to corresponding DHCP server. Static hosts is never removed. The **alarm** keyword raises an alarm indicating that the host is disconnected.

retry-timeout — Specifies the retry timeout.

Values 10 to 60 seconds

count — Specifies the number of retry requests.

Values 2 to 29

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

family — Allows the host connectivity checks to be performed for IPv4 endpoint, IPv6 endpoint or both. With family IPv6 configured, host connectivity checks is performed on the global unicast address (assigned via SLAAC or DHCPv6 IA_NA) and link-local address of a Layer 3 RG or bridged hosts. In case of SLAAC assignment, host connectivity can only be performed if the /128 is known (via downstream ND). DHCPv6 PD assigned prefixes is removed if link-local address is determined to be unreachable via host connectivity check" Reachability checks for GUA and link-local address is done simultaneously.

Values ipv4, ipv6, both

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-connectivity-verify

Syntax **host-connectivity-verify** [**source** {**vrrp** | **interface**}] [**interval** *interval*] [**action** {**remove** | **alarm**}] [**timeout** *retry-timeout*] [**retry-count** *retry-count*]

Context **[Tree]** (config>service>ies>if host-connectivity-verify)
[Tree] (config>service>vprn>if host-connectivity-verify)

Full Context configure service ies interface host-connectivity-verify
configure service vprn interface host-connectivity-verify

Description This command enables subscriber host connectivity verification for all hosts on this interface. This tool periodically scans all known hosts (from dhcp-state) and perform UC ARP requests. The subscriber host connectivity verification maintains state (connected vs. not-connected) for all hosts.

The **no** form of this command reverts to the default.

Parameters **source** {**vrrp** | **interface**} — Specifies the source to be used for generation of subscriber host connectivity verification packets. The **vrrp** keyword specifies that the VRRP state should be used to select proper IP and MAC (active uses VRID, back-up uses interface addresses). The **interface** keyword forces the use of the interface mac and ip addresses.

Note: There are up to 256 possible subnets on a given interface, therefore, the subscriber host connectivity verification tool always uses an address of the subnet to which the given host is pertaining. For group-interfaces, one of the parent subscriber interface subnets (depending on host's address) is used.

action {**remove** | **alarm**} — Defines the action taken on a subscriber host connectivity verification failure for a given host. The **remove** keyword raises an alarm and removes dhcp-state and releases all allocated resources (queues, table entries, and so on). The **alarm** keyword raises an alarm indicating that the host is disconnected.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interval — Specifies the interval, expressed in minutes, which specifies when all known sources should be verified. The actual rate is then dependent on number of known hosts and interval.

Values 1 to 6000

Note: A zero value can be used by the SNMP agent to disable host-connectivity-verification.

retry-timeout — Specifies the timeout, in seconds, before a connectivity check retransmission.

Values 10 to 60

retry-count — Specifies the number of connectivity check retransmissions.

Values 2 to 29

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-connectivity-verify

Syntax [**no**] **host-connectivity-verify**

Context **[Tree]** (debug>service>id host-connectivity-verify)

Full Context debug service id host-connectivity-verify

Description This command enables Subscriber Host Connectivity Verification (SHCV) debugging.

The **no** form of the command disables the SHCV debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-connectivity-verify

Syntax **host-connectivity-verify service** *service-id* [**sap** *sap-id*]
host-connectivity-verify subscriber *sub-ident-string* [**sla-profile** *sla-profile-name*]

Context **[Tree]** (oam host-connectivity-verify)

Full Context oam host-connectivity-verify

Description This command triggers the host connectivity verification checks and applies only to the 7450 ESS and 7750 SR.

Parameters *service-id* — Specifies the service ID to diagnose or manage.

Values 1 to 2147483647, service-name: up to 64 characters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap-id — Specifies the physical port identifier portion of the SAP definition.

Values

null	*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id*	
dot1q	*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id* | *pw-id*:[qtag1| cp-conn-prof-id]	
qinq	*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *pw-id*:[qtag1 **cp**-*conn-prof-id*].[qtag2 | **cp**-conn-prof-id]	
	cp	keyword
	conn-prof-id	1 to 8000
atm	*port-id* | *aps-id* [:vpi/vci | vpi | vpi1.vpi2 | **cp**.*conn-prof-id*]	
	cp	keyword
	conn-prof-id	1 to 8000
frame	*port-id* | *aps-id*:dlci	
cisco-hdlc	*slot/mda/port.channel*	
cem	*slot/mda/port.channel*	
ima-grp	bundle-id [:vpi/vci | vpi | vpi1.vpi2 | **cp**.*conn-prof-id*]	
	cp	keyword
	conn-prof-id	1 to 8000
port-id	*slot/mda/port*[.channel]	
	esat-*id*/*slot*/*port*	
	pxc-*id*.*sub-port*	
bundle-id	**bundle**-*type*-slot/mda.-*bundle-num*	
	bundle	keyword
	type	ima | fr | ppp
	bundle-num	1 to 336
bpgrp-id	**bpgrp**-*type-bpgrp-num*	
	bgrp	keyword
	type	ima | ppp
	bgrp-num	1 to 2000
aps-id	**aps**-*group-id*[.channel]	
	aps	keyword
	group-id	1 to 128
ccag-id	**ccag**-*id*.*path-id*[*cc-type*]:*cc-id*	
	ccag	keyword
	id	1 to 8
	path-id	a | b
	cc-type	.sap-net | .net-sap
	cc-id	1 to 4094
eth-tunnel	eth-tunnel-*id*[:*eth-tun-sap-id*]	

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	id	1 to 1024
	eth-tun-sap-id	0 to 4094
lag-id	**lag**-*id*	
	lag	keyword
	id	1 to 800
pw-id	**pw**-*id*	
	pw	keyword
	id	1 to 10239
qtag1	* | 0 to 4094	
qtag2	* | null | 0 to 4094	
vpi	0 to 4095 (NNI)	
	0 to 255 (UNI)	
vci	1 | 2 | 5 to 65535	
dlci	16 to 1022	
tunnel-id	**tunnel**-*id*.*private* | *public*:*tag*	
	tunnel	keyword
	id	1 to 16
	tag	0 to 4094

sub-indent-string — Specifies an existing subscriber-id, up to 32 characters.

sla-profile-name — Specifies an existing SLA profile name, up to 32 characters. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

Platforms All

12.69 host-identification

host-identification

Syntax **host-identification**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host host-identification)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host host-identification)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification
configure subscriber-mgmt local-user-db ppp host host-identification

Description Commands in this context configure host identification parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.70 host-ip

host-ip

Syntax **host-ip** *prefix-list-name*

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from host-ip)

Full Context configure router policy-options policy-statement entry from host-ip

Description This command specifies a prefix list host IP address as a match criterion for the route policy-statement entry.

Default no host-ip

Parameters *prefix-list-name* — Specifies the prefix-list name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The *prefix-list-name* is defined in the **config>router>policy-options>prefix-list** context.

Platforms All

12.71 host-key

host-key

Syntax **host-key** {**mac**}
no host-key

Context **[Tree]** (config>subscr-mgmt>host-lockout-plcy host-key)

Full Context configure subscriber-mgmt host-lockout-policy host-key

Description This command specifies the parameters used in host identification for lockout on a given SAP or capture SAP.

no host-key – include (MAC address, Circuit-Id, Remote-Id)

host-key mac – include MAC address only

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

"host-key mac" should be used in DHCPv4 scenarios where Circuit-Id and Remote-Id are changed with "dhcp option action replace" configuration: a host lockout context is created with the replaced Circuit-Id/Remote-Id; with the default host-key (including Circuit-Id and Remote-Id), lockout does not kick in on the original trigger packet when it is retransmitted by the client.

Changing the host-key to mac should be used with care: all hosts with the same MAC address on a given SAP or capture SAP are identified as a single host with respect to host-lockout.

This command cannot be changed when the **host-lockout-policy** is referenced (configured under a SAP context).

The **no** form of this command reverts to the default value.

Parameters **mac** — Specifies to use the MAC address only for host identification for lockout.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

12.72 host-limit

host-limit

Syntax **host-limit** *max-num-hosts*
no host-limit

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>arp-host host-limit)
[Tree] (config>service>vpls>sap>arp-host host-limit)
[Tree] (config>service>ies>sub-if>grp-if>arp-host host-limit)
[Tree] (config>service>vprn>sub-if>grp-if>arp-host host-limit)

Full Context configure service ies subscriber-interface group-interface arp-host host-limit
configure service vpls sap arp-host host-limit
configure service vprn subscriber-interface group-interface arp-host host-limit
configure subscriber-mgmt msap-policy vpls-only-sap-parameters arp-host host-limit

Description This command configures the maximum number of ARP hosts.

The **no** form of this command reverts to the default.

Default host-limit 1

Parameters *max-num-hosts* — Specifies the maximum number of ARP hosts allowed on this SAP.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Values 1 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-limit

Syntax **host-limit** *max-num-hosts*
no host-limit

Context **[Tree]** (config>service>ies>sub-if>grp-if host-limit)

Full Context configure service ies subscriber-interface group-interface host-limit

Description This command configures the maximum number of ARP hosts.

Parameters *max-num-hosts* — Specifies the maximum number of ARP hosts.

Values 1 to 32767

12.73 host-limits

host-limits

Syntax [**no**] **no host-limits**

Context **[Tree]** (config>subscr-mgmt>sla-profile host-limits)
[Tree] (config>subscr-mgmt>sub-profile host-limits)

Full Context configure subscriber-mgmt sla-profile host-limits
configure subscriber-mgmt sub-profile host-limits

Description Commands in this context configure host limits per SLA profile instance or per subscriber.

The **no** form of this command removes the host limit configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

12.74 host-lockout-policy

host-lockout-policy

Syntax **host-lockout-policy** *policy-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no host-lockout-policy

Context [Tree] (config>service>ies>if>sap host-lockout-policy)
[Tree] (config>service>ies>sub-if>grp-if>sap host-lockout-policy)
[Tree] (config>service>vpls>sap host-lockout-policy)
[Tree] (config>service>vprn>if>sap host-lockout-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap host-lockout-policy)

Full Context configure service ies interface sap host-lockout-policy
configure service ies subscriber-interface group-interface sap host-lockout-policy
configure service vpls sap host-lockout-policy
configure service vprn interface sap host-lockout-policy
configure service vprn subscriber-interface group-interface sap host-lockout-policy

Description This command selects an existing host lockout policy. The **host-lockout-policy** *policy-name* is created in the **config>subscr-mgmt** context.

The **no** form of this command removes the policy name from the SAP configuration.

Parameters *policy-name* — Specifies an existing host lockout policy, up to 32 characters, to associate with the SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-lockout-policy

Syntax **host-lockout-policy** *policy-name* [**create**]
no host-lockout-policy *policy-name*

Context [Tree] (config>subscr-mgmt host-lockout-policy)

Full Context configure subscriber-mgmt host-lockout-policy

Description This command creates a host lockout policy. The policy contains set of host lockout configuration parameters. It is applied to SAP or MSAPs (by a MSAP-policy). Any change does not impact existing locked-out hosts, but only new incoming hosts that enter lockout.

The **no** form of this command removes the policy name from the configuration. The policy must not be associated with any entity.

Parameters *policy-name* — Specifies an existing host lockout policy to associate with the SAP.

create — Specifies the keyword required to create the host lockout policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.75 host-match

host-match

Syntax **host-match dest** *destination-string* [**create**]
no host-match dest *destination-string*

Context **[Tree]** (config>port>ethernet>access>egr>qgrp host-match)

Full Context configure port ethernet access egress queue-group host-match

Description This command configures host matching for the Ethernet port egress queue-group.

The **no** form of this command removes the destination string from the configuration.

Parameters *destination-string* — Specify a host match destination string up to 32 characters.

create — Keyword used to create the host match. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

host-match

Syntax **host-match dest** *description-string* [**create**]
no host-match dest *destination-string*

Context **[Tree]** (config>port>sonet-sdh>path>access>egress>vport host-match)
[Tree] (config>port>ethernet>access>egress>vport host-match)

Full Context configure port ethernet access egress vport host-match
configure port sonet-sdh path access egress vport host-match

Description This command specifies the destination and organization strings to be used for matching subscriber hosts with this Vport.

The parent Vport of a subscriber host queue, which has the port-parent option enabled, is determined by matching the destination string **dest** string associated with the subscriber and the organization string org string associated with the subscriber host with the strings defined under a Vport on the port associated with the subscriber.

If a given subscriber host queue does not have the port-parent option enabled, it will be foster-parented to the Vport used by this subscriber and which is based on matching the dest string and org string. If the subscriber could not be matched with a Vport on the egress port, the host queue will not be bandwidth controlled and will compete for bandwidth directly based on its own PIR and CIR parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, a subscriber host queue with the port-parent option enabled is scheduled within the context of the port's port scheduler policy.

Parameters *description-string* — The destination character string. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path access egress vport host-match

All

- configure port ethernet access egress vport host-match

12.76 host-port

host-port

Syntax [**no**] **host-port** *port-id*

Context **[Tree]** (config>esa host-port)

Full Context configure esa host-port

Description This command configures an Ethernet port associated to the ESA instance.

The **no** form of this command removes the host-port.

Parameters *port-id* — Specifies the port identifier of any valid Ethernet port on a supported IOM.

Values *slot*/*mda*/*port*

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

host-port

Syntax **host-port** *port-id*
no host-port

Context **[Tree]** (config>esa>vm host-port)

Full Context configure esa vm host-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an Ethernet port associated to an ESA-VM instance. The *port-id* used must be the same as the port associated with the ESA context on which the ESA-VM is configured.

The **no** form of this command removes the specified host-port for the ESA-VM instance.

Parameters *port-id* — Specifies the port identifier of any valid Ethernet port ID on the supported IOM.

Values *slot*/*mda*/*port*

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

12.77 host-shutdown

host-shutdown

Syntax [**no**] **host-shutdown**

Context **[Tree]** (config>service>ies>if>sap host-shutdown)

Full Context configure service ies interface sap host-shutdown

Description This command administratively enables host creation on this SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

host-shutdown

Syntax [**no**] **host-shutdown**

Context **[Tree]** (config>service>vprn>if>sap host-shutdown)

Full Context configure service vprn interface sap host-shutdown

Description This command administratively enables host creation on this SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.78 host-tracking-policy

host-tracking-policy

Syntax **host-tracking-policy** *policy-name* [**create**]
no host-tracking-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt host-tracking-policy)
[Tree] (config>subscr-mgmt>sub-prof host-tracking-policy)

Full Context configure subscriber-mgmt host-tracking-policy
configure subscriber-mgmt sub-profile host-tracking-policy

Description This command configures a host tracking policy. IGMP host tracking is an option in the subscriber profile that allows the factoring in of a subscriber's (multicast) video traffic by reducing the unicast operational egress aggregate rate or the rate of the scheduler specified in the ANCP policy to account for a subscriber's multicast traffic. If no ANCP policy is defined, the egress aggregate rate configured in the subscriber profile is reduced. If an ANCP policy is defined, the **rate-modify** command in the policy specifies whether the egress aggregate rate or the rate of the egress policer specified in the policy is to be reduced to account for the subscriber's multicast traffic.

The **no** form of this command reverts to the default value.

Parameters *policy-name* — Specifies a host tracking policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

12.79 host-unreachable

host-unreachable

Syntax [**no**] **host-unreachable** *ip-address*
[**no**] **host-unreachable** *ipv6-address*

Context **[Tree]** (config>vrrp>policy>priority-event host-unreachable)

Full Context configure vrrp policy priority-event host-unreachable

Description This command creates the context to configure a host unreachable priority control event to monitor the ability to receive ICMP echo reply packets from an IP host address.

A host unreachable priority event creates a continuous ICMP echo request (ping) probe to the specified *ip-address*. If a ping fails, the event is considered to be set. If a ping is successful, the event is considered to be cleared.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Multiple unique (different *ip-address*) **host-unreachable** event nodes can be configured within the **priority-event** node to a maximum of 32 events.

The **host-unreachable** command can reference any valid local or remote IP address. The ability to ARP a local IP address or find a remote IP address within a route prefix in the route table is considered part of the monitoring procedure. The **host-unreachable** priority event operational state tracks ARP or route table entries dynamically appearing and disappearing from the system. The operational state of the **host-unreachable** event are listed in Table 62.

Table 62 **Host Unreachable Operational States**

Host Unreachable Operational State	Description
Set – no ARP	No ARP address found for *ip-addr* for **drop-count** consecutive attempts; only applies when IP address is considered local
Set – no route	No route exists for *ip-addr* for **drop-count** consecutive attempts; only when IP address is considered remote
Set – host unreachable	ICMP host unreachable message received for **drop-count** consecutive attempts
Set – no reply	ICMP echo request timed out for **drop-count** consecutive attempts
Set – reply received	Last ICMP echo request attempt received an echo reply but historically not able to clear the event
Cleared – no ARP	No ARP address found for *ip-addr* - not enough failed attempts to set the event
Cleared – no route	No route exists for *ip-addr* - not enough failed attempts to set the event
Cleared – host unreachable	ICMP host unreachable message received - not enough failed attempts to set the event
Cleared – no reply	ICMP echo request timed out - not enough failed attempts to set the event
Cleared – reply received	Event is cleared - last ICMP echo request received an echo reply

Unlike other priority event types, the **host-unreachable** priority event monitors a repetitive task. A historical evaluation is performed on the success rate of receiving ICMP echo reply messages. The operational state takes its cleared and set orientation from the historical success rate. The informational portion of the operational state is derived from the last attempt's result. It is possible for the previous attempt to fail while the operational state is still cleared due to an insufficient number of failures to cause it to become set. It is also possible for the state to be set while the previous attempt was successful.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instances in-use priority value. As the event transitions from clear to set, a hold-set timer is loaded with the value configured by the events **hold-set** command. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the **hold-set** value, extending the time before another clear can take effect.

The hold-set timer be expired and the historical success rate must be met prior to the event operational state becoming cleared.

The **no** form of the command deletes the specific IP host monitoring event. The event may be deleted at any time. When the event is deleted, the in-use priority of all associated virtual router instances must be reevaluated. The event's **hold-set** timer has no effect on the removal procedure.

Default no host-unreachable — No host unreachable priority events are created.

Parameters *ip-address* — The IP address of the host for which the specific event will monitor connectivity. The *ip-addr* can only be monitored by a single event in this policy. The IP address can be monitored by multiple VRRP priority control policies. The IP address can be used in one or multiple **ping** requests. Each VRRP priority control **host-unreachable** and **ping** destined to the same *ip-addr* is uniquely identified on a per message basis. Each session originates a unique identifier value for the ICMP echo request messages it generates. This allows received ICMP echo reply messages to be directed to the appropriate sending application.

Values The following values apply to the 7450 ESS:

ipv4-address: a.b.c.d

Values The following values apply to the 7750 SR and 7950 XRS:

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x[-interface]	
	x:	[0..FFFF]H
	interface:	32 chars maximum, mandatory for link local addresses

The link-local IPv6 address must have an interface name specified. The global IPv6 address must not have an interface name specified.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.80 host-unsolicited-na-flood-evpn

host-unsolicited-na-flood-evpn

Syntax [**no**] **host-unsolicited-na-flood-evpn**

Context **[Tree]** (config>service>vpls>proxy-nd host-unsolicited-na-flood-evpn)

Full Context configure service vpls proxy-nd host-unsolicited-na-flood-evpn

Description This command controls whether the system floods host unsolicited Neighbor Advertisements to the EVPN. The NA messages impacted by this command are NA messages with the following flags: S=0 and R=0.

The **no** form of the command will only flood to local SAPs/binds but not to the EVPN destinations. This is only recommended in networks where CEs are routers that are directly connected to the PEs. Networks using aggregation switches between the host/routers and the PEs should flood unsolicited NA messages in the EVPN to ensure that the remote caches are updated and the BGP does not miss the advertisement of these entries.

Default host-unsolicited-na-flood-evpn

Platforms All

12.81 hour

hour

Syntax **hour** *hour-number* [*..hour-number*] | **all**}
no hour

Context **[Tree]** (config>system>cron>sched hour)

Full Context configure system cron schedule hour

Description This command specifies which hour to schedule a command. Multiple hours of the day can be specified. When multiple hours are configured, each of them will cause the schedule to trigger. **Day-of-month** or **weekday** must also be specified. All days of the month or weekdays can be specified. If an hour is configured without configuring month, weekday, day-of-month, and minute, the event will not execute.

The **no** form of this command removes the specified hour from the configuration.

Default no hour

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hour-number* — Specifies the hour to schedule a command.

Values 0 to 23 (maximum 24 hour-numbers)

all — Specifies all hours.

Platforms All

12.82 hqos-algorithm

hqos-algorithm

Syntax **hqos-algorithm** {**default** | **above-offered-allowance-control**}
no hqos-algorithm

Context **[Tree]** (config>qos>port-scheduler-policy hqos-algorithm)

Full Context configure qos port-scheduler-policy hqos-algorithm

Description This command configures the port scheduler H-QoS algorithm used to calculate the operational rates for the children connected to the port scheduler. The algorithm can be changed on the fly.

Default default

Parameters **default** — Specifies that the default H-QoS algorithm is used by the port scheduler.

above-offered-allowance-control — Enables the control of the amount of bandwidth in excess of the offered rate to be given to a queue or scheduler. This algorithm is supported when only queues and schedulers are parented to the port scheduler on Ethernet Vports or Ethernet physical ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

12.83 hqos-mode

hqos-mode

Syntax **hqos-mode** {**port-scheduler** | **hw-agg-shaping**}

Context **[Tree]** (config>qos>fp-resource-policy>ports hqos-mode)

Full Context configure qos fp-resource-policy ports hqos-mode

Description This command configures the default HQoS mode for ports on the specified FP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default hqos-mode port-scheduler

Parameters **port-scheduler** — Specifies that the default HQoS mode is port scheduler.

hw-agg-shaping — Specifies that the default HQoS mode is hardware aggregate shaping.

Platforms 7750 SR-1, 7750 SR-s

12.84 hs-agg-rate-limit

hs-agg-rate-limit

Syntax **hs-agg-rate-limit** *kilobits-per-second*
no hs-agg-rate-limit

Context **[Tree]** (config>subscr-mgmt>sla-profile>egress hs-agg-rate-limit)

Full Context configure subscriber-mgmt sla-profile egress hs-agg-rate-limit

Description This command configures high scale (HS) aggregate rate limit of the SLA profile instance (SPI) associated with the subscriber in expanded SLA mode. The aggregate rate of the subscriber (the primary shaper) is configured in the **config>subscr-mgmt>sub-profile>egress>hs-agg-rate-limit** context.

The **no** form of this command removes the value from the configuration.

Parameters *kilobits-per-second* — Specifies the HS egress aggregate rate limit.

Values 1 to 100000000

Platforms 7750 SR-7/12/12e

hs-agg-rate-limit

Syntax **hs-agg-rate-limit** *kilobits-per-second* [**min-resv-bw** *min-rate*]
hs-agg-rate-limit max [**min-resv-bw** *min-rate*]
no hs-agg-rate-limit

Context **[Tree]** (config>subscr-mgmt>sub-profile>egress hs-agg-rate-limit)

Full Context configure subscriber-mgmt sub-profile egress hs-agg-rate-limit

Description This command configures the HS aggregate rate limit for the subscriber in single SLA mode. In single SLA mode, the **hs-aggregate-rate-limit** command under the **config>subscr-mgmt>sla-profile** context should not be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When both, **sub-profile>egress>hs-agg-rate-limit** and **sla-profile>egress>hs-agg-rate-limit** are configured, the system takes the minimum of the two to program the subscriber's aggregate rate.

The **no** form of this command removes the value from the configuration.

Parameters *kilobits-per-second* — Specifies the HS egress aggregate rate limit.

Values 1 to 100000000

min-rate — Specifies the minimum rate of the minimum reserved bandwidth for unicast data traffic. Since minimum rate can oversubscribe subscriber bandwidth to guarantee a minimum bandwidth for unicast traffic, care must be taken in QoS provisioning to prioritize packets accordingly (downstream network elements such as the access node or aggregation nodes) when congestion occurs.

Values 0 to 100000000

max — Specifies that the egress aggregate rate limit for the subscriber is unlimited. Scheduling for the subscriber queues will only be governed by the individual queue parameters and any congestion on the port relative to each queues scheduling priority.

Platforms 7750 SR-7/12/12e

12.85 hs-alt-port-class-pool

hs-alt-port-class-pool

Syntax [**no**] **hs-alt-port-class-pool**

Context **[Tree]** (config>qos>network-queue>queue hs-alt-port-class-pool)

Full Context configure qos network-queue queue hs-alt-port-class-pool

Description This command specifies that the HSQ queue group queues use buffers from the HS alternate port class buffer pool.

The **no** form of the command reverts to the HSQ queue group queues using buffers from HS standard port class pools.

Platforms 7750 SR-7/12/12e

hs-alt-port-class-pool

Syntax [**no**] **hs-alt-port-class-pool**

Context **[Tree]** (config>qos>sap-egress>queue hs-alt-port-class-pool)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos sap-egress queue hs-alt-port-class-pool

Description This command specifies that the HSQ queue group queues use buffers from the HS alternate port class buffer pool.

The **no** form of the command reverts to the HSQ queue group queues using buffers from HS standard port class pools.

Platforms 7750 SR-7/12/12e

hs-alt-port-class-pool

Syntax [**no**] **hs-alt-port-class-pool**

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue hs-alt-port-class-pool)

Full Context configure qos queue-group-templates egress queue-group queue hs-alt-port-class-pool

Description This command specifies that the HSQ queue group queues use the class buffers from the HS alternate port class buffer pools.

The **no** form of the command reverts to the HSQ queue group queues using buffers from HS standard port class pools.

Platforms 7750 SR-7/12/12e

12.86 hs-attachment-policy

hs-attachment-policy

Syntax **hs-attachment-policy** *policy-name* [**create**]
no hs-attachment-policy *policy-name*

Context **[Tree]** (config>qos hs-attachment-policy)

Full Context configure qos hs-attachment-policy

Description This command specifies how the queues within an HSQ queue group associated with the SAP egress policy instance, egress queue group instance, or egress network queue policy instance attaches to the HSQ scheduling classes managed by the port scheduler. On the HSQ IOM, eight queues are allocated per egress SAP or subscriber SLA profile instance (SPI), or per egress (access or network) queue group instance, or per egress network port, numbered 1 through 8. The port scheduler maintains six scheduling classes numbered from 1 through 6 (6 being the highest relative priority and 1 being the lowest). The set of eight queues may also be placed into one of two local Weighted Round Robin (WRR) groups which

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

collapse the member queues into a single scheduling class while providing a weighted fair distribution of scheduling opportunities per member. The attachment policy contains the **attachment** commands that map the queue IDs and WRR groups to the scheduling classes. The attachment policy also defines the mapping of the scheduling classes to the queue's aggregate shapers low and high burst limit thresholds.

The **no** form of the command deletes the HS attachment policy from the system, which is only possible if the policy is not being referenced.

Parameters *policy-name* — Specifies an existing attachment policy, up to 32 characters. Each HS attachment policy must be uniquely named within the system.

create — This keyword is required when first creating the configuration context. After the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7750 SR-7/12/12e

hs-attachment-policy

Syntax **hs-attachment-policy** *policy-name*
no hs-attachment-policy

Context **[Tree]** (config>qos>network-queue hs-attachment-policy)

Full Context configure qos network-queue hs-attachment-policy

Description This command associates an existing HS attachment policy with the network queue QoS policy. The HS attachment policy controls how the network queues are attached to scheduler classes or WRR groups, and how WRR groups are attached to the scheduler classes. It also defines the mapping of the scheduling classes to the queues' aggregate shaper's low and high burst limit thresholds.

Only one HS attachment policy can be associated with a network queue policy.

The **no** form of the command removes the policy name from the configuration and reapplies the default HS attachment policy.

Parameters *policy-name* — Specifies an existing attachment policy up, to 32 characters. Each HSQ attachment policy must be uniquely named within the system.

Platforms 7750 SR-7/12/12e

hs-attachment-policy

Syntax **hs-attachment-policy** *policy-name*
no hs-attachment-policy

Context **[Tree]** (config>qos>sap-egress hs-attachment-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos sap-egress hs-attachment-policy

Description This command associates an existing HS attachment policy with the SAP egress QoS policy. The HS attachment policy controls how the SAP egress queues are attached to scheduler classes or WRR groups, and how WRR groups are attached to the scheduler classes. It also defines the mapping of the scheduling classes to the queues' aggregate shaper's low and high burst limit thresholds.

Only one HS attachment policy can be associated with a SAP egress policy.

The **no** form of the command removes the policy name from the configuration and reapplies the default HS attachment policy.

Parameters *policy-name* — Specifies an existing attachment policy up, to 32 characters. Each HSQ attachment policy must be uniquely named within the system.

Platforms 7750 SR-7/12/12e

hs-attachment-policy

Syntax **hs-attachment-policy** *policy-name*
no hs-attachment-policy

Context **[Tree]** (config>qos>qgrps>egr>qgrp hs-attachment-policy)

Full Context configure qos queue-group-templates egress queue-group hs-attachment-policy

Description This command associates an existing HS attachment policy with the egress queue group template. The HS attachment policy controls how the egress queue group instance queues are attached to scheduler classes or WRR groups, and how WRR groups are attached to the scheduler classes. It also defines the mapping of the scheduling classes to the queues' aggregate shaper's low and high burst limit thresholds.

Only one HS attachment policy can be associated with an egress queue group template.

The **no** form of the command removes the policy name from the configuration and reapplies the default HS attachment policy.

Parameters *policy-name* — Specifies an existing attachment policy, up to 32 characters. Each HS attachment policy must be uniquely named within the system.

Platforms 7750 SR-7/12/12e

hs-attachment-policy

Syntax **hs-attachment-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy hs-attachment-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos copy hs-attachment-policy

Description This command copies existing QoS policy entries for a QoS policy ID to another QoS policy ID.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters *src-name dst-name* — Indicates that the source policy ID and the destination policy ID are HS policy IDs. Specify the source policy ID that the copy command attempts to copy from and specify the destination policy ID to which the command copies a duplicate of the policy.

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy is overwritten with the contents of the source policy. If **overwrite** is not specified, an error occurs if the destination policy ID exists.

```
SR>config>qos# copy hs-pool-policy policy1 policy2
MINOR: CLI Destination "policy2" exists use {overwrite}.
SR>config>qos# copy hs-pool-policy policy1 policy2
 overwrite
```

Platforms 7750 SR-7/12/12e

12.87 hs-class-weight

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue hs-class-weight)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>hs-wrr-grp hs-class-weight)

Full Context configure subscriber-mgmt sla-profile egress qos hs-wrr-group hs-class-weight
configure subscriber-mgmt sla-profile egress qos queue hs-class-weight

Description This command configures the class-weight override for expanded egress HS queues or the WRR group.

The **no** form of this command removes the weight value from the configuration.

Parameters *weight* — Specifies the weight of the scheduling class.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>service>epipe>sap>egress>queue-override>queue hs-class-weight)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue hs-class-weight)

Full Context configure service epipe sap egress queue-override queue hs-class-weight
configure service ipipe sap egress queue-override queue hs-class-weight

Description This command overrides the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the weight of the queue.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue hs-class-weight)

Full Context configure service vpls sap egress queue-override queue hs-class-weight

Description This command overrides the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the weight of the queue.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue hs-class-weight)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface sap egress queue-override queue hs-class-weight

Description This command overrides the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the weight of the queue.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue hs-class-weight)

Full Context configure service vprn interface sap egress queue-override queue hs-class-weight

Description This command overrides the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class.

The **no** form of this command removes the class weight override value from the configuration.

Parameters *weight* — Specifies the weight of the queue.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>qos>network-queue>hs-wrr-group hs-class-weight)

Full Context configure qos network-queue hs-wrr-group hs-class-weight

Description This command specifies the class weight of this WRR group at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class. This allows the capacity available at the primary shaper scheduling class to be shared in a WRR manner between the HSQ queue group queues and WRR groups attached to that scheduling class. The **hs-class-weight** *weight* can be used to give unequal shares of the available capacity to different types of service offerings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command reverts to weight to the default value.

Default hs-class-weight 1

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>qos>network-queue>queue hs-class-weight)

Full Context configure qos network-queue queue hs-class-weight

Description This command specifies the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class. This allows the capacity available at the primary shaper scheduling class to be shared in a WRR manner between the HSQ queue group queues and WRR groups attached to that scheduling class. The **hs-class-weight** *weight* parameter can be used to give unequal shares of the available capacity to different types of service offerings. This command is ignored for egress HSQ queue group queues that are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **hs-class-weight** is performed under the **hs-wrr-group** within the network queue policy.

The **no** form of the command reverts to the default value.

Default hs-class-weight 1

Parameters *weight* — Specifies class weight of the queue.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>qos>sap-egress>hs-wrr-group hs-class-weight)

Full Context configure qos sap-egress hs-wrr-group hs-class-weight

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the class weight of this WRR group at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class. This allows the capacity available at the primary shaper scheduling class to be shared in a WRR manner between the HSQ queue group queues and WRR groups attached to that scheduling class. The **hs-class-weight** parameter can be used to give unequal shares of the available capacity to different types of service offerings.

The **no** form of the command reverts the weight to the default value.

Default hs-class-weight 1

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context **[Tree]** (config>qos>sap-egress>queue hs-class-weight)

Full Context configure qos sap-egress queue hs-class-weight

Description This command specifies the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class. This allows the capacity available at the primary shaper scheduling class to be shared in a WRR manner between the HSQ queue group queues and WRR groups attached to that scheduling class. The **hs-class-weight** *weight* parameter can be used to give unequal shares of the available capacity to different types of service offerings. This command is ignored for egress HSQ queue group queues, which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **hs-class-weight** is performed under the **hs-wrr-group** within the network queue policy.

The **no** form of the command reverts to the default value.

Default hs-class-weight 1

Parameters *weight* — Specifies class weight of the queue.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no hs-class-weight

Context [Tree] (config>qos>qgrps>egr>qgrp>hs-wrr-group hs-class-weight)

Full Context configure qos queue-group-templates egress queue-group hs-wrr-group hs-class-weight

Description This command specifies the class weight of this WRR group at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class. This allows the capacity available at the primary shaper scheduling class to be shared in a WRR manner between the HSQ queue group queues and WRR groups attached to that scheduling class. The **hs-class-weight** parameter can be used to give unequal shares of the available capacity to different types of service offerings.

The **no** form of the command reverts to the default value.

Default hs-class-weight 1

Parameters *weight* — Specifies the class weight of the HS WRR group.

Values 1, 2, 4, 8

Platforms 7750 SR-7/12/12e

hs-class-weight

Syntax **hs-class-weight** *weight*
no hs-class-weight

Context [Tree] (config>qos>qgrps>egr>qgrp>queue hs-class-weight)

Full Context configure qos queue-group-templates egress queue-group queue hs-class-weight

Description This command specifies the class weight of this queue at its parent primary shaper, relative to the other queues and WRR groups in different HSQ queue groups in the same scheduling class. This allows the capacity available at the primary shaper scheduling class to be shared in a WRR manner between the HSQ queue group queues and WRR groups attached to that scheduling class. The **hs-class-weight** parameter can be used to give unequal shares of the available capacity to different types of service offerings.

This command is ignored for egress HSQ queue group queues, which are attached to an HS WRR group within an associated HS attachment policy. In this case the configuration of the **hs-class-weight** is performed under the **hs-wrr-group** within the egress queue group template.

The **no** form of the command reverts to the default value.

Default hs-class-weight 1

Parameters *weight* — Specifies the class weight of the queue.

Values 1, 2, 4, 8

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR-7/12/12e

12.88 hs-fixed-high-thresh-delta

hs-fixed-high-thresh-delta

Syntax **hs-fixed-high-thresh-delta** *size-in-bytes*
no hs-fixed-high-thresh-delta

Context **[Tree]** (config>card>fp>egress hs-fixed-high-thresh-delta)

Full Context configure card fp egress hs-fixed-high-thresh-delta

Description This command specifies the egress aggregate shaper high burst limit threshold delta for this HSQ IOM FP. An aggregate rate can be applied to each egress HSQ queue group, HS secondary shaper and (for subscribers configured with HS SLA expanded mode) primary shaper which manages the maximum burst limit over a specified shaping rate. Each aggregate shaper supports two thresholds which are used in conjunction with the low burst class setting. The system utilizes the lowest value attainable for each low threshold aggregate burst limit without causing shaper under run conditions. The high burst limit threshold is determined by adding the configured value of this command to the aggregate's low burst limit threshold value. This configured value should be set to at least two times the maximum frame size to prevent lower threshold class forwarding from also affecting the higher threshold classes when forwarding larger packet sizes. An insufficient high threshold delta defeats the intended purpose of mapping classes to the higher threshold.

The configured value for this command can be changed at any time. Modifying the setting causes all aggregate shapers on this FP to reconfigure the low and high burst limit thresholds to reflect the new value.

The **no** form of this command reverts this parameter to the default.

Default hs-fixed-high-thresh-delta 4000

Parameters *size-in-bytes* — Specifies high threshold data in bytes.

Values 0 to 65536

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.89 hs-low-burst-max-class

hs-low-burst-max-class

Syntax **hs-low-burst-max-class** *class*
no hs-low-burst-max-class

Context **[Tree]** (config>subscr-mgmt>sub-prof>egress hs-low-burst-max-class)

Full Context configure subscriber-mgmt sub-profile egress hs-low-burst-max-class

Description This command specifies which scheduling classes map to the low burst limit threshold of an egress HS primary shaper. The HS primary shaper is used to manage aggregate bandwidth of the subscriber with multiple SLA profile instances (expanded SLA mode).

Each HS primary shaper supports two burst thresholds, a low burst limit threshold and a high burst limit threshold. The two thresholds allow separation of burstiness between low and high scheduling classes.

When the low burst threshold of the HS primary shaper is reached, the lower scheduling classes, up to the scheduling class configured by this command, stops being served. Traffic on higher scheduling classes still goes through until the high burst threshold is reached. When the high burst threshold is exceeded, all scheduling classes associated with the HS primary shaper and stops being serve, which effectively shuts off the traffic flow.

Typically, the queues associated with higher scheduling classes are individually rate-limited so that their aggregate allowed throughput is less than the configured rate of the HS primary shaper. Determining the **hs-low-burst-max-class** *class* value involves anticipating the proper dividing line between the low and high scheduling classes by evaluating the forwarding behavior and SLA enforcement of each class.

By default, all scheduling classes are mapped to the low burst limit threshold. When mapping scheduling classes to the high burst limit threshold, an adequate value for the **config>card>fp>egress>hs-fixed-high-thresh-delta** should be specified (by default, it is set to 4000 bytes). This is because the queues associated with the lower scheduling classes may burst over the lower threshold during normal operation due to the scheduler forwarding whole packets. The **hs-fixed-high-thresh-delta** value should be set to at least two times the maximum frame size to prevent lower threshold class forwarding from also affecting the higher threshold classes when forwarding larger packet sizes. An insufficient high threshold delta defeats the intended purpose of mapping classes to the higher threshold.

The system uses the lowest value attainable for each low threshold aggregate burst limit without causing shaper underrun conditions. The high burst limit threshold is determined by adding the **hs-fixed-high-thresh-delta** value to the aggregate low burst limit threshold value.

The **hs-low-burst-max-class** value for HS primary shaper can be changed at any time in the subscriber profile (sub-profile).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command restores the low burst limit threshold of the scheduling classes to the default value. This causes all scheduling classes associated with the HS primary shaper to be mapped to the low burst limit threshold.

Default hs-low-burst-max-class 6

Parameters *class* — Specifies the highest scheduling class that is associated with the low burst limit threshold of the HS primary shaper. Scheduling classes that are higher than the scheduling class ID are associated with the high burst limit threshold.

Values 1 to 6

Platforms 7750 SR-7/12/12e

12.90 hs-mbs

hs-mbs

Syntax **hs-mbs** *percent-of-queue-rate*
no hs-mbs

Context **[Tree]** (config>qos>network-queue>queue hs-mbs)

Full Context configure qos network-queue queue hs-mbs

Description This command configures the queue size of an HSQ queue group network queue. Its value is calculated based on the specified percentage of one second of the queue PIR converted to bytes (the regular **mbs** parameter is ignored in the network queue policy).

The **no** form of the command reverts to the default value.

Default hs-mbs 100

Parameters *percent-of-queue-rate* — Specifies the buffer space for the queue as a percentage of its PIR (in bytes).

Values 0.00 to 100.0

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.91 hs-pool-policy

hs-pool-policy

Syntax **hs-pool-policy** *name*
no hs-pool-policy

Context **[Tree]** (config>card>fp>egress hs-pool-policy)

Full Context configure card fp egress hs-pool-policy

Description This command specifies the HS pool policy for this FP.

An HS pool policy contains the required parameters to create and size root and mid-tier buffer pools on an HSQ IOM, and apply a slope policy to each.

A single HS pool policy is supported per port FP. This command is only applicable to the HSQ IOM (iom4-e-hs) and will fail if configured on all other card types.

The **no** form of this command removes the policy and reapplies the default policy.

Default hs-pool-policy default

Parameters *name* — Specifies the HS pool policy name, up to 32 characters.

Platforms 7750 SR-7/12/12e

hs-pool-policy

Syntax **hs-pool-policy** *policy-name* [**create**]
no hs-pool-policy *policy-name*

Context **[Tree]** (config>qos hs-pool-policy)

Full Context configure qos hs-pool-policy

Description Commands in this context create HS pool policy parameters. The policy can be assigned to an egress forwarding plane of an HSQ IOM. The policy contains the required parameters to create and size root and mid-tier buffer pools on an HSQ IOM, and apply a slope policy to each. The HS pool policy can be applied using the **hs-pool-policy** command within the **config>card>fp** *fp-number* **egress** context.

The system supports 63 HS pool policies including the default HS pool policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- HSQ IOM System Reserved Buffers — The HSQ IOM maintains two types of queues; provisioned queues and system reserved queues. The HSQ IOM ensures that provisioned queues cannot consume buffers that must be available for internal system queues required for correct operating behavior. To prevent buffer starvation between the two types of queues, the system divides the available buffers into two portions. The first portion is given to system root pools and is allocated to HSQ queues reserved for internal functions. The second portion is given to the provisioned or user-defined root pools and is available for egress service queues, network queues, queue-group queues or subscriber queues. By default, 5% of the total buffers available are given to the system root pools leaving 95% for the provisioned root pools.

  The default separation between the system and the provisioned root pools can be overridden using the **system-reserve** command.
- Root Pools — Root pools are the buffer pools at the bottom of the buffer allocation hierarchy. Two sets of root pools exist: the system root pools and the provisioned root pools. The system root pools cannot be managed by the HS pool policy; only the total number of buffers given to the system root pools can be adjusted by using the **system-reserve** command.

  The HS pool policy manages sixteen provisioned root pools defined under the **root-tier** context and specified as root-pool 1 through 16. Each root pool accepts a weight command that defines the relative quantity of buffers that are allocated to each root pool. Root pools are deactivated by defining a weight equal to 0. Root pools with a non-zero weight are sized based on the pool's weight divided by the sum of all root pool weights, multiplied by the available buffer space. In this manner, all buffers not reserved for system use are distributed between the provisioned root pools without oversubscription. The lack of oversubscription prevents buffer starvation between the root pools allowing root pools, to act as protected buffer space between different types of traffic (best-effort, expedited, or real-time). Root pools allocate buffers to the FP-level mid-tier pools.
- Mid-Tier Pools — Mid-tier pools are the buffer pools that act as aggregators for port-class pools. Multiple mid-tier pools can be mapped to a single root pool and each mid-tier pool is assigned a percentage of that root pool's buffer space. The sum of the percentages may exceed 100%, allowing for oversubscription of the root pool's buffer space. Due to statistical multiplexing principles, oversubscribing the root pool's buffer allocation may allow more efficient use of the available buffers as not all mid-tier pools are expected to use their fair share simultaneously. Examples of a multiple mid-tier pool application are multiple assured forwarding (AF) or best-effort classes being grouped together in the same root pool. The HS pool policy manages the sixteen mid-tier pools on an HSQ IOM, defined under the **mid-tier** context and specified as mid-pool 1 through 16.
- Port Class Pools — The HSQ IOM maintains two sets of scheduler class pools per port: a standard (or default) set and an alternate set. Each set contains six pools, one for each scheduler class serviced by the HSQ IOM port scheduler. Each queue or WRR group is mapped to a scheduling class based on the HS attachment policy defined within the policy or template used to create the queue. Within the SAP egress policy, network queue policy and egress queue group template, an **alt-port-class-pool** command specifies whether the queues created through the policy use the standard or alternate set of port class pools on the physical port. Further, the scheduling class servicing the queue defines which port-class pool (1 through 6) within the set allocate buffers to the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Port-class pools are defined within the **hs-port-pool-policy**, which is applied to each physical port. Further information on HSQ IOM port-class pools is contained in the HS port pool policy section.

- HSQ Stable Pool Sizing Equivalency — Stable pool sizing is a feature supported on ingress and on non-HSQ egress forwarding planes. By default, the system tries to make all buffers available to active ports (provisioned and equipped). This leads to a condition where an IOM may have only a single MDA populated and the users on that MDA receive all available buffers. At a later date, the second MDA can be populated, causing the buffer space to be fragmented between the users on each MDA. The users on the earlier populated MDA may perceive a degradation in service based on the change in available buffers. The stable pool sizing feature mitigates this potential issue by segregating the buffer space per MDA.

  The HSQ IOM can be made to operate in this stable buffer allocation mechanism by utilizing per-MDA buffer pools. This is accomplished by performing the following steps:

  1. Create two sets of root-pools and two sets of mid-pools in the **hs-pool-policy** applied to the IOM's FP egress CLI context. The first set of mid-pools should be parented to the first set of root-pools. The second set of mid-pools should be parented to the second set of root-pools.
  2. Create two distinct HS port pool policies. One is applied to the ports on the first MDA and has the port-class pools parented to the first set of mid-tier pools from the FP level policy. The second HS port pool policy is applied to the ports on the second MDA (when it is provisioned) and has the port-class pools parented to the second set of mid-tier pools from the FP level policy. This provides deterministic pool sizing independent of MDA equipping events.
  3. Configure further control at the port-class level by utilizing **explicit-percent** based port-class pool sizing, which eliminates the effect of changing port states, including bandwidth changes.

- HSQ Queue Buffer Allocation — As each packet arrives at an HSQ queue, the queue must obtain buffers to admit the packet on the queue. The queue first checks the depth of the queue relative to the packet's congestion priority (based on the in, out, or exceed profile) to determine if the packet should be discarded based on early congestion detection or based on the MBS threshold. If the packet is allowed into the queue, the HSQ IOM continues to determine buffer availability using checks to the queue's port-class pool, the port-class pool's mid-tier pool, and the mid-tier pool's root pool. The same RED slope type used at the queue (high, low, or exceed) is used within each buffer pool. If a buffer is available, the buffer can be allocated, and given to the queue.
- Default HSQ Pool Policy — An HSQ pool policy with the name **default** always exists on the system and does not need to be created. The default pool policy cannot be changed and is used by all HSQ IOMs within the system unless an explicitly created **hs-pool-policy** is associated with a forwarding plane.

  The default policy contains the following parameters:

  system-reserve: 5%

  root-pool 1

  allocation-weight:75

  slope-policy:_tmnx_hs_default

  root-pool 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

allocation-weight:25
slope-policy:_tmnx_hs_default
root-pool 3 to **16**
allocation-weight:0
slope-policy:_tmnx_hs_default
mid-pool 1
parent-root-pool:1
allocation-percent:40%
slope-policy:_tmnx_hs_default
mid-pool 2
parent-root-pool:1
allocation-percent:35%
slope-policy:_tmnx_hs_default
mid-pool 3
parent-root-pool:1
allocation-percent:30%
slope-policy:_tmnx_hs_default
mid-pool 4
parent-root-pool:1
allocation-percent:25%
slope-policy:_tmnx_hs_default
mid-pool 5
parent-root-pool:2
allocation-percent:80%
slope-policy:_tmnx_hs_default
mid-pool 6
parent-root-pool:2
allocation-percent:20%
slope-policy:_tmnx_hs_default
mid-pool 7 to **16**
parent-root-pool:None
allocation-percent:1%
slope-policy:_tmnx_hs_default

The **no** form of the command removes the HS pool policy from the system. If the HS pool policy is currently associated with a forwarding plane, the command fails.

Parameters *policy-name* — Specifies pool policy name, up to 32 characters. Each HS pool policy must be uniquely named within the system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — This keyword is required when first creating the configuration context. After the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7750 SR-7/12/12e

hs-pool-policy

Syntax **hs-pool-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy hs-pool-policy)

Full Context configure qos copy hs-pool-policy

Description This command copies existing QoS policy entries for a QoS policy ID to another QoS policy ID.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters *src-name dst-name* — Indicates that the source policy ID and the destination policy ID are HS policy IDs. Specify the source policy ID that the copy command attempts to copy from and specify the destination policy ID to which the command copies a duplicate of the policy.

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy is overwritten with the contents of the source policy. If **overwrite** is not specified, an error occurs if the destination policy ID exists.

```
SR>config>qos# copy hs-pool-policy policy1 policy2
MINOR: CLI Destination "policy2" exists use {overwrite}.
SR>config>qos# copy hs-pool-policy policy1 policy2
 overwrite
```

Platforms 7750 SR-7/12/12e

12.92 hs-port-pool-policy

hs-port-pool-policy

Syntax **hs-port-pool-policy** *policy-name*
no hs-port-pool-policy

Context **[Tree]** (config>port>ethernet>egress hs-port-pool-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet egress hs-port-pool-policy

Description This command specifies an HS port pool policy to associate with the port egress.

An HS port buffer pool policy defines and sizes the port-class buffer pools on an HSQ IOM egress port.

A single HS port pool policy is supported per port egress. This command is only applicable to the HSQ IOM (iom4-e-hs) and will fail if configured on all other card types.

The **no** form of this command removes the policy and reapplies the default policy.

Default hs-port-pool-policy default

Parameters *policy-name* — Specifies the HS port pool policy up to 32 characters.

Platforms 7750 SR-7/12/12e

hs-port-pool-policy

Syntax **hs-port-pool-policy** *policy-name* [**create**]
no hs-port-pool-policy *policy-name*

Context **[Tree]** (config>qos hs-port-pool-policy)

Full Context configure qos hs-port-pool-policy

Description This command creates an HS port buffer pool policy. The policy can be assigned to an egress port on an HSQ IOM. The policy contains the required commands to define and size port-class buffer pools on an HSQ IOM. The policy can be applied using the **hs-port-pool-policy** command within the **config>port>ethernet>egress** context.

SR OS supports 2047 HS port pool policies including the default HS port pool policy.

HSQ IOM port buffer pools provide buffer control for queues based on the queue's scheduling class. Two sets of scheduling class pools exist per port: a standard (or default) set and an alternative set. The SAP egress policy, network queue policy, and egress queue group template have a parameter (**alt-port-class-pool**) that specifies that the queues created by the policy or template uses the alternate port-class pools, as opposed to the default standard port-class pools. Each set has six pools, one for each scheduling class. Based on the **alt-port-class-pool** setting and the queue's scheduling class (based on the HS attachment policy configuration), each queue is mapped to a specific port-class pool.

The HS port pool policy defines how each of these pools are parented (mapped) to an FP level mid-pool and how each pool is sized.

The system allows two separate mechanisms to size each port-class pool:

- dynamic sizing based on port bandwidth, relative to bandwidth of other ports
- explicit sizing based on a percentage of the port-class pool's parent mid-pool

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Dynamic Port-Class Pool Sizing — Dynamic port-class pool sizing is a mechanism that provides a fair share of a mid-pool's size to each of the port-class pools based on the potential bandwidth represented by each port. To understand port-class pool sizing, consider the following:

- Each port's bandwidth is the minimum of the port's line rate, the port's configured **egress-rate**, and the port's **hs-scheduler-policy** *max-rate*.
- The port's bandwidth can be further modified by the port's **egr-percentage-of-rate** command, which increases or decreases the port's bandwidth derived by the specified percent. This parameter allows the port to have a higher or lower bandwidth-derived weight based on how the port is actually being used instead of bandwidth alone.
- Because the port-class pools are user mapped to the mid-pools, not every port has a port-class pool associated with a mid-pool, requiring that the system perform the relative bandwidth calculations separately per mid-pool.
- Each port's portion of a specified mid-pool's size is calculated based on:

  Port_Portion = (Port_Adj_Bw / Sigma_Mid_Pool_Ports_Adj_Bw) * Mid_Pool_Size

  where Sigma_Mid_Pool_Ports_Adj_Bw is the sum of the adjusted bandwidths for all ports with port-class pools mapped to the mid-pool that are not sized using explicit-percent.
- A port without any port-class pools associated with a given mid-pool has a port portion of zero for that mid-pool.
- Multiple port-class pools on the same port can be mapped to the same mid-pool, requiring a mechanism to distribute the portion of the mid-pool given to the port between multiple port-class pools. Each mid-pool's **port-bw-weight** parameter is used to determine how much of the port's mid-pool portion is given to each port-class pool associated with mid-pool. Port-class pools sized using an **explicit-percent** value instead of port bandwidth are assumed to have a **port-bw-weight** equal to 0, causing those port-class pools to not participate in the port portion distribution. It is expected (but not required) that one of port bandwidth-based sizing or explicit percent-based sizing is used and any concurrent use of both mechanisms is transitory in nature.
- The port bandwidth weighting mechanism allocates 100% of the mid-pool size to the associated port-class pools. To allow the port-class pools to oversubscribe the parent mid-pool, a mid-pool **port-bw-oversub-factor** parameter is supported that allows the port-class pools sized by dynamic port bandwidth to increase in size by the specified oversubscription factor. This oversubscription factor can provide a more efficient use of the mid-pool's available buffers because it is not expected that all port-class pools are utilizing their allotted size simultaneously.

Explicit Port-Class Pool Sizing — The port-class pool's allocation **explicit-percent** *percent-of-parent-pool* command is used to override the dynamic pool sizing mechanism for a given mid-pool. The specified percentage value is applied to the port-class's parent mid-pool's size to derive the port-class pool size.

Explicit and Dynamic Sizing from the Same Mid-Pool Parent — If explicit and dynamic pool sizing are used simultaneously for port-class pools parented to the same mid-pool, unexpected contention or underutilization of the mid-pool's available buffers may result. While this is not a proscribed condition, it is expected most instances of dual-sizing mechanisms are transitory, based on moving between the two mechanisms.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Port-Class Pool Slope Policy Association — The HS port pool policy also provides the ability to specify a slope policy on each port-class pool. The slope policy is used to define the high, low, and exceed slope parameters used to manage contention within the port-class pool.

Default HS Port Pool Policy — An HS port pool policy with the name **default** always exists on the system and does not need to be created. The default port pool policy cannot be changed and is used by all HSQ IOMs within the system unless an explicitly created **hs-port-pool-policy** is associated with an HSQ egress port.

The default policy contains the following parameters:

Standard Port-Class Pools

Port-Class-Pool 1

Parent:Mid-Pool 1

Port-Class-Pool 2

Parent:Mid-Pool 2

Port-Class-Pool 3

Parent:Mid-Pool 3

Port-Class-Pool 4

Parent:Mid-Pool 4

Port-Class-Pool 5

Parent:Mid-Pool 5

Port-Class-Pool 6

Parent:Mid-Pool 6

Port-Class-Pool 1 to 6

Port-Bw-Weight:1

Slope-Policy:_tmnx_hs_default

Alternate Port-Class Pools

Port-Class-Pool 1 to 6

Parent:None

Port-Bw-Weight:1

Slope-Policy:_tmnx_hs_default

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies an HS port pool policy name up to 32 characters.

create — This keyword is required when first creating the configuration context. After the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7750 SR-7/12/12e

hs-port-pool-policy

Syntax **hs-port-pool-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy hs-port-pool-policy)

Full Context configure qos copy hs-port-pool-policy

Description This command copies existing QoS policy entries for a QoS policy ID to another QoS policy ID.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters *src-name dst-name* — Indicates that the source policy ID and the destination policy ID are HS policy IDs. Specify the source policy ID that the copy command attempts to copy from and specify the destination policy ID to which the command copies a duplicate of the policy.

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy is overwritten with the contents of the source policy. If **overwrite** is not specified, an error occurs if the destination policy ID exists.

```
SR>config>qos# copy hs-pool-policy policy1 policy2
MINOR: CLI Destination "policy2" exists use {overwrite}.
SR>config>qos# copy hs-pool-policy policy1 policy2
 overwrite
```

Platforms 7750 SR-7/12/12e

12.93 hs-queue-stat-mode

hs-queue-stat-mode

Syntax **hs-queue-stat-mode** *mode*
no hs-queue-stat-mode

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos hs-queue-stat-mode)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt sla-profile egress qos hs-queue-stat-mode

Description This command configures the mode of statistics collected for all the HS queues.

The **no** form of this command reverts to the default.

Default hs-queue-stat-mode no-override

Parameters *mode* — Specifies the egress HS queue stats mode.

Values no-override — Indicates no overrides are used.

v4-v6 — Indicates separate counters are collected for IPv4 and IPv6 instead of the normal queue statistics.

Platforms 7750 SR-7/12/12e

12.94 hs-scheduler-overrides

hs-scheduler-overrides

Syntax **hs-scheduler-overrides** [**create**]
no hs-scheduler-overrides

Context **[Tree]** (config>port>ethernet>egress hs-scheduler-overrides)

Full Context configure port ethernet egress hs-scheduler-overrides

Description Commands in this context configure HS scheduler overrides which override parameters in the applied HS scheduler policy. This command is only applicable to the HSQ IOM (iom4-e-hs) and will fail if configured on all other card types.

Parameters **create** — Keyword used to create HS scheduler overrides. This keyword is requirement and can be enabled or disabled in the **environment>create** context.

Platforms 7750 SR-7/12/12e

12.95 hs-scheduler-policy

hs-scheduler-policy

Syntax **hs-scheduler-policy** *policy-name*
no hs-scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>ethernet>egress hs-scheduler-policy)

Full Context configure port ethernet egress hs-scheduler-policy

Description This command specifies an HS scheduler policy to associate with the port egress which provisions the scheduling behavior of the HSQ scheduler classes.

A single HS scheduler policy is supported per port egress. This command is only applicable to the HSQ IOM (iom4-e-hs) and will fail if configured on all other card types.

The **no** form of this command removes the policy and reapplies the default policy.

Default hs-scheduler-policy default

Parameters *policy-name* — Specifies the policy name up to 32 characters.

Platforms 7750 SR-7/12/12e

hs-scheduler-policy

Syntax **hs-scheduler-policy** *policy-name* [**create**]
no hs-scheduler-policy *policy-name*

Context [Tree] (config>qos hs-scheduler-policy)

Full Context configure qos hs-scheduler-policy

Description This command configures an HS scheduler policy. The HS scheduler policies are applied to egress HSQ ports in the **config>port>ethernet>egress** context. The policy contains the required commands to provision the scheduling behavior of the HSQ scheduler classes. When assigned to an HSQ egress port, the policy is used to define the scheduling behavior for all queues associated with the egress port. The values defined in the policy can be overridden on each scheduler instance using the **config>port>ethernet>egress>hs-scheduler-overrides** command.

HSQ Queue Groups — A fundamental concept on an HSQ IOM is the queue group. Queue groups are not directly managed by the provisioning. Instead, they are indirectly assigned when creating SAPs or subscribers on an HSQ port. A queue group has eight queue members, numbered from 1 through 8. When creating a SAP or subscriber associated on an HSQ egress port, a queue group is allocated to the object. Within the SAP egress policy, network queue policy and egress queue group template, provisioned queue IDs 1 through 8 correspond directly to queue group queue IDs 1 through 8. Each group also allows each queue to be dynamically placed in a scheduling class or on one of two WRR groups local to the queue group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each queue within the group has three RED slopes (managed by associating a slope policy to the queue), an MBS defined in bytes, a packet byte offset parameter used to add or subtract bytes to or from each packet handled by the queue for accounting purposes, and a PIR shaper used to rate limit the queue. An HSQ attachment policy associated with the queue group defines how each queue maps either directly to a scheduling class or one of the WRR groups within the queue group. The attachment policy also defines the scheduling class attachments for the WRR groups.

The queue group supports an aggregate shaper used to manage an aggregate rate limit for all queues within the group. Scheduling for queues within the queue group is stopped and started based on the rate set on the shaper.

Scheduling Classes and Scheduling Priorities — HSQ supports six scheduler classes (1 through 6). The scheduler class should not be confused with a QoS policy forwarding class. Forwarding classes within the system are used between the ingress and egress forwarding complexes and help the system to map a packet to per-hop and per-domain behavior. Scheduling classes are slices of scheduling opportunity within a port-scheduling context. Each port scheduler maintains six strict priority levels, where 6 is the highest priority and 1 is the lowest. As a rule, the scheduler services all active queues associated with priority level 6 before moving to queues on priority level 5. This strict behavior continues through priority level 1. Scheduling classes are mapped either to their corresponding scheduling priority level (scheduling class 1 mapped to priority level 1 through scheduling class 6 mapped to priority level 6) or to a single port level WRR group. The WRR group allows collapsing up to 6 of the scheduling classes into a single scheduling priority. The WRR group provides a weighted fair scheduling behavior for its member scheduling classes at that strict priority level.

Strict Priority Level PIR — The scheduler supports a strict scheduling level PIR that limits the amount of bandwidth allowed for the level. The rate is defined in increments of megabits per second and can be set to **max** (the default setting) which disables the shaping function. The scheduler includes the full Ethernet frame encapsulation overhead when updating the priority level PIR, including the 12-byte inter-frame gap and the 8-byte preamble.

Scheduler Maximum Rate — A maximum scheduling rate can be defined for the scheduler. The rate is specified in megabits per second and the default rate is **max** which allows the scheduler to operate without a set limit. When the HS scheduling policy is applied to an egress port, the maximum scheduling rate can be used to define a rate less than the available line rate of the port. The scheduler includes the full Ethernet frame encapsulation overhead when updating the scheduler level PIR, including the 12-byte inter-frame gap and the 8-byte preamble.

HS Scheduler Policy Overrides — After an HS scheduler is applied to an egress port, the various parameters can be overridden, allowing an HS scheduler policy to be adapted to changing needs on a port without requiring a new policy to be created.

Default HS Scheduling Policy — An HS scheduling policy with the name **default** always exists on the system and does not need to be created. The default policy cannot be modified or deleted.

The default policy contains the following parameters:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 63 **HS Scheduler Policy Parameter Defaults**

Parameter	Sub-Parameter	Default
max-rate	—	max
scheduling-class 1 through 6	rate	max
	group	—
	weight	—
group 1	rate	max

Default The **no** form of the command removes an HS scheduler policy from the system. If the HS scheduler policy is currently associated with an egress port, the command fails.

Parameters *policy-name* — Specifies the HS scheduler policy up to 32 characters. Each HS scheduler policy must be uniquely named within the system.

create — This keyword is required when first creating the configuration context. After the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7750 SR-7/12/12e

hs-scheduler-policy

Syntax **hs-scheduler-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy hs-scheduler-policy)

Full Context configure qos copy hs-scheduler-policy

Description This command copies existing QoS policy entries for a QoS policy ID to another QoS policy ID.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters *src-name dst-name* — Indicates that the source policy ID and the destination policy ID are HS policy IDs. Specify the source policy ID that the copy command attempts to copy from and specify the destination policy ID to which the command copies a duplicate of the policy.

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy is overwritten with the contents of the source policy. If **overwrite** is not specified, an error occurs if the destination policy ID exists.

```
SR>config>qos# copy hs-pool-policy policy1 policy2
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
MINOR: CLI Destination "policy2" exists use {overwrite}.
SR>config>qos# copy hs-pool-policy policy1 policy2
 overwrite
```

Platforms 7750 SR-7/12/12e

12.96 hs-secondary-shaper

hs-secondary-shaper

Syntax **hs-secondary-shaper** *secondary-shaper-name* [**create**]
no hs-secondary-shaper *secondary-shaper-name*

Context **[Tree]** (config>port>ethernet>egress hs-secondary-shaper)

Full Context configure port ethernet egress hs-secondary-shaper

Description This command specifies an HS secondary shaper on the port egress. HS secondary shapers are used to apply an aggregate rate and per-scheduling class rates to the set of SAP egress HSQ queue groups which reference them using the SAP egress queue-override **hs-secondary-shaper** command.

By default, the **hs-secondary-shaper** default is applied to each port egress on all HSQ ports and the settings under it can be modified.

Multiple HS secondary shapers are supported per port egress, up to the number supported per-HSQ FP, which is 4096 HS secondary shapers. The number of HS secondary shapers allocated on an HSQ FP can be seen using the **tools dump resource-usage card** *slot-number* **fp** *fp-number* command.

Non-default HS secondary shapers are only configurable on access or hybrid mode ports.

This command is only applicable to the HSQ IOM (iom4-e-hs) and will fail if configured on all other card types.

The **no** form of this command removes the HS secondary shaper from the port egress configuration. An HS scheduler policy cannot be removed when HS scheduler overrides exist on the port egress.

Default hs-secondary-shaper default

Parameters *secondary-shaper-name* — Specifies the secondary shaper name up to 32 characters.

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hs-secondary-shaper

Syntax **hs-secondary-shaper** *policy-name*
no hs-secondary-shaper

Context **[Tree]** (config>service>epipe>sap>egress>queue-override hs-secondary-shaper)
[Tree] (config>service>ipipe>sap>egress>queue-override hs-secondary-shaper)

Full Context configure service epipe sap egress queue-override hs-secondary-shaper
configure service ipipe sap egress queue-override hs-secondary-shaper

Description This command configures the HS secondary shaper to be used to apply an aggregate rate and per-scheduling class rates to the SAP egress HSQ queue group.

The **no** form of this command removes the HS secondary shaper override from the configuration, reverting the SAP egress HSQ queue group to the default HS secondary shaper on that port.

Parameters *policy-name* — Specifies the secondary shaper name, up to 32 characters.

Platforms 7750 SR-7/12/12e

hs-secondary-shaper

Syntax **hs-secondary-shaper** *policy-name*
no hs-secondary-shaper

Context **[Tree]** (config>service>vprn>sap>queue-override hs-secondary-shaper)

Full Context configure service vprn sap queue-override hs-secondary-shaper

Description This command configures the HS secondary shaper to be used to apply an aggregate rate and per-scheduling class rates to the SAP egress HSQ queue group.

The **no** form of this command removes the HS secondary shaper override from the configuration, reverting the SAP egress HSQ queue group to the default HS secondary shaper on that port.

Parameters *policy-name* — Specifies the secondary shaper name, up to 32 characters.

hs-secondary-shaper

Syntax **hs-secondary-shaper** *policy-name*
no hs-secondary-shaper

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override hs-secondary-shaper)

Full Context configure service ies interface sap egress queue-override hs-secondary-shaper

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the HS secondary shaper to be used to apply an aggregate rate and per-scheduling class rates to the SAP egress HSQ queue group.

The **no** form of this command removes the HS secondary shaper override from the configuration returning the SAP egress HSQ queue group to the default HS secondary shaper on that port.

Parameters *policy-name* — Specifies the secondary shaper name, up to 32 characters.

Platforms 7750 SR-7/12/12e

hs-secondary-shaper

Syntax **hs-secondary-shaper** *policy-name*
no hs-secondary-shaper

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override hs-secondary-shaper)

Full Context configure service vprn interface sap egress queue-override hs-secondary-shaper

Description This command configures the HS secondary shaper to be used to apply an aggregate rate and per-scheduling class rates to the SAP egress HSQ queue group.

The **no** form of this command removes the HS secondary shaper override from the configuration, returning the SAP egress HSQ queue group to the default HS secondary shaper on that port.

Parameters *policy-name* — Specifies the secondary shaper name, up to 32 characters.

Platforms 7750 SR-7/12/12e

12.97 hs-sla-mode

hs-sla-mode

Syntax **hs-sla-mode** {**expanded** | **single**}
no hs-sla-mode

Context **[Tree]** (config>subscr-mgmt>sub-prof hs-sla-mode)

Full Context configure subscriber-mgmt sub-profile hs-sla-mode

Description This command specifies the SLA profile handling mode for the subscriber if on an HS board.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **expanded** — Specifies the expanded SLA profile handling mode for the subscriber if on an HS board.

single — Specifies a single SLA profile handling mode for the subscriber if on an HS board.

Platforms 7750 SR-7/12/12e

12.98 hs-turbo

hs-turbo

Syntax [**no**] **hs-turbo**

Context **[Tree]** (config>port>ethernet>access>egress>queue-group hs-turbo)
[Tree] (config>port>ethernet>network>egress>queue-group hs-turbo)

Full Context configure port ethernet access egress queue-group hs-turbo
configure port ethernet network egress queue-group hs-turbo

Description This command enables HS turbo queues which allows the corresponding HSQ queue group queues to achieve a higher throughput. The **hs-turbo** command is not applicable to 10G ports and is ignored when configured under a queue group instance on a 10G port.

This command is only applicable to the HSQ IOM (iom4-e-hs) and will fail if configured on all other card types.

The **no** form of this command disables the command.

Platforms 7750 SR-7/12/12e

12.99 hs-wred-queue

hs-wred-queue

Syntax **hs-wred-queue policy** *slope-policy-name*
no hs-wred-queue

Context **[Tree]** (config>service>epipe>sap>egress>queue-override>queue hs-wred-queue)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue hs-wred-queue)

Full Context configure service epipe sap egress queue-override queue hs-wred-queue
configure service ipipe sap egress queue-override queue hs-wred-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command overrides the slope policy applied to the HSQ queue group queue.

The **no** form of this command removes the WRED queue policy override value from the configuration.

Parameters *slope-policy-name* — Specifies an existing slope policy name to apply to this HSQ queue group queue, up to 32 characters.

Platforms 7750 SR-7/12/12e

hs-wred-queue

Syntax **hs-wred-queue policy** *slope-policy-name*
no hs-wred-queue

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue hs-wred-queue)

Full Context configure service vpls sap egress queue-override queue hs-wred-queue

Description This command overrides the slope policy applied to the HSQ queue group queue.

The **no** form of this command removes the WRED queue policy override value from the configuration.

Parameters *slope-policy-name* — Specifies an existing slope policy name to apply to this HSQ queue group queue.

Platforms 7750 SR-7/12/12e

hs-wred-queue

Syntax **hs-wred-queue policy** *slope-policy-name*
no hs-wred-queue

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue hs-wred-queue)

Full Context configure service ies interface sap egress queue-override queue hs-wred-queue

Description This command overrides the slope policy applied to the HSQ queue group queue.

The **no** form of this command removes the WRED queue policy override value from the configuration.

Parameters *slope-policy-name* — Specifies an existing slope policy name to apply to this HSQ queue group queue.

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hs-wred-queue

Syntax **hs-wred-queue policy** *slope-policy-name*
no hs-wred-queue

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue hs-wred-queue)

Full Context configure service vprn interface sap egress queue-override queue hs-wred-queue

Description This command overrides the slope policy applied to the HSQ queue group queue.

The **no** form of this command removes the WRED queue policy override value from the configuration.

Parameters *slope-policy-name* — Specifies an existing slope policy name to apply to this HSQ queue group queue.

Platforms 7750 SR-7/12/12e

hs-wred-queue

Syntax **hs-wred-queue** [**policy** *slope-policy-name*]
no hs-wred-queue

Context **[Tree]** (config>qos>network-queue>queue hs-wred-queue)

Full Context configure qos network-queue queue hs-wred-queue

Description This command reverts the slope policy applied to the HSQ queue group queue to the default policy. Specifying an existing slope policy applies the named slope policy to the queue.

The **no** form of the command reverts to the default slope policy.

Default hs-wred-queue policy "_tmnx_hs_default"

Parameters *slope-policy-name* — Specifies an existing slope policy to apply to this HSQ queue group queue.

Platforms 7750 SR-7/12/12e

hs-wred-queue

Syntax **hs-wred-queue** [**policy** *slope-policy-name*]
no hs-wred-queue

Context **[Tree]** (config>qos>sap-egress>queue hs-wred-queue)

Full Context configure qos sap-egress queue hs-wred-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command reverts the slope policy applied to the HSQ queue group queue to the default policy. Specifying an existing slope policy applies the named slope policy to the queue.

The **no** form of the command reverts to the default slope policy.

Default hs-wred-queue policy "_tmnx_hs_default"

Parameters *slope-policy-name* — Specifies an existing slope policy to apply to this HSQ queue group queue.

Platforms 7750 SR-7/12/12e

hs-wred-queue

Syntax **hs-wred-queue** [**policy** *slope-policy-name*]
no hs-wred-queue

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue hs-wred-queue)

Full Context configure qos queue-group-templates egress queue-group queue hs-wred-queue

Description This command reverts the slope policy applied to the HSQ queue group queue to the default policy. Specifying an existing slope policy applies the named slope policy to the queue.

The **no** form of the command reverts to the default slope policy.

Default hs-wred-queue policy "_tmnx_hs_default"

Parameters *slope-policy-name* — Specifies an existing slope policy name to apply to this HSQ queue group queue.

Platforms 7750 SR-7/12/12e

12.100 hs-wred-queue-policy

hs-wred-queue-policy

Syntax **hs-wred-queue-policy** *name*
no hs-wred-queue-policy

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue hs-wred-queue-policy)

Full Context configure subscriber-mgmt sla-profile egress qos queue hs-wred-queue-policy

Description This command specifies the name of the slope-policy override to be applied for the HS queue of this SLA profile instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — Specifies the policy name up to 32 characters.

Platforms 7750 SR-7/12/12e

12.101 hs-wrr-group

hs-wrr-group

Syntax [**no**] **hs-wrr-group** *group-id*

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos hs-wrr-group)

Full Context configure subscriber-mgmt sla-profile egress qos hs-wrr-group

Description This command configures the egress HS WRR group override parameters.

The **no** form of this command removes the group ID from the configuration.

Parameters *group-id* — Specifies the HS WRR group ID to override in the QoS policy table.

Values 1, 2

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax **hs-wrr-group** *group-id* [**create**]
no hs-wrr-group *group-id*

Context **[Tree]** (config>service>epipe>sap>egress>queue-override hs-wrr-group)
[Tree] (config>service>ipipe>sap>egress>queue-override hs-wrr-group)

Full Context configure service epipe sap egress queue-override hs-wrr-group
configure service ipipe sap egress queue-override hs-wrr-group

Description This command configures the egress HS WRR group override parameters.

The **no** form of this command removes the group ID from the configuration.

Parameters *group-id* — Specifies the HS WRR group ID to override.

Values 1, 2

create — Keyword used to create an HSS WRR group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax **hs-wrr-group** *group-id* [**create**]
no hs-wrr-group *group-id*

Context **[Tree]** (config>service>vpls>sap>egress>queue-override hs-wrr-group)

Full Context configure service vpls sap egress queue-override hs-wrr-group

Description This command configures the egress HS WRR group override parameters.

The **no** form of this command removes the group ID from the configuration.

Parameters *group-id* — Specifies the HS WRR group ID to override.

Values 1, 2

create — Keyword used to create an HSS WRR group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax **hs-wrr-group** *group-id* [**create**]
hs-wrr-group *group-id*

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override hs-wrr-group)

Full Context configure service ies interface sap egress queue-override hs-wrr-group

Description This command configures the egress HS WRR group override parameters.

The **no** form of this command removes the group ID from the configuration.

Parameters *group-id* — Specifies the HS WRR group ID to override.

Values 1, 2

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax **hs-wrr-group** *group-id* [**create**]
no hs-wrr-group *group-id*

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override hs-wrr-group)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap egress queue-override hs-wrr-group

Description This command configures the egress HS WRR group override parameters.

The **no** form of this command removes the group ID from the configuration.

Parameters *group-id* — Specifies the HS WRR group ID to override.

Values 1, 2

create — Keyword used to create the HS WRR group override instance.

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax [**no**] **hs-wrr-group** *group-id*

Context **[Tree]** (config>qos>network-queue hs-wrr-group)

Full Context configure qos network-queue hs-wrr-group

Description Commands in this context configure HS WRR group information in the network queue policy. This command provisions the rate and class weight of each of the two WRR scheduling groups that can be utilized by the egress queue-group instance HSQ queues.

The **no** form of the command reverts the HS WRR group parameters to their default values.

Parameters *group-id* — Specifies the HS WRR group identifier. WRR group ID 1 or 2 must be specified when executing the **hs-wrr-group** command. The specified group ID identifies which WRR group context is entered for editing.

Values 1, 2

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax **hs-wrr-group** *group-id*
no hs-wrr-group

Context **[Tree]** (config>qos>sap-egress hs-wrr-group)

Full Context configure qos sap-egress hs-wrr-group

Description Commands in this context configure HS WRR group information in the SAP egress QoS policy. The **hs-wrr-group** command is used to provision the rate and class weight of each of the two WRR scheduling groups that can be utilized by the SAP egress HSQ queues.

The **no** form of the command resets the HS WRR group parameters to their default values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-id* — Specifies the HS WRR group identifier. WRR group ID 1 or 2 must be specified when executing the **hs-wrr-group** command. The specified group ID identifies which WRR group context is entered for editing.

Values 1, 2

Platforms 7750 SR-7/12/12e

hs-wrr-group

Syntax [**no**] **hs-wrr-group** *group-id*

Context **[Tree]** (config>qos>qgrps>egr>qgrp hs-wrr-group)

Full Context configure qos queue-group-templates egress queue-group hs-wrr-group

Description Commands in this context configure HS WRR group information in the egress queue group template. The **hs-wrr-group** command is used to provision the rate and class weight of each of the two WRR scheduling groups that can be utilized by the egress queue group instance HSQ queues.

The **no** form of the command resets the HS WRR group parameters to their default values.

Parameters *group-id* — Specifies the HS WRR group identifier. WRR group ID 1 or 2 must be specified when executing the **hs-wrr-group** command. The specified group ID identifies which WRR group context is entered for editing.

Values 1, 2

Platforms 7750 SR-7/12/12e

12.102 hs-wrr-weight

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue hs-wrr-weight)

Full Context configure subscriber-mgmt sla-profile egress qos queue hs-wrr-weight

Description This command configures the SLA profile instance WRR weight override for the HS queue. When a weight value is not specified, there is no override, meaning, the WRR weight is taken from the sap-egress policy.

The **no** form of this command removes the weight value from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *weight* — Specifies the class-weight override for expanded egress HS queues.

Values 1 to 127

Platforms 7750 SR-7/12/12e

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>service>epipe>sap>egress>queue-override>queue hs-wrr-weight)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue hs-wrr-weight)

Full Context configure service epipe sap egress queue-override queue hs-wrr-weight
configure service ipipe sap egress queue-override queue hs-wrr-weight

Description This command overrides the WRR relative weight as defined within the associated HS attachment policy.

The **no** form of this command removes the WRR weight override value from the configuration.

Parameters *weight* — Specifies the HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue hs-wrr-weight)

Full Context configure service vpls sap egress queue-override queue hs-wrr-weight

Description This command overrides the WRR relative weight with which this queue should parent into an HSQ WRR group defined within the associated HS attachment policy.

The **no** form of this command removes the WRR weight override value from the configuration.

Parameters *weight* — Specifies the HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue hs-wrr-weight)

Full Context configure service ies interface sap egress queue-override queue hs-wrr-weight

Description This command overrides the Weighted Round Robin (WRR) relative weight with which this queue should parent into an HSQ WRR group defined within the associated HS attachment policy.

The **no** form of this command removes the WRR weight override value from the configuration.

Parameters *weight* — Specifies the HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue hs-wrr-weight)

Full Context configure service vprn interface sap egress queue-override queue hs-wrr-weight

Description This command overrides the WRR relative weight with which this queue should parent into an HSQ Weighted Round Robin (WRR) group defined within the associated HS attachment policy.

The **no** form of this command removes the WRR weight override value from the configuration.

Parameters *weight* — Specifies the HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>qos>network-queue>queue hs-wrr-weight)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos network-queue queue hs-wrr-weight

Description This command specifies the WRR relative weight, with which this queue should parent into an HSQ WRR group defined within the associated HS attachment policy. The weight of each queue determines how much bandwidth that queue gets out of the total rate for the HSQ WRR group.

The **no** form of the command reverts to the default value.

Default hs-wrr-weight 1

Parameters *weight* — Specifies the HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>qos>sap-egress>queue hs-wrr-weight)

Full Context configure qos sap-egress queue hs-wrr-weight

Description This command specifies the WRR relative weight, with which this queue should parent into an HSQ WRR group defined within the associated HS attachment policy. The weight of each queue determines how much bandwidth that queue gets out of the total rate for the HSQ WRR group.

The **no** form of the command reverts to the default value.

Default hs-wrr-weight 1

Parameters *weight* — Specifies the HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

hs-wrr-weight

Syntax **hs-wrr-weight** *weight*
no hs-wrr-weight

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue hs-wrr-weight)

Full Context configure qos queue-group-templates egress queue-group queue hs-wrr-weight

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the WRR relative weight, with which this queue should parent into an HSQ WRR group defined within the associated HS attachment policy. The weight of each queue determines how much bandwidth that queue gets out of the total rate for the HSQ WRR group.

The **no** form of the command reverts to the default value.

Default hs-wrr-weight 1

Parameters *weight* — Specifies HS WRR group queue weight.

Values 1 to 127

Platforms 7750 SR-7/12/12e

12.103 http-auth

http-auth

Syntax **http-auth password** *password* [**hash | hash2**]
http-auth username *user-name*
http-auth username *user-name* **password** *password* [**hash | hash2**]
no http-auth

Context **[Tree]** (config>system>security>pki>est-profile http-auth)

Full Context configure system security pki est-profile http-auth

Description This command configures HTTP authentication parameters. HTTP authentication is used by a client when requested by the server. When disabled, there is no HTTP-level client authentication.

The **no** form of the command reverts to the default value.

Default no http-auth

Parameters *password* — Specifies a text string containing the password. Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

user-name — Specifies the name of the user to authenticate, up to 32 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

Platforms All

12.104 http-connections

http-connections

Syntax **http-connections** [*ip-address/prefix-length*]
http-connections any
http-connections [*ipv6-address/prefix-length*]
no http-connections

Context **[Tree]** (debug>system http-connections)

Full Context debug system http-connections

Description This command displays HTTP connections debug information.

Parameters *ip-address/prefix-length* — Displays information for the specified host IP address and prefix length.

Values ip-address: a.b.c.d
prefix-length: 0 to 32

any — Specifies that any address can be used.

ipv6-address/prefix-length — Displays information for the specified host IPv6 address and prefix length.

Values ipv6-address:
- x:x:x:x:x:x:x:x: (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x [0 to FFFFF] H
- d [0 to 255] D

prefix-length: 0 to 128

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.105 http-enrich

http-enrich

Syntax **http-enrich** *http-enrich-name* [**create**]
no http-enrich *http-enrich-name*

Context **[Tree]** (config>app-assure>group http-enrich)

Full Context configure application-assurance group http-enrich

Description This command configures an HTTP enrichment policy.

The **no** form of this command removes the http enrichment policy from the configuration.

Parameters *http-enrich-name* — Specifies the name of the http enrichment policy up to 32 characters.

create — Mandatory keyword used when creating an application profile. The create keyword requirement can be enabled and disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

http-enrich

Syntax **http-enrich** *http-enrich-name*
no http-enrich

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action http-enrich)

Full Context configure application-assurance group policy app-qos-policy entry action http-enrich

Description This command configures the HTTP header enrichment template name that will be applied as defined in the tmnxBsxHttpEnrichTable. An empty value specifies no HTTP header enrichment template.

Default no http-enrich

Parameters *http-enrich-name* — Specifies the HTTP header enrichment template name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.106 http-enrich-max-pkt

http-enrich-max-pkt

Syntax [**no**] **http-enrich-max-pkt** *size*

Context **[Tree]** (config>isa>aa-grp http-enrich-max-pkt)

Full Context configure isa application-assurance-group http-enrich-max-pkt

Description This command configures the maximum HTTP enriched packet size.

Parameters *size* — Specifies the maximum HTTP enriched packet size in octets.

Values 576 to 9212

Default 1500

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.107 http-error-redirect

http-error-redirect

Syntax **http-error-redirect** *redirect-name* [**create**]
no http-error-redirect *redirect-name*

Context **[Tree]** (config>app-assure>group http-error-redirect)

Full Context configure application-assurance group http-error-redirect

Description This command configures an HTTP error redirect policy. The policy contains important information relevant to the redirect server.

The **no** form of this command removes the redirect name from the group configuration.

Parameters *redirect-name* — Specifies a string, up to 32 characters, that identifies the HTTP error redirect policy.

create — Keyword to create the HTTP error redirect policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

http-error-redirect

Syntax **http-error-redirect** *redirect-name*
no http-error-redirect

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action http-error-redirect)

Full Context configure application-assurance group policy app-qos-policy entry action http-error-redirect

Description This command specifies the HTTP error redirect that will be applied as defined in the redirect table. An empty value specifies no HTTP error redirect.

Default no http-error-redirect

Parameters *redirect-name* — Specifies an http-error redirect action, up to 32 characters, for flows matching this entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.108 http-host

http-host

Syntax **http-host** *http-host*
no http-host

Context **[Tree]** (config>app-assure>group>http-error-redirect http-host)

Full Context configure application-assurance group http-error-redirect http-host

Description This command refers to the http host name of the landing server (Barefruit or Xerocole). It is used in the HTTP GET operation from the client (which is being redirected) to the redirect search landing server. It must contain a valid IP address or HTTP host name / URI for the HTTP GET from the client to the landing server to work.

The **no** form of this command removes the HTTP host string from the configuration.

Default no http-host

Parameters *http-host* — Specifies a string of 255 chars max length, that refers to the HTTP host name of the landing server (barefruit or xerocole).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.109 http-host-recorder

http-host-recorder

Syntax [**no**] **http-host-recorder**

Context **[Tree]** (debug>app-assure>group http-host-recorder)

Full Context debug application-assurance group http-host-recorder

Description This command enables the http-host-recorder feature on a particular group:partition.

The **no** form of the command disables the http-host-recorder feature.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.110 http-listening-port

http-listening-port

Syntax **http-listening-port** *http-listening-port*
no http-listening-port

Context **[Tree]** (config>service>upnp>upnp-policy http-listening-port)

Full Context configure service upnp upnp-policy http-listening-port

Description This command specifies the listening port of UPnP server.

The **no** form of the command reverts to the default.

Default http-listening-port 5000

Parameters *http-listening-port* — Specifies the HTTP TCP port this UPnP IGD listens to.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.111 http-match-all-requests

http-match-all-requests

Syntax [**no**] **http-match-all-requests**

Context **[Tree]** (config>app-assure>group http-match-all-requests)
[Tree] (config>app-assure>group>policy>app-filter>entry http-match-all-requests)

Full Context configure application-assurance group http-match-all-requests
configure application-assurance group policy app-filter entry http-match-all-requests

Description This command enables HTTP matching for all requests for a given HTTP expression.

The **no** form of this command restores the default (removes http-match-all-request for this particular expression) by this app-filter entry.

Default no http-match-all-requests

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.112 http-notification

http-notification

Syntax **http-notification** *http-notification-name* [**create**]
no http-notification *http-notification-name*

Context **[Tree]** (config>app-assure>group http-notification)

Full Context configure application-assurance group http-notification

Description This command configures an http-notification object for subscriber in browser notification.

The **no** form of this command removes the http notification policy from the configuration.

Parameters *http-notification-name* — Specifies the name of the HTTP Notification policy.

create — Specifies the mandatory keyword to create the policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

http-notification

Syntax **http-notification** *http-notification*
no http-notification

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action http-notification)

Full Context configure application-assurance group policy app-qos-policy entry action http-notification

Description This command configures an HTTP notification action for flows matching this entry.

Default no http-notification

Parameters *http-notification* — specifies the Application-Assurance HTTP Notification that will be applied as defined in the tmnxBsxHttpNotifTable. If no string is configured then no HTTP notification will occur.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.113 http-port

http-port

Syntax **http-port** {**eq** | **neq**} *port-num*
http-port {**eq** | **neq**} **port-list** *port-list-name*
no http-port

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry http-port)

Full Context configure application-assurance group policy app-filter entry http-port

Description This command specifies an HTTP server TCP or UDP port number or port list to use in the application definition.

The **no** form of this command restores the default by removing the HTTP port or port list from the application criteria defined by this app-filter entry.

Default no http-port

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

port-list-name — Specifies the name of the port list containing a set or range of ports, up to 32 characters.

port-num — Specifies a valid server port number.

Values 0 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.114 http-redirect

http-redirect

Syntax **http-redirect** *redirect-name* [**create**]
no http-redirect *redirect-name*

Context **[Tree]** (config>app-assure>group http-redirect)

Full Context configure application-assurance group http-redirect

Description This command configures an HTTP redirect.

The **no** form of this command removes the HTTP redirect policy from the configuration.

Parameters *redirect-name* — Specifies the HTTP redirect that will be applied. If no redirect name is specified, then HTTP redirect is not enabled.

create — Keyword to create the HTTP redirect policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

http-redirect

Syntax **http-redirect** *http-redirect–name* **flow-type** *flow-type*
no http-redirect

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action http-redirect)

Full Context configure application-assurance group policy app-qos-policy entry action http-redirect

Description This command assigns an existing http redirect policy as an action on flows matching this AQP entry.

The redirect only takes effect if the matching flows are HTTP and the condition specified after the **http-redirect** command, admitted flows or dropped-flows, is met. The condition specified by “dropped-flows” means the flow is dropped due to an AQP actions such as “flow rate/count policers” or “drop” actions. HTTP Policy Redirect on admitted-flows allows the operator to redirect HTTP traffic to a web portal while allowing non-HTTP matching the same AQP rule to be forwarded.

No HTTP redirect will take place if HTTP redirect action and a “drop/flow-police” action are part of the default AQP policy, because in this case, any flow drop actions will take place before identification of the application/application-group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes http redirect from actions on flows matching this AQP entry.

Default no http-redirect

Parameters *http-redirect-name* — Specifies the name of the existing http policy redirect for this application assurance profile. The HTTP redirect name is configured in the **config>app-assure>group>http-redirect** context.

flow-type — Specifies the flow type.

Values **admitted-flows** — Redirect HTTP flows matching the AQP criteria.
dropped-flows — Redirects those HTTP flows that are dropped due to an AQP action.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

http-redirect

Syntax **http-redirect** *http-redirect-name*

Context **[Tree]** (config>app-assure>group>sess-fltr>entry>action http-redirect)

Full Context configure application-assurance group session-filter entry action http-redirect

Description This command configures a session filter entry action to HTTP redirect the subscriber flows. The HTTP redirect policy referenced within this session filter entry is configured for captive redirect with the appropriate VLAN id assigned.

Parameters *http-redirect-name* — Specifies the name of the http-redirect-policy.

http-redirect

Syntax **http-redirect** *http-redirect-name*
no http-redirect

Context **[Tree]** (config>app-assure>group>url-filter http-redirect)

Full Context configure application-assurance group url-filter http-redirect

Description This command specifies the HTTP redirect that will be applied when the URL filter blocks an HTTP request.

Default no http-redirect

Parameters *http-redirect-name* — Specifies the HTTP redirect name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

http-redirect

Syntax **http-redirect** *http-redirect-name*
no http-redirect

Context [Tree] (config>app-assure>group>url-filter>icap http-redirect)
[Tree] (config>app-assure>group>url-filter>web-service http-redirect)
[Tree] (config>app-assure>group>url-filter>local-filtering>deny-list http-redirect)

Full Context configure application-assurance group url-filter icap http-redirect
configure application-assurance group url-filter local-filtering deny-list http-redirect
configure application-assurance group url-filter web-service http-redirect

Description This command creates or modifies an HTTP redirect policy.

Default no http-redirect

The **no** form of this command removes the HTTP redirect policy from the configuration.

Parameters *http-redirect-name* — Specifies the name of the HTTP redirect policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

http-redirect

Syntax **http-redirect** *rdr-url-string* [**allow-radius-override**]
http-redirect url-from-cpf

Context [Tree] (config>filter>ip-filter>entry>action http-redirect)
[Tree] (config>filter>ipv6-filter>entry>action http-redirect)

Full Context configure filter ip-filter entry action http-redirect
configure filter ipv6-filter entry action http-redirect

Description This command sets the filter entry action to **http-redirect** and specifies the redirect URL.

Parameters *rdr-url-string* — Specifies the HTTP redirect URL, up to 255 characters. This option can be used for any session.

Values The following macro substitutions may be used:

$URL — request-URI in the HTTP GET request received

$MAC — a string that represents the MAC address of the subscriber host

$IP — a string that represents the IP address of the subscriber host

$SUB — a string that represents the subscriber ID

$SAP — a string that represents a SAP ID

$SAPDESC — description string configured on the SAP

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

$CID — a string that represents the circuit ID or interface ID of the subscriber host (hexadecimal format)

$RID — a string that represents the remote ID of the subscriber host (hexadecimal format)

allow-radius-override — Specifies that the HTTP redirect URL configured by *rdr-url-string* can be optionally overridden by a URL returned by the RADIUS server; this does not apply for the **url-from-cpf** option.

url-from-cpf — Specifies that the HTTP redirect URL is from the BNG CUPS CPF. This option can be used for BNG CUPS ESM sessions only.

Platforms All

http-redirect

Syntax **http-redirect** *url*

Context **[Tree]** (config>filter>mac-filter>entry>action http-redirect)

Full Context configure filter mac-filter entry action http-redirect

Description This command sets the MAC filter entry action to HTTP redirect.

Parameters *url* — Specifies the URL, up to 255 characters.

Platforms All

12.115 http-redirect-policy

http-redirect-policy

Syntax **http-redirect-policy** *policy-name*
no http-redirect-policy

Context **[Tree]** (config>subscr-mgmt http-redirect-policy)

Full Context configure subscriber-mgmt http-redirect-policy

Description This command configures the redirect policy to constrain forwarding of an unauthenticated “migrant” WIFI user.

Parameters *policy-name* — Specifies the HTTP redirect policy name up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

http-redirect-policy

Syntax **http-redirect-policy** *policy-name*
no http-redirect-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range http-redirect-policy)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range http-redirect-policy)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range http-redirect-policy
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range http-redirect-policy

Description This command specifies http redirect policy on ISA to redirect http traffic to the URL specified in the policy.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the name of the http redirect policy under subscriber-management context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.116 http-request-filtering

http-request-filtering

Syntax **http-request-filtering** {**all** | **first**}

Context **[Tree]** (config>app-assure>group>url-filter http-request-filtering)

Full Context configure application-assurance group url-filter http-request-filtering

Description HTTP Filtering can either be enabled for all HTTP request within a flow or limited to the first HTTP request in a flow.

Default http-request-filtering all

Parameters **all** — Specifies all HTTP Request within a flow.

first — Specifies the first HTTP Request within a flow.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.117 http-response-timeout

http-response-timeout

Syntax **http-response-timeout** *timeout*
no http-response-timeout

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 http-response-timeout)

Full Context configure system security pki ca-profile cmpv2 http-response-timeout

Description This command specifies the timeout value for HTTP response that is used by CMPv2.

The **no** form of this command reverts to the default.

Default http-response-timeout 30

Parameters *timeout* — Specifies the HTTP response timeout, in seconds.

Values 1 to 3600

Platforms All

http-response-timeout

Syntax **http-response-timeout** *timeout*
no http-response-timeout

Context **[Tree]** (config>system>security>pki>ca-profile>cmp2 http-response-timeout)

Full Context configure system security pki ca-profile cmp2 http-response-timeout

Description This command specifies the timeout value for HTTP response that is used by CMPv2.

The **no** form of this command reverts to the default.

Default http-response-timeout 30

Parameters *timeout* — Specifies the HTTP response timeout in seconds.

Values 1 to 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

12.118 http-version

http-version

Syntax **http-version** [**1.0** | **1.1**]

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 http-version)

Full Context configure system security pki ca-profile cmpv2 http-version

Description This command configures the HTTP version for CMPv2 messages.

Default http-version 1.1

Platforms All

12.119 http-x-online-host

http-x-online-host

Syntax [**no**] **http-x-online-host**

Context **[Tree]** (config>app-assure>group http-x-online-host)

Full Context configure application-assurance group http-x-online-host

Description This command specifies whether X-Online-Host header field is used as a replacement for the HTTP Host header field.

The **no** form of this command disables the use of X-Online-Host header field used as a replacement.

Default no http-x-online-host

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

12.120 hw-agg-shaper-scheduler-policy

hw-agg-shaper-scheduler-policy

Syntax **hw-agg-shaper-scheduler-policy** *policy-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no hw-agg-shaper-scheduler-policy

Context [Tree] (config>port>ethernet>access>egress>vport hw-agg-shaper-scheduler-policy)

Full Context configure port ethernet access egress vport hw-agg-shaper-scheduler-policy

Description This command assigns a hardware aggregate shaper scheduler policy to the specified vport.

The **no** form removes the policy from the vport.

Parameters *policy-name* — Specifies the policy name.

Platforms 7750 SR-1, 7750 SR-s

hw-agg-shaper-scheduler-policy

Syntax **hw-agg-shaper-scheduler-policy** *policy-name* **[create]**
no hw-agg-shaper-scheduler-policy

Context [Tree] (config>qos hw-agg-shaper-scheduler-policy)

Full Context configure qos hw-agg-shaper-scheduler-policy

Description This command configures the name of the hardware aggregate shaper scheduler policy.

The **no** form removes the policy.

Parameters *policy-name* — Specifies the policy name, up to 64 characters.

create — Creates a new policy.

Platforms 7750 SR-1, 7750 SR-s

12.121 hw-agg-shapers

hw-agg-shapers

Syntax **hw-agg-shapers [subscribers] [saps] [queue-groups]**
no hw-agg-shapers

Context [Tree] (config>qos>fp-resource-policy>aggregate-shapers hw-agg-shapers)

Full Context configure qos fp-resource-policy aggregate-shapers hw-agg-shapers

Description This command enables the use of hardware aggregate shapers for subscribers, SAPs, or queue groups on the specified FP.

The **no** form disables the use of hardware aggregate shapers on a the specified FP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **subscribers** — Enables hardware aggregate shapers for subscribers.

saps — Enables hardware aggregate shapers for SAPs. This functionality is not currently supported.

queue-groups — Enables hardware aggregate shapers for queue groups. This functionality is not currently supported.

Platforms 7750 SR-1, 7750 SR-s

12.122 hybrid-buffer-allocation

hybrid-buffer-allocation

Syntax **hybrid-buffer-allocation**

Context **[Tree]** (config>port hybrid-buffer-allocation)

Full Context configure port hybrid-buffer-allocation

Description Commands in this context configure hybrid port buffer allocation parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13 i Commands

13.1 i-counters

i-counters

Syntax **i-counters** [**all**]
no i-counters

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue i-counters)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue i-counters)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters

Description This command configures ingress counter parameters for this custom record.

The **no** form of this command reverts to the default.

Parameters **all** — Includes all counters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

i-counters

Syntax **i-counters** [**all**]
no i-counters

Context **[Tree]** (config>log>acct-policy>cr>policer i-counters)
[Tree] (config>log>acct-policy>cr>queue i-counters)
[Tree] (config>log>acct-policy>cr>ref-policer i-counters)
[Tree] (config>log>acct-policy>cr>ref-queue i-counters)

Full Context configure log accounting-policy custom-record policer i-counters
configure log accounting-policy custom-record queue i-counters
configure log accounting-policy custom-record ref-policer i-counters
configure log accounting-policy custom-record ref-queue i-counters

Description This command configures ingress counter parameters for this custom record.

The **no** form of this command reverts all ingress counters to their default value.

Default i-counters

Parameters **all** — Specifies that all ingress counters should be included.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

13.2 i-sid

i-sid

Syntax **i-sid** *i-sid*
no i-sid

Context **[Tree]** (config>test-oam>build-packet>header>pbb i-sid)
[Tree] (debug>oam>build-packet>packet>field-override>header>pbb i-sid)

Full Context configure test-oam build-packet header pbb i-sid
debug oam build-packet packet field-override header pbb i-sid

Description This command defines the iSID value to be used in the test PBB header.

The **no** form of this command reverts to the default value.

Default i-sid 0

Parameters *i-sid* — Specifies the iSID value to be used in the test PBB header.

Values 0 to 16777215

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.3 ia-na

ia-na

Syntax **ia-na**

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client ia-na)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client ia-na)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client ia-na
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client ia-na

Description This command configures the IA-NA for the DHCPv6 client.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.4 ibgp-multipath

ibgp-multipath

Syntax [**no**] **ibgp-multipath**

Context **[Tree]** (config>service>vprn>bgp ibgp-multipath)

Full Context configure service vprn bgp ibgp-multipath

Description This command defines the type of IBGP multipath to use when adding BGP routes to the route table if the route resolving the BGP nexthop offers multiple next-hops.

The **no** form of this command disables the IBGP multipath load balancing feature.

Platforms All

ibgp-multipath

Syntax [**no**] **ibgp-multipath**

Context **[Tree]** (config>router>bgp ibgp-multipath)

Full Context configure router bgp ibgp-multipath

Description This command enables IBGP multipath load balancing when adding BGP routes to the route table if the route resolving the BGP nexthop offers multiple next-hops.

The **no** form of this command disables the IBGP multipath load balancing feature.

Default no ibgp-multipath

Platforms All

13.5 icmp

icmp

Syntax **icmp**

Context **[Tree]** (config>service>ies>if icmp)
[Tree] (config>service>ies>sub-if>grp-if icmp)
[Tree] (config>service>vprn>if icmp)
[Tree] (config>service>vprn>nw-if icmp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface icmp
configure service ies subscriber-interface group-interface icmp
configure service vprn interface icmp
configure service vprn network-interface icmp

Description Commands in this context configure Internet Control Message Protocol (ICMP) parameters on a service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface icmp

All

- configure service vprn interface icmp
- configure service vprn network-interface icmp
- configure service ies interface icmp

icmp

Syntax **icmp**

Context **[Tree]** (config>subscr-mgmt>git>ipv4 icmp)

Full Context configure subscriber-mgmt group-interface-template ipv4 icmp

Description Commands in this context configure IPv4 Internet Control Message Protocol (ICMP) parameters.

Default icmp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

icmp

Syntax **icmp**

Context **[Tree]** (config>router>if icmp)

Full Context configure router interface icmp

Description This command enables access to the context to configure Internet Control Message Protocol (ICMP) parameters on a network IP interface. ICMP is a message control and error reporting protocol that also provides information relevant to IP packet processing.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

icmp

Syntax [**no**] **icmp**

Context **[Tree]** (debug>router>ip icmp)

Full Context debug router ip icmp

Description This command enables ICMP debugging.

Platforms All

icmp

Syntax [**no**] **icmp**

Context **[Tree]** (config>sys>security>cpu-protection>ip>included-protocols icmp)

Full Context configure system security cpu-protection ip-src-monitoring included-protocols icmp

Description This command includes the extracted IPv4 ICMP packets for ip-src-monitoring. IPv4 ICMP packets will be subject to the per-source-rate of CPU protection policies.

Default no icmp

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

icmp

Syntax **icmp**

Context **[Tree]** (config>test-oam icmp)

Full Context configure test-oam icmp

Description This command configures test ICMP OAM parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.6 icmp-code

icmp-code

Syntax **icmp-code** *icmp-code*
no -code

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>ip-exception>entry>match icmp-code)
[Tree] (config>filter>ip-filter>entry>match icmp-code)
[Tree] (config>filter>ipv6-exception>entry>match icmp-code)
[Tree] (config>filter>ipv6-filter>entry>match icmp-code)

Full Context configure filter ip-exception entry match icmp-code
configure filter ip-filter entry match icmp-code
configure filter ipv6-exception entry match icmp-code
configure filter ipv6-filter entry match icmp-code

Description Configures matching on /ICMPv6 code field in the /ICMPv6 header of an IPv4 or IPv6 packet as a filter match criterion or configures matching on the ICMP code field in the ICMP header of an IPv4 packet as an exception filter match criterion. An entry containing Layer 4 non-zero match criteria will not match non-initial (for example, 2nd, 3rd) fragments of a fragmented packet since only the first fragment contains the Layer 4 information. Similarly an entry containing "**icmp-code** 0" match criterion, may match non-initial fragments when the Layer 4 header is not present in a packet fragment and other match criteria are also met.

The **no** form of the command removes the criterion from the match entry.

Default no icmp-code

Parameters *icmp-code* — Specifies the /ICMPv6 code value that must be present to match. Value can be expressed as a decimal integer, as well as in hexadecimal or binary format, or even using keywords. The following value shows decimal integer only.

Values 0 to 255

Platforms All

- configure filter ipv6-filter entry match icmp-code
- configure filter ip-filter entry match icmp-code

VSR

- configure filter ip-exception entry match icmp-code
- configure filter ipv6-exception entry match icmp-code

icmp-code

Syntax **icmp-code** *icmp-code*
no icmp-code

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match icmp-code)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match icmp-code)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match icmp-code)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match icmp-code)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match icmp-code

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match icmp-code
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match icmp-code
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match icmp-code

Description This command configures the ICMP code match condition.

The **no** form of this command reverts to the default.

Parameters *icmp-code* — Specifies the ICMP code numbers accepted in DHB.

Values [0 to 255]D, [0X0..0XFF]H, [0b0..0b11111111]B

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

icmp-code

Syntax **icmp-code** *icmp-code*
no icmp-code

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match icmp-code)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match icmp-code)

Full Context configure system security cpm-filter ip-filter entry match icmp-code
configure system security cpm-filter ipv6-filter entry match icmp-code

Description This command configures matching on ICMP code field in the ICMP header of an IP packet as an IP filter match criterion.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The behavior of the **icmp-code** value is dependent on the configured **icmp-type** value, thus a configuration with only an **icmp-code** value specified will have no effect. To match on the **icmp-code**, an associated **icmp-type** must also be specified.

The **no** form of this command removes the criterion from the match entry.

Default no icmp-code

Parameters *icmp-code* — Specifies the ICMP code values that must be present to match.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.7 icmp-echo-reply

icmp-echo-reply

Syntax [**no**] **icmp-echo-reply**

Context **[Tree]** (config>router>nat>outside>pool icmp-echo-reply)
[Tree] (config>service>vprn>nat>outside>pool icmp-echo-reply)

Full Context configure router nat outside pool icmp-echo-reply
configure service vprn nat outside pool icmp-echo-reply

Description IPv4 addresses in a NAT pool can be configured to respond to ICMP Echo Requests (PINGs). The configuration can be toggled online while the pool is in use.

In L2-aware NAT when **port-block-extensions** is disabled, the reply from an outside IP address is generated only when this IP address has at least one host (binding) behind it.

In L2-aware NAT when **port-block-extensions** is enabled, the reply from an outside IP address is generated regardless if a binding is present.

In LSN, the reply from an outside IP address is generated regardless if a binding is present.

The **no** form of the command disables ICMP echo replies.

Default no icmp-echo-reply

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.8 icmp-generation

icmp-generation

Syntax **icmp-generation**

Context **[Tree]** (config>ipsec>tunnel-template icmp-generation)
[Tree] (config>router>if>ipsec>ipsec-tunnel icmp-generation)
[Tree] (config>service>ies>if>sap>ip-tunnel icmp-generation)
[Tree] (config>service>vprn>if>sap>ip-tunnel icmp-generation)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel icmp-generation)

Full Context configure ipsec tunnel-template icmp-generation
configure router interface ipsec ipsec-tunnel icmp-generation
configure service ies interface sap ip-tunnel icmp-generation
configure service vprn interface sap ip-tunnel icmp-generation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ipsec-tunnel icmp-generation

Description This command enables the context to configure ICMP generation information.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ip-tunnel icmp-generation
- configure service ies interface sap ip-tunnel icmp-generation
- configure ipsec tunnel-template icmp-generation
- configure service vprn interface sap ipsec-tunnel icmp-generation

VSR

- configure router interface ipsec ipsec-tunnel icmp-generation

13.9 icmp-ping

icmp-ping

Syntax **icmp-ping** {*ip-address* | *dns-name*} [{**bypass-routing** | {**interface** *interface-name*} | {**next-hop** *ip-address*}}] [**count** *requests*] [**do-not-fragment**] [**fc** *fc-name*] [**interval** {*centisecs* | *secs*}] [**pattern** *pattern*] [**rapid**] [{**router** *router-or-service* | **router-instance** *router-instance* | **service-name** *service-name*}] [**size** *bytes*] [**source** *ip-address*] [**timeout** *timeout*] [**tos** *type-of-service*] [**ttl** *time-to-live*]

Context **[Tree]** (config>saa>test>type icmp-ping)

Full Context configure saa test type icmp-ping

Description This command configures an ICMP traceroute test.

Parameters *ip-address* | *dns-name* — Specifies the far-end IP address or DNS name to which to send the **svc-ping** request message in dotted decimal notation.

Values

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D
	interface	up to 32 characters. This is mandatory for link local addresses.
dns-name	up to 128 characters	

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bypass-routing — Specifies whether to send the ping request to a host on a directly attached network bypassing the routing table.

interface-name — Specifies the name used to refer to the interface, up to 32 characters. The name must already exist in the **config>router>interface** context.

next-hop *ip-address* — Displays only static routes with the specified next-hop IP address.

Values

ipv4-address:	a.b.c.d (host bits must be 0)
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

requests — Specifies the number of times to perform an OAM ping probe operation. Each OAM echo message request must either time out or receive a reply before the next message request is sent.

Values 1 to 100000

Default 5

do-not-fragment — Sets the DF (Do Not Fragment) bit in the ICMP ping packet (does not apply to ICMPv6).

fc-name — Specifies the forwarding class of the SAA.

Values be, l2, af, l1, h2, ef, h1, nc

Default nc

interval {*centisecs* | *secs*} — Specifies the minimum amount of time, in seconds, that must expire before the next message request is sent. If the **rapid** parameter is configured, this value is measured in centiseconds (hundredths of a second) instead of seconds.

Values 1 to 10000

Default 1

pattern — Specifies the date portion in a ping packet is filled with the pattern value specified. If not specified, a system-generated sequential pattern is used.

Values 0 to 65535

rapid — Configures the *interval* parameter to use centiseconds (hundredths of a second) instead of seconds.

router-or-service — Specifies the numerical reference to the router instance or service. Well known router names "Base", "management", “vpm-vr-name”, and " vpls-management" are allowed for convenience, but are mapped numerically.

Values {*router-name* | *vprn-svc-id*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-name: Base, management, cmp-vr-name, vpls-management
vprn-svc-id: 1 to 2147483647
cpm-vr-name: Up to 32 characters

The parameter *router-instance* is preferred for specifying the router or service.

Default Base

router-instance — Specifies the preferred method for entering a service name. Stored as the service name. Only the service linking function is allowed for both mixed-mode and model-driven configuration modes.

Values *router-name*, *vprn-svc-name*
router-name: Base, management, vpls-management, *cpm-vr-name*
vprn-svc-name: up to 64 characters
cpm-vr-name: up to 32 characters

service-name — Specifies the alias function that allows the service name to be used, converted and stored as a service ID, up to 64 characters.
The *router-instance* parameter is preferred for specifying the router or service.

bytes — Specifies the request packet size in bytes, expressed as a decimal integer.

Values 0 to 16384

Default 56

source *ip-address* — Specifies the IP address to be used.

Values
ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

timeout — Specifies the override time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of the time out, the test is marked complete and no more packets are processed for any of those request probes.

Values 1 to 10

Default 5

type-of-service — Specifies the service type.

Values 0 to 255

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

time-to-live — Specifies the TTL value for the MPLS label, expressed as a decimal integer.

Values 1 to 128

Default 64

Platforms All

13.10 icmp-query

icmp-query

Syntax **icmp-query** [**min** *minutes*] [**sec** *seconds*]
no icmp-query

Context **[Tree]** (config>service>nat>nat-policy>timeouts icmp-query)
[Tree] (config>service>nat>up-nat-policy>timeouts icmp-query)

Full Context configure service nat nat-policy timeouts icmp-query
configure service nat up-nat-policy timeouts icmp-query

Description This command configures the timeout applied to an ICMP query session.

Default icmp-query min 1

Parameters **min** *minutes* — Specifies the timeout, in minutes, applied to an ICMP query session.

Values 1 to 4

Default 1

sec *seconds* — Specifies the timeout, in seconds, applied to an ICMP query session.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.11 icmp-trace

icmp-trace

Syntax **icmp-trace** [*ip-address* | *dns-name*] [**router** *router-or-service* | **router-instance** *router-instance* | **service-name** *service-name*] [**source** *ip-address*] [**tos** *type-of-service*] [**ttl** *ttl*] [**wait** *milliseconds*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>saa>test>type icmp-trace)

Full Context configure saa test type icmp-trace

Description This command configures an ICMP traceroute test.

Parameters *ip-address* — Specifies the far-end IP address to which to send the **svc-ping** request message in dotted decimal notation.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
dns-name	up to 63 characters

dns-name — Specifies the DNS name of the far-end device to which to send the **svc-ping** request message, up to 63 characters.

router-instance — Specifies the preferred method for entering a service name. Stored as the service name. Only the service linking function is allowed for both mixed-mode and model-driven configuration modes.

Values {*router-name* | *vprn-svc-name*}
router-name: Base, management, vpls-management, *cpm-vr-name*
vprn-svc-name: up to 64 characters
cpm-vr-name: up to 32 characters

Default Base

router-or-service — Specifies the numerical reference to the router instance or service. Well known router names "Base", "management" and " vpls-management" are allowed for convenience, but are mapped numerically.

Values {*router-name* | *vprn-svc-id*}

router-name:	Base, management, vpls-management
vprn-svc-id:	1 to 2147483647

The parameter *router-instance* is preferred for specifying the router or service.

Default Base

service-name — Specifies the alias function that allows the service name to be used, converted and stored as service ID, up to 64 characters.
The parameter *router-instance* is preferred for specifying the router or service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

source *ip-address* — Specifies the IP address to be used.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
x:	[0 to FFFF]H
d:	[0 to 255]D

type-of-service — Specifies the service type.

Values 0 to 255

Default 0

ttl — Specifies the TTL value for the MPLS label, expressed as a decimal integer.

Values 1 to 255

Default 30

milliseconds — Specifies the time, in milliseconds, to wait for a response to a probe, expressed as a decimal integer.

Values 10 to 60000

Default 5000

Platforms All

13.12 icmp-tunneling

icmp-tunneling

Syntax [**no**] **icmp-tunneling**

Context **[Tree]** (config>router icmp-tunneling)

Full Context configure router icmp-tunneling

Description This command enables the tunneling of ICMP reply packets over MPLS LSP at a LSR node as per RFC 3032.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The LSR part of this feature consists of crafting the reply ICMP packet of type=11- 'time exceeded', with a source address set to a local address of the LSR node, and appending the IP header and leading payload octets of the original datagram. The system skips the lookup of the source address of the sender of the label TTL expiry packet, which becomes the destination address of the ICMP reply packet. Instead, CPM injects the ICMP reply packet in the forward direction of the MPLS LSP the label TTL expiry packet was received from. The TTL of pushed labels should be set to 255.

The source address of the ICMP reply packet is determined as follows. The LSR uses the address of the outgoing interface for the MPLS LSP. With LDP LSP or BGP LSP multiple ECMP next-hops can exist and in such a case the first outgoing interface is selected. If that interface does not have an address of the same family (IPv4 or IPv6) as the ICMP packet, then the system address of the same family is selected. If one is not configured, the packet is dropped.

When the packet is received by the egress LER, it performs a regular user packet lookup in the data path in the GRT context for BGP shortcut, 6PE, and BGP label route prefixes, or in VPRN context for VPRN and 6VPE prefixes. It then forwards it to the destination, which is the sender of the original packet which TTL expired at the LSR.

If the egress LER does not have a route to the destination of the ICMP packet, it drops the packets.

The rate of the tunneled ICMP replies at the LSR can be directly or indirectly controlled by the existing IOM level and CPM levels mechanisms. Specifically, the rate of the incoming UDP traceroute packets received with a label stack can be controlled at ingress IOM using the distributed CPU protection feature. The rate of the ICMP replies by CPM can also be directly controlled by configuring a system wide rate limit for packets ICMP replies to MPLS expired packets which are successfully forwarded to CPM using the command 'configure system security vprn-network-exceptions'. While this command's name refers to VPRN service, this feature rate limits ICMP replies for packets received with any label stack, including VPRN and shortcuts.

The 7450 ESS, 7750 SR, and 7950 XRS implementation supports appending to the ICMP reply of type Time Exceeded the MPLS label stack object defined in RFC 4950. It does not include it in the ICMP reply type of Destination unreachable.

The new MPLS Label Stack object permits an LSR to include label stack information including label value, EXP, and TTL field values, from the encapsulation header of the packet that expired at the LSR node. The ICMP message continues to include the IP header and leading payload octets of the original datagram.

In order to include the MPLS Label Stack object, SR OS implementation adds support of RFC 4884 which defines extensions for a multi-part ICMPv4/v6 message of type Time Exceeded.

The **no** form of command disables the tunneling of ICMP reply packets over MPLS LSP at a LSR node.

Default no icmp-tunneling

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.13 icmp-type

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context **[Tree]** (config>filter>ip-exception>entry>match icmp-type)
[Tree] (config>filter>ip-filter>entry>match icmp-type)
[Tree] (config>filter>ipv6-exception>entry>match icmp-type)
[Tree] (config>filter>ipv6-filter>entry>match icmp-type)

Full Context configure filter ip-exception entry match icmp-type
configure filter ip-filter entry match icmp-type
configure filter ipv6-exception entry match icmp-type
configure filter ipv6-filter entry match icmp-type

Description This command configures matching on the /ICMPv6 type field in the /ICMPv6 header of an IPv4 or IPv6 packet as a filter match criterion or configures matching on the ICMP type field in the ICMP header of an IPv4 packet as an exception filter match criterion. An entry containing Layer 4 non-zero match criteria will not match non-initial (2nd, 3rd, etc.) fragments of a fragmented packet since only the first fragment contains the Layer 4 information. Similarly an entry containing "**icmp-type** 0" match criterion, may match non-initial fragments when the Layer 4 header is not present in a packet fragment and other match criteria are also met.

The **no** form of the command removes the criterion from the match entry.

Default no icmp-type

Parameters *icmp-type* — Specifies the /ICMPv6 type value that must be present to match. Value can be expressed as a decimal integer, as well as in hexadecimal or binary format, or even using keywords. The following value shows decimal integer only.

Values 0 to 255

Platforms All

- configure filter ipv6-filter entry match icmp-type
- configure filter ip-filter entry match icmp-type

VSR

- configure filter ipv6-exception entry match icmp-type
- configure filter ip-exception entry match icmp-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match icmp-type)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match icmp-type)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match icmp-type)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match icmp-type)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match icmp-type
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match icmp-type
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match icmp-type
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match icmp-type

Description This command configures the ICMP type match condition.

The **no** form of this command reverts to the default.

Parameters *icmp-type* — Specifies the ICMP type numbers accepted in DHB.

Values [0 to 255]D, [0X0..0XFF]H, [0b0..0b11111111]B

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context **[Tree]** (config>qos>network>egress>ip-criteria>entry>match icmp-type)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match icmp-type)

Full Context configure qos network egress ip-criteria entry match icmp-type
configure qos network egress ipv6-criteria entry match icmp-type

Description This command configures matching on the ICMP or ICMPv6 type field in the ICMP or ICMPv6 header of an IPv4 or IPv6 packet as a network QoS match criterion.

An entry containing Layer 4 non-zero match criteria will not match non-initial (2nd, 3rd, etc.) fragments of a fragmented packet since only the first fragment contains the Layer 4 information. Similarly, an entry containing "**icmp-type** 0" match criterion, may match non-initial fragments when the Layer 4 header is not present in a packet fragment and other match criteria are also met.

The **no** form of the command removes the criterion from the match entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no icmp-type

Parameters *icmp-type* — Specifies the ICMP or ICMPv6 type value that must be present to match. Value can be expressed as a decimal integer, or in hexadecimal or binary format, or even using keywords.

Values 0 to 255 (Decimal)
0 to FF (Hexadecimal)
0 to 11111111 (Binary)

Platforms All

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match icmp-type)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match icmp-type)

Full Context configure system security cpm-filter ip-filter entry match icmp-type
configure system security cpm-filter ipv6-filter entry match icmp-type

Description This command configures matching on ICMP type field in the ICMP header of an IP packet as an IP filter match criterion.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of this command removes the criterion from the match entry.

Default no icmp-type

Parameters *icmp-type* — Specifies the ICMP type values that must be present to match.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.14 icmp6

icmp6

Syntax **icmp6**

Context **[Tree]** (config>service>ies>if>ipv6 icmp6)
[Tree] (config>service>vprn>if>ipv6 icmp6)

Full Context configure service ies interface ipv6 icmp6
configure service vprn interface ipv6 icmp6

Description This command configures ICMPv6 parameters for the interface.

Platforms All

icmp6

Syntax **icmp6**

Context **[Tree]** (config>router>if>ipv6 icmp6)

Full Context configure router interface ipv6 icmp6

Description Commands in this context configure ICMPv6 parameters for the interface.

Platforms All

icmp6

Syntax **icmp6** [*ip-int-name*]
no icmp6

Context **[Tree]** (debug>router>ip icmp6)

Full Context debug router ip icmp6

Description This command enables ICMPv6 debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.15 icmp6-generation

icmp6-generation

Syntax **icmp6-generation**

Context [Tree] (config>ipsec>tnl-temp icmp6-generation)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn icmp6-generation)
[Tree] (config>router>if>ipsec>ipsec-tunnel icmp6-generation)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel icmp6-generation)
[Tree] (config>service>ies>if>sap>ip-tunnel icmp6-generation)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel icmp6-generation)
[Tree] (config>service>vprn>if>sap>ip-tunnel icmp6-generation)
[Tree] (config>service>vprn>if>sap>ipsec-tun icmp6-generation)

Full Context configure ipsec tunnel-template icmp6-generation
configure router interface ipsec ipsec-tunnel dyn icmp6-generation
configure router interface ipsec ipsec-tunnel icmp6-generation
configure service ies interface ipsec ipsec-tunnel icmp6-generation
configure service ies interface sap ip-tunnel icmp6-generation
configure service vprn interface ipsec ipsec-tunnel icmp6-generation
configure service vprn interface sap ip-tunnel icmp6-generation
configure service vprn interface sap ipsec-tunnel icmp6-generation

Description This command enables the ICMPv6 packet generation configuration context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel icmp6-generation
- configure ipsec tunnel-template icmp6-generation
- configure service ies interface sap ip-tunnel icmp6-generation
- configure service vprn interface sap ip-tunnel icmp6-generation

VSR

- configure router interface ipsec ipsec-tunnel icmp6-generation
- configure service vprn interface ipsec ipsec-tunnel icmp6-generation
- configure service ies interface ipsec ipsec-tunnel icmp6-generation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.16 icmp6-query

icmp6-query

Syntax **icmp6-query** [**min** *minutes*] [**sec** *seconds*]
no icmp6-query

Context **[Tree]** (config>service>nat>firewall-policy>timeouts icmp6-query)

Full Context configure service nat firewall-policy timeouts icmp6-query

Description This command configures the timeout interval for ICMPv6 query mappings.

The **no** form of the command reverts the timeout interval to the default of 1 minute.

Default icmp6-query min 1

Parameters *minutes* — Specifies the number of minutes in the ICMP query mapping timeout interval.

Values 1 to 4

seconds — Specifies the number of seconds in the ICMP query mapping timeout interval.

Values 0 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.17 id

id

Syntax [**no**] **id** *service-id*

Context **[Tree]** (debug>service id)

Full Context debug service id

Description This command enables debugging for the specified service ID.

The **no** form of this command disables the debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

id

Syntax **id** *service-id*

Context **[Tree]** (debug>service id)

Full Context debug service id

Description This command debugs commands for a specific service.

The **no** form of the command disables debugging.

Parameters *service-id* — The ID that uniquely identifies a service.

Values service-id: 1 to 214748364
svc-name: A string up to 64 characters in length

Platforms All

13.18 id-permission

id-permission

Syntax **id-permission** {**chassis**}
no id-permission

Context **[Tree]** (cfg>eth-cfm>domain>assoc>bridge id-permission)

Full Context configure eth-cfm domain association bridge-identifier id-permission

Description This command allows the operator to include the sender-id TLV information that was specified under the **config>eth>system>sender-id** configuration for service MEPs and MIPs. When this option is present under the maintenance association, the specific MPs in the association includes the **sender-id** TLV information in ETH-CFM PDUs. MEPs include the **sender-id** TLV for CCM (not sub second CCM enabled MEPs), LBM/LBR, and LTM/LTR. MIPs includes this value in the LBR and LTR PDUs.

Note: LBR functions reflect all TLVs received in the LBM unchanged including the SenderID TLV. Transmission of the Management Domain and Management Address fields are not supported in this TLV.

Parameters **chassis** — Sends the configured chassis information defined under in the **eth-cfm>system>sender-id** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

id-permission

Syntax **id-permission** {**chassis** | **defer**}
no id-permission

Context **[Tree]** (config>eth-cfm>default-domain>bridge-identifier id-permission)

Full Context configure eth-cfm default-domain bridge-identifier id-permission

Description This command enables the inclusion of the Sender ID TLV information specified under the **config**>**eth**>**system**>**sender-id** command for installed MEPs and MIPs. The inclusion of the Sender ID TLV is based on the configured value. The Sender ID TLV is supported for ETH-CC, ETH-LB, and ETH-LB PDUs.

Note: LBR functions reflect back all TLVs received in the LBM, unchanged, including the Sender ID TLV. Transmission of the Management Domain and Management Address fields are not supported in this TLV.

The **no** form of this command disables the inclusion of the Sender ID TLV.

Default id-permission defer (config>eth-cfm>default-domain>bridge-identifier)

no id-permission (config>eth-cfm>domain>association>bridge)

Parameters **chassis** — Keyword to include the Sender ID TLV with a value equal to the *sender-id* configured under the eth-cfm>system context.

defer — Keyword to specify that **id-permission** will inherit the value from the global read-only system values.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.19 identification-strings

identification-strings

Syntax **identification-strings** *option-number* [**create**]
no identification-strings

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host identification-strings)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host identification-strings)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings
configure subscriber-mgmt local-user-db ppp host identification-strings

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies identification strings for the subscriber. This is useful when the server is centralized with Enhanced Subscriber Management (ESM) in a lower level in the network. These strings are parsed by a downstream Python script or they can be used literally if the **strings-from-option** option in the **config>subscr-mgmt>sub-ident-policy** context is set to this option number. In this case, the option number may be set to any allowed number (between 224 and 254 is suggested, as these are not dedicated to specific purposes). If the option number is not given, a default value of 254 is used. For PPPoE only, if the local user database is attached to the PPPoE node under the group interface and not to a local DHCP server, the strings are used internally so the option number is not used.

The **no** form of this command returns to the default.

Parameters *option-number* — Specifies identification strings for the subscriber.

Values 1 to 254

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.20 identifier

identifier

Syntax **identifier** *frf16-identifier*
no identifier

Context **[Tree]** (config>port>ml-bundle>mlfr identifier)

Full Context configure port multilink-bundle mlfr identifier

Description This command defines the identifier for the MLFR bundle. The **no** form of this command resets the value to null.

Default null

Parameters *frf16-identifier* — Specifies the bundle ID string. The string can be up to 49 characters long.

Platforms 7450 ESS, 7750 SR-7/12/12e

identifier

Syntax **identifier** *frf16-identifier*
no identifier

Context **[Tree]** (config>port>tdm>ds1>channel-group>frame-relay identifier)
[Tree] (config>port>tdm>e1>channel-group>frame-relay identifier)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port tdm ds1 channel-group frame-relay identifier
configure port tdm e1 channel-group frame-relay identifier

Description This command defines the identifier for a frame-relay link when used in an MLFR bundle.

The **no** form of this command resets the value to null.

Default no identifier

Parameters *frf16-identifier* — Specifies the bundle ID string. The string can be up to 49 characters long.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

identifier

Syntax **identifier** *identifier*
no identifier

Context **[Tree]** (config>system>bluetooth>module identifier)

Full Context configure system bluetooth module identifier

Description This command defines an identifier string to be used to advertise the Bluetooth module during pairing operations.

If there is no identifier specified by the user, the default is derived from the platform type, the CPM slot, and the serial number of the chassis.

For example, a device with a platform field of 7750, SR-12 chassis, and a CPM serial number of NS23456 would have a Bluetooth identifier of "7750-SR-12-CPM-A-NS23456." for the CPM in slot A.

The **no** form of the command resets the identifier back to the default.

Parameters *identifier* — Specifies string, up to 32 characters, using the values in the range 0-9, a-z, or A-Z.

Platforms 7750 SR-1, 7750 SR-s

13.21 idi

idi

Syntax **idi any**
idi ipv4-prefix {**any** | *ipv4-prefix/ipv4-prefix-length*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

idi ipv6-prefix {**any** | *ipv6-prefix/ipv6-prefix-length*}
idi string-type *string-type* **string-value** *string-value*
no idi

Context **[Tree]** (config>ipsec>client-db>client>client-id idi)

Full Context configure ipsec client-db client client-identification idi

Description This command specifies a match criteria that uses the peer's identification initiator (IDi) as the input, only one IDi criteria can be configured for a given client entry. This command supports the following matching methods:

- **idi any**: Matches any type of IDi with any value.
- **idi ipv4-prefix**: Matches an IDi with the type ID_IPV4_ADDR. If the **any** parameter is specified, then it will match any IPv4 address. If an IPv4 prefix is specified, then it will match an IPv4 address that is within the specified prefix.
- **idi ipv6-prefix**: Matches an IDi with the type ID_IPV6_ADDR. If the **any** parameter is specified, then it will match any IPv6 address. If an IPv6 prefix is specified, then it will match an IPv6 address that is within the specified prefix.
- **idi string-type**: Supports following type of IDi:
  - FQDN: Either a full match or a suffix match
  - RFC822: Either a full match or a suffix match

The **no** form of this command reverts to the default.

Default no idi

Parameters **any** — Matches any type of IDi with any value.

ipv4-prefix/ipv4-prefix-length — Matches any IPv4 address and prefix.

ipv6-prefix/ipv6-prefix-length — Matches any IPv6 address and prefix.

string-type — Matches the type of IDi value for this IPsec client entry.

Values fqdn, fqdn-suffix, rfc822, rfc822-suffix

string-value — Matches the IDi value within the client ID for this IPsec client entry up to 256 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

idi

Syntax [**no**] **idi**

Context **[Tree]** (config>ipsec>client-db>match-list idi)

Full Context configure ipsec client-db match-list idi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the Identification Initiator (IDi) type in the IPsec client matching process.

The **no** form of this command disables the IDi matching process.

Default no idi

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.22 idle-cycle-flag

idle-cycle-flag

Syntax **idle-cycle-flag** {**flags** | **ones**}
no idle-cycle-flag

Context **[Tree]** (config>port>tdm>ds1>channel-group idle-cycle-flag)
[Tree] (config>port>tdm>ds3 idle-cycle-flag)
[Tree] (config>port>tdm>e1>channel-group idle-cycle-flag)
[Tree] (config>port>tdm>e3 idle-cycle-flag)

Full Context configure port tdm ds1 channel-group idle-cycle-flag
configure port tdm ds3 idle-cycle-flag
configure port tdm e1 channel-group idle-cycle-flag
configure port tdm e3 idle-cycle-flag

Description This command configures the value that the HDLC TDM DS-0, E-1, E-3, DS-1, or DS-3 interface transmits during idle cycles. For ATM ports/channels/channel-groups, the configuration does not apply and only the no form is accepted.

The **no** form of this command reverts the idle cycle flag to the default value.

Default flags (0x7E)

no flags (ATM)

Parameters **flags** — Specifies that 0x7E is used as the idle cycle flag.

ones — Specifies that 0xFF is used as the idle cycle flag.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.23 idle-filter

idle-filter

Syntax [**no**] **idle-filter**

Context **[Tree]** (config>service>vpls>gsmp>group idle-filter)
[Tree] (config>service>vprn>gsmp>group idle-filter)

Full Context configure service vpls gsmp group idle-filter
configure service vprn gsmp group idle-filter

Description This command when applied will filter out new incoming ANCP messages while the subscriber DSL-line-state is idle. The command takes effect at the time that it is applied. Existing subscribers already in idle state are not purged from the database.

The **no** form of this command reverts to the default.

Platforms All

idle-filter

Syntax [**no**] **idle-filter**

Context **[Tree]** (config>service>vpls>gsmp idle-filter)

Full Context configure service vpls gsmp idle-filter

Description This command when applied will filter out new subscriber's ANCP messages from subscriber with "DSL-line-state" IDLE.

Default no idle-filter

idle-filter

Syntax **idle-filter**
no idle-filter

Context **[Tree]** (config>service>vprn>gsmp idle-filter)

Full Context configure service vprn gsmp idle-filter

Description This command when applied will filter out new subscriber's ANCP messages from subscriber with "DSL-line-state" IDLE.

Default no idle-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.24 idle-payload-fill

idle-payload-fill

Syntax **idle-payload-fill** {**all-ones**}
idle-payload-fill pattern *pattern*
no idle-payload-fill

Context **[Tree]** (config>port>tdm>ds1>channel-group idle-payload-fill)
[Tree] (config>port>tdm>e1>channel-group idle-payload-fill)

Full Context configure port tdm ds1 channel-group idle-payload-fill
configure port tdm e1 channel-group idle-payload-fill

Description This command defines the data pattern to be transmitted when the circuit emulation service is not operational or temporarily experiences under-run conditions. This command is only valid for cesopsn and cesopsn-cas circuit emulation services. It is blocked with a warning for unstructured (satop) circuit emulation services.

Default idle-payload-fill all-ones

Parameters **all-ones** — Defines the 8 bit value to be transmitted as 11111111.

pattern — Transmits a user-defined pattern.

Values 0 to 255, accepted in decimal, hex or binary

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

13.25 idle-signal-fill

idle-signal-fill

Syntax **idle-signal-fill** {**all-ones**}
idle-signal-fill pattern *pattern*
no idle-signal-fill

Context **[Tree]** (config>port>tdm>ds1>channel-group idle-signal-fill)
[Tree] (config>port>tdm>e1>channel-group idle-signal-fill)

Full Context configure port tdm ds1 channel-group idle-signal-fill
configure port tdm e1 channel-group idle-signal-fill

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the signaling pattern to be transmitted when the circuit emulation service is not operational or temporarily experiences under-run conditions. This command is only valid for cesopsn-cas circuit emulation services. It is blocked with a warning for unstructured (satop) and basic cesopsn circuit emulation services.

Default idle-signal-fill all-ones

Parameters **all-ones** — Defines the 8 bit value to be transmitted as 11111111.

pattern — Transmits a user-defined pattern.

Values 0 to 15, accepted in decimal, hex or binary

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

13.26 idle-time

idle-time

Syntax **idle-time** *idle*
no idle-time

Context **[Tree]** (config>system>grpc>tcp-keepalive idle-time)
[Tree] (config>system>grpc-tunnel>destination-group>tcp-keepalive idle-time)
[Tree] (config>system>telemetry>destination-group>tcp-keepalive idle-time)

Full Context configure system grpc tcp-keepalive idle-time
configure system grpc-tunnel destination-group tcp-keepalive idle-time
configure system telemetry destination-group tcp-keepalive idle-time

Description This command configures the amount of time, in seconds, that the connection must remain idle before TCP keepalive probes are sent.

The **no** form of this command reverts to the default value.

Default idle-time 600

Parameters *idle* — Specifies the number of seconds before the first TCP keepalive probe is sent.

Values 1 to 100000

Default 600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.27 idle-timeout

idle-timeout

Syntax **idle-timeout** *idle-timeout*
idle-timeout infinite
no idle-timeout

Context **[Tree]** (config>router>l2tp>group idle-timeout)
[Tree] (config>router>l2tp>group>tunnel idle-timeout)
[Tree] (config>service>vprn>l2tp idle-timeout)
[Tree] (config>service>vprn>l2tp>group idle-timeout)
[Tree] (config>service>vprn>l2tp>group>tunnel idle-timeout)

Full Context configure router l2tp group idle-timeout
configure router l2tp group tunnel idle-timeout
configure service vprn l2tp group idle-timeout
configure service vprn l2tp group tunnel idle-timeout
configure service vprn l2tp idle-timeout

Description This command configures the period of time that an established tunnel with no active sessions persists before being disconnected.

Enter the **no** form of this command to maintain a persistent tunnel.

The **no** form of this command removes the idle timeout from the configuration.

Default no idle-timeout

Parameters *idle-timeout* — Specifies the idle timeout value, in seconds until the group is removed.

Default no idle-timeout

Values 0 to 3600

infinite — Specifies that the tunnel is not closed when idle.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

idle-timeout

Syntax **idle-timeout** *timeout*
no idle-timeout

Context **[Tree]** (config>subscr-mgmt>sla-prof>cat-map>category idle-timeout)

Full Context configure subscriber-mgmt sla-profile category-map category idle-timeout

Description This command defines the idle-timeout value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *timeout* — Specifies the idle-timeout, in seconds.

Values 60 to 15552000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

idle-timeout

Syntax **idle-timeout action** *idle-timeout-action*
no idle-timeout

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range idle-timeout)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range idle-timeout)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range idle-timeout
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range idle-timeout

Description This command specifies idle-timeout behavior for DSM UEs and UEs undergoing (ISA-based) portal authentication. This knob only specifies the desired action, idle-timeout is activated by RADIUS on a per-UE basis.

The **no** form of this command resets the idle-timeout to its default

Default idle-timeout action remove

Parameters *action* — Specifies which action to perform when the idle-timeout timer goes off.

Values remove, shcv

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

idle-timeout

Syntax **idle-timeout** {*minutes* | **disable**}
no idle-timeout

Context **[Tree]** (config>system>login-control idle-timeout)

Full Context configure system login-control idle-timeout

Description This command configures the idle timeout for console, Telnet, SSH, and FTP sessions before the session is terminated by the system.

By default, each idle console, Telnet, SSH, or FTP session times out after 30 minutes of inactivity.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default idle-timeout 30

Parameters *minutes* — Specifies the idle timeout in minutes. Allowed values are 1 to 1440.

Values 1 to 1440

disable — When the **disable** option is specified, a session will never timeout. To re-enable idle timeout, enter the command without the disable option.

Platforms All

13.28 idle-timeout-action

idle-timeout-action

Syntax **idle-timeout-action** {**shcv-check** | **terminate**}
no idle-timeout-action

Context **[Tree]** (config>subscr-mgmt>sla-prof>cat-map>category idle-timeout-action)

Full Context configure subscriber-mgmt sla-profile category-map category idle-timeout-action

Description This command defines the action to be executed when the idle-timeout is reached. The action is performed for all hosts associated with the sla-profile instance.

The **no** form of this command reverts to the default.

Default idle-timeout-action terminate

Parameters **shcv-check** — Performs a subscriber host connectivity verification check (IPoE hosts only).

Note: Host connectivity verification must be enabled on the group-interface where the host is connected.

If the check is successful, the hosts are not disconnected and the idle-timeout timer is reset.

If the check fails, the hosts are deleted, similar as for **idle-timeout-action terminate**.

terminate — Deletes the subscriber host from the system: for PPP hosts, a terminate request is send; for IPoE hosts a DHCP release is send to the DHCP server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.29 ies

ies

Syntax **ies** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**name** *name*]
no ies *service-id*

Context **[Tree]** (config>service ies)

Full Context configure service ies

Description This command creates or edits an IES service instance.

The **ies** command creates or maintains an Internet Ethernet Service (IES). If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

IES services allow the creation of customer facing IP interfaces in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber must be unique between it and other addressing schemes used by the provider and potentially the entire Internet.

IP interfaces defined within the context of an IES service ID must have a SAP created as the access point to the subscriber network. This allows a combination of bridging and IP routing for redundancy purposes.

When a service is created, the **customer** keyword and *customer-id* must be specified and associates the service with a customer. The *customer-id* must already exist having been created using the **customer** command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified results in an error.

Multiple IES services are created to separate customer owned IP interfaces. More than one IES service may be created for a single customer ID. More than one IP interface may be created within a single IES service ID. All IP interfaces created within an IES service ID belongs to the same customer.

By default, no IES service instances exist until they are explicitly created.

The **no** form of this command deletes the IES service instance with the specified *service-id*. The service cannot be deleted until all the IP interfaces defined within the service ID have been shut down and deleted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — Specifies the unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every router on which this service is defined.

Values *service-id*: 1 to 214748364

svc-name: A string up to 64 characters

customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn-id — Specifies the VPN ID number used to identify virtual private networks (VPNs) by a VPN identification number.

Values 1 to 2147483647

Default **null** (0)

create — Keyword used to create the service ID. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

name *name* — This parameter configures an optional service name, up to 64 characters, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider or administrator to identify and manage services within the SR OS platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

If a name is not specified at creation time, then SR OS assigns a string version of the service-id as the name.

Service names may not begin with an integer (0 to 9).

Values *name*: up to 64 characters

Platforms All

ies

Syntax [**no**] **ies** *service-id* **interface** *ip-int-name*
[**no**] **ies** *service-id* **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name*

Context **[Tree]** (config>cflowd>collector>exp-filter>if-list>svc ies)

Full Context configure cflowd collector export-filter interface-list service ies

Description This command configures which IES service interfaces' flow data is being sent to this collector.

The **no** form of the command removes the values from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — Specifies the unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every SR OS on which this service is defined.

Values *service-id*:1 to 2147483647
svc-name:64 characters maximum

interface *ip-int-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters and must start with a letter. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

subscriber-interface *ip-int-name* — Specifies the interface name of a subscriber interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes and must start with a letter.

group-interface *ip-int-name* — Specifies the interface name of a group interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes and must start with a letter.

Platforms All

13.30 ies-vprn-only-sap-parameters

ies-vprn-only-sap-parameters

Syntax **ies-vprn-only-sap-parameters**

Context **[Tree]** (config>subscr-mgmt>msap-policy ies-vprn-only-sap-parameters)

Full Context configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters

Description Commands in this context configure managed SAP IES and VPRN properties. VPRN services are supported on the 7750 SR only.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.31 if-attribute

if-attribute

Syntax **if-attribute**

Context **[Tree]** (config>router if-attribute)
[Tree] (config>router>interface if-attribute)
[Tree] (config>service>ies>interface if-attribute)
[Tree] (config>service>vprn>interface if-attribute)

Full Context configure router if-attribute
configure router interface if-attribute
configure service ies interface if-attribute
configure service vprn interface if-attribute

Description This command creates the context to configure or apply IP interface attributes such as administrative group (admin-group) or Shared Risk Loss Group (SRLG).

Platforms All

13.32 if-num

if-num

Syntax **if-num** *if-num*
no if-num

Context **[Tree]** (config>router>mpls>if>mpls-tp-mep if-num)

Full Context configure router mpls interface mpls-tp-mep if-num

Description This command configures the MPLS-TP interface number for the MPLS interface. This is a 32-bit unsigned integer that is node-wide unique.

Parameters *if-num* — Specifies a 32-bit value that is unique to the node.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.33 if-num-validation

if-num-validation

Syntax **if-num-validation** {**enable** | **disable**}
no if-num-validation

Context **[Tree]** (config>router>mpls>if>mpls-tp-mep if-num-validation)

Full Context configure router mpls interface mpls-tp-mep if-num-validation

Description The if-num-validation command is used to enable or disable validation of the if-num in LSP Trace packet against the locally configured if-num for the interface over which the LSP Trace packet was received at the egress LER. This is because some third-party implementations may not perform interface validation for unnumbered MPLS-TP interfaces and instead set the if-num in the DSMAP TLV to 0. If the value is **enable**, the node performs the validation of the ingress and egress if-nums received in the LSP echo request messages that ingress on this MPLS-interface. It validates that the message arrives on the interface as identified by the ingress if-num, and is forwarded on the interface as identified by the egress if-num.

If the value is **disable**, no validation is performed for the ingress and egress if-nums received in the LSP echo request messages that ingress on this MPLS-interface.

Default if-num-validation enable

Parameters **enable** — Enables interface number validation.

disable — Disables interface number validation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.34 if-policy

if-policy

Syntax **if-policy** *mcac-if-policy-name*
no if-policy

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac if-policy)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac if-policy

Description This command assigns an existing MCAC interface policy to this MSAP policy.

The **no** form of this command removes the MCAC interface policy association.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mcac-if-policy-name* — Specifies an existing MCAC interface policy up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

if-policy

Syntax **if-policy** *if-policy-name*
no if-policy

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping>mcac if-policy)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping>mcac if-policy)
[Tree] (config>service>vpls>sap>igmp-snooping>mcac if-policy)
[Tree] (config>service>vpls>sap>mld-snooping>mcac if-policy)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping>mcac if-policy)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping>mcac if-policy)

Full Context configure service vpls mesh-sdp igmp-snooping mcac if-policy
configure service vpls mesh-sdp mld-snooping mcac if-policy
configure service vpls sap igmp-snooping mcac if-policy
configure service vpls sap mld-snooping mcac if-policy
configure service vpls spoke-sdp igmp-snooping mcac if-policy
configure service vpls spoke-sdp mld-snooping mcac if-policy

Description This command assigns existing MCAC interface policy to this interface. MCAC interface policy is not supported with MLD-snooping, therefore executing the command in the mld-snooping contexts will return an error.

The **no** form of this command removes the MCAC interface policy association.

Default no if-policy

Parameters *mcac-if-policy-name* — Specifies an existing MCAC interface policy

Platforms All

if-policy

Syntax **if-policy** *if-policy-name*
no if-policy

Context **[Tree]** (config>service>vprn>igmp>grp-if>mcac if-policy)
[Tree] (config>service>vprn>igmp>if>mcac if-policy)
[Tree] (config>service>vprn>mld>grp-if>mcac if-policy)
[Tree] (config>service>vprn>mld>if>mcac if-policy)
[Tree] (config>service>vprn>pim>if>mcac if-policy)

Full Context configure service vprn igmp group-interface mcac if-policy
configure service vprn igmp interface mcac if-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn mld group-interface mcac if-policy
configure service vprn mld interface mcac if-policy
configure service vprn pim interface mcac if-policy

Description This command assigns existing an MCAC interface policy to this interface.

The **no** form of this command removes the MCAC interface policy association.

Default no if-policy

Parameters *if-policy-name* — Specifies an existing MCAC interface policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface mcac if-policy
- configure service vprn mld group-interface mcac if-policy

All

- configure service vprn mld interface mcac if-policy
- configure service vprn igmp interface mcac if-policy
- configure service vprn pim interface mcac if-policy

if-policy

Syntax **ip-policy** *if-policy-name*
no if-policy

Context **[Tree]** (config>router>igmp>grp-if>mcac if-policy)
[Tree] (config>router>igmp>if>mcac if-policy)
[Tree] (config>router>mld>grp-if>mcac if-policy)
[Tree] (config>router>mld>if>mcac if-policy)
[Tree] (config>router>pim>if>mcac if-policy)

Full Context configure router igmp group-interface mcac if-policy
configure router igmp interface mcac if-policy
configure router mld group-interface mcac if-policy
configure router mld interface mcac if-policy
configure router pim interface mcac if-policy

Description This command assigns an existing MCAC interface policy to the interface.

The **no** form removes the MCAC interface policy association.

Default no if-policy

Parameters *if-policy-name* — Specifies an existing MCAC interface policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router igmp group-interface mcac if-policy
- configure router mld group-interface mcac if-policy

All

- configure router igmp interface mcac if-policy
- configure router pim interface mcac if-policy
- configure router mld interface mcac if-policy

if-policy

Syntax [**no**] **if-policy** *if-policy-name*

Context **[Tree]** (config>router>mcac if-policy)

Full Context configure router mcac if-policy

Description This command creates an MCAC interface policy and enables the context to configure parameters for the policy.

The **no** form of this command deletes the MCAC interface policy.

Parameters *if-policy-name* — Specifies the name of the MCAC interface policy, up to 32 characters.

Platforms All

13.35 ifdv-avg

ifdv-avg

Syntax [**no**] **ifdv-avg** {**forward** | **backward** | **round-trip**}

Context **[Tree]** (config>oam-pm>streaming>delay-template ifdv-avg)

Full Context configure oam-pm streaming delay-template ifdv-avg

Description This command specifies the sending of average inter-frame delay variation for a specified direction.

The **no** form of this command deletes the specified average direction.

Note: All directions can be specified if all directions are important for reporting. However, only enable those directions that are required.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **forward** — Specifies the measurement in the forward direction.

backward — Specifies the measurement in the backward direction.

round-trip — Specifies the measurement for the round trip.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.36 iff-attribute-uniform-propagation

iff-attribute-uniform-propagation

Syntax [**no**] **iff-attribute-uniform-propagation**

Context **[Tree]** (config>service>system>bgp-evpn>ip-prefix-routes iff-attribute-uniform-propagation)

Full Context configure service system bgp-evpn ip-prefix-routes iff-attribute-uniform-propagation

Description This command enables the uniform propagation of BGP attributes for EVPN Interface-ful (EVPN-IFF) routes. EVPN-IFF is used in R-VPLS services with **bgp-evpn**>**ip-route-advertisement**. When enabled, the received EVPN-IFF routes for the R-VPLS can be propagated with the original BGP path attributes into EVPN-IFL, IPVPN, EVPN-IFF (in other R-VPLS services), or BGP IP routes advertised for the attached VPRN. This command also enables the attribute propagation in the opposite direction; for example, from EVPN-IFL, IPVPN, IP, or EVPN-IFF routes into EVPN-IFF routes.

The propagation is in accordance with the uniform mode defined in *draft-ietf-bess-evpn-ipvpn-interworking*.

The **no** form of this command re-originates the BGP path attributes when propagating EVPN-IFF routes into other inter-subnet forwarding families.

Default no iff-attribute-uniform-propagation

Platforms All

13.37 iff-bgp-path-selection

iff-bgp-path-selection

Syntax **iff-bgp-path-selection** [**d-path-length-ignore**]
no iff-bgp-path-selection

Context **[Tree]** (config>service>system>bgp-evpn>ip-prefix-routes iff-bgp-path-selection)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service system bgp-evpn ip-prefix-routes iff-bgp-path-selection

Description This command enables BGP path selection for EVPN-IFF (Interface-ful) routes.

Once the command is enabled, the EVPN-IFF routes are ordered and selected in a similar manner as IPVPN or EVPN-IFL routes, that is, based on the regular BGP path selection process.

The **no** form of this command causes the system to order EVPN-IFF routes based on their {R-VPLS Ifindex, RD, Ethernet Tag}. For example, if two EVPN-IFF routes with different Route Distinguishers (RDs) are received for the same prefix on the same R-VPLS, the route with the lowest RD is selected.

Default no iff-bgp-path-selection

Parameters **d-path-length-ignore** — Keyword used to make EVPN ignore the D-PATH length when **iff-bgp-path-selection** is enabled.

Platforms All

13.38 igmp

igmp

Syntax [**no**] **igmp** [**host** *ip-address*] [**group** *grp-address*]

Context **[Tree]** (debug>mcast-mgmt>mcast-rprt-dest igmp)

Full Context debug mcast-management mcast-reporting-dest igmp

Description This command sets mcast reporting dest debug filtering options and applies only to the 7750 SR.

Platforms All

igmp

Syntax [**no**] **igmp**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync igmp)

Full Context configure redundancy multi-chassis peer sync igmp

Description This command specifies whether IGMP protocol information should be synchronized with the multi-chassis peer.

Default no igmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

igmp

Syntax [**no**] **igmp**

Context **[Tree]** (config>service>vprn igmp)

Full Context configure service vprn igmp

Description Commands in this context configure IGMP parameters.

The **no** form of this command disables IGMP.

Default no igmp

Platforms All

igmp

Syntax [**no**] **igmp**

Context **[Tree]** (config>router igmp)

Full Context configure router igmp

Description This command enables the Internet Group Management Protocol (IGMP) context. When the context is created, the IGMP protocol is enabled.

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to neighboring multicast routers. An IP multicast router can be a member of one or more multicast groups, in which case it performs both the “multicast router part” of the protocol which collects the membership information needed by its multicast routing protocol, and the “group member part” of the protocol which informs itself and other neighboring multicast routers of its memberships.

The **no** form of the command disables the IGMP instance. To start or suspend execution of IGMP without affecting the configuration, use the **no shutdown** command.

Platforms All

igmp

Syntax [**no**] **igmp**

Context **[Tree]** (config>sys>security>cpu-protection>ip>included-protocols igmp)

Full Context configure system security cpu-protection ip-src-monitoring included-protocols igmp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command includes the extracted IPv4 IGMP packets for ip-src-monitoring. IPv4 IGMP packets will be subject to the per-source-rate of CPU protection policies.

Default no igmp

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

13.39 igmp-host-tracking

igmp-host-tracking

Syntax **igmp-host-tracking**

Context **[Tree]** (config>subscr-mgmt>msap-policy igmp-host-tracking)

Full Context configure subscriber-mgmt msap-policy igmp-host-tracking

Description Commands in this context configure IGMP host tracking parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

igmp-host-tracking

Syntax **igmp-host-tracking**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap igmp-host-tracking)

Full Context configure service vprn subscriber-interface group-interface sap igmp-host-tracking

Description Commands in this context configure IGMP host tracking parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

igmp-host-tracking

Syntax **igmp-host-tracking**

Context **[Tree]** (config>service>vpls igmp-host-tracking)
[Tree] (config>service>vpls>sap igmp-host-tracking)

Full Context configure service vpls igmp-host-tracking
configure service vpls sap igmp-host-tracking

Description Commands in this context configure IGMP host tracking parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

igmp-host-tracking

Syntax **igmp-host-tracking**

Context **[Tree]** (config>service>ies igmp-host-tracking)
[Tree] (config>service>ies>sub-if>grp-if>sap igmp-host-tracking)

Full Context configure service ies igmp-host-tracking
configure service ies subscriber-interface group-interface sap igmp-host-tracking

Description Commands in this context configure IGMP host tracking parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

igmp-host-tracking

Syntax **igmp-host-tracking**

Context **[Tree]** (config>service>vprn igmp-host-tracking)
[Tree] (config>service>vprn>sap igmp-host-tracking)

Full Context configure service vprn igmp-host-tracking
configure service vprn sap igmp-host-tracking

Description Commands in this context configure IGMP host tracking parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.40 igmp-policy

igmp-policy

Syntax **igmp-policy** *policy-name* [**create**]
no igmp-policy

Context **[Tree]** (config>subscr-mgmt igmp-policy)

Full Context configure subscriber-mgmt igmp-policy

Description This command configures an IGMP policy.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the policy name up to 32 characters.

create — Keyword used to create the IGMP policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

igmp-policy

Syntax **igmp-policy** *policy-name*
no igmp-policy

Context **[Tree]** (config>subscr-mgmt>sub-prof igmp-policy)

Full Context configure subscriber-mgmt sub-profile igmp-policy

Description This command will enable IGMP processing per subscriber host. Without this command IGMP states will not be maintained per subscriber hosts. The referenced policy is defined under the **configure>subscr-mgmt** context and can be only applied via the sub-profile.

The referenced policy contains entries such as:

- description statement
- import statement — IGMP filters
- egress-rate-modify statement—HQoS Adjustment
- mcast-redirection statement—redirection to alternate interface
- static statement—definition of static IGMP groups
- version statement —IGMP version
- fast-leave statement
- max-num-groups statement—the maximum number of multicast groups allowed

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the name of the IGMP policy for the subscriber. The policy itself is defined under the **configure>sub-mgmt** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.41 igmp-snooping

igmp-snooping

Syntax **igmp-snooping**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls igmp-snooping)
[Tree] (config>service>vpls>sap igmp-snooping)
[Tree] (config>service>vpls>spoke-sdp igmp-snooping)
[Tree] (config>service>vpls>mesh-sdp igmp-snooping)
[Tree] (config>service>vpls>allow-ip-int-bind igmp-snooping)

Full Context configure service vpls allow-ip-int-bind igmp-snooping
configure service vpls igmp-snooping
configure service vpls mesh-sdp igmp-snooping
configure service vpls sap igmp-snooping
configure service vpls spoke-sdp igmp-snooping

Description This command enables the Internet Group Management Protocol (IGMP) snooping context.

Platforms All

igmp-snooping

Syntax **igmp-snooping**

Context [Tree] (config>subscr-mgmt>msap-policy>vpls-only igmp-snooping)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping

Description Commands in this context configure Internet Group Management Protocol (IGMP) snooping parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

igmp-snooping

Syntax [**no**] **igmp-snooping**

Context [Tree] (config>redundancy>multi-chassis>peer>sync igmp-snooping)

Full Context configure redundancy multi-chassis peer sync igmp-snooping

Description This command specifies whether IGMP snooping information should be synchronized with the multi-chassis peer.

Default no igmp-snooping

Platforms All

igmp-snooping

Syntax **igmp-snooping**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>service>vpls>vxlan igmp-snooping)

Full Context configure service vpls vxlan igmp-snooping

Description This command enables the Internet Group Management Protocol (IGMP) snooping context.

Platforms All

igmp-snooping

Syntax **igmp-snooping**

Context **[Tree]** (config>service>vpls>pbb>bvpls igmp-snooping)
[Tree] (config>service>vpls>pbb>bvpls>sap igmp-snooping)
[Tree] (config>service>vpls>pbb>bvpls>sdp igmp-snooping)

Full Context configure service vpls pbb backbone-vpls igmp-snooping
configure service vpls pbb backbone-vpls sap igmp-snooping
configure service vpls pbb backbone-vpls sdp igmp-snooping

Description This command configures IGMP snooping attributes for I-VPLS.

Platforms All

igmp-snooping

Syntax [**no**] **igmp-snooping**

Context **[Tree]** (debug>service>id igmp-snooping)

Full Context debug service id igmp-snooping

Description This command enables and configures IGMP-snooping debugging.

Platforms All

igmp-snooping

Syntax **igmp-snooping**

Context **[Tree]** (config>service>pw-template igmp-snooping)

Full Context configure service pw-template igmp-snooping

Description This command enables the Internet Group Management Protocol (IGMP) snooping context.

Default none

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.42 ignore-app-profile

ignore-app-profile

Syntax **ignore-app-profile**
no ignore-app-profile

Context **[Tree]** (config>subscr-mgmt>http-redirect-policy ignore-app-profile)

Full Context configure subscriber-mgmt http-redirect-policy ignore-app-profile

Description When enabled, the Alc-App-Prof-Str VSA is ignored in a RADIUS Accept that enables portal redirection using this redirect policy. AA functionality is disabled during portal authentication.

The **no** form of this command allows an Alc-App-Prof-Str to be present and enables Application Assurance during portal authentication. In this case redirection rules defined in this policy are bypassed and it is assumed the AA function is configured for portal redirection.

Default no ignore-app-profile

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.43 ignore-attached-bit

ignore-attached-bit

Syntax **ignore-attached-bit**
no ignore-attached-bit

Context **[Tree]** (config>service>vprn>isis ignore-attached-bit)

Full Context configure service vprn isis ignore-attached-bit

Description This command configures IS-IS to ignore the attached bit on received Level 1 LSPs to disable installation of default routes.

Platforms All

ignore-attached-bit

Syntax **ignore-attached-bit**
[**no**] **ignore-attached-bit**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis ignore-attached-bit)

Full Context configure router isis ignore-attached-bit

Description This command configures IS-IS to ignore the attached bit on received Level 1 LSPs to disable installation of default routes.

Platforms All

13.44 ignore-avps

ignore-avps

Syntax **ignore-avps** [**sequencing-required**]
no ignore-avps

Context [Tree] (config>router>l2tp ignore-avps)
[Tree] (config>service>vprn>l2tp ignore-avps)

Full Context configure router l2tp ignore-avps
configure service vprn l2tp ignore-avps

Description This command specifies the L2TP AVPs that should be ignored in L2TP session control.

The **no** form of this command reverts to the default.

Parameters **sequencing-required** — Ignores the [39] Sequencing Required AVP on LNS when present in the L2TP ICCN message received from LAC. By default, the session at LNS would be disconnected, in this case with the Call Disconnect Notify (CDN) error code unknownMandatoryReceive(8). Note that when configured, to ignore the Sequencing Required AVP there is no Sequence Numbers inserted into the data channel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.45 ignore-default

ignore-default

Syntax [**no**] **ignore-default**

Context [Tree] (config>service>ies>if ignore-default)
[Tree] (config>service>ies>if>ipv6 ignore-default)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>ipv6 ignore-default)
[Tree] (config>service>ies>sub-if>grp-if ignore-default)
[Tree] (config>service>vprn>sub-if>grp-if ignore-default)

Full Context configure service ies interface ignore-default
configure service ies interface ipv6 ignore-default
configure service ies subscriber-interface group-interface ignore-default
configure service ies subscriber-interface group-interface ipv6 ignore-default
configure service vprn subscriber-interface group-interface ignore-default

Description This command enables the default route when performing a uRPF check.

The **no** form of this command disables the default route.

ignore-default

Syntax [**no**] **ignore-default**

Context [Tree] (config>router>if>urpf-check ignore-default)
[Tree] (config>router>if>ipv6>urpf-check ignore-default)

Full Context configure router interface ipv6 urpf-check ignore-default
configure router interface urpf-check ignore-default

Description This command configures the uRPF check (if enabled) to ignore default routes for purposes of determining the validity of incoming packets. By default, default routes are considered eligible.

Platforms All

13.46 ignore-df-bit

ignore-df-bit

Syntax [**no**] **ignore-df-bit**

Context [Tree] (config>subscr-mgmt>loc-user-db>ppp>host ignore-df-bit)

Full Context configure subscriber-mgmt local-user-db ppp host ignore-df-bit

Description When this command is enabled for a subscriber host, the do-not-fragment (DF) bit in the IPv4 header for frames egressing the subscriber interface is ignored, the frames are fragmented according the applicable egress MTU. The DF bit is reset for frames that are fragmented.

This command applies to PPPoE PTA and L2TP LNS frames only. It is not applicable for L2TP LAC frames.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ignore-df-bit

Syntax [**no**] **ignore-df-bit**

Context **[Tree]** (config>service>ies>sub-if>grp-if ignore-df-bit)
[Tree] (config>service>vprn>sub-if>grp-if ignore-df-bit)

Full Context configure service ies subscriber-interface group-interface ignore-df-bit
configure service vprn subscriber-interface group-interface ignore-df-bit

Description This command enables the **ignore-df-bit** flag that ignores the **do-not-fragment** (DF) bit for frames egressing the WLAN-GW group interface and fragments the frame according to the applicable egress MTU. The DF bit is reset for the frames that are fragmented.

The **no** form of this command causes the router to fragment a packet larger than the MTU if the DF bit is set to 0 and drops the packet if the DF bit is set to 1.

Default no ignore-df-bit

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.47 ignore-dn-bit

ignore-dn-bit

Syntax [**no**] **ignore-dn-bit**

Context **[Tree]** (config>service>vprn>ospf ignore-dn-bit)
[Tree] (config>service>vprn>ospf3 ignore-dn-bit)

Full Context configure service vprn ospf ignore-dn-bit
configure service vprn ospf3 ignore-dn-bit

Description This command specifies whether to ignore the DN bit for OSPF LSA packets for this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets are ignored.

The **no** form of this command does not ignore the DN bit for OSPF LSA packets.

Default no ignore-dn-bit

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.48 ignore-efm-state

ignore-efm-state

Syntax [**no**] **ignore-efm-state**

Context **[Tree]** (config>port>ethernet>efm-oam ignore-efm-state)

Full Context configure port ethernet efm-oam ignore-efm-state

Description When the **ignore-efm-state** command is configured, any failure in the protocol state machine (discovery, configuration, timeout, loops, and so on) does not impact the state of the port. There is only be a protocol warning message on the port. If this optional command is not configured, the port state is affected by any existing EFM-OAM protocol fault condition.

Default no ignore-efm-state

Platforms All

13.49 ignore-l2vpn-mtu-mismatch

ignore-l2vpn-mtu-mismatch

Syntax **ignore-l2vpn-mtu-mismatch**
no ignore-l2vpn-mtu-mismatch

Context **[Tree]** (config>service>epipe ignore-l2vpn-mtu-mismatch)

Full Context configure service epipe ignore-l2vpn-mtu-mismatch

Description This command enables the router to bring up a BGP-VPWS service regardless of any MTU mismatch. The router does not check the value of the Layer 2 MTU in the Layer2 Info Extended Community received in a BGP update message against the local service MTU or locally signaled MTU.

The **no** form of this command disables the functionality. When this command is disabled, the router does not bring up a BGP-VPWS service if an MTU mismatch occurs.

Default no ignore-l2vpn-mtu-mismatch

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ignore-l2vpn-mtu-mismatch

Syntax **ignore-l2vpn-mtu-mismatch**
no ignore-l2vpn-mtu-mismatch

Context **[Tree]** (config>service>vpls ignore-l2vpn-mtu-mismatch)

Full Context configure service vpls ignore-l2vpn-mtu-mismatch

Description This command enables the router to bring up a BGP-VPLS service regardless of any MTU mismatch. The router does not check the value of the Layer 2 MTU in the Layer2 Info Extended Community received in a BGP update message against the local service MTU or locally signaled MTU.

The **no** form of this command disables the functionality. When this command is disabled, the router does not bring up a BGP-VPLS service if an MTU mismatch occurs.

Default no ignore-l2vpn-mtu-mismatch

Platforms All

13.50 ignore-lsp-errors

ignore-lsp-errors

Syntax [**no**] **ignore-lsp-errors**

Context **[Tree]** (config>router>isis ignore-lsp-errors)
[Tree] (config>service>vprn>isis ignore-lsp-errors)

Full Context configure router isis ignore-lsp-errors
configure service vprn isis ignore-lsp-errors

Description This command specifies that for this VPRN instance, ISIS will ignore LSP packets with errors. When enabled, IS-IS LSP errors will be ignored and the associated record will not be purged.

This command enables ISIS to ignore the ATT bit and therefore suppress the installation of default routes.

The **no** form of this command specifies that ISIS will not ignore LSP errors.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.51 ignore-match

ignore-match

Syntax **ignore-match**

Context **[Tree]** (config>filter>ip-filter>entry>action ignore-match)
[Tree] (config>filter>ipv6-filter>entry>action ignore-match)
[Tree] (config>filter>mac-filter>entry>action ignore-match)

Full Context configure filter ip-filter entry action ignore-match
configure filter ipv6-filter entry action ignore-match
configure filter mac-filter entry action ignore-match

Description This command sets the filter entry action to **ignore-match**, as a result this filter entry is ignored and not programmed in hardware.

Platforms All

13.52 ignore-mclt-on-takeover

ignore-mclt-on-takeover

Syntax [**no**] **ignore-mclt-on-takeover**

Context **[Tree]** (config>router>dhcp>server>failover ignore-mclt-on-takeover)
[Tree] (config>router>dhcp>server>pool>failover ignore-mclt-on-takeover)
[Tree] (config>router>dhcp6>server>failover ignore-mclt-on-takeover)
[Tree] (config>router>dhcp6>server>pool>failover ignore-mclt-on-takeover)
[Tree] (config>service>vprn>dhcp>server>failover ignore-mclt-on-takeover)
[Tree] (config>service>vprn>dhcp>server>pool>failover ignore-mclt-on-takeover)
[Tree] (config>service>vprn>dhcp6>server>failover ignore-mclt-on-takeover)
[Tree] (config>service>vprn>dhcp6>server>pool>failover ignore-mclt-on-takeover)

Full Context configure router dhcp local-dhcp-server failover ignore-mclt-on-takeover
configure router dhcp server pool failover ignore-mclt-on-takeover
configure router dhcp6 local-dhcp-server failover ignore-mclt-on-takeover
configure router dhcp6 server pool failover ignore-mclt-on-takeover
configure service vprn dhcp local-dhcp-server failover ignore-mclt-on-takeover
configure service vprn dhcp local-dhcp-server pool failover ignore-mclt-on-takeover
configure service vprn dhcp6 local-dhcp-server failover ignore-mclt-on-takeover
configure service vprn dhcp6 local-dhcp-server pool failover ignore-mclt-on-takeover

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description With this flag enabled, the remote IP address or prefix can be taken over immediately upon entering the PARTNER-DOWN state of the intercommunication link, without having to wait for the Maximum Client Lead Time (MCLT) to expire. By setting this flag, the lease times of the existing DHCP clients, while the intercommunication link is in the PARTNER-DOWN state, will still be reduced to the MCLT over time and all new lease times are set to MCLT. This behavior remains the same as originally intended for MCLT.

Some deployments require that the remote IP address/prefix range starts delegating new IP addresses and prefixes upon the failure of the intercommunication link, without waiting for the intercommunication link to transition from the COMM-INT state into the PARTNER-DOWN state and the MCLT to expire while in PARTNER-DOWN state.

This can be achieved by enabling the **ignore-mclt-on-takeover** flag and by configuring the **partner-down-delay** to 0.

Enabling this functionality must be exercised with caution. One needs to keep in mind that the partner-down-delay and MCLT timers were originally introduced to prevent IP address duplication in cases where DHCP redundant nodes transition out-of-sync due to the failure of intercommunication link. These timers (**partner-down-delay** and MCLT) would ensure that during their duration, the new IP addresses and prefixes are delegated only from one node, the one with local IP address-range/prefix. This causes the new IP address delegation to be delayed and the service is impacted.

If it can be assured that the intercommunication link is always available, then the DHCP nodes would stay in sync and the two timers would not be needed. Therefore, it is important that in this mode of operation, the intercommunication link is well protected by providing multiple paths between the two DHCP nodes. The only event that should cause intercommunication link to fail is the entire nodal failure. This failure is acceptable since in this case only one DHCP node is available to provide new IP addresses and prefixes.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.53 ignore-narrow-metric

ignore-narrow-metric

Syntax [**no**] **ignore-narrow-metric**

Context **[Tree]** (config>service>vprn>isis ignore-narrow-metric)

Full Context configure service vprn isis ignore-narrow-metric

Description This command specifies that IS-IS ignores links with narrow metrics when wide-metrics support has been enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command specifies that IS-IS does not ignore these links.

Platforms All

ignore-narrow-metric

Syntax [**no**] **ignore-narrow-metric**

Context **[Tree]** (config>router>isis ignore-narrow-metric)

Full Context configure router isis ignore-narrow-metric

Description This command specifies that IS-IS will ignore links with narrow metrics when wide-metrics support has been enabled.

The **no** form of this command specifies that IS-IS will not ignore these links.

Platforms All

13.54 ignore-nh-metric

ignore-nh-metric

Syntax [**no**] **ignore-nh-metric**

Context **[Tree]** (config>router>bgp>best-path-selection ignore-nh-metric)
[Tree] (config>service>vprn ignore-nh-metric)
[Tree] (config>service>vprn>bgp>best-path-selection ignore-nh-metric)

Full Context configure router bgp best-path-selection ignore-nh-metric
configure service vprn bgp best-path-selection ignore-nh-metric
configure service vprn ignore-nh-metric

Description This command instructs BGP to disregard the resolved distance to the BGP next-hop in its decision process for selecting the best route to a destination. When configured in the config>router>bgp>best-path-selection context, this command applies to the comparison of two BGP routes with the same NLRI learned from base router BGP peers. When configured in the config>service>vprn context, this command applies to the comparison of two BGP-VPN routes for the same IP prefix imported into the VPRN from the base router BGP instance. When configured in the config>service>vprn>bgp>best-path-selection context, this command applies to the comparison of two BGP routes for the same IP prefix learned from VPRN BGP peers.

The **no** form of this command (no ignore-nh-metric) restores the default behavior whereby BGP factors distance to the next-hop into its decision process.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no ignore-nh-metric

Platforms All

13.55 ignore-oper-down

ignore-oper-down

Syntax [**no**] **ignore-oper-down**

Context **[Tree]** (config>service>epipe>sap ignore-oper-down)

Full Context configure service epipe sap ignore-oper-down

Description This command enables the ability to ignore the operationally down status for service oper state calculation. An Epipe service does not transition to Oper State: Down when a SAP fails and when this optional command is configured under that specific SAP. Only a single SAP in an Epipe may have this optional command included. The command can be used in Epipes with or without EVPN enabled.

The **no** form of this command disables whether a service ignores the operationally down state of the SAP.

Default no ignore-oper-down

Platforms All

13.56 ignore-rapid-commit

ignore-rapid-commit

Syntax [**no**] **ignore-rapid-commit**

Context **[Tree]** (config>router>dhcp6>server ignore-rapid-commit)
[Tree] (config>service>vprn>dhcp6>server ignore-rapid-commit)

Full Context configure router dhcp6 local-dhcp-server ignore-rapid-commit
configure service vprn dhcp6 local-dhcp-server ignore-rapid-commit

Description This command enables the Rapid Commit Option for DHCP6.

The **no** form of this command disables the Rapid Commit Option.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.57 ignore-received-srv6-tlvs

ignore-received-srv6-tlvs

Syntax [**no**] **ignore-received-srv6-tlvs**

Context **[Tree]** (config>router>bgp>srv6>family ignore-received-srv6-tlvs)

Full Context configure router bgp segment-routing-v6 family ignore-received-srv6-tlvs

Description This command specifies that SRv6 TLVs are ignored when present in received routes of the associated family. In this case the route resolution is only based on the BGP next hop.

The **no** form of this command specifies that the SRv6 TLV is processed when a route of the family is received with a prefix SID attribute carrying an SRv6 TLV. In this case, a route is resolved only if both its BGP next hop and the locator prefix are reachable. The datapath programming and IGP cost to reach the next hop (used by the BGP decision process) is based on the route to the locator prefix.

Default ignore-received-srv6-tlvs

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

13.58 ignore-router-id

ignore-router-id

Syntax **ignore-router-id include-internal** *family* [*family*]
[**no**] **ignore-router-id**

Context **[Tree]** (config>router>bgp>best-path-selection ignore-router-id)
[Tree] (config>service>vprn>bgp>best-path-selection ignore-router-id)

Full Context configure router bgp best-path-selection ignore-router-id
configure service vprn bgp best-path-selection ignore-router-id

Description When the **ignore-router-id** command is present, and the current best path to a destination was learned from EBGP peer X with BGP identifier x and a new path is received from EBGP peer Y with BGP identifier y, the best path remains unchanged if the new path is equivalent to the current best path up to the BGP identifier comparison – even if y is less than x.

The **no** form of this command restores the default behavior of selecting the route with the lowest BGP identifier (y) as best.

Default no ignore-router-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *family* — Specifies up to two internal families to be included in this configuration.

Values mvpn-ipv4, mvpn-ipv6

include-internal — Specifies to ignore the router ID value even when comparing two IGBP paths or an EBGP and an IBGP path.

Platforms All

13.59 ignore-standby-signaling

ignore-standby-signaling

Syntax [**no**] **ignore-standby-signaling**

Context **[Tree]** (config>service>vpls>endpoint ignore-standby-signaling)
[Tree] (config>service>vpls>spoke-sdp ignore-standby-signaling)

Full Context configure service vpls endpoint ignore-standby-signaling
configure service vpls spoke-sdp ignore-standby-signaling

Description When this command is enabled, the node ignores the standby-bit received from the TLDP peers for the specific spoke-SDP and performs internal tasks without taking it into account.

This command is present at the endpoint level and the spoke-SDP level. If the spoke-SDP is part of the explicit-endpoint, this setting cannot be changed at the spoke-SDP level. The existing spoke-SDP will become part of the explicit-endpoint only if the setting is not conflicting. The newly created spoke-SDP, which is a part of the specified explicit-endpoint, will inherit this setting from the endpoint configuration.

Default no ignore-standby-signaling

Platforms All

13.60 ignore-tos

ignore-tos

Syntax [**no**] **ignore-tos**

Context **[Tree]** (config>service>vprn>inside>nat64 ignore-tos)

Full Context configure service vprn inside nat64 ignore-tos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies if the IPv4 Type-of-Service (ToS) is ignored and the IPv6 traffic class bits set to zero.

If this command is disabled, the system copies the IPv4 ToS into the IPv6 traffic class.

Default disabled

ignore-tos

Syntax [**no**] **ignore-tos**

Context **[Tree]** (config>service>vprn>nat>inside>nat64 ignore-tos)
[Tree] (config>router>nat>inside>nat64 ignore-tos)

Full Context configure router nat inside nat64 ignore-tos
configure service vprn nat inside nat64 ignore-tos

Description This command specifies whether the IPv4 ToS is ignored and the IPv6 traffic class bits set to zero.

When disabled, the system copies the IPv4 ToS into the IPv6 traffic class.

The **no** form of the command recognizes the IPv4 ToS.

Default disabled

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.61 igp-shortcut

igp-shortcut

Syntax **igp-shortcut** [**lfa-protect** | **lfa-only**] [**relative-metric** [*offset*]]
no igp-shortcut

Context **[Tree]** (config>router>mpls>lsp igp-shortcut)
[Tree] (config>router>mpls>lsp-template igp-shortcut)

Full Context configure router mpls lsp igp-shortcut
configure router mpls lsp-template igp-shortcut

Description This command enables the use of a specific RSVP LSP by IS-IS and OSPF routing protocols as a shortcut or as a forwarding adjacency for resolving IGP routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **igp-shortcut** or the **advertise-tunnel-link** option is enabled at the IGP instance level, all RSVP LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured in **config>router>mpls>lsp>to**, corresponds to a router-id of a remote node.

The **lfa-protect** option allows an LSP to be included in both the main SPF and the Loop-Free Alternate (LFA) SPF. For a given prefix, the LSP can be used either as a primary next-hop or as an LFA next-hop, but not both. If the main SPF computation selected a tunneled primary next-hop for a prefix, the LFA SPF will not select an LFA next-hop for this prefix and the protection of this prefix will rely on the RSVP LSP FRR protection. If the main SPF computation selected a direct primary next-hop, then the LFA SPF will select an LFA next-hop for this prefix but will prefer a direct LFA next-hop over a tunneled LFA next-hop.

The **lfa-only** option allows an LSP to be included in the LFA SPF only such that the introduction of IGP shortcuts does not impact the main SPF decision. For a given prefix, the main SPF always selects a direct primary next-hop. The LFA SPF will select a an LFA next-hop for this prefix but will prefer a direct LFA next-hop over a tunneled LFA next-hop.

When the **relative-metric** option is enabled, IGP will apply the shortest IGP cost between the endpoints of the LSP plus the value of the offset (instead of the LSP operational metric) when computing the cost of a prefix which is resolved to the LSP. The offset value is optional and it defaults to zero. The minimum net cost for a prefix is one (1) after applying the offset. The TTM continues the show the LSP operational metric as provided by MPLS. In other words, applications such as LDP-over-RSVP (when IGP shortcut is disabled) and BGP and static route shortcuts will continue to use the LSP operational metric.

The **relative-metric** option is mutually exclusive with the **lfa-protect** or the **lfa-only** options. In other words, an LSP with the **relative-metric** option enabled cannot be included in the LFA SPF, and vice-versa, when the **igp-shortcut** option is enabled in the IGP.

Finally, the **relative-metric** option is ignored when forwarding adjacency is enabled in IS-IS or OSPF. In this case, IGP advertises the LSP as a point-to-point unnumbered link along with the LSP operational metric as returned by MPLS and capped to maximum link metric allowed in that IGP. Both the main SPF and the LFA SPFs will use the local IGP database to resolve the routes.

The **no** form of this command disables the use of a specific RSVP LSP by IS-IS and OSPF routing protocols as a shortcut or a forwarding adjacency for resolving IGP routes.

Default igp-shortcut. All RSVP LSPs originating on this node are eligible by default as long as the destination address of the LSP corresponds to a router-id of a remote node.

Parameters **lfa-protect** — Specifies an LSP is included in both the main SPF and the LFA SPF.

lfa-only — Specifies an LSP is included in the LFA SPF only.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

relative-metric [*offset*] — Specifies the shortest IGP cost between the endpoints of the LSP plus the configured offset, instead of the LSP operational metric returned by MPLS, is used when calculating the cost of prefix resolved to this LSP. The offset parameter is an integer and is optional. An offset value of zero is used when the relative-metric option is enabled without specifying the offset parameter value.

Values [-10, +10]

Platforms All

igp-shortcut

Syntax **igp-shortcut**

Context **[Tree]** (config>router>isis igp-shortcut)

Full Context configure router isis igp-shortcut

Description This command enables the use of an RSVP-TE or SR-TE shortcut for resolving IGP routes by OSPF or IS-IS routing protocols.

This command instructs IGP to include RSVP LSPs and SR-TE LSPs originating on this node and terminating on the router ID of a remote node as direct links with a metric equal to the metric provided by MPLS.

During the IP reach calculation to determine the reachability of nodes and prefixes, LSPs are overlaid and the LSP metric is used to determine the subset of paths that are equal lowest cost to reach a node or a prefix. If the user enabled the **relative-metric** option for this LSP, IGP will apply the shortest IGP cost between the endpoints of the LSP plus the value of the offset, instead of the LSP operational metric, when computing the cost of a prefix that is resolved to the LSP.

When a prefix is resolved to a tunnel next-hop, the packet is sent labeled with the label stack corresponding to the NHLFE of the RSVP-TE or SR-TE LSP, as well as the explicit-null IPv6 label at the bottom of the stack in the case of an IPv6 prefix. Any network event causing one or more IGP shortcuts to go down will trigger a full SPF computation, which may result in installing a new route over an updated set of tunnel next-hops and IP next-hops.

When **igp-shortcut** is enabled at the IGP instance level, all RSVP-TE and SR-TE LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured in **config>router>mpls>lsp>to**, corresponds to a router ID of a remote node. LSPs with a destination corresponding to an interface address or any other loopback interface address of a remote node are automatically not considered by IGP. The user can, however, exclude a specific RSVP-TE or SR-TE LSP from being used as a shortcut for resolving IGP routes by entering the **config>router>mpls>lsp>no igp-shortcut** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SPF in IGP only uses RSVP LSPs as forwarding adjacencies, IGP shortcuts, or as endpoints for LDP-over-RSVP. These applications of RSVP LSPs are mutually exclusive at the IGP instance level. If two or more options are enabled in the same IGP instance, then forwarding adjacency takes precedence over the shortcut application, which takes precedence over the LDP-over-RSVP application.

The SPF in IGP uses SR-TE LSPs as IGP shortcuts only.

When ECMP is enabled on the system and multiple equal-cost paths exist for a prefix, the following selection criteria are used to pick up the set of tunnel and IP next-hops to program in the data path.

- Where a destination is a tunnel-endpoint (including external prefixes with tunnel-endpoint as the next-hop), the tunnel with lowest tunnel-index is selected (the IP next-hop is never used in this case).
- Where a destination is not a tunnel-endpoint:
  - LSPs with metric higher than underlying IGP cost between the endpoint of the LSP are excluded
  - Tunnel next-hops are preferred over IP next-hops
  - Within tunnel next-hops, the following priority applies to selection:
    i. The lowest endpoint-to-destination cost is selected
    ii. If the endpoint-to-destination costs are the same, the lowest endpoint node router ID is selected
    iii. If the router IDs are the same, the lowest tunnel index is selected
  - Within IP next-hops, the following priority applies to selection:
    i. The lowest downstream router ID is selected
    ii. If the downstream router IDs are the same, the lowest interface-index is selected

Note: Although ECMP is not performed across both the IP and tunnel next-hops, the tunnel endpoint may lie in one of the shortest IGP paths for that prefix. In that case, the tunnel next-hop is always selected as long as the prefix cost using the tunnel is equal to or lower than the IGP cost.

When both RSVP-TE and SR-TE IGP shortcuts are available, the IP reach calculation, in the unicast routing table, will first follow the above ECMP tunnel and IP next-hop selection rules when resolving a prefix over IGP shortcuts. After the set of ECMP tunnel and IP next-hops have been selected, the preference of tunnel type is then applied based on the user setting for prefix family resolution. If the user enabled resolution of the prefix family to both RSVP-TE and SR-TE tunnel types, the TTM tunnel preference value is used to select one type for the prefix. In other words, an RSVP-TE LSP type is preferred to an SR-TE LSP type on a per-prefix basis.

The ingress IOM sprays the packets for this prefix over the set of tunnel next-hops and IP next-hops based on the hashing routine currently supported for IPv4 packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This feature provides IGP with the capability to populate the multicast RTM with the prefix IP next-hop when both the **igp-shortcut** and the **multicast-import** options are enabled in IGP. The unicast RTM can still use the tunnel next-hop for the same prefix. The SPF keeps track of both the direct first hop and the tunneled first hop of a node, which is added to the Dijkstra tree.

Platforms All

igp-shortcut

Syntax **igp-shortcut**

Context **[Tree]** (config>router>ospf igp-shortcut)
[Tree] (config>router>ospf3 igp-shortcut)

Full Context configure router ospf igp-shortcut
configure router ospf3 igp-shortcut

Description This command enables the use of an RSVP-TE or SR-TE shortcut for resolving IGP routes by OSPF or IS-IS routing protocols.

This command instructs IGP to include RSVP LSPs and SR-TE LSPs originating on this node and terminating on the router ID of a remote node as direct links with a metric equal to the metric provided by MPLS.

During the IP reach calculation to determine the reachability of nodes and prefixes, LSPs are overlaid and the LSP metric is used to determine the subset of paths that are equal lowest cost to reach a node or a prefix. If the user enabled the **relative-metric** option for this LSP, IGP will apply the shortest IGP cost between the endpoints of the LSP plus the value of the offset, instead of the LSP operational metric, when computing the cost of a prefix that is resolved to the LSP.

When a prefix is resolved to a tunnel next hop, the packet is sent labeled with the label stack corresponding to the NHLFE of the RSVP-TE or SR-TE LSP, as well as the explicit-null IPv6 label at the bottom of the stack in the case of an IPv6 prefix. Any network event causing one or more IGP shortcuts to go down will trigger a full SPF computation, which may result in installing a new route over an updated set of tunnel next-hops and IP next-hops.

When **igp-shortcut** is enabled at the IGP instance level, all RSVP-TE and SR-TE LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured in **config>router>mpls>lsp>to**, corresponds to a router ID of a remote node. LSPs with a destination corresponding to an interface address or any other loopback interface address of a remote node are automatically not considered by IGP. The user can, however, exclude a specific RSVP-TE or SR-TE LSP from being used as a shortcut for resolving IGP routes by entering the **config>router>mpls>lsp>no igp-shortcut** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SPF in IGP only uses RSVP LSPs as forwarding adjacencies, IGP shortcuts, or as endpoints for LDP-over-RSVP. These applications of RSVP LSPs are mutually exclusive at the IGP instance level. If two or more options are enabled in the same IGP instance, then forwarding adjacency takes precedence over the shortcut application, which takes precedence over the LDP-over-RSVP application.

The SPF in IGP uses SR-TE LSPs as IGP shortcuts only.

When ECMP is enabled on the system and multiple equal-cost paths exist for a prefix, the following selection criteria are used to pick up the set of tunnel and IP next-hops to program in the data path.

- Where a destination is a tunnel-endpoint (including external prefixes with tunnel-endpoint as the next hop), the tunnel with lowest tunnel-index is selected (the IP next hop is never used in this case).
- Where a destination is not a tunnel-endpoint:
  - LSPs with metric higher than underlying IGP cost between the endpoint of the LSP are excluded
  - Tunnel next-hops are preferred over IP next-hops
  - Within tunnel next-hops:
    i. The lowest endpoint-to-destination cost is selected
    ii. If the endpoint-to-destination costs are the same, the lowest endpoint node router ID is selected
    iii. If the router IDs are the same, the lowest tunnel index is selected
  - Within IP next-hops:
    i. The lowest downstream router ID is selected
    ii. If the downstream router IDs are the same, the lowest interface-index is selected

Note: Although ECMP is not performed across both the IP and tunnel next-hops, the tunnel endpoint may lie in one of the shortest IGP paths for that prefix. In that case, the tunnel next hop is always selected as long as the prefix cost using the tunnel is equal or lower than the IGP cost.

When both RSVP-TE and SR-TE IGP shortcuts are available, the IP reach calculation, in the unicast routing table, will first follow the above ECMP tunnel and IP next hop selection rules when resolving a prefix over IGP shortcuts. After the set of ECMP tunnel and IP next-hops have been selected, the preference of tunnel type is then applied based on the user setting of the resolution of the family of the prefix. If the user enabled resolution of the prefix family to both RSVP-TE and SR-TE tunnel types, the TTM tunnel preference value is used to select one type for the prefix. In other words, the RSVP-TE LSP type is preferred to an SR-TE LSP type on a per-prefix basis.

The ingress IOM sprays the packets for this prefix over the set of tunnel next-hops and IP next-hops based on the hashing routine currently supported for IPv4 packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This feature provides IGP with the capability to populate the multicast RTM with the prefix IP next hop when both the **igp-shortcut** and the **multicast-import** options are enabled in IGP. The unicast RTM can still make use of the tunnel next hop for the same prefix. This change is made possible with the enhancement by which SPF keeps track of both the direct first hop and the tunneled first hop of a node which is added to the Dijkstra tree.

Platforms All

13.62 iid-tlv-enable

iid-tlv-enable

Syntax [**no**] **iid-tlv-enable**

Context **[Tree]** (config>service>vprn>isis iid-tlv-enable)

Full Context configure service vprn isis iid-tlv-enable

Description This command enables IS-IS multi-instance (MI) as described in draft-ietf-isis-mi-02. Multiple instances allow instance-specific adjacencies to be formed that support multiple network topologies on the same physical interfaces. Each instance has an LSDB, and each PDU contains a TLV identifying the instance and the topology to which the PDU belongs.

The **iid-tlv-enable** (based on draft-ietf-isis-mi-02) and **standard-multi-instance** (based on draft-ginsberg-isis-mi-bis-01) commands cannot be configured in the same instance, because the MAC addresses and PDUs in each standard are incompatible.

Default no iid-tlv-enable

Platforms All

iid-tlv-enable

Syntax [**no**] **iid-tlv-enable**

Context **[Tree]** (config>router>isis iid-tlv-enable)

Full Context configure router isis iid-tlv-enable

Description This command enables IS-IS multi-instance (MI) as described in *draft-ietf-isis-mi-02*. Multiple instances allows the formation of instance-specific adjacencies that support multiple network topologies on the same physical interfaces. Each instance has an LSDB, and each PDU contains a TLV that identifies the instance and the topology to which the PDU belongs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **iid-tlv-enable** (based on *draft-ietf-isis-mi-02*) and **standard-multi-instance** (based on *draft-ginsberg-isis-mi-bis-01*) commands cannot be configured in the same instance, because the MAC addresses and PDUs in each standard are incompatible.

The **no** form of this command disables IS-IS MI.

Platforms All

13.63 ike-auth-algorithm

ike-auth-algorithm

Syntax **ike-auth-algorithm** {**md5** | **sha1** | **sha256** | **sha384** | **sha512** | **aes-xcbc** | **auth-encryption**}

Context **[Tree]** (config>ipsec>ike-transform ike-auth-algorithm)

Full Context configure ipsec ike-transform ike-auth-algorithm

Description This command specifies the IKE authentication algorithm for the IKE transform

Default ike-auth-algorithm sha1

Parameters *auth-algorithm* — Specifies the values used to identify the hashing algorithm

Values
- **md5** — Configures the use of the hmac-md5 algorithm for authentication
- **sha1** — Configures the use of the hmac-sha1 algorithm for authentication
- **sha256** — Configures the use of the hmac-sha256 algorithm for authentication.
- **sha384** — Configures the use of the hmac-sha384 algorithm for authentication
- **sha512** — Configures the use of the hmac-sha512 algorithm for authentication.
- **aes-xcbc** — Configures the use of aes-xcbc (RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*) algorithm for authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.64 ike-encryption-algorithm

ike-encryption-algorithm

Syntax **ike-encryption-algorithm** {**des** | **3des** | **aes128** | **aes192** | **aes256** | **aes128-gcm8** | **aes128-gcm16** | **aes256-gcm8** | **aes256-gcm16**}

Context **[Tree]** (config>ipsec>ike-transform ike-encryption-algorithm)

Full Context configure ipsec ike-transform ike-encryption-algorithm

Description This command specifies the IKE encryption algorithm to be used in the IKE transform instance.

Default ike-encryption-algorithm aes128

Parameters *encryption-algorithm* — Specifies the IKE encryption algorithm.

Values

des — Configures the 56-bit des algorithm for encryption. This is an older algorithm with relatively weak security. While better than nothing, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

3des — Configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make information more secure.

aes128 — Configures the aes algorithm with a block size of 128 bits. This is a mandatory implementation size for aes. This is a very strong algorithm choice.

aes192 — Configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

aes256 — Configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

aes128-gcm8 - Configures ESP to use aes-gcm with a 128-bit key size and an 8-byte ICV for encryption and authentication.

aes128-gcm16 - Configures ESP to use aes-gcm with a 128-bit key size and a 16-byte ICV for encryption and authentication.

aes256-gcm8 - Configures ESP to use aes-gcm with a 256-bit key size and an 8-byte ICV for encryption and authentication.

aes256-gcm16 - This parameter configures ESP to use aes-gcm with a 256-bit key size and a 16-byte ICV for encryption and authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.65 ike-mode

ike-mode

Syntax **ike-mode** {**main** | **aggressive**}
no ike-mode

Context **[Tree]** (config>ipsec>ike-policy ike-mode)

Full Context configure ipsec ike-policy ike-mode

Description This command specifies one of either two modes of operation. IKE version 1 can support main mode and aggressive mode. The difference lies in the number of messages used to establish the session.

The **no** form of this command reverts to the default.

Default no ike-mode

Parameters **main** — Specifies identity protection for the hosts initiating the IPsec session. This mode takes slightly longer to complete.

aggressive — Specifies that the aggressive mode provides no identity protection but is faster.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.66 ike-policy

ike-policy

Syntax **ike-policy** *ike-policy-id* [**create**]
no ike-policy *ike-policy-id*

Context **[Tree]** (config>ipsec ike-policy)

Full Context configure ipsec ike-policy

Description Commands in this context configure an IKE policy.

The **no** form of this command

Parameters *ike-policy-id* — Specifies a policy ID value to identify the IKE policy.

Values 1 to 2048

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ike-policy

Syntax **ike-policy** *ike-policy-id*
no ike-policy

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>dyn ike-policy)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn ike-policy)
[Tree] (config>service>ies>if>sap>ipsec-gw ike-policy)
[Tree] (config>service>vprn>if>sap>ipsec-gw ike-policy)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn ike-policy)
[Tree] (config>ipsec>trans-mode-prof>dyn ike-policy)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying ike-policy
configure router interface ipsec ipsec-tunnel dynamic-keying ike-policy
configure service ies interface ipsec ipsec-tunnel dynamic-keying ike-policy
configure service ies interface sap ipsec-gw ike-policy
configure service vprn interface ipsec ipsec-tunnel dynamic-keying ike-policy
configure service vprn interface sap ipsec-gw ike-policy

Description This command specifies the ID of the IKE policy used for IKE negotiation.

The **no** form of this command removes the IKE policy ID from the configuration.

Parameters *ike-policy-id* — Specifies the IKE policy ID.

Values 1 to 2048

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-gw ike-policy
- configure ipsec ipsec-transport-mode-profile dynamic-keying ike-policy
- configure service ies interface sap ipsec-gw ike-policy

VSR

- configure router interface ipsec ipsec-tunnel dynamic-keying ike-policy
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying ike-policy
- configure service ies interface ipsec ipsec-tunnel dynamic-keying ike-policy

13.67 ike-prf-algorithm

ike-prf-algorithm

Syntax **ike-prf-algorithm** {**md5** | **sha1** | **sha256** | **sha384** | **sha512** | **aes-xcbc** | **same-as-auth**}

Context **[Tree]** (config>ipsec>ike-transform ike-prf-algorithm)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure ipsec ike-transform ike-prf-algorithm

Description This command specifies the PRF algorithm to use for IKE security association.

Note: If an authenticated encryption algorithm like AES-GCM is used for IKE encryption algorithm, **same-as-auth** cannot be used for **ike-prf-algorithm**.

Default ike-prf-algorithm same-as-auth

Parameters **md5** — This parameter configures IKE to use the **hmac-md5** algorithm for PRF.

sha1 — This parameter configures IKE to use the **hmac-sha1** algorithm for PRF.

sha256 — This parameter configures IKE to use the **hmac-sha256** algorithm for PRF.

sha384 — This parameter configures IKE to use the **hmac-sha384** algorithm for PRF.

sha512 — This parameter configures IKE to use the **hmac-sha512** algorithm for PRF.

aes-xcbc — This parameter configures IKE to use the **aes128-xcbc** algorithm for PRF.

same-as-auth — This parameter configures the same algorithm as IKE authentication algorithm.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.68 ike-transform

ike-transform

Syntax **ike-transform** *ike-transform-id* [*ike-transform-id* ...(up to 4 max)]
no ike-transform

Context **[Tree]** (config>ipsec>ike-policy ike-transform)

Full Context configure ipsec ike-policy ike-transform

Description This command specifies the IKE transform to be used in the IKE policy. Up to four IKE transforms can be specified. If multiple IDs are specified, the system selects an IKE transform based on the peer's proposal. If the system is a tunnel initiator, it uses the configured IKE transform to generate the SA payload.

Default no ike-transform

Parameters *ike-transform-id* — Specifies up to four existing IKE transform instances to be associated with this IKE policy.

Values 1 to 4096

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ike-transform

Syntax **ike-transform** *ike-transform-id* [**create**]
no ike-transform *ike-transform-id*

Context **[Tree]** (config>ipsec ike-transform)

Full Context configure ipsec ike-transform

Description This commands creates a new or enters an existing IKE transform instance. The IKE transform include following configuration for IKE SA:

- DH Group
- IKE authentication algorithm
- IKE encryption algorithm
- IKE SA lifetime

The *ike-transform-id* is referenced in the **ike-policy** configuration.

Parameters *ike-transform* — Specifies a number used to uniquely identify an IKE transform instance.

Values 1 to 4096

create — Keyword used to create the ike-transform instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.69 ike-version

ike-version

Syntax **ike-version** {**1** | **2**}

Context **[Tree]** (config>ipsec>ike-policy ike-version)

Full Context configure ipsec ike-policy ike-version

Description This command sets the IKE version (1 or 2) that the ike-policy will use.

Default ike-version 1

Parameters **1 | 2** — Specifies the version of IKE protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.70 ikev1-ph1-responder-delete-notify

ikev1-ph1-responder-delete-notify

Syntax [**no**] **ikev1-ph1-responder-delete-notify**

Context **[Tree]** (config>ipsec>ike-policy ikev1-ph1-responder-delete-notify)

Full Context configure ipsec ike-policy ikev1-ph1-responder-delete-notify

Description This command specifies the system, when deleting an IKEv1 phase 1 SA for which it was the responder, to send a delete notification to the peer. This command only applies when the configured ike-version 1. This command is ignored with IKE version 2.

The **no** form of this command reverts to the default.

Default ikev1-ph1-responder-delete-notify

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.71 ikev2-fragment

ikev2-fragment

Syntax **ikev2-fragment mtu** *octets* **reassembly-timeout** *seconds*
no ikev2-fragment

Context **[Tree]** (config>ipsec>ike-policy ikev2-fragment)

Full Context configure ipsec ike-policy ikev2-fragment

Description This command enables IKEv2 protocol level fragmentation (RFC 7383). The specified MTU is the maximum size of IKEv2 packet.

Default no ikev2-fragment

Parameters *octets* — Specifies the MTU for IKEv2 messages.

Values 512 to 9000

seconds — Specifies the timeout for reassembly.

Values 1 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.72 ilmi

ilmi

Syntax **ilmi** [*vpi/vci*]
no ilmi

Context **[Tree]** (config>port>sonet-sdh>path>atm ilmi)

Full Context configure port sonet-sdh path atm ilmi

Description This command creates an ILMI link PVCC by default on VPI/VCI 0/16. Deleting an ILMI link deletes the PVCC. ILMI is supported only on ATM interfaces on SONET/SDH paths.

Parameters *vpi/vci* — Specifies the PVC identifier (vpi/vci).

Values

vpi	0 to 4095 (NNI) 0 to 255 (UNI)
vci	1, 2, 5 to 65535

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

ilmi

Syntax **ilmi** [*port-id*]
no ilmi *port-id*

Context **[Tree]** (debug>atm ilmi)

Full Context debug atm ilmi

Description This command enables debugging for ATM ILMI.

The **no** form of this command turns off ILMI and debugging.

Parameters *port-id* — Specifies the port ID.

Values slot/mda/port [.channel] or
bundle-ima-slot/mda. bundle-num
bundle: keyword
ima: keyword
bundle-num: 1 to 56

Output The following output is an example of ATM ILMI information

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Sample Output

```
A:CHRISILMI# debug atm no ilmi 1/2/2
A:CHRISILMI# debug atm ilmi 1/2/4

In kernel:
ILMI_DEBUG_LOG {557907970}: 21:32:28
PDU DUMP (RAW):
 30 77 02 01 00 04 04 49 4c 4d 49 a4
 6c 06 07 2b 06 01 04 01 82 61 40 04
 00 00 00 00 02 01 06 02 01 02 43 03
 1b 24 b1 30 50 30 12 06 0d 2b 06 01
 04 01 82 61 02 05 01 01 01 00 02 01
 00 30 12 06 0d 2b 06 01 04 01 82 61
 02 05 01 01 03 00 02 01 21 30 12 06
 0d 2b 06 01 04 01 82 61 02 05 01 01
 02 00 02 01 00 30 12 06 0d 2b 06 01
 04 01 82 61 02 05 01 01 04 00 02 01

 00 00 00
PDU DUMP (DECODED):
  PDU Length: 123
   Community: ILMI
     Version: 1
    Msg Type: SNMP TRAP
    ObjectId: 1.3.6.1.4.1.353.2.5.1.1.1.0
    ObjectId: 1.3.6.1.4.1.353.2.5.1.1.3.0
    ObjectId: 1.3.6.1.4.1.353.2.5.1.1.2.0
    ObjectId: 1.3.6.1.4.1.353.2.5.1.1.4.0
...
```

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

13.73 ima

ima

Syntax **ima**

Context **[Tree]** (config>port>multilink-bundle ima)

Full Context configure port multilink-bundle ima

Description Commands in this context configure parameters for an Inverse Multiplexing over ATM (IMA) group. An IMA group is a collection of physical links bundled together and assigned to an ATM interface. IMA enables a high-speed channel that is composed of ATM cells to be transported as a number of lower-speed circuits. Then they are reassembled as the original high-speed ATM channel. This command is only valid for IMA bundles.

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.74 imei

imei

Syntax [**no**] **imei**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute imei)
[Tree] (config>subscr-mgmt>auth-plcy>include-radius-attribute imei)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute imei
configure subscriber-mgmt authentication-policy include-radius-attribute imei

Description This command enables the inclusion of the IMEI in AA protocols as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

imei

Syntax [**no**] **imei**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp imei)

Full Context configure subscriber-mgmt diameter-application-policy nasreq include-avp imei

Description This command enables the inclusion of the IMEI AVP, as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the AVP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.75 implicit-generation

implicit-generation

Syntax [**no**] **implicit-generation**

Context **[Tree]** (config>subscr-mgmt>auto-sub-id-key implicit-generation)

Full Context configure subscriber-mgmt auto-sub-id-key implicit-generation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description By default, the system automatically generates a subscriber identifier, using the characters A to Z and 0 to 9, that is used when a subscriber ID is not provided during the authentication of a subscriber host or session and when no explicit default **def-sub-id** is configured at the SAP or in the MSAP policy.

A subscriber ID obtained from authentication sources can conflict with the format of an implicit, automatically generated subscriber ID. When this happens, the subscriber host or session setup fails and generates the following message: “Non auto-generated sub-id 4574233754 with an auto sub-id format not allowed”. Therefore, when implicit subscriber ID generation is enabled (the default behavior), a 10-character string containing characters A to Z and 0 to 9 should not be returned from authentication sources.

The **no** form of this command disables the implicit automatic generation of subscriber IDs. When a subscriber ID is not provided in authentication and no explicit **def-sub-id** is configured, then the host or session setup fails and generates the following message: “Missing subscriber id”. A 10-character (A to Z and 0 to 9) subscriber ID format can be returned from authentication sources without the risk of conflicts.

Disabling the implicit automatic generation of subscriber IDs fail when there are active subscribers with an implicit automatically generated subscriber ID.

Enabling the implicit automatic generation of subscriber IDs fails when there are active subscribers.

Default implicit-generation

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.76 implicit-null-label

implicit-null-label

Syntax [**no**] **implicit-null-label**

Context **[Tree]** (config>router>ldp implicit-null-label)

Full Context configure router ldp implicit-null-label

Description This command enables the use of the implicit null label. Use this command to signal the implicit null option for all LDP FECs for which this node is the egress LER.

The **no** form of this command disables the signaling of the implicit null label.

Default no implicit-null-label

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

implicit-null-label

Syntax [**no**] **implicit-null-label**

Context **[Tree]** (config>router>rsvp implicit-null-label)

Full Context configure router rsvp implicit-null-label

Description This command enables the use of the implicit null label.

Signaling the IMPLICIT NULL label value for all RSVP LSPs can be enabled for which this node is the egress LER. RSVP must be shut down before being able to change this configuration option.

The egress LER does not signal the implicit null label value on P2MP RSVP LSPs. However, the Penultimate Hop Popping (PHP) node can honor a Resv message with the label value set to the implicit null.

The **no** form of this command disables the signaling of the implicit null label.

Default no implicit-null-label

Platforms All

implicit-null-label

Syntax **implicit-null-label** [**enable** | **disable**]
no implicit-null-label

Context **[Tree]** (config>router>rsvp>interface implicit-null-label)

Full Context configure router rsvp interface implicit-null-label

Description This command enables the use of the implicit null label over a specific RSVP interface.

All LSPs for which this node is the egress LER and for which the path message is received from the previous hop node over this RSVP interface will signal the implicit null label. This means that if the egress LER is also the merge-point (MP) node, then the incoming interface for the path refresh message over the bypass dictates if the packet will use the implicit null label or not. The same for a 1-to-1 detour LSP.

The user must shut down the RSVP interface before being able to change the implicit null configuration option.

The **no** form of this command returns the RSVP interface to use the RSVP level configuration value.

Default no implicit-null-label

Parameters *enable* — Enables the implicit null label.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

disable — Disables the implicit null label.

Platforms All

13.77 import

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>mld-parameters import)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>mld-parameters import)

Full Context configure subscriber-mgmt local-user-db ipoe host mld-parameters import
configure subscriber-mgmt local-user-db ppp host mld-parameters import

Description This command configures an MLD import policy.

The LUDB allows a list of up to 14 MLD import policies per host. The MLD policy also allows the configuration of an additional import policy, providing a total of 15 MLD import policies per host. The import policy inside the MLD policy is always applied last, which determines if the list is a black list or a white list. To configure an MLD white list, the import policies in the LUDB should all be allowed or forward entries and the import policy in the MLD policy should have a default action to deny all. To configure a black list, the import policies inside the LUDB should drop entries and the MLD policy import policy default action should be to forward all. The 15 import policies can be configured to be a mixed white and black list. Since it is difficult to control the order of the import policies within the LUDB, it is recommended to provision the import policy inside the MLD policy first for deterministic behavior.

The **no** form of this command removes the specified import policy.

Parameters *policy-name* — Specifies the MLD import policy, up to 32 characters, used to control the multicast group accessible for the subscriber host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>vpls>sap>igmp-snooping import)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping import)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping import)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>sap>mld-snooping import)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping import)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping import)

Full Context configure service vpls mesh-sdp igmp-snooping import
configure service vpls mesh-sdp mld-snooping import
configure service vpls sap igmp-snooping import
configure service vpls sap mld-snooping import
configure service vpls spoke-sdp igmp-snooping import
configure service vpls spoke-sdp mld-snooping import

Description This command specifies the import routing policy to be used for IGMP packets to be used on this SAP or SDP. Only a single policy can be imported on a SAP at any time.

The **no** form of this command removes the policy association from the SAP or SDP.

Default no import

Parameters *policy-name* — Specifies the routing policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the **config>router>policy-options** context The router policy must be defined before it can be imported.

Platforms All

import

Syntax **import** *policy* [*policy*]
no import

Context [Tree] (config>subscr-mgmt>bgp-prng-plcy import)

Full Context configure subscriber-mgmt bgp-peering-policy import

Description This command specifies the import policies to be used to control routes advertised to BGP neighbors. Route policies are configured in the **config>router>policy-options** context. When multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The **no** form of this command removes all route policy names from the import list.

Default no import — BGP accepts all routes from configured BGP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

Parameters *policy* — Specifies route policy statement name, up to 32 characters. Up to five policies can be specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>subscr-mgmt>igmp-policy import)

Full Context configure subscriber-mgmt igmp-policy import

Description This command specifies the import policy to filter IGMP packets.

The **no** form of this command reverts to the default value.

Parameters *policy-name* — Specifies the policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>subscr-mgmt>msap-policy>igmp-host-tracking import)

Full Context configure subscriber-mgmt msap-policy igmp-host-tracking import

Description This command specifies the import routing policy to be used for IGMP packets to be used on this SAP or SDP. Only a single policy can be imported on a single SAP at any time.

The **no** form of this command removes the policy association from the SAP or SDP.

Parameters *policy-name* — Specifies the routing policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp import)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping import

Description This command specifies the import routing policy to be used for IGMP packets to be used on this SAP or SDP. Only a single policy can be imported on a single SAP at any time.

The **no** form of this command removes the policy association from the SAP or SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the routing policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the **config>router>policy-options** context The router policy must be defined before it can be imported.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>subscr-mgmt>mld-policy import)

Full Context configure subscriber-mgmt mld-policy import

Description This command specifies the import routing policy to be used. Only a single policy can be imported at a time.

The **no** form of this command removes the policy association.

Parameters *policy-name* — Specifies the import policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the **config>router>policy-options** context The router policy must be defined before it can be imported.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-snooping import)

Full Context configure service vprn subscriber-interface group-interface sap igmp-snooping import

Description This command specifies the import routing policy to be used for IGMP packets to be used on this SAP or SDP. Only a single policy can be imported on a single SAP at any time.

The **no** form of this command removes the policy association from the SAP or SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the routing policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the config>router>policy-options context The router policy must be defined before it can be imported.

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>vpls>sap>igmp-host-tracking import)

Full Context configure service vpls sap igmp-host-tracking import

Description This command associates an import policy to filter IGMP packets.

The **no** form of this command removes the values from the configuration.

Default no import

Parameters *policy-name* — Specifies the import policy name

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>igmp-host-tracking import)

Full Context configure service ies subscriber-interface group-interface sap igmp-host-tracking import

Description This command specifies the import routing policy to be used for IGMP packets to be used on this SAP. Only a single policy can be imported on a single SAP at any time.

The **no** form of this command removes the policy association from the SAP.

Default no import — No import policy is specified.

Parameters *policy-name* — Specifies the import policy name. Values can be string up to 32 characters long of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. These policies are configured in the **config>router> policy-options** context. The router policy must be defined before it can be imported.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import

Syntax **import** *plcy-or-long-expr* [*plcy-or-expr*]
no import

Context **[Tree]** (config>service>vprn>bgp import)
[Tree] (config>service>vprn>bgp>group import)
[Tree] (config>service>vprn>bgp>group>neighbor import)

Full Context configure service vprn bgp group import
configure service vprn bgp group neighbor import
configure service vprn bgp import

Description This command is used to specify route policies that control the handling of inbound routes received from certain peers. Route policies are configured in the **config>router>policy-options** context.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in a peer-group) or neighbor level (only applies to the specified peer). The most specific level is used

The **import** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine the modifications of each route and the final action to accept or reject the route.

Only one of the 15 objects referenced by the **import** command can be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters while the remaining 14 objects have a maximum length of 64 characters each.

When multiple **import** commands are issued, the last command entered overrides the previous command.

When an import policy is not specified, BGP routes are accepted by default.

The **no** form of this command removes the policy association.

Default no import

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters).

plcy-or-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters).

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>vprn>igmp>grp-if import)
[Tree] (config>service>vprn>igmp>if import)

Full Context configure service vprn igmp group-interface import
configure service vprn igmp interface import

Description This command imports a policy to filter IGMP packets.

The **no** form of this command removes the policy association from the IGMP instance.

Default no import — No import policy specified.

Parameters *policy-name* — Specifies the import route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

The specified name(s) must already be defined.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface import

All

- configure service vprn igmp interface import

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>vprn>sap>igmp-trk import)

Full Context configure service vprn sap igmp-trk import

Description This command associates an import policy to filter IGMP packets.

The **no** form of this command removes the values from the configuration.

Default no import

Parameters *policy-name* — Specifies the import policy name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import

Syntax **import** *policy-name* [*policy-name* ... (up to 5 max)]
no import

Context **[Tree]** (config>service>vprn>isis import)

Full Context configure service vprn isis import

Description This command applies one or more (up to five) route polices as IS-IS import policies.

When a prefix received in an IS-IS LSP is accepted by an entry in an IS-IS import policy, it is installed in the routing table, if it is the most preferred route to the destination.

When a prefix received in an IS-IS LSP is rejected by an entry in an IS-IS import policy, it is not installed in the routing table, even if it has the lowest preference value among all the routes to that destination.

The flooding of LSPs is unaffected by IS-IS import policy actions.

The **no** form of this command removes all policies from the configuration.

Default no import

Parameters *policy-name* — Identifies the export route policy name. Allowed values are any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. The specified name(s) must already be defined.

Platforms All

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>vprn>mld>if import)

Full Context configure service vprn mld interface import

Description This command specifies the import route policy to be used for determining which membership reports are accepted by the router. Route policies are configured in the **config>router>policy-options** context.

When an import policy is not specified, all the MLD reports are accepted.

The **no** form of this command removes the policy association from the MLD instance.

Default no import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*...(**up to 5 max**)]
no import

Context **[Tree]** (config>service>vprn>msdp import)
[Tree] (config>service>vprn>msdp>group import)
[Tree] (config>service>vprn>msdp>group>peer import)
[Tree] (config>service>vprn>msdp>peer import)

Full Context configure service vprn msdp group import
configure service vprn msdp group peer import
configure service vprn msdp import
configure service vprn msdp peer import

Description This command specifies the policies to import source active state from Multicast Source Discovery Protocol (MSDP) into source active list.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

If you configure an import policy at the global level, each individual peer inherits the global policy.

If you configure an import policy at the group level, each individual peer in a group inherits the group's policy.

If you configure an import policy at the peer level, then policy only applies to the peer where it is configured.

The **no** form of this command removes all policies from the configuration.

Default no import

Parameters *policy-name* — Specifies the import policy name. Up to five policy-name arguments can be specified.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import

Syntax **import** {**unicast** | *ext-community*}

Context **[Tree]** (config>service>vprn>mvpn>vrf-target import)

Full Context configure service vprn mvpn vrf-target import

Description This command specifies communities to be accepted from peers.

Parameters **unicast** — Specifies to use unicast vrf-target ext-community for the multicast VPN.

ext-comm — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values

target:{*ip-address*:*comm-val* | *2byte-asnumber:ext-comm-val* | 4byte-asnumber:comm-val}

ip-address:	a.b.c.d
comm-val:	0 to 65535
2byte-asnumber:	1 to 65535
4byte-asnumber	0 to 4294967295

Platforms All

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context **[Tree]** (config>service>vprn>ospf>area import)
[Tree] (config>service>vprn>ospf3>area import)

Full Context configure service vprn ospf area import
configure service vprn ospf3 area import

Description This command configures ABR import policies to filter OSPFv2 Type 3 Summary-LSAs or OSPFv3 Inter-Area-Prefix-LSA between areas, to only permit the specified routes from being imported into an area.

This command cannot be used in OSPF area 0.

The **no** form of this command reverts to the default value.

Default no import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the export route policy name. A maximum of five policy names can be specified. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified policy names must be predefined and already exist in the system.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context **[Tree]** (config>service>vprn>ospf import)
[Tree] (config>service>vprn>ospf3 import)

Full Context configure service vprn ospf import
configure service vprn ospf3 import

Description This command applies one or more (up to five) route polices as OSPF import policies. When a prefix received in an OSPF LSA is accepted by an entry in an OSPF import policy it is installed in the routing table if it is the most preferred route to the destination. When a prefix received in an OSPF LSA is rejected by an entry in an OSPF import policy it is not installed in the routing table, even if it has the lowest preference value among all the routes to that destination. The flooding of LSAs is unaffected by OSPF import policy actions. This command only applies to the 7750 SR.

Default If an OSPF route has the lowest preference value among all routes to a destination it is installed in the routing table.

Parameters *policy-name* — Specifies the import route policy name. A maximum of five policy names can be specified. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

The specified policy name(s) must be predefined and already exist in the system.

Platforms All

import

Syntax **import** {**join-policy** | **register-policy**} *policy-name* [*policy-name* **...**(**up to 5 max**)]
no import {**join-policy** | **register-policy**}

Context **[Tree]** (config>service>vprn>pim import)

Full Context configure service vprn pim import

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the import route policy to be used for determining which routes are accepted from peers. Route policies are configured in the **config>router>policy-options** context. When an import policy is not specified, BGP routes are accepted by default.

The **no** form of this command removes the policy association from the IGMP instance.

Default no import join-policy

no import register-policy

Parameters **join-policy** — Use this command to filter PIM join messages which prevents unwanted multicast streams from traversing the network.

register-policy — This keyword filters register messages. PIM register filters prevent register messages from being processed by the RP. This filter can only be defined on an RP. When a match is found, the RP immediately sends back a register-stop message.

policy-name — Specifies the route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*...(**up to 5 max**)]
no import

Context **[Tree]** (config>service>vprn>rip import)
[Tree] (config>service>vprn>rip>group import)
[Tree] (config>service>vprn>rip>group>neighbor import)
[Tree] (config>service>vprn>ripng import)
[Tree] (config>service>vprn>ripng>group import)
[Tree] (config>service>vprn>ripng>group>neighbor import)

Full Context configure service vprn rip group import
configure service vprn rip group neighbor import
configure service vprn rip import
configure service vprn ripng group import
configure service vprn ripng group neighbor import
configure service vprn ripng import

Description This command configures import route policies to determine routes that will be accepted from RIP neighbors. If no import policy is specified, RIP accepts all routes from configured RIP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If multiple policy names are specified, the policies are evaluated in the order that they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no import

Parameters *policy-name* — The import route policy name. Allowed values are any string up to 32 characters in length and composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. The specified names must already be defined.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context **[Tree]** (config>router>ldp import)

Full Context configure router ldp import

Description This command configures import route policies to determine which label bindings (FECs) are accepted from LDP neighbors. Policies are configured in the **config>router>policy-options** context.

If no import policy is specified, LDP accepts all label bindings from configured LDP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of this command removes all policies from the configuration.

Default no import

Parameters *policy-name* — Specifies up to five import route policy names, up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>router>igmp>group-interface import)
[Tree] (config>router>igmp>if import)

Full Context configure router igmp group-interface import
configure router igmp interface import

Description This command applies the referenced IGMP policy (filter) to an interface subscriber or a group-interface. An IGMP filter is also known as a black/white list and it is defined under the **config>router>policy-options**.

When redirection is applied, only the import policy from the subscriber will be in effect. The import policy under the group interface is applicable only for IGMP states received directly on the SAP (AN in IGMP proxy mode).

The **no** form of the command removes the policy association from the IGMP instance.

Default no import

Parameters *policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface import

All

- configure router igmp interface import

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>router>mld>if import)
[Tree] (config>router>mld>group-interface import)

Full Context configure router mld group-interface import
configure router mld interface import

Description This command specifies the import route policy to determine which membership reports are accepted by the router. Route policies are configured in the **config>router>policy-options** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an import policy is not specified, all the MLD reports are accepted.

The **no** form of this command removes the policy association from the MLD instance.

Default no import

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router mld group-interface import

All

- configure router mld interface import

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context **[Tree]** (config>router>msdp import)
[Tree] (config>router>msdp>peer import)
[Tree] (config>router>msdp>group import)
[Tree] (config>router>msdp>group>peer import)

Full Context configure router msdp group import
configure router msdp group peer import
configure router msdp import
configure router msdp peer import

Description This command specifies the policies to import source active state from Multicast Source Discovery Protocol (MSDP) into source active list.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

If an import policy is configured at the global level, each individual peer inherits the global policy.

If an import policy is configured at the group level, each individual peer in a group inherits the group's policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If an import policy is configured at the peer level, then policy only applies to the peer where it is configured.

The **no** form of the command applies no import policies and all source active messages are allowed.

Default no import

Parameters *policy-name* — Specifies the import policy name, up to 32 characters. Up to five policy-name arguments can be specified.

Platforms All

import

Syntax **import** {**join-policy** | **register-policy**} [*policy-name* [*policy-name*]]
no import {**join-policy** | **register-policy**}

Context **[Tree]** (config>router>pim import)

Full Context configure router pim import

Description This command specifies the import route policy to be used. Route policies are configured in the **config>router>policy-options** context.

When an import policy is not specified, BGP routes are accepted by default. Up to five import policy names can be specified.

The **no** form of this command removes the policy association from the instance.

Default no import

Parameters **join-policy** — Filters PIM join messages which prevents unwanted multicast streams from traversing the network.

register-policy — Filters register messages. PIM register filters prevent register messages from being processed by the RP. This filter can only be defined on an RP. When a match is found, the RP immediately sends back a register-stop message.

policy-name — Specifies the route policy name, up to 32 characters. Route policies are configured in the **config>router>policy-options** context.

Platforms All

import

Syntax **import** *policy-name*
no import

Context **[Tree]** (config>service>pw-template>igmp-snooping import)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service pw-template igmp-snooping import

Description This command specifies the import routing policy to be used for IGMP packets. Only a single policy can be imported at a time.

The **no** form of the command removes the policy association.

Default no import

Parameters *policy-name* — Specifies the import policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the config>router>policy-options context The router policy must be defined before it can be imported.

Platforms All

import

Syntax **import type** {**cert** | **key** | **crl**} **input** *url-string* **output** *filename* **format** *input-format* [**password** [*32 chars max*]]

Context **[Tree]** (admin>certificate import)

Full Context admin certificate import

Description This command converts an input file (key/certificate/CRL) to a system format file. The following list summarizes the formats supported by this command:

- Certificate
  - PKCS #12
  - PKCS #7 PEM encoded
  - PKCS #7 DER encoded
  - PEM
  - DER
- Key
  - PKCS #12
  - PEM
  - DER
- CRL
  - PKCS #7 PEM encoded
  - PKCS #7 DER encoded
  - PEM
  - DER

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: If there are multiple objects with the same type in the input file, only the first object is extracted and converted.

Parameters **input** *url-string* — Specifies the URL for the input file. This URL could be either a local CF card URL file or a FP URL to download the input file.

Values

url-string	<local-url> up to 99 characters
local-url	<cflash-id>/<file-path>
cflash-id	cf1:| cf2:| cf3:

output *filename* — Specifies the name of output file up to 95 characters. The output directory depends on the file type like following:

- Key: cf3:\system-pki\key
- Cert: cf3:\system-pki\cert
- CRL: cf3:\system-pki\CRL

type — The type of input file.

Values cert, key, crl

format — Specifies the format of input file.

Values pkcs12, pkcs7-der, pkcs7-pem, pem, der

password — Specifies the password to decrypt the input file in case that it is an encrypted PKCS#12 file.

Platforms All

import

Syntax **import** *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]]
no import

Context **[Tree]** (config>router>bgp import)
[Tree] (config>router>bgp>group import)
[Tree] (config>router>bgp>group>neighbor import)

Full Context configure router bgp group import
configure router bgp group neighbor import
configure router bgp import

Description This command specifies route policies that control the handling of inbound routes received from certain peers. Route policies are configured in the **config>router>policy-options** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific level is used.

The **import** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine the modifications of each route and the final action to accept or reject the route.

Only one of the 15 objects referenced by the **import** command is allowed to be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters; the remaining 14 objects have a maximum length of 64 characters each.

When multiple **import** commands are issued, the last command entered overrides the previous command.

When an import policy is not specified, BGP routes are accepted by default.

The **no** form of this command removes the policy association.

Default no import

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters long) or a policy logical expression (up to 255 characters long). Allowed values are any string up to 255 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

plcy-or-expr — Specifies the route policy name (up to 64 characters long) or a policy logical expression (up to 64 characters long). Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context **[Tree]** (config>router>isis import)

Full Context configure router isis import

Description This command specifies up to five route polices as IS-IS import policies.

When a prefix received in an IS-IS LSP is accepted by an entry in an IS-IS import policy, it is installed in the routing table, if it is the most preferred route to the destination.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a prefix received in an IS-IS LSP is rejected by an entry in an IS-IS import policy, it is not installed in the routing table, even if it has the lowest preference value among all the routes to that destination.

The flooding of LSPs is unaffected by IS-IS import policy actions.

The **no** form of this command removes all policies from the configuration.

Default no import

Parameters *policy-name* — Specifies the import route policy name. Allowed values are any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified names must already be defined.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context **[Tree]** (config>router>ospf import)
[Tree] (config>router>ospf3 import)

Full Context configure router ospf import
configure router ospf3 import

Description This command applies one or more (up to 5) route polices as OSPF import policies. When a prefix received in an OSPF LSA is accepted by an entry in an OSPF import policy, it is installed in the routing table if it is the most preferred route to the destination. When a prefix received in an OSPF LSA is rejected by an entry in an OSPF import policy, it is not installed in the routing table, even if it has the lowest preference value among all the routes to that destination. The flooding of LSAs is unaffected by OSPF import policy actions. The **no** form of this command removes all policies from the configuration.

Default no import

Parameters *policy-name* — Specifies up to 5 export route policy names. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified names must already be defined.

Platforms All

import

Syntax [**no**] **import** *policy-name* [*policy-name*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ospf>area import)
[Tree] (config>router>ospf3>area import)

Full Context configure router ospf area import
configure router ospf3 area import

Description This command configures ABR import policies to filter OSPFv2 Type 3 Summary-LSAs or OSPFv3 Inter-Area-Prefix-LSA between areas, in order to only permit the specified routes from being imported into an area.

This command cannot be used in OSPF area 0.

The **no** form of this command reverts to the default value.

Default no import

Parameters *policy-name* — Specifies up to five import route policy names. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified names must already be defined.

Platforms All

import

Syntax **import** *policy-name* [*policy-name*]
no import

Context [Tree] (config>router>rip import)
[Tree] (config>router>rip>group import)
[Tree] (config>router>rip>group>neighbor import)
[Tree] (config>router>ripng import)
[Tree] (config>router>ripng>group import)
[Tree] (config>router>ripng>group>neighbor import)

Full Context configure router rip group import
configure router rip group neighbor import
configure router rip import
configure router ripng group import
configure router ripng group neighbor import
configure router ripng import

Description This command configures import route policies to determine which routes are accepted from RIP neighbors. If no import policy is specified, RIP accepts all routes from configured RIP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

Default no import

Parameters *policy-name* — Specifies up to five import route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified names must already be defined.

Platforms All

13.78 import-grt

import-grt

Syntax **import-grt** *plcy-or-long-expr* [*plcy-or-expr*]
no import-grt

Context **[Tree]** (config>service>vprn>grt import-grt)

Full Context configure service vprn grt-lookup import-grt

Description This command associates policies to control the leaking of GRT routes into the associated VPRN.

The GRT route must have first been leaked by a **leak-export** policy defined under the **config>router** context. Then the route must match a route entry in the specified **import-grt** policy with an accept action. Refer to the *IP Router Configuration Command Reference* section in the *7750 SR Extensible Routing System Virtualized Service Router*.

The **no** form of this command removes route leaking policy associations and disables the leaking of GRT routes into the local VPRN.

Parameters *plcy-or-long-expr* — Specifies route policy names, up to 64 characters, or a policy logical expression, up to 255 characters.

Values *plcy-or-long-expr*: *policy-name* | *long-expr*
policy-name: up to 64 characters
long-expr: up to 255 characters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

plcy-or-expr — Specifies up to four route policy names, up to 64 characters, or a policy logical expression, up to 64 characters.

Values *plcy-or-expr*: *policy-name* | *expr*
policy-name: up to 64 characters
expr: up to 64 characters

Platforms All

13.79 import-mcast-policy

import-mcast-policy

Syntax **import-mcast-policy** *policy-name* [*policy-name*]
no import-mcast-policy

Context **[Tree]** (config>router>ldp import-mcast-policy)

Full Context configure router ldp import-mcast-policy

Description This command configures an import policy for mLDP FECs arriving on the node. This command does not work for self-generated mLDP FECs. The action of the policy will accept or reject the FEC. If the FEC is rejected, it will be kept but is not resolved.

The **no** form of this command removes all policies from the configuration.

Default no import-mcast-policy

Parameters *policy-name* — Specifies up to five import route policy names, up to 32 characters, to be assigned to mLDP. The specified name(s) must already be defined.

Platforms All

13.80 import-pmsi-routes

import-pmsi-routes

Syntax **import-pmsi-routes**

Context **[Tree]** (config>router>ldp import-pmsi-routes)

Full Context configure router ldp import-pmsi-routes

Description Commands in this context configure import-pmsi-routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For option B, the leafs or ABR/ASBR that are not directly connected to the root have no visibility of the root. As such, for LDP to build the recursive FEC it needs to cache the MVPN PMSI AD routes, this command gives the user the ability to manually enable caching of MVPN PMSI AD routes internally in LDP for EVPN or MVPN inter-as or **mvpn_no_export_community** intra-as.

Platforms All

13.81 import-prefixes

import-prefixes

Syntax [**no**] **import-prefixes** *policy-name*

Context **[Tree]** (config>router>ldp>session-params>peer import-prefixes)

Full Context configure router ldp session-parameters peer import-prefixes

Description This command configures the import FEC prefix policy to determine which prefixes received from this LDP peer are imported and installed by LDP on this node. If resolved these FEC prefixes are then re-distributed to other LDP and T-LDP peers. A FEC prefix that is filtered out (deny) will not be imported. A FEC prefix that is filtered in (accept) will be imported.

If no import policy is specified, the node will import all prefixes received from this LDP/T-LDP peer. This policy is applied in addition to the global LDP policy and targeted session policy.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified. Peer address has to be the peer LSR-ID address.

The **no** form of the command removes the policy from the configuration.

Default no import-prefixes - no import route policy is specified

Parameters *policy-name* — Specifies up to five import-prefix route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined.

Platforms All

import-prefixes

Syntax **import-prefixes** *policy-name* [*policy-name*]
no import-prefixes

Context **[Tree]** (config>router>ldp>targeted-session import-prefixes)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ldp targeted-session import-prefixes

Description This command configures the import route policy to determine which FEC prefix label bindings are accepted from targeted LDP neighbors into this node. A label binding that is filtered out (deny) will not be imported. A route that is filtered in (accept) will be imported.

If no import policy is specified, this node session will accept all bindings from configured targeted LDP neighbors. This policy is applied in addition to the global LDP policy.

Policies are configured in the **config>router>policy-option**s context. A maximum of five policy names can be specified.

The **no** form of this command removes the policy from the configuration.

Parameters *policy-name* — Specifies up to five import policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

13.82 import-tunnel-table

import-tunnel-table

Syntax **import-tunnel-table** *policy-name* [*policy-name*]
no import-tunnel-table

Context **[Tree]** (config>router>ldp import-tunnel-table)

Full Context configure router ldp import-tunnel-table

Description This command controls the import, in the tunnel table, of LDP tunnels to non-host prefixes. This command is only intended for importing tunnels; it cannot be used for preventing the import of any specific prefix and only non-host prefixes will be considered when evaluating this policy in this context. The LDP tunnels to these non-host prefixes must be created before they can be imported.

This command does not affect the automatic import of LDP tunnels to host prefixes.

The **no** version of this command removes all of the import policies and, by consequence, any tunnels to non-host prefixes from the tunnel table. If a non-host prefix tunnel is currently being used for forwarding, disabling this command may be service-impacting.

Default no import-tunnel-table

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies up to five import route policy names. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified policy names must already be defined.

Platforms All

13.83 imported-format

imported-format

Syntax **imported-format** {**any** | **secure**}

Context **[Tree]** (config>system>security>pki imported-format)

Full Context configure system security pki imported-format

Description This command specifies the allowed format of imported certificates or keys in the cf3:/system-pki directory.

Default imported-format any

Parameters **any** — Allows any imported format.

secure — Only allows enhanced secure imported formats.

Platforms All

13.84 improved-assert

improved-assert

Syntax [**no**] **improved-assert**

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>pim improved-assert)

Full Context configure service vprn mvpn provider-tunnel inclusive pim improved-assert

Description This command enables improved assert procedure on the PIM inclusive provider tunnel.

The **no** form of this command disables improved assert procedure.

Default enabled

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

improved-assert

Syntax [**no**] **improved-assert**

Context **[Tree]** (config>service>vprn>pim>if improved-assert)

Full Context configure service vprn pim interface improved-assert

Description This command enables improved assert processing on this interface. The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes.

The assert process is started when data is received on an outgoing interface. This could impact performance if data is continuously received on an outgoing interface.

When enabled, the PIM assert process is done entirely on the control-plane with no interaction between the control and forwarding plane.

Default improved-assert

Platforms All

improved-assert

Syntax [**no**] **improved-assert**

Context **[Tree]** (config>router>pim>interface improved-assert)

Full Context configure router pim interface improved-assert

Description This command enables improved assert processing. The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes. The assert process is started when data is received on an outgoing interface meaning that duplicate traffic is forwarded to the LAN until the forwarder is negotiated among the routers.

When the **improved-assert** command is enabled, the PIM assert process is done entirely in the control plane. The advantages are that it eliminates duplicate traffic forwarding to the LAN. It also improves performance since it removes the required interaction between the control and data planes.

Note: improved-assert is still fully interoperable with the RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)* and RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM)*, implementations. However, there may be conformance tests that may fail if the tests expect control-data plane interaction in determining the assert winner. Disabling the **improved-assert** command when performing conformance tests is recommended.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default improved-assert

Platforms All

13.85 imsi

imsi

Syntax [**no**] **imsi** *imsi*

Context **[Tree]** (debug>gtp imsi)

Full Context debug gtp imsi

Description This command restricts debugging to only data related to the specified IMSI. This command can be repeated multiple times, where only data for any of the specified IMSIs is debugged.

The **no** form of this command removes the filter for the specified IMSI. If the last IMSI filter is removed, all data is debugged again, but may be restricted by other filters.

Parameters *imsi* — Specifies the mobile subscriber identity, as a string of up to 15 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

imsi

Syntax [**no**] **imsi**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute imsi)
[Tree] (config>subscr-mgmt>auth-plcy>include-radius-attribute imsi)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute imsi
configure subscriber-mgmt authentication-policy include-radius-attribute imsi

Description This command includes the IMSI RADIUS attribute for FWA sessions.

The **no** form of this command excludes the RADIUS IMSI attribute.

Default no imsi

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.86 imsi-apn-filter

imsi-apn-filter

Syntax **imsi-apn-filter**

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter imsi-apn-filter)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter imsi-apn-filter

Description This command configures a TCA for the counter capturing hits due to the GTP IMSI-APN filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

imsi-apn-filter

Syntax **imsi-apn-filter**

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr imsi-apn-filter)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter

Description This command specifies the context for configuring IMSI and APN filtering.

The **gtpc-inspection** command must be enabled before using this command.

This command applies only to the GTP packets that contain IMSI or APN information elements (IEs).

Default None - No APN or IMSI filtering is performed.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.87 in-band-control-path

in-band-control-path

Syntax **in-band-control-path**

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring in-band-control-path)
[Tree] (config>redundancy>mc>peer>mc>l3-ring in-band-control-path)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring in-band-control-path
configure redundancy multi-chassis peer mc-ring ring in-band-control-path

Description Commands in this context configure control path parameters.

The **no** form of this command reverts to the default.

Platforms All

13.88 in-label

in-label

Syntax **in-label** *in-label* **out-label** *out-label* **out-link** *if-name* [**next-hop** *next-hop*]
no in-label

Context **[Tree]** (config>router>mpls>mpls-tp>transit-path>forward-path in-label)
[Tree] (config>router>mpls>mpls-tp>transit-path>reverse-path in-label)

Full Context configure router mpls mpls-tp transit-path forward-path in-label
configure router mpls mpls-tp transit-path reverse-path in-label

Description This command configures the label mapping associated with a forward path or reverse path of an MPLS-TP transit path to be configured.

The incoming label, outgoing label and outgoing interface must be configured, using the **in-label**, **out-label** and **out-link** parameters. If the out-link refers to a numbered IP interface, the user may optionally configure the **next-hop** parameter and the system will determine the interface to use to reach the configured next-hop, but will check that the user-entered value for the *out-link* corresponds to the link returned by the system. If they do not correspond, then the path will not come up.

Default no in-label

Parameters *in-label* — Specifies the in label.

Values 32 to 16415

out-label — Specifies the out label.

Values 32 to 16415

if-name — Specifies the name of the outgoing interface use for the path.

next-hop — Specifies the next-hop.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

in-label

Syntax **in-label** *in-label*
no in-label

Context **[Tree]** (config>router>mpls>lsp>working-tp-path in-label)
[Tree] (config>router>mpls>lsp>protect-tp-path in-label)

Full Context configure router mpls lsp protect-tp-path in-label
configure router mpls lsp working-tp-path in-label

Description This command configures the incoming label for the reverse path or the working path or the protect path of an MPLS-TP LSP. MPLS-TP LSPs are bidirectional, and so an incoming label value must be specified for each path.

Default no in-label

Parameters *in-label* — Specifies the in label.

Values 32 to 16415

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.89 in-plus-profile-octets-discarded-count

in-plus-profile-octets-discarded-count

Syntax [**no**] **in-plus-profile-octets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-plus-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters
in-plus-profile-octets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters
in-plus-profile-octets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters
in-plus-profile-octets-discarded-count

Description This command includes the in-plus profile octets discarded count.

The **no** form of this command excludes the in-plus profile octets discarded count.

Default no in-plus-profile-octets-discarded-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.90 in-plus-profile-octets-forwarded-count

in-plus-profile-octets-forwarded-count

Syntax [**no**] **in-plus-profile-octets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-plus-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-plus-profile-octets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters in-plus-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters in-plus-profile-octets-forwarded-count

Description This command includes the in-plus profile octets forwarded count.

The **no** form of this command excludes the in-plus profile octets forwarded count.

Default no in-plus-profile-octets-forwarded-count

Platforms All

13.91 in-plus-profile-octets-offered-count

in-plus-profile-octets-offered-count

Syntax [**no**] **in-plus-profile-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-plus-profile-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-plus-profile-octets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters in-plus-profile-octets-offered-count
configure log accounting-policy custom-record ref-policer e-counters in-plus-profile-octets-offered-count

Description This command includes the in-plus profile octets offered count.

The **no** form of this command excludes the in-plus profile octets offered count.

Default no in-plus-profile-octets-offered-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

13.92 in-plus-profile-packets-discarded-count

in-plus-profile-packets-discarded-count

Syntax [**no**] **in-plus-profile-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-plus-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-plus-profile-packets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters in-plus-profile-packets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters in-plus-profile-packets-discarded-count

Description This command includes the in-plus profile packets discarded count.

The **no** form of this command excludes the in-plus profile packets discarded count.

Default no in-plus-profile-packets-discarded-count

Platforms All

13.93 in-plus-profile-packets-forwarded-count

in-plus-profile-packets-forwarded-count

Syntax [**no**] **in-plus-profile-packets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-plus-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-plus-profile-packets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters in-plus-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters in-plus-profile-packets-forwarded-count

Description This command includes the in-plus profile packets forwarded count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command excludes the in-plus profile packets forwarded count.

Default no in-plus-profile-packets-forwarded-count

Platforms All

13.94 in-plus-profile-packets-offered-count

in-plus-profile-packets-offered-count

Syntax [**no**] **in-plus-profile-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-plus-profile-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-plus-profile-packets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters in-plus-profile-packets-offered-count
configure log accounting-policy custom-record ref-policer e-counters in-plus-profile-packets-offered-count

Description This command includes the in-plus profile packets offered count.

The **no** form of this command excludes the in-plus profile packets offered count.

Default no in-plus-profile-packets-offered-count

Platforms All

13.95 in-profile-octets-discarded-count

in-profile-octets-discarded-count

Syntax [**no**] **in-profile-octets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-counters in-profile-octets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-counters in-profile-octets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters in-profile-octets-discarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters in-profile-octets-discarded-count

Description This command includes the in-profile octets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv4 octets discarded count instead.

The **no** form of this command excludes the in-profile octets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

in-profile-octets-discarded-count

Syntax [**no**] **in-profile-octets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters in-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters in-profile-octets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters in-profile-octets-discarded-count
configure log accounting-policy custom-record queue e-counters in-profile-octets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters in-profile-octets-discarded-count
configure log accounting-policy custom-record ref-queue e-counters in-profile-octets-discarded-count

Description This command includes the in-profile octets discarded count.

The **no** form of this command excludes the in-profile octets discarded count.

Default no in-profile-octets-discarded-count

Platforms All

in-profile-octets-discarded-count

Syntax [**no**] **in-profile-octets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters in-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters in-profile-octets-discarded-count)

Full Context configure log accounting-policy custom-record policer i-counters in-profile-octets-discarded-count
configure log accounting-policy custom-record ref-policer i-counters in-profile-octets-discarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command includes the in-profile octets discarded count.

The **no** form of this command excludes the in-profile octets discarded count.

Default no in-profile-octets-discarded-count

Platforms All

13.96 in-profile-octets-forwarded-count

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-count in-profile-octets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>queue>i-count in-profile-octets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-count in-profile-octets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-count in-profile-octets-forwarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters in-profile-octets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters in-profile-octets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters in-profile-octets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters in-profile-octets-forwarded-count

Description This command includes the in-profile octets forwarded count. For queues with **stat-mode v4-v6**, this command includes the IPv4 octets forwarded count instead.

The **no** form of this command excludes the in-profile octets forwarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters in-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters in-profile-octets-forwarded-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log accounting-policy custom-record policer e-counters in-profile-octets-forwarded-count
configure log accounting-policy custom-record queue e-counters in-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters in-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-queue e-counters in-profile-octets-forwarded-count

Description This command includes the in-profile octets forwarded count.

The **no** form of this command excludes the in-profile octets forwarded count.

Default no in-profile-octets-forwarded-count

Platforms All

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters in-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>i-counters in-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters in-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters in-profile-octets-forwarded-count)

Full Context configure log accounting-policy custom-record policer i-counters in-profile-octets-forwarded-count
configure log accounting-policy custom-record queue i-counters in-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-policer i-counters in-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-queue i-counters in-profile-octets-forwarded-count

Description This command includes the in profile octets forwarded count.

The **no** form of this command excludes the in profile octets forwarded count.

Default no in-profile-octets-forwarded-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.97 in-profile-octets-offered-count

in-profile-octets-offered-count

Syntax [**no**] **in-profile-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-profile-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-profile-octets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters in-profile-octets-offered-count
configure log accounting-policy custom-record ref-policer e-counters in-profile-octets-offered-count

Description This command includes the in profile octets offered count.

The **no** form of this command excludes the in-profile octets offered count.

Default no in-profile-octets-offered-count

Platforms All

in-profile-octets-offered-count

Syntax [**no**] **in-profile-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters in-profile-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters in-profile-octets-offered-count)

Full Context configure log accounting-policy custom-record policer i-counters in-profile-octets-offered-count
configure log accounting-policy custom-record ref-policer i-counters in-profile-octets-offered-count

Description This command includes the in-profile octets offered count.

The **no** form of this command excludes the in-profile octets offered count.

Default no in-profile-octets-offered-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.98 in-profile-packets-discarded-count

in-profile-packets-discarded-count

Syntax [**no**] **in-profile-packets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-counters in-profile-packets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-counters in-profile-packets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters in-profile-packets-discarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters in-profile-packets-discarded-count

Description This command includes the in-profile packets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv4 packets discarded count instead.

The **no** form of this command excludes the in-profile packets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

in-profile-packets-discarded-count

Syntax [**no**] **in-profile-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters in-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters in-profile-packets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters in-profile-packets-discarded-count
configure log accounting-policy custom-record queue e-counters in-profile-packets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters in-profile-packets-discarded-count
configure log accounting-policy custom-record ref-queue e-counters in-profile-packets-discarded-count

Description This command includes the in-profile packets discarded count.

The **no** form of this command excludes the in-profile packets discarded count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no in-profile-packets-discarded-count

Platforms All

in-profile-packets-discarded-count

Syntax [**no**] **in-profile-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters in-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters in-profile-packets-discarded-count)

Full Context configure log accounting-policy custom-record policer i-counters in-profile-packets-discarded-count
configure log accounting-policy custom-record ref-policer i-counters in-profile-packets-discarded-count

Description This command includes the in-profile packets discarded count.

The **no** form of this command excludes the in-profile packets discarded count.

Default no in-profile-packets-discarded-count

Platforms All

13.99 in-profile-packets-forwarded-count

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-count in-profile-packets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>queue>i-count in-profile-packets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-count in-profile-packets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-count in-profile-packets-forwarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters in-profile-packets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters in-profile-packets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters in-profile-packets-forwarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters in-profile-packets-forwarded-count

Description This command includes the in-profile packets forwarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv4 packets forwarded count instead.

The **no** form of this command excludes the in-profile packets forwarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters in-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters in-profile-packets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters in-profile-packets-forwarded-count
configure log accounting-policy custom-record queue e-counters in-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters in-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-queue e-counters in-profile-packets-forwarded-count

Description This command includes the in-profile packets forwarded count.

The **no** form of this command excludes the in-profile packets forwarded count.

Default no in-profile-packets-forwarded-count

Platforms All

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters in-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>i-counters in-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters in-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters in-profile-packets-forwarded-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log accounting-policy custom-record policer i-counters in-profile-packets-forwarded-count
configure log accounting-policy custom-record queue i-counters in-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-policer i-counters in-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-queue i-counters in-profile-packets-forwarded-count

Description This command includes the in profile packets forwarded count.

The **no** form of this command excludes the in profile packets forwarded count.

Default no in-profile-packets-forwarded-count

Platforms All

13.100 in-profile-packets-offered-count

in-profile-packets-offered-count

Syntax [**no**] **in-profile-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters in-profile-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters in-profile-packets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters in-profile-packets-offered-count
configure log accounting-policy custom-record ref-policer e-counters in-profile-packets-offered-count

Description This command includes the in profile packets offered count.

The **no** form of this command excludes the in profile packets offered count.

Default no in-profile-packets-offered-count

Platforms All

in-profile-packets-offered-count

Syntax [**no**] **in-profile-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters in-profile-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters in-profile-packets-offered-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log accounting-policy custom-record policer i-counters in-profile-packets-offered-count
configure log accounting-policy custom-record ref-policer i-counters in-profile-packets-offered-count

Description This command includes the in-profile packets offered count.

The **no** form of this command excludes the in-profile packets offered count.

Default no in-profile-packets-offered-count

Platforms All

13.101 in-remark

in-remark

Syntax **in-remark** {**dscp** *dscp-name* | **prec** *ip-prec-value*}
no in-remark

Context **[Tree]** (config>qos>sap-ingress>fc in-remark)

Full Context configure qos sap-ingress fc in-remark

Description This command is used in a SAP ingress QoS policy to define an explicit in-profile remark action for a forwarding class or subclass. While the SAP ingress QoS policy may be applied to any SAP, the remarking functions are only enforced when the SAP is associated with an IP or subscriber interface (in an IES or VPRN). When the policy is applied to a Layer 2 SAP (i.e., Epipe or VPLS), the remarking definitions are silently ignored.

In the case where the policy is applied to a Layer 3 SAP, the in-profile remarking definition will be applied to packets that have been classified to the forwarding class or subclass. It is possible for a packet to match a classification command that maps the packet to a particular forwarding class or subclass, only to have a more explicit (higher priority match) override the association. Only the highest priority match forwarding class or subclass association will drive the in-profile marking.

The in-remark command is only applicable to ingress IP routed packets that are considered in-profile. The profile of a SAP ingress packet is affected by either the explicit in-profile/out-of-profile definitions or the ingress policing function applied to the packet. Table 64 shows the effect of the in-remark command on received SAP ingress packets. Within the in-profile IP packet's ToS field, either the six DSCP bits or the three precedence bits are remarked.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 64 **Effect of In-Remark Command on Received SAP Ingress Packets**

SAP Ingress Packet State	in-remark Command Effect
Non-Routed, Policed In-Profile	No Effect (non-routed packet)
Non-Routed, Policed Out-of-Profile	No Effect (non-routed packet)
Non-Routed, Explicit In-Profile	No Effect (non-routed packet)
Non-Routed, Explicit Out-of-Profile	No Effect (non-routed packet)
IP Routed, Policed In-Profile	in-remark value applied to IP header ToS field
IP Routed, Policed Out-of-Profile	No Effect (out-of-profile packet)
IP Routed, Explicit In-Profile	in-remark value applied to IP header ToS field
IP Routed, Explicit Out-of-Profile	No Effect (out-of-profile packet)

The **no** form of this command disables ingress remarking of in-profile packets classified to the forwarding class or subclass.

Parameters **dscp** *dscp-name* — Specifies that the matching packet's DSCP bits should be overridden with the value represented by dscp-name.

The *dscp-name* parameter is a 6-bit value. It must be one of the predefined DSCP names defined on the system.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

prec *ip-prec-value* — Specifies that the matching packet's precedence bits should be overridden with the value represented by *ip-prec-value*.

Values 0 to 7

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.102 inactive-flow-timeout

inactive-flow-timeout

Syntax **inactive-flow-timeout** *seconds*
no inactive-flow-timeout

Context **[Tree]** (config>cflowd inactive-flow-timeout)

Full Context configure cflowd inactive-flow-timeout

Description This command specifies the length of time, in seconds, that must elapse without a packet matching a flow before the flow is considered inactive.

The **no** form of this command resets the inactive flow timeout back to the default of 15 seconds.

Existing flows do not inherit the new **inactive-flow-timeout** value if this parameter is changed while **cflowd** is active. The **inactive-flow-timeout** value for a flow is set when the flow is first created in the active cache table and does not change dynamically.

Default inactive-flow-timeout 15

Parameters *seconds* — Specifies the length of time, in seconds, without a packet matching a flow before the flow is considered inactive.

Values 10 to 600

Platforms All

13.103 inactivity-mon

inactivity-mon

Syntax [**no**] **inactivity-mon**

Context **[Tree]** (config>app-assure>group>transit-ip-policy>transit-auto-create inactivity-mon)

Full Context configure application-assurance group transit-ip-policy transit-auto-create inactivity-mon

Description This command enables auto removal of inactive transit subscribers. Periodically AA removes any inactive auto-created subscriber where an inactive sub is defined as having no active flows in the last period.

The **no** form of this command disables the auto removal of inactive transit subscribers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.104 inactivity-timeout

inactivity-timeout

Syntax **inactivity-timeout** *seconds*
no inactivity-timeout

Context **[Tree]** (config>test-oam>twamp>server inactivity-timeout)

Full Context configure test-oam twamp server inactivity-timeout

Description This command configures the inactivity time out for all TWAMP-control connections. If no TWAMP control message is exchanged over the TCP connection for this duration of time the connection is closed and all in-progress tests are terminated.

The **no** form of this command returns the value to the default.

Default inactivity-timeout 900

Parameters *seconds* — Specifies the duration of the inactivity time out.

Values 60 to 3600

Default 900

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

inactivity-timeout

Syntax **inactivity-timeout** *seconds*
no inactivity-timeout

Context **[Tree]** (config>test-oam>twamp>twamp-light inactivity-timeout)

Full Context configure test-oam twamp twamp-light inactivity-timeout

Description This command configures the length of time to maintain stale state on the session reflector. Stale state is test data that has not been refreshed or updated by newly arriving probes for that specific test in a predetermined length of time. Any single reflector can maintain up state for a maximum of 12000 tests. If the maximum value is exceeded, the session reflector lacks memory to allocate to new tests.

The **no** form of this command returns the value to the default.

Default inactivity-timeout 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the value in seconds for maintaining stale state.

Values 10 to 100

Default 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.105 inactivity-timer

inactivity-timer

Syntax **inactivity-timer** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no inactivity-timer

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-sol inactivity-timer)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-sol inactivity-timer)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-sol inactivity-timer)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-sol inactivity-timer)

Full Context configure service ies subscriber-interface group-interface ipv6 router-solicit inactivity-timer
configure service ies subscriber-interface ipv6 router-solicit inactivity-timer
configure service vprn subscriber-interface ipv6 router-solicit inactivity-timer

Description This command specifies the time before an inactive host is removed.

The **no** form of this command reverts to the default.

Parameters **infinite** — Specifies that the idle host is never removed.

days — Specifies that the idle host is removed if idle within the number of specified days.

hours — Specifies that the idle host is removed if idle within the number of specified hours.

minutes — Specifies that the idle host is removed if idle within the number of specified minutes.

seconds — Specifies that the idle host is removed if idle within the number of specified seconds.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

inactivity-timer

Syntax **inactivity-timer** *timer*
no inactivity-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>eth-cfm>slm inactivity-timer)

Full Context configure eth-cfm slm inactivity-timer

Description The time the responder keeps a test active. Should the time between packets exceed this values within a test the responder will mark the previous test as complete. It will treat any new packets from a peer with the same test-id, source-mac and MEP-ID as a new test responding with the sequence number one.

The **no** form of the command reverts the timeout to the default value.

Default inactivity-timer 100

Parameters *timer* — Specifies the amount of time in seconds.

Values 10 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.106 inband

inband

Syntax **inband** *service-id*
no inband

Context [Tree] (config>system>security>vprn-aaa-server inband)

Full Context configure system security vprn-aaa-server inband

Description This command configures TACACS+ or RADIUS servers in a VPRN to be used for AAA by that VPRN and by sessions in the Base routing instance.

The **no** form of this command disables the use of servers for in-band management.

Default no inband

Parameters *service-id* — Specifies the VPRN server for AAA to use for in-band sessions.

Values *service-id*: 1 to 2147483648
svc-name: 64 characters maximum

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.107 inband-collector-export-only

inband-collector-export-only

Syntax [**no**] **inband-collector-export-only**

Context **[Tree]** (config>cflowd inband-collector-export-only)

Full Context configure cflowd inband-collector-export-only

Description This command, when the **inband-collector-export-only** command is enabled, allows only collectors that are reachable through inband interfaces and enables a higher flow export rate.

The **no** form of this command, the default, re-enables the use of the out-of-band management Ethernet port.

Platforms All

13.108 inbound-max-sessions

inbound-max-sessions

Syntax **inbound-max-sessions** *number-of-sessions*
no inbound-max-sessions

Context **[Tree]** (config>system>login-control>ftp inbound-max-sessions)

Full Context configure system login-control ftp inbound-max-sessions

Description This command configures the maximum number of concurrent inbound FTP sessions.

This value is the combined total of inbound and outbound sessions.

The **no** form of this command reverts to the default value.

Default inbound-max-sessions 3

Parameters *value* — Specifies the maximum number of concurrent FTP sessions on the node.

Values 0 to 5

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

inbound-max-sessions

Syntax **inbound-max-sessions** *number-of-sessions*
no inbound-max-sessions

Context **[Tree]** (config>system>login-control>telnet inbound-max-sessions)
[Tree] (config>system>login-control>ssh inbound-max-sessions)

Full Context configure system login-control ssh inbound-max-sessions
configure system login-control telnet inbound-max-sessions

Description This parameter limits the number of inbound Telnet and SSH sessions. A maximum of 30 telnet and ssh connections can be established to the router. The local serial port cannot be disabled.

Telnet and SSH maximum sessions can also use the combined total of both inbound sessions (SSH+Telnet). While it is acceptable to continue to internally limit the combined total of SSH and Telnet sessions to N, either SSH or Telnet sessions can use the inbound maximum sessions, if so required by the Operator.

The **no** form of this command reverts to the default value.

Default inbound-max-sessions 5

Parameters *number-of-sessions* — The maximum number of concurrent inbound Telnet sessions, expressed as an integer.

Values 0 **to** 50 (default = 5) or 0 **to** N where N is the new total number of SSH+Telnet sessions if they are scaled

Platforms All

13.109 incl-mcast-orig-ip

incl-mcast-orig-ip

Syntax **incl-mcast-orig-ip** *ip-address*
no incl-mcast-orig-ip

Context **[Tree]** (config>service>vpls>bgp-evpn>mpls incl-mcast-orig-ip)

Full Context configure service vpls bgp-evpn mpls incl-mcast-orig-ip

Description The IP address configured by the user in the **incl-mcast-orig-ip** command is encoded in the **originating-ip** field of EVPN Inclusive Multicast Routes with tunnel type Ingress Replication (value 6), mLDP (2), and Composite IR and mLDP (130).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured address does not need to be reachable in the base router or have an interface in the base router. The originating-ip address is used solely for BGP route-key selection.

The originating-ip is never changed for Inclusive Multicast Routes with tunnel type AR (Assisted Replication, value 10).

The **no** version of the command withdraws the affected Inclusive Multicast Routes and re-advertises it with the default system-ip address in the originating-ip field.

Default incl-mcast-orig-ip 1

Parameters *ip-address* — Specifies the IPv4 address value.

Values a.b.c.d

13.110 include

include

Syntax **include** *group-name* [*group-name*]
no include [*group-name* [*group-name*]]

Context **[Tree]** (config>router>mpls>lsp include)
[Tree] (config>router>mpls>lsp>primary include)
[Tree] (config>router>mpls>lsp>primary-p2mp-instance include)
[Tree] (config>router>mpls>lsp>secondary include)
[Tree] (config>router>mpls>lsp-template include)

Full Context configure router mpls lsp include
configure router mpls lsp primary include
configure router mpls lsp primary-p2mp-instance include
configure router mpls lsp secondary include
configure router mpls lsp-template include

Description This command specifies the admin groups to be included when an LSP is set up. Up to five groups per operation can be specified, up to 32 maximum. The **include** statement instructs the CSPF algorithm to pick TE links among the links which belong to one or more of the specified admin groups. A link that does not belong to at least one of the specified admin groups is excluded and thus pruned from the TE database before the CSPF computation. However, a link can still be selected if it belongs to one of the groups in a **include** statement but also belongs to other groups which are not part of any **include** statement in the LSP or primary/secondary path configuration. In other words, the **include** statements implements the “include-any” behavior.

The **config**>**router**>**mpls**>**lsp**>**primary-p2mp-instance**>**include** command is not supported on the 7450 ESS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the specified groups in the specified context.

Default no include

Parameters *group-name* — Specifies admin groups to be included when an LSP is set up.

Platforms All

include

Syntax [**no**] **include**

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy include)

Full Context configure service nat syslog syslog-export-policy include

Description Commands in this context specify the optional fields to include in the NAT syslog messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

include

Syntax [**no**] **include** *tag*

Context **[Tree]** (config>router>admin-tags>route-admin-tag-policy include)

Full Context configure router admin-tags route-admin-tag-policy include

Description This configures an admin tag to be included when matching a route against an LSP.

Up to eight inclusion statements are supported per policy.

The **no** form of this command removes the admin tag from the include statement.

Parameters *tag* — Specifies the value of the admin tag, up to 32 characters.

Platforms All

13.111 include-all

include-all

Syntax **include-all**

Context **[Tree]** (config>router>fad>flex-algo include-all)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router flexible-algorithm-definitions flex-algo include-all

Description Commands in this context configure administrative groups to include in the flexible algorithm topology graph. Administrative groups are attributes associated with a link and are generally referred to as link colors.

Flexible algorithms provide the possibility to restrict inclusion into the topology graph to links that have a pre-defined combination of associated administrative groups. The **include-all** command requires that all configured administrative groups must be present in a link before the link can be included in the topology graph.

Platforms All

13.112 include-any

include-any

Syntax **include-any**

Context **[Tree]** (config>router>fad>flex-algo include-any)

Full Context configure router flexible-algorithm-definitions flex-algo include-any

Description Commands in this context configure administrative groups to include in the flexible algorithm topology graph. Administrative groups are attributes associated with a link and are generally referred to as link colors.

Flexible algorithms provide the possibility to restrict inclusion into the topology graph to links that have a pre-defined combination of associated administrative groups. The **include-any** command requires that one of the configured administrative groups must be present on a link before the link can be included in the topology graph.

Platforms All

13.113 include-avp

include-avp

Syntax [**no**] **include-avp**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy include-avp)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gx include-avp)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq include-avp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp
configure subscriber-mgmt diameter-application-policy gy include-avp
configure subscriber-mgmt diameter-application-policy nasreq include-avp

Description Commands in this context configure AVPs and their format to be included in Diameter Gx, Gy, or NASREQ application messages. For full description each AVP, refer to the 7750 SR and VSR RADIUS Attributes Reference Guide.

AVP name:

- an-gw-address
- apn-ambr
- called-station-id
- calling-station-id
- charging-characteristics
- dynamic-address-flag
- ip-can-type
- logical-access-id
- nas-port
- nas-port-id
- nas-port-type
- pdn-connection-id
- physical-access-id
- rai
- rat-type
- selection-mode
- sgsn-mcc-mnc
- supported-features
- user-equipment-info
- user-location-info

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.114 include-dns

include-dns

Syntax [**no**] **include-dns**

Context **[Tree]** (config>subscr-mgmt>rtr-adv-plcy>dns-opt include-dns)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv include-dns)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>ipv6 include-dns)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv include-dns)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 include-dns)

Full Context configure service ies subscriber-interface group-interface ipv6 include-dns
configure service ies subscriber-interface ipv6 rtr-adv include-dns
configure service vprn subscriber-interface group-interface ipv6 include-dns
configure service vprn subscriber-interface ipv6 rtr-adv include-dns
configure subscriber-mgmt router-advertisement-policy dns-options include-dns

Description This command specifies to include the Recursive DNS Server (RDNSS) Option as defined in RFC 6106 in IPv6 router advertisements for DNS name resolution of IPv6 SLAAC hosts.

The **no** form of this command returns the command to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

include-dns

Syntax [**no**] **include-dns**

Context [Tree] (config>service>ies>sub-if>ipv6>rtr-adv>dns-opt include-dns)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv>dns-opt include-dns)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv>dns-opt include-dns)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv>dns-opt include-dns)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements dns-options include-dns
configure service ies subscriber-interface ipv6 router-advertisements dns-options include-dns
configure service vprn subscriber-interface group-interface ipv6 router-advertisements dns-options include-dns
configure service vprn subscriber-interface ipv6 router-advertisements dns-options include-dns

Description This command specifies to include the Recursive DNS Server (RDNSS) Option as defined in RFC 6106 in IPv6 Router Advertisements for DNS name resolution of IPv6 SLAAC hosts.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

include-dns

Syntax [**no**] **include-dns**

Context [Tree] (config>service>vprn>router-advert>if>dns-options include-dns)

Full Context configure service vprn router-advertisement interface dns-options include-dns

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the Recursive DNS Server (RDNSS) Option in router advertisements. This must be enabled for each interface on which the RDNSS option is required in router advertisement messages.

The **no** form of this command disables the RDNSS option in router advertisements.

Default include-dns

Platforms All

include-dns

Syntax [**no**] **include-dns**

Context **[Tree]** (config>router>router-advert>if>dns-opt include-dns)

Full Context configure router router-advertisement interface dns-options include-dns

Description This command enables the Recursive DNS Server (RDNSS) Option in router advertisements. This must be enabled for each interface on which the RDNSS option is required in router advertisement messages.

The **no** form of this command disables the RDNSS option in router advertisements.

Default include-dns

Platforms All

13.115 include-group

include-group

Syntax **include-group** *ip-admin-group-name* [**pref** *preference*]
no include-group *ip-admin-group-name*

Context **[Tree]** (config>router>route-next-hop-policy>template include-group)

Full Context configure router route-next-hop-policy template include-group

Description This command configures the admin group constraint into the route next-hop policy template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each group is entered individually. The **include-group** statement instructs the LFA SPF selection algorithm to pick up a subset of LFA next-hops among the links which belong to one or more of the specified admin groups. A link which does not belong to at least one of the admin-groups is excluded. However, a link can still be selected if it belongs to one of the groups in a include-group statement but also belongs to other groups which are not part of any include-group statement in the route next-hop policy.

The **pref** option is used to provide a relative preference for the admin group to select. A lower preference value means that LFA SPF will first attempt to select a LFA backup next-hop which is a member of the corresponding admin group. If none is found, then the admin group with the next higher preference value is evaluated. If no preference is configured for a given admin group name, then it is supposed to be the least preferred, that is, numerically the highest preference value.

When evaluating multiple **include-group** statements within the same preference, any link which belongs to one or more of the included admin groups can be selected as an LFA next-hop. There is no relative preference based on how many of those included admin groups the link is a member of.

The **exclude-group** statement simply prunes all links belonging to the specified admin group before making the LFA backup next-hop selection for a prefix.

If the same group name is part of both include and exclude statements, the exclude statement will win. It other words, the exclude statement can be viewed as having an implicit preference value of 0.

The admin-group criteria are applied before running the LFA next-hop selection algorithm.

The **no** form deletes the admin group constraint from the route next-hop policy template.

Parameters *ip-admin-group-name* — Specifies the name of the group, up to 32 characters.

preference — An integer specifying the relative preference of a group.

Values 1 to 255

Default 255

Platforms All

13.116 include-radius-attribute

include-radius-attribute

Syntax [**no**] **include-radius-attribute**

Context **[Tree]** (config>aaa>l2tp-acct-plcy include-radius-attribute)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context specify the RADIUS attributes that the system should include into RADIUS Access-Request (for authentication) and Accounting-Request (for accounting) messages.

The **no** form of this command disables the RADIUS attributes to be included.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

include-radius-attribute

Syntax [**no**] **include-radius-attribute**

Context **[Tree]** (config>subscr-mgmt>auth-plcy include-radius-attribute)
[Tree] (config>subscr-mgmt>acct-plcy include-radius-attribute)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute
configure subscriber-mgmt authentication-policy include-radius-attribute

Description Commands in this context specify the RADIUS attributes that the system should include in RADIUS Access-Request (for authentication) and Accounting-Request (for accounting) messages.

The **no** form of this command reverts to the default values.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

include-radius-attribute

Syntax [**no**] **include-radius-attribute**

Context **[Tree]** (config>ipsec>rad-acct-plcy include-radius-attribute)
[Tree] (config>ipsec>rad-auth-plcy include-radius-attribute)

Full Context configure ipsec radius-accounting-policy include-radius-attribute
configure ipsec radius-authentication-policy include-radius-attribute

Description Commands in this context specify the RADIUS attributes that the system should include into RADIUS Access-Request (for authentication) and Accounting-Request (for accounting) messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.117 include-system-info

include-system-info

Syntax [**no**] **include-system-info**

Context **[Tree]** (config>log>accounting-policy include-system-info)

Full Context configure log accounting-policy include-system-info

Description This command allows the operator to optionally include router information at the top of each accounting file generated for a given accounting policy.

The **no** form of this command configures the router to not include optional router information at the top of the file.

Default no include-system-info

Platforms All

13.118 included-protocols

included-protocols

Syntax **included-protocols**

Context **[Tree]** (config>sys>security>cpu-protection>ip included-protocols)

Full Context configure system security cpu-protection ip-src-monitoring included-protocols

Description This context allows configuration of which protocols are included for ip-src-monitoring. This is system-wide configuration that applies to cpu protection globally.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

13.119 inclusive

inclusive

Syntax **inclusive**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>provider-tunnel inclusive)

Full Context configure service vpls provider-tunnel inclusive

Description Commands in this context configure the use of a P2MP LSP as the default tree for forwarding Broadcast, Unknown unicast, and Multicast (BUM) packets of a VPLS or B-VPLS instance. The P2MP LSP is referred to, in this case, as the Inclusive Provider Multicast Service Interface (I-PMSI).

When enabled, this feature relies on BGP Auto-Discovery (BGP-AD), BGP-VPLS or BGP-EVPN to discover the PE nodes participating in a specified VPLS/B-VPLS instance. In the case of BGP-AD or BGP-VPLS, the BGP route contains the information required to signal both point-to-point (P2P) PWs used to forward unicast known Ethernet frames, and the RSVP or mLDP P2MP LSP used to forward the BUM frames. In the case of BGP-EVPN, the EVPN IMET route contains the information to set up the mLDP P2MP LSP and may also contain the information that enables the remote leaf-only nodes to setup an EVPN destination to the sending PE.

Note: The provider-tunnel for a specified service must be configured with an owner protocol (BGP-AD, BGP-VPLS or BGP-EVPN); only one owner must be configured. Use the **owner {bgp-ad|bgp-vpls|bgp-evpn-mpls}** command to configure an owner.

With an mLDP I-PMSI, each leaf node will initiate the signaling of the mLDP P2MP LSP upstream using the P2MP FEC information in the I-PMSI tunnel information discovered through the BGP.

If IGMP or PIM snooping are configured on the VPLS/B-VPLS instance, multicast packets matching an L2 multicast Forwarding Information Base (FIB) record will also be forwarded over the P2MP LSP.

Use the **mldp** command to enable the use of an LDP P2MP LSP as the I-PMSI for forwarding Ethernet BUM and IP multicast packets in a VPLS instance:

config>service>vpls [b-vpls]>provider-tunnel>inclusive>mldp

When a **no shutdown** is performed under the context of the inclusive node and the expiration of a delay timer, BUM packets will be forwarded over an automatically signaled mLDP P2MP LSP.

Use the **root-and-leaf** command to configure the node to operate as both root and leaf in the VPLS instance:

config>service>vpls [b-vpls]>provider-tunnel>inclusive>root-and-leaf

The node behaves as a leaf-only node by default. For the I-PMSI of type mLDP, the leaf-only node will join I-PMSI rooted at other nodes it discovered but will not include a PMSI Tunnel Attribute in BGP route update messages. This way a leaf-only node will forward packets to other nodes in the VPLS/B-VPLS using the point-to-point spoke-SDPs in the case of BGP-AD or BGP-VPLS, or using EVPN destinations in the case of BGP-EVPN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: Either BGP-AD/VPLS or BGP-EVPN must be enabled in the VPLS/B-VPLS instance otherwise the execution of the **no shutdown** command under the context of the inclusive node will fail and the I-PMSI will not come up.

If the P2MP LSP instance goes down, the VPLS/B-VPLS immediately reverts the forwarding of BUM packets to the P2P PWs or EVPN destinations (in the case of BGP-EVPN). Performing a shutdown under the context of the inclusive node will allow the user to restore BUM packet forwarding over the P2P PWs or EVPN destinations.

This feature is supported with VPLS and B-VPLS; it is not supported with I-VPLS. Although Routed VPLS is supported, routed traffic cannot be sent over the I-PMSI tree.

Platforms All

inclusive

Syntax **inclusive**

Context **[Tree]** (config>service>vprn>mvpn>provider-tunnel inclusive)

Full Context configure service vprn mvpn provider-tunnel inclusive

Description Commands in this context specify inclusive provider tunnels.

Platforms All

inclusive

Syntax **inclusive**

Context **[Tree]** (config>router>gtm>provider-tunnel inclusive)

Full Context configure router gtm provider-tunnel inclusive

Description Commands in this context configure inclusive provider tunnels parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.120 incoming-sid

incoming-sid

Syntax **incoming-sid** *static label*
no incoming-sid

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment incoming-sid)

Full Context configure router p2mp-sr-tree replication-segment incoming-sid

Description This command configures the incoming replication SID for this P2MP SR tree replication segment entry.

The **no** form of this command removes the incoming replication SID.

Parameters *static label* — Specifies the incoming replication SID label.

Values 0 to 4294967295

Platforms All

13.121 incremental-spf-wait

incremental-spf-wait

Syntax **incremental-spf-wait** *incremental-spf-wait*
no incremental-spf-wait

Context **[Tree]** (config>router>ospf>timers incremental-spf-wait)
[Tree] (config>router>ospf3>timers incremental-spf-wait)

Full Context configure router ospf timers incremental-spf-wait
configure router ospf3 timers incremental-spf-wait

Description This command sets the delay before an incremental SPF calculation is performed when LSA types 3, 4, 5, or 7 are received. This allows multiple updates to be processed in the same SPF calculation. Type 1 or type 2 LSAs are considered a topology change and will always trigger a full SPF calculation.

The **no** form of this command resets the timer value back to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is ≥ 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default incremental-spf-wait 1000

Parameters *incremental-spf-wait* — Specifies the OSPF incremental SPF calculation delay, in milliseconds.

Values 0 to 1000

Platforms All

13.122 index

index

Syntax **index** *index* [**create**]
no index *index*

Context **[Tree]** (config>service>dynsvc>ladb>user index)

Full Context configure service dynamic-services local-auth-db user-name index

Description This command creates an index entry containing authentication data for a dynamic service SAP. Up to 32 indexes can be created per user name entry, representing up to 32 dynamic service SAPs that can be instantiated with a single dynamic service data trigger. One of the dynamic service SAPs must be the data trigger SAP.

The **no** form of this command removes the index entry from the user name entry in the local authentication database configuration.

Parameters *index* — Specifies the index entry identifier.

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.123 indirect

indirect

Syntax [**no**] **indirect** *ip-address*

Context **[Tree]** (config>service>vprn>static-route-entry indirect)

Full Context configure service vprn static-route-entry indirect

Description This command specifies that the route is indirect and specifies the next hop IP address used to reach the destination.

The configured *ip-addr*ess is not directly connected to a network configured on this node. The destination can be reached via multiple paths. The indirect address can only be resolved from dynamic routing protocol. Another static route cannot be used to resolve the indirect address.

The *ip-address* configured here can be either on the network side or the access side and is typically at least one hop away from this node.

Default no indirect

Parameters *ip-address* — The IP address of the IP interface.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x-[interface]

Platforms All

indirect

Syntax [**no**] **indirect** *ip-address*

Context **[Tree]** (config>router>static-route-entry indirect)

Full Context configure router static-route-entry indirect

Description This command specifies that the route is indirect and specifies the next hop IP address used to reach the destination.

The configured *ip-addr*ess is not directly connected to a network configured on this node. The destination can be reached via multiple paths. The indirect address can only be resolved from dynamic routing protocol. Another static route cannot be used to resolve the indirect address.

The *ip-address* configured here can be either on the network side or the access side and is typically at least one hop away from this node.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no indirect

Parameters *ip-address* — Specifies the IP address of the IP interface.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x-[interface]

Platforms All

13.124 ine-identifier

ine-identifier

Syntax **ine-identifier** *identifier*
no ine-identifier

Context **[Tree]** (config>li>x-interfaces ine-identifier)

Full Context configure li x-interfaces ine-identifier

Description This command configures the Intercepting Network Element (INE).

The **no** form of this command reverts to the default.

Parameters *identifier* — Specifies the INE name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.125 info

info

Syntax **info** [**detail**] [**objective**]
info [**detail**] [**objective**] **operational**

Context **[Tree]** (configure info)

Full Context configure info

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command displays the running configuration for the configuration context where it is entered and all branches below that context level. It can be used in any branch under configure, but not with **configure** itself.

By default, the command only enters the configuration parameters that vary from the default values.

The **detail** keyword causes all configuration parameters to be displayed. The **include-dynamic** objective keyword includes configuration parameters from dynamic sources such as VSD or dynamic data services Python scripts. These dynamic configuration parameters are not saved in the configuration file.

The **operational** keyword is available in edit-cfg mode only, in which case the keyword is mandatory when using the **info** command.

Example:

```
A:ALA-48>config>router>if-attr# info
----------------------------------
            admin-group "green" value 15
            admin-group "red" value 25
            admin-group "yellow" value 20
A:ALA-48>config>router>mpls# info
----------------------------------
            interface "system"
            exit
            interface "to-104"
                admin-group "green"
                admin-group "red"
                admin-group "yellow"
                label-map 35
                    swap 36 nexthop 10.10.10.91
                    no shutdown
                exit
            exit
            path "secondary-path"
                hop 1 10.10.0.111  strict
                hop 2 10.10.0.222  strict
                hop 3 10.10.0.123  strict
                no shutdown
            exit
            path "to-NYC"
                hop 1 10.10.10.104  strict
                hop 2 10.10.0.210  strict
                no shutdown
            exit
            path "to-104"
                no shutdown
            exit
            lsp "to-104"
                to 10.10.10.104
                from 10.10.10.103
                rsvp-resv-style ff
                cspf
...
--------------------------------------------
A:ALA-48>config>router>mpls#
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
A:ALA-48>config>router>mpls# info detail
----------------------------------------------
            frr-object
            no resignal-timer
            interface "system"
                no admin-group
                no shutdown
            exit
            interface "to-104"
                admin-group "green"
                admin-group "red"
                admin-group "yellow"
                label-map 35
                    swap 36 nexthop 10.10.10.91
                    no shutdown
                exit
                no shutdown
            exit
            path "secondary-path"
                hop 1 10.10.0.111  strict
                hop 2 10.10.0.222  strict
                hop 3 10.10.0.123  strict
                no shutdown
            exit
            path "to-NYC"
                hop 1 10.10.10.104  strict
                hop 2 10.10.0.210  strict
                no shutdown
            exit
            path "to-104"
                no shutdown
            exit
            lsp "to-104"
                to 10.10.10.104
                from 10.10.10.103
                rsvp-resv-style ff
                adaptive
                cspf
                include "red"
                exclude "green"
                adspec
                fast-reroute one-to-one
                    no bandwidth
                    no hop-limit
                    node-protect
                exit
                hop-limit 10
                retry-limit 0
                retry-timer 30
                secondary "secondary-path"
                    no standby
                    no hop-limit
                    adaptive
                    no include
                    no exclude
                    record
                    record-label
                    bandwidth 50000
                    no shutdown
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
                exit
                primary "to-NYC"
                    hop-limit 50
                    adaptive
                    no include
                    no exclude
                    record
                    record-label
                    no bandwidth
                    no shutdown
                exit
                no shutdown
            exit
...
-------------------------------------------------
A:ALA-48>config>router>mpls#
```

Parameters **detail** — Displays all configuration parameters including parameters at their default values.

objective — Provides an output objective that controls the configuration parameters to be displayed.

Values **include-dynamic**: includes configuration parameters from dynamic sources such as VSD or dynamic data services Python scripts.

info

Syntax **info**

Context **[Tree]** (debug>system>netconf info)

Full Context debug system netconf info

Description This command displays debug information for NETCONF sessions.

Output The following is an example of debug information for NETCONF sessions.

Sample Output

```
17 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
session started"

"18 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF
NETCONF: INFO user: ncuser session 36:
received <hello>"

19 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36: setting 1.1 capability, chunk framing mode e
nabled"

20 2018/03/17 12:29:54.785 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
successfully processed <hello> message"

21 2018/03/17 12:29:54.844 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
received <edit-config>"

22 2018/03/17 12:29:54.848 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
error occurred while processing <edit-config> RPC"

23 2018/03/17 12:29:54.892 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
successfully processed <edit-config> RPC"

24 2018/03/17 12:29:54.893 UTC minor: DEBUG #2001 Base NETCONF
"NETCONF: INFO user: ncuser session 36:
session terminated"
```

13.126 info-notification

info-notification

Syntax **info-notification**

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>local-sf-action info-notification)

Full Context configure port ethernet efm-oam link-monitoring local-sf-action info-notification

Description The context allows the operator to set different flags in the Information OAM PDU. The flags can be used to notify the peer that a local signal failure threshold has been exceeded within the configured window. This is useful when the local node supports the link monitoring function, but the remote peer does not support this capability. Information OAM PDUs are sent on the interval where the Event Notification OAM PDU is typically only sent on the initial sf-threshold crossing event. It is strongly suggested one of the Information OAM PDU Flag fields used to continually communicate current monitor state to the peer.

Interactions: The signal failure threshold will trigger these actions.

Platforms All

13.127 ing-percentage-of-rate

ing-percentage-of-rate

Syntax **ing-percentage-of-rate** *ing-rate-percentage*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ing-percentage-of-rate

Context [Tree] (config>port>modify-buffer-allocation-rate ing-percentage-of-rate)

Full Context configure port modify-buffer-allocation-rate ing-percentage-of-rate

Description This command increases or decreases the active bandwidth associated with the ingress port that affects the amount of ingress buffer space managed by the port. Changing a port's active bandwidth using the **ing-percentage-of-rate** command is an effective means of artificially lowering the buffers managed by one ingress port and giving them to other ingress ports on the same MDA.

The **ing-percentage-of-rate** command accepts a percentage value that increases or decreases the active bandwidth based on the defined percentage. A value of 50% causes the active bandwidth to be reduced by 50%. A value of 150% causes the active bandwidth to be increased by 50%. Values from 1 to 1000 percent are supported.

A value of 100 (the default value) is equivalent to executing the **no ing-percentage-of-rate** command and restores the ingress active rate to the normal value.

The **no** form of this command removes any artificial increase or decrease of the ingress active bandwidth used for ingress buffer space allocation to the port. The **no ing-percentage-of-rate** command sets the ingress rate percentage to 100%.

Parameters *ing-rate-percentage* — The *ing-rate-percentage* parameter is required and specifies the percentage value used to modify the current ingress active bandwidth of the port. This does not actually change the bandwidth available on the port in any way. The defined *ing-rate-percentage* parameter is multiplied by the ingress active bandwidth of the port. A value of 150 results in an increase of 50% (1.5 x Rate).

Values 1 to 1000

Default 100 (no change to active rate)

Platforms All

13.128 ing-weight

ing-weight

Syntax **ing-weight access** *access-weight* **network** *network-weight*
no ing-weight

Context [Tree] (config>port>hybrid-buffer-allocation ing-weight)

Full Context configure port hybrid-buffer-allocation ing-weight

Description This command configures the sharing of the ingress buffers allocated to a hybrid port among the access and network contexts. By default, it is split equally between network and access.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default values for the ingress access and network weights.

Parameters *access-weight* — Specifies the access weight as an integer.

Values 0 to 100

Default 50

network-weight — Specifies the network weight as an integer.

Values 0 to 100

Default 50

Platforms All

13.129 ingress

ingress

Syntax **ingress**

Context **[Tree]** (config>card>fp ingress)

Full Context configure card fp ingress

Description This command enables access to the ingress fp CLI context.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>subscr-mgmt>ancp>ancp-policy ingress)

Full Context configure subscriber-mgmt ancp ancp-policy ingress

Description Commands in this context configure ingress ANCP policy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>msap-policy>ies-vprn ingress)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only ingress)

Full Context configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters ingress
configure subscriber-mgmt msap-policy vpls-only-sap-parameters ingress

Description Commands in this context configure ingress policies for Managed SAPs (MSAPs).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context [Tree] (config>subscr-mgmt>sla-profile ingress)

Full Context configure subscriber-mgmt sla-profile ingress

Description Commands in this context configure ingress parameters for the SLA profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context [Tree] (config>service>vprn>sub-if>grp-if ingress)

Full Context configure service vprn subscriber-interface group-interface ingress

Description Commands in this context configure ingress network filter parameters for the interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context [Tree] (config>service>ies>sub-if>grp-if>sap ingress)
[Tree] (config>service>vprn>sub-if>grp-if>sap ingress)

Full Context configure service ies subscriber-interface group-interface sap ingress
configure service vprn subscriber-interface group-interface sap ingress

Description Commands in this context configure ingress SAP Quality of Service (QoS) policies and filter policies.

If no SAP ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>if>sap ingress)
[Tree] (config>service>ies>if>spoke-sdp ingress)
[Tree] (config>service>ies>red-if>spoke-sdp>egress ingress)
[Tree] (config>service>vpls>mesh-sdp ingress)
[Tree] (config>service>vpls>sap ingress)
[Tree] (config>service>vpls>spoke-sdp ingress)

Full Context configure service ies interface sap ingress
configure service ies interface spoke-sdp ingress
configure service ies red-if spoke-sdp egress ingress
configure service vpls mesh-sdp ingress
configure service vpls sap ingress
configure service vpls spoke-sdp ingress

Description Commands in this context configure ingress Quality of Service (QoS) policies and filter policies.

If no QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>atm ingress)
[Tree] (config>service>vprn>if>sap>atm ingress)
[Tree] (config>service>vprn>sub-if>grp-if>sap>atm ingress)

Full Context configure service ies subscriber-interface group-interface sap atm ingress
configure service vprn interface sap atm ingress
configure service vprn subscriber-interface group-interface sap atm ingress

Description This command configures ingress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service vprn subscriber-interface group-interface sap atm ingress
- configure service ies subscriber-interface group-interface sap atm ingress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service vprn interface sap atm ingress

ingress

Syntax **ingress**

Context **[Tree]** (config>card>mda>access ingress)
[Tree] (config>port>access ingress)

Full Context configure card mda access ingress
configure port access ingress

Description Commands in this context configure ingress buffer pool parameters which define the percentage of the pool buffers that are used for CBS calculations and specify the slope policy that is configured in the **config>qos>slope-policy** context.

On the MDA level, access ingress pools are only allocated on channelized MDAs.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>port>ethernet>access ingress)

Full Context configure port ethernet access ingress

Description This command configures Ethernet access ingress port parameters.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>port>ml-bundle>mlfr ingress)

Full Context configure port multilink-bundle mlfr ingress

Description Commands in this context configure the ingress QoS profile for the MLFR bundle.

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ingress

Syntax **ingress**

Context **[Tree]** (config>port>ml-bundle>mlppp ingress)

Full Context configure port multilink-bundle mlppp ingress

Description Commands in this context configure ingress MLPPP QoS profile parameters for the multilink bundle.

Platforms 7450 ESS, 7750 SR-7/12/12e

ingress

Syntax **ingress**

Context **[Tree]** (config>port>sonet-sdh>path>atm>ilmi ingress)

Full Context configure port sonet-sdh path atm ilmi ingress

Description Commands in this context configure ingress traffic attributes for the ILMI link.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

ingress

Syntax **ingress**

Context **[Tree]** (config>service>apipe>sap>atm ingress)
[Tree] (config>service>epipe>sap>atm ingress)

Full Context configure service apipe sap atm ingress
configure service epipe sap atm ingress

Description This command configures ingress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

ingress

Syntax **ingress**

Context **[Tree]** (config>service>apipe>sap ingress)
[Tree] (config>service>cpipe>sap ingress)
[Tree] (config>service>epipe>sap ingress)
[Tree] (config>service>fpipe>sap ingress)
[Tree] (config>service>ipipe>sap ingress)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service apipe sap ingress
configure service cpipe sap ingress
configure service epipe sap ingress
configure service fpipe sap ingress
configure service ipipe sap ingress

Description Commands in this context configure ingress SAP Quality of Service (QoS) policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress
- configure service fpipe sap ingress

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress

All

- configure service epipe sap ingress
- configure service ipipe sap ingress

ingress

Syntax **ingress**

Context **[Tree]** (config>service>apipe>spoke-sdp ingress)
[Tree] (config>service>cpipe>spoke-sdp ingress)
[Tree] (config>service>epipe>spoke-sdp ingress)
[Tree] (config>service>fpipe>spoke-sdp ingress)
[Tree] (config>service>ipipe>spoke-sdp ingress)

Full Context configure service apipe spoke-sdp ingress
configure service cpipe spoke-sdp ingress
configure service epipe spoke-sdp ingress
configure service fpipe spoke-sdp ingress
configure service ipipe spoke-sdp ingress

Description This command configures the ingress SDP context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp ingress
- configure service cpipe spoke-sdp ingress

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe spoke-sdp ingress

All

- configure service epipe spoke-sdp ingress
- configure service ipipe spoke-sdp ingress

ingress

Syntax **ingress**

Context **[Tree]** (config>service>template>epipe-sap-template ingress)

Full Context configure service template epipe-sap-template ingress

Description Commands in this context configure ingress SAP Quality of Service (QoS) policies and filter policies.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vpls>vxlan>network ingress)

Full Context configure service vpls vxlan network ingress

Description Commands in this context configure network ingress parameters for the VPLS VXLAN service.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vpls>sap>atm ingress)

Full Context configure service vpls sap atm ingress

Description Commands in this context configure ingress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>aarp-interface>spoke-sdp ingress)

Full Context configure service ies aarp-interface spoke-sdp ingress

Description Commands in this context configure the ingress for a spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>if>vpls ingress)

Full Context configure service ies interface vpls ingress

Description The ingress node in this context under the vpls binding is used to define the routed IPv4 and IPv6 optional filter overrides.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>if ingress)

Full Context configure service ies interface ingress

Description This command enters context to configure ingress parameters for network interfaces.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>if>sap>atm ingress)

Full Context configure service ies interface sap atm ingress

Description This command configures ingress ATM attributes for the SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vprn>network ingress)

Full Context configure service vprn network ingress

Description Commands in this context configure network ingress parameters for the VPRN service.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vprn>aarp-interface>spoke-sdp ingress)

Full Context configure service vprn aarp-interface spoke-sdp ingress

Description Commands in this context configure the ingress for a spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vprn>if ingress)

Full Context configure service vprn interface ingress

Description This command enters context to configure ingress parameters for network interfaces.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vprn>if>sap ingress)

Full Context configure service vprn interface sap ingress

Description Commands in this context configure ingress SAP Quality of Service (QoS) policies and filter policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>vprn>if>vpls ingress)

Full Context configure service vprn interface vpls ingress

Description The ingress node in this context under the vpls binding is used to define the routed IPv4 and IPv6 optional filter overrides.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>aa-interface>sap ingress)
[Tree] (config>service>vprn>aa-interface>sap ingress)

Full Context configure service ies aa-interface sap ingress
configure service vprn aa-interface sap ingress

Description Commands in this context configure ingress parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ingress

Syntax **ingress**

Context **[Tree]** (config>card>mda>network ingress)

Full Context configure card mda network ingress

Description Commands in this context configure MDA-level IOM Quality of Service (QoS).

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>ies>video-interface>video-sap ingress)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>video-interface>video-sap ingress)
[Tree] (config>service>vprn>video-interface>video-sap ingress)

Full Context configure service ies video-interface video-sap ingress
configure service vpls video-interface video-sap ingress
configure service vprn video-interface video-sap ingress

Description Commands in this context configure in parameters for the service's video SAP.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

ingress

Syntax **ingress**

Context [Tree] (config>mirror>mirror-dest>spoke-sdp ingress)
[Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp ingress)
[Tree] (config>service>vprn>ipmirrorif>spoke-sdp ingress)
[Tree] (config>service>vprn>red-if>spoke-sdp ingress)

Full Context configure mirror mirror-dest remote-source spoke-sdp ingress
configure mirror mirror-dest spoke-sdp ingress
configure service vprn ip-mirror-interface spoke-sdp ingress
configure service vprn redundant-interface spoke-sdp ingress

Description Commands in this context configure spoke SDP ingress parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure mirror mirror-dest spoke-sdp ingress

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp ingress

All

- configure service vprn ip-mirror-interface spoke-sdp ingress
- configure mirror mirror-dest remote-source spoke-sdp ingress

ingress

Syntax **ingress**

Context [Tree] (config>qos>network ingress)

Full Context configure qos network ingress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to enter the CLI node that creates or edits policy entries that specify the DiffServ code points-to-forwarding class mapping for all IP packets and define the MPLS EXP bits-to-forwarding class mapping for all labeled packets.

When premarked IP or MPLS packets ingress on a network port, they get a Per Hop Behavior (that is, the QoS treatment through the router, based on the mapping defined under the current node).

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>qos>queue-group-templates ingress)

Full Context configure qos queue-group-templates ingress

Description Commands in this context create ingress queue group templates. Ingress queue group templates can be applied to ingress ports to create an ingress queue group of the same name.

An ingress template must be created for a group-name prior to creating a queue group with the same name on an ingress port.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>router>if ingress)

Full Context configure router interface ingress

Description This command enables access to the context to configure ingress network filter policies for the IP interface. If an ingress filter is not defined, no filtering is performed.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>cust>multi-service-site ingress)

Full Context configure service customer multi-service-site ingress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the ingress node associate an existing scheduler policy name with the customer site. The ingress node is an entity to associate commands that complement the association.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>pw-template ingress)

Full Context configure service pw-template ingress

Description Commands in this context configure spoke SDP binding ingress filter parameters.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>service>sdp>binding>pw-port ingress)

Full Context configure service sdp binding pw-port ingress

Description This command configures ingress parameters for the PW port.

Platforms All

ingress

Syntax **ingress**

Context **[Tree]** (config>subscr-mgmt>msap-policy>atm ingress)

Full Context configure subscriber-mgmt msap-policy atm ingress

Description Commands in this context configure MSAP ATM ingress parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

ingress

Syntax **ingress**

Context **[Tree]** (config>subscr-mgmt>sub-prof ingress)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt sub-profile ingress

Description Commands in this context configure subscriber profile ingress setting parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.130 ingress-buffer-allocation

ingress-buffer-allocation

Syntax **ingress-buffer-allocation** *percentage*
no ingress-buffer-allocation

Context **[Tree]** (config>card>fp ingress-buffer-allocation)

Full Context configure card fp ingress-buffer-allocation

Description This command allows the user to configure an ingress buffer allocation percentage per forwarding plane from 20.00% to 80.00%. Ingress buffer allocation applies to user-accessible buffers (total buffers less those reserved for system use).

The ingress buffer allocation percentage determines how much of the user-accessible buffers will be available for ingress purposes. The remaining buffers will be available for egress purposes.

This command is supported on all 50G FP2-based and 100G/200G FP3-based hardware. It is not supported on other FP2 or FP3-based hardware, nor on FP4-based hardware.

The **no** form of this command reverts the ingress buffer allocation to the default value.

Default ingress-buffer-allocation 50.00

Parameters *percentage* — Specifies the buffer allocation percentage.

Values 20.00 to 80.00

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

13.131 ingress-counter-map

ingress-counter-map

Syntax **ingress-counter-map policer** *policer-id* **traffic-type** {**unicast** | **multicast** | **broadcast**} [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ingress-counter-map queue *queue-id* **traffic-type** {**unicast** | **multicast** | **broadcast**} [**create**]
no ingress-counter-map policer *policer-id*
no ingress-counter-map queue *queue-id*

Context [Tree] (config>sflow ingress-counter-map)

Full Context configure sflow ingress-counter-map

Description This command configures the ingress counter map for sFlow. The map must be configured so sFlow agent understands how to interpret data collected against SAP queues and policers. Multiple queues/policers can be mapped to the same **traffic-type** using separate line entries.

The **no** form of this command deletes a SAP policy queue/policer from the map.

Parameters *policer-id* — Specifies the policer ID in a SAP ingress QoS policy. If the SAP policy does not have a policer with the specified ID, the map entry will be ignored for this SAP.

Values 1 to 32

queue-id — Specifies the queue ID in a SAP ingress QoS policy. If the SAP policy does not have a queue with the specified ID, the map entry will be ignored for this SAP.

Values 1 to 32

Platforms 7750 SR, 7750 SR-s, 7950 XRS

13.132 ingress-ip-filter-entries

ingress-ip-filter-entries

Syntax [**no**] **ingress-ip-filter-entries**

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl ingress-ip-filter-entries)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries

Description Commands in this context configure the ingress IP filter parameters.

The **no** form of this command reverts to the default.

Default ingress-ip-filter-entries

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.133 ingress-ipv6-filter-entries

ingress-ipv6-filter-entries

Syntax [**no**] **ingress-ipv6-filter-entries**

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl ingress-ipv6-filter-entries)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries

Description Commands in this context configure the ingress IPv6 filter parameters.

The **no** form of this command reverts to the default.

Default ingress-ipv6-filter-entries

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.134 ingress-label

ingress-label

Syntax **ingress-label** *label* [*label*]
no ingress-label [*label*]

Context **[Tree]** (debug>mirror-source ingress-label)

Full Context debug mirror-source ingress-label

Description This command enables ingress mirroring based on MPLS labels with the following limitations.

- The ingress label provisioned must be a MPLS transport label and can be at any label stack as long as it is known by the system. Transport label distributed by LDP, RSVP, and segment routing are supported. For BGP-specific label distribution mirroring, the following are supported.
  - BGP label-unicast (RFC 3107, *Carrying Label Information in BGP-4*)
  - VPN service labels distributed by BGP for Carrier Supporting Carrier (CSC) VPNs (RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*)
  - VPN service labels distributed by BGP in an ASBR (inter-as-option-B)
  - VPN service labels distributed by BGP in a route reflector with next-hop-self (RR + NHS)
- VPN service label mirroring is not supported in a provider edge (PE) router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The ingress label can only be mirrored to a single mirror destination. If the same label is defined with multiple mirror destinations, an error is generated and the original mirror destination remains unchanged.

The ingress label mirror source overrides all other mirror source definitions. The MPLS frame is mirrored to the mirror destination as it is received on the ingress network port. The router MPLS label space is global for the system. A specific label is mirrored to a mirror destination regardless of the ingress interface. In addition to mirroring known labels, debug also allows pre-provisioning label values which are yet to be known by the system. Be aware that debug mirroring requires provisioning of static label values while labels distributed by label distribution protocols are dynamic in nature. Therefore, when label values change due to network changes, labels provisioned in debug mirroring must be changed or deleted manually.

By default, no ingress MPLS frames are mirrored. The **ingress-label** command must be executed to start mirroring on a specific MPLS label.

Parameters *label* — Specifies up to eight transport labels received on ingress to be mirrored. Each label can only be mirrored to a single mirror destination.

If the label does not exist on any ingress network ports, no packets are mirrored for that label. An error will not occur. Once the label exists on a network port, ingress mirroring begins for that label.

Values 0 to 1048575

The local MPLS stack may not support portions of this range.

Platforms All

13.135 ingress-percent-of-total

ingress-percent-of-total

Syntax **ingress-percent-of-total** *percent-of-total-queues*
no ingress-percent-of-total

Context **[Tree]** (config>qos>fp-resource-policy>queues ingress-percent-of-total)

Full Context configure qos fp-resource-policy queues ingress-percent-of-total

Description This command configures the percentage of the total number of queues on the FP on which the policy is applied that are allocated to ingress, with the remainder allocated to egress. The ingress and egress buffer pool sizes are not affected by the queue allocation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The allocation is performed in sets of 8192 queues, with a minimum of 8192 queues at ingress and 8192 queues at egress. If the percentage configured results in the queue allocation not being a multiple of 8192, the number of queues at ingress is rounded down to the next 8192 boundary, and consequently the number of queues at egress is rounded up to the next 8192 boundary, both while respecting the minimum at ingress and egress.

If the FP resources policy being applied to any FP and the updated allocation is not achievable with the current ingress or egress queue consumption on any of the related FPs, then the command fails.

The configuration of **ingress-percent-of-total** command, including removing this parameter to return to its default configuration, causes the router to immediately reset the associated cards, XIOMs, and MDAs, except on the 7750 SR-1 where the configuration must be saved, and the router rebooted, immediately after committing the configuration transaction.

The **no** form of this command reverts the percentage of ingress queues, and consequently egress queues, to their default allocation.

Default ingress-percent-of-total 50.00

Parameters *percent-of-total-queues* — Specifies the percentage of total ingress queues as two fraction digits.

Values 4.00 to 97.00

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

13.136 ingress-policer

ingress-policer

Syntax **ingress-policer** *policer-name*
no ingress-policer

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm ingress-policer)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm ingress-policer)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt ingress-policer
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt ingress-policer

Description .This command specifies the ingress policer applied to all UEs corresponding to default vlan-range (such as group-interface) or the specified vlan-range. The policer can be created in the **config>subscr-mgmt>isa-policer** context. The ingress policer can be overridden per UE from RADIUS via access-accept or COA.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policer-name* — Specifies the identifier of the distributed-sub-mgmt policer for ingress traffic.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.137 ingress-rate

ingress-rate

Syntax **ingress-rate** *sub-rate*
no ingress-rate

Context **[Tree]** (config>port>ethernet ingress-rate)

Full Context configure port ethernet ingress-rate

Description This command configures the maximum amount of ingress bandwidth that this port can receive with the configured sub-rate using packet-based accounting.

The **no** form of this command returns the value to the default.

Default no ingress-rate

Parameters *sub-rate* — Specifies the ingress rate, in Mb/s.

Values 1 to 400000

Platforms All

13.138 ingress-repl-inc-mcast-advertisement

ingress-repl-inc-mcast-advertisement

Syntax [**no**] **ingress-repl-inc-mcast-advertisement**

Context **[Tree]** (config>service>vpls>bgp-evpn ingress-repl-inc-mcast-advertisement)

Full Context configure service vpls bgp-evpn ingress-repl-inc-mcast-advertisement

Description This command enables and disables the advertisement of the Inclusive Multicast Ethernet Tag route (IMET route) with tunnel-type Ingress-Replication in the PMSI Tunnel Attribute, or with the tunnel-type Composite Point-to-Multipoint and Ingress-Replication (P2MP+IR) in the root-and-leaf nodes. The following must be considered:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- When **no ingress-repl-inc-mcast-advertisement** is configured, no IMET routes will be sent for the service unless the **provider-tunnel** is configured with **owner bgp-evpn-mpls** and **root-and-leaf**, in which case, an IMET-P2MP route is sent.
- When **ingress-repl-inc-mcast-advertisement** and **provider-tunnel** are configured for **bgp-evpn-mpls** with **root-and-leaf**, the system will send an IMET-P2MP-IR route, that is, an IMET route with a composite P2MP+IR tunnel type.
- When **no ingress-repl-inc-mcast-advertisement** and **assisted-replication replicator** are configured, the system will send IMET-AR routes, but IMET-IR routes will not be sent.

Default ingress-repl-inc-mcast-advertisement

Platforms All

13.139 ingress-replication-bum-label

ingress-replication-bum-label

Syntax [**no**] **no-ingress-replication-bum-label**

Context **[Tree]** (config>service>vpls>bgp-evpn>mpls ingress-replication-bum-label)

Full Context configure service vpls bgp-evpn mpls ingress-replication-bum-label

Description This command allows the user to configure the system so that a separate label is sent for BUM (Broadcast, Unknown unicast and Multicast) traffic in a specified service. By default (**no ingress-replication-bum-label**), the same label is used for unicast and flooded BUM packets when for-warding traffic to remote PEs.

When saving labels, this might cause transient traffic duplication for all-active multi-homing. By enabling **ingress-replication-bum-label**, the system will advertise two labels per EVPN VPLS instance, one for unicast and one for BUM traffic. The ingress PE will use the BUM label for flooded traffic to the advertising egress PE, so that the egress PE can determine if the unicast traffic has been flooded by the ingress PE. Depending on the scale required in the network, the user may choose between saving label space or avoiding transient packet duplication sent to an all-active multi-homed CE for certain macs.

Default no ingress-replication-bum-label

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.140 ingress-statistics

ingress-statistics

Syntax **ingress-statistics**

Context **[Tree]** (config>router>mpls ingress-statistics)

Full Context configure router mpls ingress-statistics

Description Commands in this context enable ingress-statistics on an MPLS-TP LSP.

Platforms All

ingress-statistics

Syntax **ingress-statistics**

Context **[Tree]** (config>router>mpls>lsp ingress-statistics)

Full Context configure router mpls lsp ingress-statistics

Description Commands in this context enter the LSP names for the purpose of enabling ingress data path statistics at the terminating node of the LSP, for example, egress LER.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ingress-statistics

Syntax [**no**] **ingress-statistics**

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy ingress-statistics)

Full Context configure router mpls forwarding-policies forwarding-policy ingress-statistics

Description This command configures ingress statistics in an MPLS forwarding policy.

The ingress statistics are associated with a binding label, that is the ILM of the forwarding policy, and provides aggregate packet and byte counters for packets matching the binding label.

The **no** form of this command removes the statistics from the MPLS forwarding policy.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ingress-statistics

Syntax **ingress-statistics**

Context **[Tree]** (config>router>isis>segm-rtng ingress-statistics)
[Tree] (config>router>ospf>segm-rtng ingress-statistics)
[Tree] (config>router>ospf3>segm-rtng ingress-statistics)

Full Context configure router isis segment-routing ingress-statistics
configure router ospf segment-routing ingress-statistics
configure router ospf3 segment-routing ingress-statistics

Description Commands in this context configure the ingress statistics for IGP SIDs.

Platforms All

ingress-statistics

Syntax [**no**] **ingress-statistics**

Context **[Tree]** (config>router>segment-routing>sr-policies ingress-statistics)

Full Context configure router segment-routing sr-policies ingress-statistics

Description This command administratively enables the collection of ingress traffic statistics for all segment routing policies. The statistics provide counts for the number of incoming packets and bytes corresponding to each (color, endpoint) combination.

If there are any SR-MPLS interfaces on an FP2 or older line-cards, an attempt to enable this command will fail.

The **no** form of this command disables ingress stats collection for all segment routing policies.

Default no ingress-statistics

Platforms All

ingress-statistics

Syntax [**no**] **ingress-statistics**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action ingress-statistics)
[Tree] (config>router>policy-options>policy-statement>default-action ingress-statistics)

Full Context configure router policy-options policy-statement default-action ingress-statistics
configure router policy-options policy-statement entry action ingress-statistics

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the allocation of statistical indexes to BGP-LU route entries that are programmed on ingress data paths. For effective operation, a prefix must be advertised with a label per prefix for ILM statistics.

The **no** form of this command disables the allocation of statistical indexes to BGP-LU route entries.

Default no ingress-statistics

Platforms All

13.141 ingress-xpl

ingress-xpl

Syntax **ingress-xpl**

Context **[Tree]** (config>card>mda ingress-xpl)

Full Context configure card mda ingress-xpl

Description Commands in this context configure ingress MDA XPL interface error parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.142 init

init

Syntax **init** [**detail**]
no init

Context **[Tree]** (debug>router>ldp>peer>packet init)

Full Context debug router ldp peer packet init

Description This command enables debugging for LDP Init packets.

The **no** form of the command disables the debugging output.

Parameters **detail** — Displays detailed information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.143 init-cwnd-size

init-cwnd-size

Syntax **init-cwnd-size** *init-cwnd-size*

Context **[Tree]** (config>app-assure>group>tcp-optimizer init-cwnd-size)

Full Context configure application-assurance group tcp-optimizer init-cwnd-size

Description This command configures the initial TCP congestion window (cwnd) used during the TCP Slow Start (SS) period.

Parameters *init-cwnd-size* — Specifies the initial TCP congestion window size value in maximum segment size (mss).

Values 1 to 256

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

Default 10

13.144 init-delay

init-delay

Syntax **init-delay** *seconds*
no init-delay

Context **[Tree]** (config>service>ies>if>ipv6>vrrp init-delay)

Full Context configure service ies interface ipv6 vrrp init-delay

Description This command configures a VRRP initialization delay timer.

Default no init-delay

Parameters *seconds* — Specifies the initialization delay timer for VRRP, in seconds.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

init-delay

Syntax **init-delay** *seconds*
no init-delay

Context **[Tree]** (config>service>ies>if>vrrp init-delay)

Full Context configure service ies interface vrrp init-delay

Description This command configures a VRRP initialization delay timer.

Default no init-delay

Parameters *seconds* — Specifies the initialization delay timer for VRRP, in seconds.

Values 1 to 65535

Platforms All

init-delay

Syntax **init-delay** *seconds*
no init-delay

Context **[Tree]** (config>service>vprn>if>vrrp init-delay)
[Tree] (config>service>vprn>if>ipv6>vrrp init-delay)

Full Context configure service vprn interface ipv6 vrrp init-delay
configure service vprn interface vrrp init-delay

Description This command configures a VRRP initialization delay timer.

Default no init-delay

Parameters *seconds* — Specifies the initialization delay timer for VRRP, in seconds.

Values 1 to 65535

Platforms All

init-delay

Syntax **init-delay** *seconds*
no init-delay

Context **[Tree]** (config>router>if>vrrp init-delay)
[Tree] (config>router>if>ipv6>vrrp init-delay)

Full Context configure router interface ipv6 vrrp init-delay
configure router interface vrrp init-delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a VRRP initialization delay timer.

Default no init-delay

Parameters *seconds* — Specifies the initialization delay timer for VRRP, in seconds.

Values 1 to 65535

Platforms All

13.145 init-extract-prio-mode

init-extract-prio-mode

Syntax **init-extract-prio-mode** {**uniform** | **l3-classify**}

Context **[Tree]** (config>card>fp init-extract-prio-mode)

Full Context configure card fp init-extract-prio-mode

Description This command determines the scheme used to select the initial drop priority of extracted control plane traffic. The initial drop priority of extracted packets can be either low or high priority. The drop priority of the extracted packets can be subsequently altered by mechanisms such as CPU protection. High-priority traffic receives preferential treatment in control plane congestion situations over low-priority traffic.

Default init-extract-prio-mode uniform

Parameters **uniform** — Initializes the drop priority of all extracted control traffic as high priority. Drop priority can then be altered (marked low priority) by distributed CPU protection (DCP) or centralized CPU protection rate-limiting functions in order to achieve protocol and interface isolation.

l3-classify — Initializes the drop priority of Layer 3 extracted control traffic (BGP and OSPF) based on the QoS classification of the packets. This is useful in networks where the DSCP and EXP markings can be trusted as the primary method to distinguish, protect, and isolate good terminating protocol traffic from unknown or potentially harmful protocol traffic instead of using the rate-based DCP and centralized CPU protection traffic marking/coloring mechanisms (for example, **out-profile-rate** and **exceed-action low-priority**).

For network interfaces, the QoS classification profile result selects the drop priority (in = high priority, out = low priority) for extracted control traffic, and the default QoS classification maps different DSCP and EXP values to different in/out profile states.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For access interfaces, the QoS classification priority result typically selects the drop priority for extracted control traffic. The default access QoS classification (**default-priority**) maps all traffic to **low**. If the queues in the access QoS policy are configured as **profile-mode** queues (rather than the default **priority-mode**) extracted traffic will use the QoS classification profile value configured against the associated FC (rather than the priority result) to select the drop priority.

Layer 2 extracted control traffic (ARP or ETH-CFM) and protocols that cannot always be QoS-classified, such as IS-IS, are initialized as low drop priority in order to protect Layer 2 protocol traffic on uniform interfaces (which would typically be subject to centralized CPU protection). Alternately, DCP can be used (by configuring a non-zero rate with **exceed-action** of **low-priority** for the **all-unspecified** protocol) to mark some of this traffic as high priority.

Platforms All

13.146 init-ss-threshold

init-ss-threshold

Syntax **init-ss-threshold** *init-ss-threshold*

Context **[Tree]** (config>app-assure>group>tcp-optimizer init-ss-threshold)

Full Context configure application-assurance group tcp-optimizer init-ss-threshold

Description This command configures the initial Slow Start (SS) threshold for a given TCP optimizer policy. Nokia recommends to set the threshold close to the access network Bandwidth Delay Product (BDP).

Default 1000000

Parameters *init-ss-threshold* — Specifies the initial SS threshold value in kilobytes.

Values auto, 0 to 1000000

The auto value instructs the system to use an intelligent mechanismto set the optimum value for the initial SS threshold to dynamicallytrack the BDP of the access network.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.147 initial-app-profile

initial-app-profile

Syntax **initial-app-profile** *app-profile-name*
no initial-app-profile

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>wpp initial-app-profile)
[Tree] (config>service>ies>sub-if>grp-if>wpp initial-app-profile)
[Tree] (config>service>vprn>sub-if>grp-if>wpp initial-app-profile)

Full Context configure service ies subscriber-interface group-interface wpp initial-app-profile
configure service vprn subscriber-interface group-interface wpp initial-app-profile
configure subscriber-mgmt local-user-db ipoe host wpp initial-app-profile

Description This command specifies the initial app-profile for the hosts created on the group-interface. This initial app-profile is replaced after hosts pass web portal authentication.

The **no** form of this command reverts to the default.

Default no initial-app-profile

Parameters *app-profile-name* — Specifies the initial application profile, up to 32 characters, to be used during the WPP authentication phase of the IPoE hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.148 initial-hold-time

initial-hold-time

Syntax **initial-hold-time** *seconds*
initial-hold-time [**min** *min*] [**sec** *sec*]
no initial-hold-time

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile initial-hold-time)

Full Context configure subscriber-mgmt vrgw brg brg-profile initial-hold-time

Description This hold time applies to BRG instances that are created without any hosts; for example, triggered due to proxy authentication. During this initial hold-time the BRG is not deleted and no connectivity-verification is started. When this timer expires, connectivity verification is started. If connectivity verification is disabled and no hosts are associated with the BRG upon expiry, the regular hold time is started and the BRG instance will be removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command allows an operator to have fast BRG removal (no connectivity-verification and **no hold-time**) but still use BRG proxy authentication. Without an initial hold time the BRG would be removed immediately after creation.

This command does not apply to BRG instances that are created through host setup.

The **no** form of this command reverts to the default.

Default initial-hold-time min 5

Parameters *seconds* — Specifies the initial time, in seconds, to hold on to a BRG after the system considered it down.

Values 0 to 900

min — Specifies the initial time in minutes.

Values 1 to 15

sec — Specifies the initial time in seconds.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.149 initial-lease-time

initial-lease-time

Syntax **initial-lease-time** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no initial-lease-time

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>dhcp initial-lease-time)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>dhcp initial-lease-time)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp initial-lease-time)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp initial-lease-time)

Full Context configure service ies subscriber-interface group-interface wlan-gw dhcp initial-lease-time
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp initial-lease-time
configure service vprn subscriber-interface group-interface wlan-gw dhcp initial-lease-time
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp initial-lease-time

Description This command configures the lease time for a user which is migrant (unauthenticated).

Default initial-lease-time min 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hours* — Specifies the number of initial lease time hours.

Values 1 to 1

minutes — Specifies the number of initial lease time minutes.

Values 5 to 59

seconds — Specifies the number of initial lease time.

Values 1 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.150 initial-preferred-lifetime

initial-preferred-lifetime

Syntax **initial-preferred-lifetime** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no initial-preferred-lifetime

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 initial-preferred-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 initial-preferred-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>slaac initial-preferred-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>slaac initial-preferred-lifetime)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 initial-preferred-lifetime
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac initial-preferred-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 initial-preferred-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac initial-preferred-lifetime

Description This command specifies the signaled preferred lifetime in DHCPv6 or SLAAC after full authentication (DSM and/or ESM).

The **no** form of this command reverts to the default.

Default initial-preferred-lifetime min 5

Parameters *hours* — Specifies the number of initial preferred lifetime hours.

Values 1 to 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

minutes — Specifies the number of initial preferred lifetime minutes.

Values 5 to 59

seconds — Specifies the number of initial preferred lifetime seconds.

Values 1 to 59

Combined values: min 5 – hrs 1

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.151 initial-registration

initial-registration

Syntax **initial-registration ca** *ca-profile-name* **key-to-certify** *key-filename* **protection-alg** {**password** *password* **reference** *ref-number* | **signature** [**cert** *cert-file-name* [**send-chain** [**with-ca** *ca-profile-name*]]] [**protection-key** *key-file-name*] [**hash-alg** {**md5** | **sha1** | **sha224** | **sha256** | **sha384** | **sha512**}]} **subject-dn** *dn* [**domain-name** *domain-names*] [**ip-addr** *ip-address* | *ipv6-address*] **save-as** *save-path-of-result-cert*

Context **[Tree]** (admin>certificate>cmpv2 initial-registration)

Full Context admin certificate cmpv2 initial-registration

Description This command request initial certificate from CA by using CMPv2 initial registration procedure.

The **ca** parameter specifies a CA-profile which includes CMP server information.

The **key-to-certify** is an imported key file to be certified by the CA.

The protection-key is an imported key file used to for message protection if protection-alg is signature.

The request is authenticated either of following methods:

- A password and a reference number that pre-distributed by CA via out-of-band means.
- The specified password and reference number are not necessarily in the cmp-keylist configured in the corresponding CA-Profile
- A signature signed by the protection-key or key-to-certify, optionally along with the corresponding certificate. If the protection-key is not specified, system will use the key-to-certify for message protection. The hash algorithm used for signature is depends on key type:
- DSA key: SHA1
- RSA key: MD5/SHA1/SHA224 | SHA256 | SHA384 | SHA512, by default is SHA1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Optionally, the system could also send a certificate or a chain of certificates in extraCerts field. Certificate is specified by the “cert” parameter, it must include the public key of the key used for message protection.

Sending a chain is enabled by specify the **send-chain** parameter.

subject-dn specifies the subject of the requesting certificate.

save-as specifies full path name of saving the result certificate.

In some cases, CA may not return certificate immediately, due to reason like request processing need manual intervention. In such cases, the **admin certificate cmpv2** poll command could be used to poll the status of the request. If key-list is not configured in the corresponding **ca-profile**, then the system will use the existing password to authenticate the CMPv2 packets from server if it is in password protection.

If key-list is configured in the corresponding **ca-profile** and server does not send SenderKID, then the system will use lexicographical first key in the key-list to authenticate the CMPv2 packets from server in case it is in password protection.

Parameters *ca-profile-name* — Specifies a ca-profile name which includes CMP server information up to 32 characters.

key-filename — Specifies the file name of the key to certify up to 95 characters.

password — Specifies an ASCII string up to 64 characters.

ref-number — Specifies the reference number for this CA initial authentication key up to 64 characters.

cert-file-name — specifies the certificate file up to 95 characters.

ca-profile-name — Specifies to send the chain.

key-file-name — Specifies the protection key associated with the action on the CA profile.

hash-algorithm — Specifies the hash algorithm for RSA key.

Values md5,sha1,sha224,sha256,sha384,sha512

dn — Specifies the subject of the requesting certificate up to 256 characters.

Values attr1 equals val1
attr2 equals val2 where: attrN equals {C | ST | O | OU | CN}

save-path-of-result-cert — Specifies the save full path name of saving the result certificate up to 200 characters.

domain-name *domain-names* — Specifies FQDNs for SubjectAltName of the requesting certificate, separated by commas, up to 512 characters.

ip-address **|** *ipv6-address* — Specifies an IPv4 or IPv6 address for SubjectAtName of the requesting certificate.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.152 initial-send-delay-zero

initial-send-delay-zero

Syntax [**no**] **initial-send-delay-zero**

Context **[Tree]** (config>service>vprn>bgp initial-send-delay-zero)
[Tree] (config>service>vprn>bgp>group initial-send-delay-zero)
[Tree] (config>service>vprn>bgp>group>neighbor initial-send-delay-zero)

Full Context configure service vprn bgp group initial-send-delay-zero
configure service vprn bgp group neighbor initial-send-delay-zero
configure service vprn bgp initial-send-delay-zero

Description This command configures BGP to send UPDATE messages announcing reachability information to a peer or set of peers immediately after the sessions come up (become established) with these peers.

The default behavior, provided by the **no** form of this command, is to wait for min-route-advertisement time after each session is established before sending the first set of UPDATE messages.

Platforms All

initial-send-delay-zero

Syntax [**no**] **initial-send-delay-zero**

Context **[Tree]** (config>router>bgp initial-send-delay-zero)
[Tree] (config>router>bgp>group initial-send-delay-zero)
[Tree] (config>router>bgp>group>neighbor initial-send-delay-zero)

Full Context configure router bgp group initial-send-delay-zero
configure router bgp group neighbor initial-send-delay-zero
configure router bgp initial-send-delay-zero

Description This command configures BGP to send UPDATE messages announcing reachability information to a peer or set of peers immediately after the sessions become established with these peers.

The **no** form of this command waits for **min-route-advertisement** time after each session is established before sending the first set of UPDATE messages.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.153 initial-sla-profile

initial-sla-profile

Syntax **initial-sla-profile** *sla-profile-name*
no initial-sla-profile

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>wpp initial-sla-profile)
[Tree] (config>service>ies>sub-if>grp-if>wpp initial-sla-profile)
[Tree] (config>service>vprn>sub-if>grp-if>wpp initial-sla-profile)

Full Context configure service ies subscriber-interface group-interface wpp initial-sla-profile
configure service vprn subscriber-interface group-interface wpp initial-sla-profile
configure subscriber-mgmt local-user-db ipoe host wpp initial-sla-profile

Description This command specifies the initial sla-profile for the hosts created on the group-interface. This initial sla-profile is replaced after hosts pass web portal authentication.

The **no** form of this command reverts to the default.

Parameters *sla-profile-name* — Specifies the initial SLA profile, up to 32 characters, to be used during the WPP authentication phase of the IPOE host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

initial-sla-profile

Syntax **initial-sla-profile** *profile-name*
no initial-sla-profile

Context **[Tree]** (config>router>wpp initial-sla-profile)

Full Context configure router wpp initial-sla-profile

Description This command specifies the initial sla-profile for the hosts created on the group-interface. This initial sla-profile is replaced after hosts pass the web portal authentication.

Default no initial-sla-profile

Parameters *profile-name* — Specifies the name of sla-profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.154 initial-sub-profile

initial-sub-profile

Syntax **initial-sub-profile** *sub-profile-name*
no initial-sub-profile

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>wpp initial-sub-profile)
[Tree] (config>service>ies>sub-if>grp-if>wpp initial-sub-profile)
[Tree] (config>service>vprn>sub-if>grp-if>wpp initial-sub-profile)

Full Context configure service ies subscriber-interface group-interface wpp initial-sub-profile
configure service vprn subscriber-interface group-interface wpp initial-sub-profile
configure subscriber-mgmt local-user-db ipoe host wpp initial-sub-profile

Description This command specifies the initial sub-profile for the hosts created on the group-interface. This initial sub-profile is replaced after hosts pass web portal authentication.

The **no** form of this command reverts to the default.

Default no initial-sub-profile

Parameters *sub-profile-name* — Specifies the initial subscriber profile, up to 32 characters, to be used during the WPP authentication phase of the IPoE host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.155 initial-valid-lifetime

initial-valid-lifetime

Syntax **initial-valid-lifetime** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no initial-valid-lifetime

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 initial-valid-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp6 initial-valid-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>slaac initial-valid-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>slaac initial-valid-lifetime)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 initial-valid-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac initial-valid-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp6 initial-valid-lifetime
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range slaac initial-valid-lifetime

Description This command specifies the signaled preferred lifetime in DHCPv6 or SLAAC during a migrant phase.

The **no** form of this command reverts to the default.

Default initial-valid-lifetime min 5

Parameters *hours* — Specifies the number of initial preferred lifetime hours.

Values 1 to 1

minutes — Specifies the number of initial preferred lifetime minutes.

Values 5 to 59

seconds — Specifies the number of initial preferred lifetime seconds.

Values 1 to 59

Combined values: min 5 – hrs 1

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.156 initiation-message

initiation-message

Syntax **initiation-message** [*initiation-message*]
no initiation-message

Context **[Tree]** (config>bmp>station initiation-message)

Full Context configure bmp station initiation-message

Description This command configures a free-form initiation message for a type 0 TLV to be sent to the BMP monitoring station. The message is transmitted when a BMP monitoring station establishes a connection to the device. Information can be provided to the BMP station system administrator (for example, a contact phone number). The initiation message includes a type 1 TLV containing the SNMP sysDescr value specified in RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*, and a type 2 TLV containing the SNMP sysName value also from RFC 1213. The string in the initiation-message is UTF-8 encoded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes initiation message from the configuration and causes a free-form message to be included in the type 0 information TLV and the corresponding tlv-length is made 0.

Parameters *initiation-message* — Specifies an initiation message up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

13.157 inner-tag

inner-tag

Syntax **inner-tag** *value* [*vid-mask*]
no inner-tag

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match inner-tag)

Full Context configure qos sap-ingress mac-criteria entry match inner-tag

Description This command configures the matching of the second tag that is carried transparently through the service. The inner tag on ingress is the second tag on the frame if there are no service delimiting tags. The inner tag is the second tag before any service delimiting tags on egress but is dependent in the ingress configuration and may be set to 0 even in cases where additional tags are on the frame. This allows matching VLAN tags for explicit filtering or QoS setting when using default or null encapsulations.

The inner tag is not applicable in ingress on dot1Q SAPs. The inner tag may be populated on egress depending on the ingress SAP type.

On QinQ SAPs of null and default that do not strip tags, the inner-tag will contain the second tag (which is still the second tag carried transparently through the service.) On ingress SAPs that strip any tags, the inner tag will contain 0 even if there are more than two tags on the frame.

The optional vid_mask is defaulted to 4095 (exact match) but may be specified to allow pattern matching. The masking operation is ((value and vid-mask) = = (tag and vid-mask)). A value of 6 and a mask of 7 would match all VIDs with the lower 3 bits set to 6.

For QoS, the VID type cannot be specified on the default QoS policy.

The default vid-mask is set to 4095 for exact match.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

inner-tag

Syntax **inner-tag** *value* [*vid-mask*]
no inner-tag

Context **[Tree]** (config>filter>mac-filter>entry>match inner-tag)

Full Context configure filter mac-filter entry match inner-tag

Description This command configures the matching of the second tag that is carried transparently through the service. The inner-tag on ingress is the second tag on the frame if there are no service delimiting tags. Inner tag is the second tag before any service delimiting tags on egress but is dependent in the ingress configuration and may be set to 0 even in cases where additional tags are on the frame. This allows matching VLAN tags for explicit filtering or QoS setting when using default or null encapsulations.

The inner-tag is not applicable in ingress on dot1Q SAPs. The inner-tag may be populated on egress depending on the ingress SAP type.

On QinQ SAPs of null and default that do not strip tags inner-tag will contain the second tag (which is still the second tag carried transparently through the service.) On ingress SAPs that strip any tags, inner-tag will contain 0 even if there are more than 2 tags on the frame.

The optional *vid-mask* is defaulted to 4095 (exact match) but may be specified to allow pattern matching. The masking operation is ((value and vid-mask) = = (tag and vid-mask)). A value of 6 and a mask of 7 would match all VIDs with the lower 3 bits set to 6.

For QoS the VID type cannot be specified on the default QoS policy.

The default vid-mask is set to 4095 for exact match.

Default no inner-tag

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.158 input

input

Syntax **input**

Context **[Tree]** (config>system>sync-if-timing>bits input)

Full Context configure system sync-if-timing bits input

Description This command provides a context to enable or disable the external BITS timing reference inputs to the central clock of the router. In redundant systems with BITS ports, there are two possible BITS-in interfaces, one for each CPM or CCM.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.159 input-power-mode

input-power-mode

Syntax **input-power-mode** *amperage*

Context **[Tree]** (config>system>pwr-mgmt>peq input-power-mode)

Full Context configure system power-management peq input-power-mode

Description This command sets the input-power-mode of the APEQ for the designated APEQ slot. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Parameters *amperage* — Sets the APEQ input power mode.

Values 60, 80

Default 60

Platforms 7750 SR-12e, 7950 XRS

13.160 insert

insert

Syntax **insert** [*line*]

Context **[Tree]** (candidate insert)

Full Context candidate insert

Description This command inserts the contents of the temporary buffer (populated by a previous copy or delete command) into the candidate configuration. The contents are inserted by default after the current edit point. Optional parameters allow the insertion after some other point of the candidate. The contents of the temporary buffer are deleted when the operator exits candidate edit mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Insertions are context-aware. The temporary buffer always stores the CLI context (such as the current CLI branch) for each line deleted or copied. If the lines to be inserted are supported at the context of the insertion point then the lines are simply inserted into the configuration. If the lines to be inserted are not supported at the context of the insertion point, then the context at the insertion point is first closed using multiple exit statements, the context of the lines to be inserted is built (added) into the candidate at the insertion point, then the lines themselves are added, the context of the inserted lines is closed using exit statements and finally the context from the original insertion point is built again leaving the context at the same point as it was before the insertion.

Parameters *line* — Indicates where to insert the line starting at the point indicated by the following options.

Values

line, offset, **first**, **edit-point**, **last**

line	absolute line number
offset	relative line number to current edit point. Prefixed with '+' or '-'
first	keyword - first line
edit-point	keyword - current edit point
last	keyword - last line that is not 'exit'

13.161 insert-ipv6-fragment-header

insert-ipv6-fragment-header

Syntax [**no**] **insert-ipv6-fragment-header**

Context **[Tree]** (config>service>vprn>inside>nat64 insert-ipv6-fragment-header)

Full Context configure service vprn inside nat64 insert-ipv6-fragment-header

Description This command specifies if the system always inserts an IPv6 fragment header, to indicate that the sender allows fragmentation.

The **no** form of the command does not allow the system to insert an IPv6 fragment header.

Default disabled

insert-ipv6-fragment-header

Syntax [**no**] **insert-ipv6-fragment-header**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>nat>inside>nat64 insert-ipv6-fragment-header)
[Tree] (config>router>nat>inside>nat64 insert-ipv6-fragment-header)

Full Context configure router nat inside nat64 insert-ipv6-fragment-header
configure service vprn nat inside nat64 insert-ipv6-fragment-header

Description This command specifies whether the NAT64 node will insert IPv6 fragment header to IPv6 packets for which the DF bit is not set in the corresponding IPv4 packet, and is not already a fragment.

The **no** form of the command disables the insertion.

Default disabled

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.162 insert-nsh

insert-nsh

Syntax [**no**] **insert-nsh**

Context [Tree] (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action insert-nsh)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action insert-nsh

Description Commands in this context configure NSH parameters in the steered traffic.

The **no** form of this command removes insert NSA parameters from the configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.163 insert-subscriber-id

insert-subscriber-id

Syntax [**no**] **insert-subscriber-id**

Context [Tree] (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action>insert-nsh>meta-data insert-subscriber-id)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action insert-nsh meta-data insert-subscriber-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies that the metadata to be inserted in NSH (with MD-Type set to 1) must contain a subscriber identifier that is derived from the subscriber string that comes from the AAA server (in Alc-Subsc-Id-Str VSA). The subscriber string is truncated after the first 16 bytes, and therefore, the first 16 bytes should be unique. The **insert-subscriber-id** and **insert-subscriber-id** commands are mutually exclusive.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.164 inside

inside

Syntax **inside**

Context **[Tree]** (config>service>vprn>nat inside)
[Tree] (config>router>nat inside)

Full Context configure router nat inside
configure service vprn nat inside

Description Commands in this context the inside NAT instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.165 inside-service-id

inside-service-id

Syntax [**no**] **inside-service-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes inside-service-id)

Full Context configure aaa isa-radius-policy acct-include-attributes inside-service-id

Description This command enables the inclusion of the NAT inside service ID attributes.

The **no** form of the command excludes NAT inside service ID attributes.

Default no inside-service-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.166 install-backup-path

install-backup-path

Syntax **install-backup-path**
no install-backup-path

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action install-backup-path)
[Tree] (config>router>policy-options>policy-statement>default-action install-backup-path)

Full Context configure router policy-options policy-statement default-action install-backup-path
configure router policy-options policy-statement entry action install-backup-path

Description When the best BGP route for an IPv4 or IPv6 prefix is matched by a policy entry or policy default action with this command, BGP attempts to find and install a preprogrammed backup path for the prefix in order to provide BGP fast reroute protection.

The **install-backup-path** command overrides and has no dependency on commands such as the BGP instance **backup-path** command or the VPRN-level **enable-bgp-vpn-backup** command, which enable BGP fast reroute for an entire address family. The **install-backup-path** command provides more precise control over which IP prefixes are supported with preprogrammed backup paths.

In VPRN, if the best path for an IP prefix is provided by a VPRN BGP route, the backup path can be provided by another VPRN BGP route or an imported VPN-IP route. If the best path for an IP prefix is provided by an imported VPN-IP route, the backup path can be provided by another VPN-IP route.

The **install-backup-path** command is supported only in BGP and VRF import policies and has no effect on other types. The **install-backup-path** command applies only to the following types of matched routes: IPv4, IPv6, label-IPv4, label-IPv6, VPN-IPv4, and VPN-IPv6.

The **no** form of this command disables the install-backup-path functionality.

Default no install-backup-path

Platforms All

13.167 instance

instance

Syntax **instance** *instance*

Context **[Tree]** (debug>dynsvc>scripts instance)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug dynamic-services scripts instance

Description Commands in this context configure dynamic services script debugging for a specific instance.

Parameters *instance* — Specifies the instance name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

instance

Syntax [**no**] **instance** *instance*

Context **[Tree]** (debug>vsd>scripts instance)

Full Context debug vsd scripts instance

Description This command enables/disables the generation of script debugging for a specific instance

Parameters *instance* — Specifies the instance name.

Platforms All

instance

Syntax **instance** *instance-id* **instance-value** *instance-value*
no instance *instance-id*

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy>p2mp-candidate-path>instances instance)

Full Context configure router p2mp-sr-tree p2mp-policy p2mp-candidate-path instances instance

Description This command configures the candidate path instance for the P2MP SR tree as primary or secondary, and the instance identifier.

The **no** form of this command removes the candidate path instance.

Parameters *instance-id* — Specifies the instance as primary (1) or secondary (2).

Values 1, 2

instance-value — Specifies the instance identifier.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.168 instance-id

instance-id

Syntax **instance-id** *instance-id*
no instance-id

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment instance-id)

Full Context configure router p2mp-sr-tree replication-segment instance-id

Description This command configures the instance ID for the P2MP SR tree replication segment entry.

The ID is a unique identifier for the P2MP LSP on the root. The combination of root ID, tree ID, and instance ID uniquely identifies a P2MP LSP throughout the network.

The **no** form of this command removes the instance.

Parameters *instance-id* — Specifies the ID of the instance.

Values 1 to 4294967295

Platforms All

13.169 instances

instances

Syntax **instances**

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy>p2mp-candidate-path instances)

Full Context configure router p2mp-sr-tree p2mp-policy p2mp-candidate-path instances

Description Commands in this context configure the instance entries of the candidate path.

Multiple path instances can exist in a candidate path for the P2MP SR tree. Each path instance is a P2MP LSP and has an instance ID. Path instances are used for global optimization of the active candidate path.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.170 instant-prune-echo

instant-prune-echo

Syntax [**no**] **instant-prune-echo**

Context **[Tree]** (config>service>vprn>pim>if instant-prune-echo)

Full Context configure service vprn pim interface instant-prune-echo

Description This command enables PIM to send an instant prune echo when the router starts the prune pending timer for a group on the interface. All downstream routers will see the prune message immediately, and can send a join override if they are interested in receiving the group. Configuring instant-prune-echo is recommended on broadcast interfaces with more than one PIM neighbor to optimize multicast convergence.

The **no** form of this command disables instant Prune Echo on the PIM interface.

Default no instant-prune-echo

Platforms All

instant-prune-echo

Syntax [**no**] **instant-prune-echo**

Context **[Tree]** (config>router>pim>interface instant-prune-echo)

Full Context configure router pim interface instant-prune-echo

Description This command enables PIM to send an instant prune echo when the router starts the prune pending timer for a group on the interface. All downstream routers will see the prune message immediately, and can send a join override if they are interested in receiving the group. Configuring instant-prune-echo is recommended on broadcast interfaces with more than one PIM neighbor to optimize multicast convergence.

The **no** form of this command disables instant Prune Echo on the PIM interface.

Default no instant-prune-echo

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.171 int-dest-id

int-dest-id

Syntax **int-dest-id** *int-dest-id*
no int-dest-id

Context **[Tree]** (config>service>sdp>binding>pw-port>egress>shaper int-dest-id)

Full Context configure service sdp binding pw-port egress shaper int-dest-id

Description This command configures an intermediate destination identifier applicable to ESM PW SAPs.

The **no** form of the command removes the intermediate destination identifier from the configuration.

Default no int-dest-id

Parameters *int-dest-id* — Specifies the intermediate destination ID.

Platforms All

int-dest-id

Syntax **int-dest-id** *name*
no int-dest-id

Context **[Tree]** (config>service>epipe>pw-port>egress>shaper int-dest-id)

Full Context configure service epipe pw-port egress shaper int-dest-id

Description This command configures an intermediate destination identifier applicable to ESM PW SAPs.

Parameters *name* — Specifies the default intermediate destination identifier, up to 32 characters in length, on the egress side for this PW-port entry.

Platforms All

13.172 inter-chassis-redundancy

inter-chassis-redundancy

Syntax **inter-chassis-redundancy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>isa>nat-group inter-chassis-redundancy)

Full Context configure isa nat-group inter-chassis-redundancy

Description Commands in this context configure inter-chassis redundancy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.173 inter-dest-id

inter-dest-id

Syntax **inter-dest-id** *intermediate-destination-id*
no inter-dest-id

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings inter-dest-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings inter-dest-id)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings inter-dest-id
configure subscriber-mgmt local-user-db ppp host identification-strings inter-dest-id

Description This command specifies the intermediate destination identifier which is encoded in the identification strings.

The **no** form of this command returns to the default.

Parameters *intermediate-destination-id* — Specifies the intermediate destination identifier, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

inter-dest-id

Syntax **inter-dest-id** *intermediate-destination-id*
no inter-dest-id

Context [Tree] (config>service>ies>if>sap>static-host inter-dest-id)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host inter-dest-id)
[Tree] (config>service>vpls>sap>static-host inter-dest-id)
[Tree] (config>service>vprn>if>sap>static-host inter-dest-id)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host inter-dest-id)

Full Context configure service ies interface sap static-host inter-dest-id
configure service ies subscriber-interface group-interface sap static-host inter-dest-id
configure service vpls sap static-host inter-dest-id
configure service vprn interface sap static-host inter-dest-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap static-host inter-dest-id

Description This command specifies to which intermediate destination (for example a DSLAM) this host belongs.

The **no** form of this command reverts to the default.

Parameters *intermediate-destination-id* — Specifies the intermediate destination identifier, up to 32 characters in length.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.174 inter-vlan

inter-vlan

Syntax [**no**] **inter-vlan**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>mobility inter-vlan)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>mobility inter-vlan)

Full Context configure service ies subscriber-interface group-interface wlan-gw mobility inter-vlan
configure service vprn subscriber-interface group-interface wlan-gw mobility inter-vlan

Description This command enables mobility within different VLANs of the same range. When enabled, mobility between different VLANs in a single vlan-range is allowed for the configured mobility triggers.

The **no** form of this command disables mobility between VLANs.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.175 interactive-authentication

interactive-authentication

Syntax [**no**] **interactive-authentication**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius interactive-authentication)

Full Context configure service vprn aaa remote-servers radius interactive-authentication

Description This command enables RADIUS interactive authentication for the system. Enabling interactive-authentication forces RADIUS to fall into challenge/response mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no interactive-authentication

Platforms All

interactive-authentication

Syntax [**no**] **interactive-authentication**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus interactive-authentication)

Full Context configure service vprn aaa remote-servers tacplus interactive-authentication

Description This configuration instructs the SR OS to send no username nor password in the TACACS+ start message, and to display the *server_msg* in the GETUSER and GETPASS response from the TACACS+ server. Interactive authentication can be used to support a One Time Password scheme (such as an S/Key). An example flow (such as with a telnet connection) is as follows:

- The SR OS sends an authentication start request to the TACACS+ server with no username nor password.
- TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETUSER and a *server_msg*.
- The SR OS displays the *server_msg*, and collects the username.
- The SR OS sends a continue message with the username.
- TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETPASS and a *server_msg*.
- The SR OS displays the *server_msg* (which may contain, for example, an S/Key for One Time Password operation), and collects the password.
- The SR OS sends a continue message with the password.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is disabled the SR OS will send the username and password in the *tacplus* start message. An example flow (e.g. with a telnet connection) is as follows:

- TAC_PLUS_AUTHEN_TYPE_ASCII.
  - the login username in the “user” field.
  - the password in the *user_msg* field (while this is non-standard, it does not cause interoperability problems).
- TACACS+ server ignores the password and replies with TAC_PLUS_AUTHEN_STATUS_GETPASS.
- The SR OS sends a continue packet with the password in the *user_msg* field.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is enabled, tacplus must be the first method specified in the authentication-order configuration.

Default no interactive-authentication

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

interactive-authentication

Syntax [**no**] **interactive-authentication**

Context **[Tree]** (config>system>security>radius interactive-authentication)

Full Context configure system security radius interactive-authentication

Description This command enables RADIUS interactive authentication for the system. Enabling interactive-authentication forces RADIUS to fall into challenge/response mode.

Default no interactive-authentication

Platforms All

interactive-authentication

Syntax [**no**] **interactive-authentication**

Context **[Tree]** (config>system>security>tacplus interactive-authentication)

Full Context configure system security tacplus interactive-authentication

Description This configuration instructs the SR OS to send no username nor password in the TACACS+ start message, and to display the *server_msg* in the GETUSER and GETPASS response from the TACACS+ server. Interactive authentication can be used to support a One Time Password scheme (e.g. S/Key). An example flow (e.g. with a telnet connection) is as follows:

- The SR OS sends an authentication start request to the TACACS+ server with no username nor password.
- TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETUSER and a *server_msg*.
- The SR OS displays the *server_msg*, and collects the user name.
- The SR OS sends a continue message with the user name.
- TACACS+ server replies with TAC_PLUS_AUTHEN_STATUS_GETPASS and a *server_msg*.
- The SR OS displays the *server_msg* (which may contain, for example, an S/Key for One Time Password operation), and collects the password.
- The SR OS sends a continue message with the password.
- TACACS+ server replies with PASS or FAIL.

When interactive-authentication is disabled the SR OS sends the username and password in the *tacplus* start message. An example flow (e.g. with a telnet connection) is as follows:

- TAC_PLUS_AUTHEN_TYPE_ASCII.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- the login username in the “user” field.
- the password in the *user_msg* field (while this is non-standard, it does not cause interoperability problems).

• TACACS+ server ignores the password and replies with TAC_PLUS_AUTHEN_STATUS_GETPASS.
• The SR OS sends a continue packet with the password in the *user_msg* field.
• TACACS+ server replies with PASS or FAIL.

When interactive-authentication is enabled, tacplus must be the first method specified in the authentication-order configuration.

Default no interactive-authentication

Platforms All

13.176 intercept-id

intercept-id

Syntax **intercept-id** *id*
no intercept-id

Context **[Tree]** (config>li>li-source>nat>classic-lsn-sub intercept-id)
[Tree] (config>li>li-source>nat>dslite-lsn-sub intercept-id)
[Tree] (config>li>li-source>nat>ethernet-header intercept-id)
[Tree] (config>li>li-source>nat>l2-aware-sub intercept-id)
[Tree] (config>li>li-source>nat>nat64-lsn-sub intercept-id)

Full Context configure li li-source nat classic-lsn-sub intercept-id
configure li li-source nat dslite-lsn-sub intercept-id
configure li li-source nat ethernet-header intercept-id
configure li li-source nat l2-aware-sub intercept-id
configure li li-source nat nat64-lsn-sub intercept-id

Description This command configures the intercept-id that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This **intercept-id** can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs.

For nat mirroring (a **nat li-source** entry type), when the mirror service is not configured with any routable encap (for example, no ip-udp-shim or ip-gre configured under **config>mirror>mirror-dest>encap**), the presence of a configured intercept-id against an li-source (nat) entry will cause the insertion of the intercept-id after a configurable mac-da, mac-sa and etype (configured under **li-source>nat>ethernet-header**), at the front of each packet mirrored for that particular li-source entry. If there is no **intercept-id** configured (for a

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat entry using a mirror service without routable encap), then a configurable mac-da and mac-sa are added to the front of the packets (but no intercept-id). In both cases a non-configurable etype is also added immediately before the mirrored customer packet. Note that routable encapsulation configured in the mirror-dest takes precedence over the ethernet-header configuration in the li-source nat entries. If routable encapsulation is configured, then the ethernet-header config is ignored and no mac header is added to the packet (the encap is determined by the mirror-dest in this case).

For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, an intercept-id field (as part of the routable encap) is always present in the mirrored packets. If there is no intercept ID configured for an li-source entry, then the default value will be inserted. When the mirror service is configured with ip-gre routable encap, no intercept-id is inserted and none should be specified against the **li-source** entries.

The **no** form of this command removes the value from the configuration.

Default no intercept-id (an id of 0, or no id)

Parameters *id* — Specifies the intercept ID value to insert into the header of the mirrored packets.

Values 1 to 4294967295 (32b) For nat li-source entries that are using a mirror service that is not configured with routable encap

Values 1 to 1,073,741,824 (30b) For all types of li-source entries that are using a mirror service with routable ip-udp-shim encap and no direction-bit.

Values 1 to 536,870,912 (29b) For all types of li-source entries that are using a mirror service with routable ip-udp-shim encap and with the direction-bit enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

intercept-id

Syntax **intercept-id** [*intercept-id*]
no intercept-id

Context **[Tree]** (config>li>li-source>wlan-gw intercept-id)

Full Context configure li li-source wlan-gw intercept-id

Description This command configures the intercept-id inserted in the packet header for all mirrored packets of the associated li-source. When the mirror service is configured with the **ip-udp-shim** routable encapsulation, the intercept-id field (as part of the routable encap) is always present in the mirrored packets. The intercept ID can be used by the LIG to identify a particular LI session to which the packet belongs.

Parameters *intercept-id* — Specifies the intercept ID inserted in the LI header.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.177 interconnect

interconnect

Syntax **interconnect** {**ring-id** *ring-index* | **vpls**}
no interconnect

Context **[Tree]** (config>eth-ring>sub-ring interconnect)

Full Context configure eth-ring sub-ring interconnect

Description This command links the G.8032 sub-ring to a ring instance or to a VPLS instance. The ring instance must be a complete ring with two paths but may itself be a sub-ring or a major ring (declared by its configuration on another node).

When the interconnection is to another node, the sub-ring may have a virtual link or a non-virtual-link.

When the sub-ring is configured with a non-virtual link, the sub ring may be alternatively connected to a VPLS service.

This command is only valid on the interconnection node where a single sub-ring port connects to a major ring or terminates on a VPLS service.

The **no** form of this command removes the interconnect node.

Default no interconnect

Parameters *ring-id* — Specifies the identifier for the ring instance of the connection ring for this sub-ring on this node.

Values 0 to 128

vpls — Specifies that the sub-ring is connected to the VPLS instance that contains the sub-ring SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.178 interface

interface

Syntax **interface** *ip-int-name* **service-id** *service-id*
no interface

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host interface)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt local-user-db ipoe host interface

Description This command specifies the interface where IPoE sessions are terminated.

The **no** version of this command disables the parameter.

Parameters *ip-int-name* — Specifies the name of the group interface.

service-id — Specifies the service ID or name where the group interface resides.

Values *service-id* — 1 to 2147483647
service-name — up to 64 characters

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

interface

Syntax **interface** *ip-int-name* **service-id** *service-id*
no interface

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host interface)

Full Context configure subscriber-mgmt local-user-db ppp host interface

Description This command configures the interface where PPP sessions are terminated.

The **no** form of this command reverts to the default.

Parameters *ip-int-name* — Specifies the name of the group interface, up to 32 characters, where the PPP sessions are established.

service-id — Specifies the service ID or name of the service where the PPP sessions are established.

Values *service-id*: 1 to 2147483647
service-name: up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

interface

Syntax **interface** *ip-int-name*
no interface

Context **[Tree]** (config>service>vprn>dhcp interface)
[Tree] (config>service>vprn>dhcp6 interface)

Full Context configure service vprn dhcp interface
configure service vprn dhcp6 interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure interface parameters.

Parameters *ip-int-name* — Specifies the name of the IP interface, up to 32 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

interface

Syntax **interface** *ip-int-name* [**create**]
interface *ip-int-name* [**create**] **tunnel**
no interface *ip-int-name*

Context **[Tree]** (config>service>vprn interface)
[Tree] (config>service>ies interface)

Full Context configure service ies interface
configure service vprn interface

Description This command creates a logical IP routing interface. Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The **interface** command, under the context of services, is used to create and maintain IP routing interfaces within service IDs. The **interface** command can be executed in the context of a service ID. The IP interface created is associated with the service core network routing instance and default routing table. The typical use for IP interfaces created in this manner is for subscriber Internet access. An IP address cannot be assigned to an IES interface. Multiple SAPs can be assigned to a single group interface.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for **config>router>interface**, **config>service>ies>interface** and **config>service>vprn>interface** (that is, the network core router instance). Interface names must not be in the dotted decimal notation of an IP address. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The **no** form of this command removes IP the interface and all the associated configuration. The interface must be administratively shut down before issuing the **no interface** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IP interface must be shut down before the SAP on that interface may be removed. IES and VPRN services do not have the **shutdown** command in the SAP CLI context. The service SAPs rely on the interface status to enable and disable them.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and config service vprn interface commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

If *ip-int-name* already exists within the service ID, the context will be changed to maintain that IP interface. If *ip-int-name* already exists within another service ID or is an IP interface defined within the **config router** commands, an error will occur and context will not be changed to that IP interface. If *ip-int-name* does not exist, the interface is created and context is changed to that interface for further command processing.

tunnel — Specifies that the interface is configured as tunnel interface, which could be used to terminate IPsec or GRE runnels in the private service.

create — Creates the IPsec interface instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>igmp interface)

Full Context configure router igmp interface

Description Commands in this context configure an IGMP interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of the command deletes the IGMP interface. The **shutdown** command in the **config>router>igmp>interface** context can be used to disable an interface without removing the configuration for the interface.

Default no interface

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>mld interface)

Full Context configure router mld interface

Description Commands in this context configure an Multicast Listener Discovery (MLD) interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of this command deletes the MLD interface. The **shutdown** command in the **config>router>mld>interface** context can be used to disable an interface without removing the configuration for the interface.

Default no interface — No interfaces are defined.

Parameters *ip-int-name* — Specifies the IP interface name. Interface names must be unique within the group of defined IP interfaces for **config>router>interface** and **config>service>ies>interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

Platforms All

interface

Syntax **interface** *interface-name* [**create**]
no interface *interface-name*

Context **[Tree]** (config>router>gtp>s11 interface)
[Tree] (config>service>vprn>gtp>s11 interface)

Full Context configure router gtp s11 interface
configure service vprn gtp s11 interface

Description This command activates GTP termination on the specified interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables GTP termination on the specified interface, if there are no active sessions associated with the interface.

Parameters *interface-name* — Specifies the name of the interface, up to 32 characters. The name must begin with a letter.

create — Creates an entry.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

interface

Syntax **interface** *ip-int-name*
no interface

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring>in-band-control-path interface)
[Tree] (config>redundancy>mc>peer>mc>l3-ring>in-band-control-path interface)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring in-band-control-path interface
configure redundancy multi-chassis peer mc-ring ring in-band-control-path interface

Description This command specifies the name of the IP interface used for the inband control connection.

If an interface name is not configured, the ring cannot become operational.

The **no** form of this command reverts to the default.

Parameters *ip-int-name* — Specifies an interface name up to 32 characters.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>radius-proxy>server interface)
[Tree] (config>service>vprn>radius-proxy>server interface)

Full Context configure router radius-proxy server interface
configure service vprn radius-proxy server interface

Description This command configures the IP interface the RADIUS-proxy server will bind to. One RADIUS-proxy server could bind to multiple interfaces.

Parameters *ip-int-name* — Specifies the name of an IP interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interface

Syntax **interface router** *router-instance* **name** *interface-name*
no interface

Context **[Tree]** (config>subscr-mgmt>pfcp-association interface)

Full Context configure subscriber-mgmt pfcp-association interface

Description This command configures the interface from which PFCP messages are sent and on which PFCP messages are received.

The **no** form of this command removes the interface.

Default no interface

Parameters *router-instance* — Specifies the router instance.

Values *router-name* | *vprn-svc-id*
router-name: Base Default - Base
vprn-svc-id: 1 to 2147483647

interface-name — Specifies the interface name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>service>vpls interface)

Full Context configure service vpls interface

Description This command creates a logical IP routing interface for a VPLS service. Once created, attributes such as IP address and service access points (SAP) can be associated with the IP interface.

The interface command, under the context of services, is used to create and maintain IP routing interfaces within the VPLS service IDs. The IP interface created is associated with the VPLS management routing instance. This instance does not support routing.

Interface names are case-sensitive and must be unique within the group of defined IP interfaces defined for the network core router instance. Interface names in the dotted decimal notation of an IP address are not allowed. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. Duplicate interface names can exist in different router instances.

Enter a new name to create a logical router interface. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, no default IP interface names are defined within the system. All VPLS IP interfaces must be explicitly defined in an enabled state.

The no form of this command removes the IP interface and the entire associated configuration. The interface must be administratively shut down before issuing the no interface command.

For VPLS services, the IP interface must be shut down before the SAP on that interface is removed.

For VPLS service, ping and traceroute are the only applications supported.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP.

An interface name:

- Should not be in the form of an IP address.
- Can be from 1 to 32 alphanumeric characters.
- If the string contains special characters (such as #,$,spaces), the entire string must be enclosed within double quotes.

If ip-int-name already exists within the service ID, the context changes to maintain that IP interface. If ip-int-name already exists within another service ID, an error occurs and the context does not change to that IP interface. If ip-int-name does not exist, the interface is created and the context is changed to that interface for further command processing.

Platforms All

interface

Syntax [**no**] **interface** [*ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>igmp interface)

Full Context debug router igmp interface

Description This command enables debugging for IGMP interfaces.

The **no** form of this command disables the IGMP interface debugging for the specifies interface name or IP address.

Parameters *ip-int-name* — Debugs the information associated with the specified IP interface name.

ip-address — Debugs the information associated with the specified IP address.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>service>vprn>igmp interface)

Full Context configure service vprn igmp interface

Description Commands in this context configure interface parameters.

Parameters *ip-int-name* — Specifies the name of the IP interface, up to 32 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>service>vprn>isis interface)

Full Context configure service vprn isis interface

Description This command creates the context to configure an IS-IS interface.

When an area is defined, the interfaces belong to that area. Interfaces cannot belong to separate areas.

When the interface is a POS channel, the OSI Network Layer Control Protocol (OSINLCP) is enabled when the interface is created and removed when the interface is deleted.

The **no** form of this command removes IS-IS from the interface.

The **shutdown** command in the **config>router>isis>if** context administratively disables IS-IS on the interface without affecting the IS-IS configuration.

Default no interface — No IS-IS interfaces are defined.

Parameters *ip-int-name* — Identify the IP interface name created in the **config>router>if** context. The IP interface name must already exist.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>service>vprn>mld interface)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn mld interface

Description Commands in this context configure an Multicast Listener Discovery (MLD) interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of this command deletes the MLD interface. The **shutdown** command in the **config>router>mld>if** context can be used to disable an interface without removing the configuration for the interface.

Default no interface

Parameters *ip-int-name* — Specifies the IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

Platforms All

interface

Syntax **interface** *ip-int-name* [**secondary**]
no interface *ip-int-name*

Context **[Tree]** (config>service>vprn>ospf>area interface)
[Tree] (config>service>vprn>ospf3>area interface)

Full Context configure service vprn ospf area interface
configure service vprn ospf3 area interface

Description This command creates a context to configure an OSPF interface.

By default interfaces are not activated in any interior gateway protocol, such as OSPF, unless explicitly configured.

The **no** form of this command deletes the OSPF interface configuration for this interface. The **shutdown** command in the **config>router>ospf>if** context can be used to disable an interface without removing the configuration for the interface.

Default no interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-int-name* — Specifies the IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service vprn interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

secondary — Keyword used to allow multiple secondary adjacencies, in addition to the primary adjacency, to be established over a single IP interface. This keyword can also be applied to the system interface and to loopback interfaces to allow them to participate in multiple areas, although no adjacencies are formed over these types of interfaces.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>service>vprn>pim interface)

Full Context configure service vprn pim interface

Description This command enables PIM on an interface and enables the context to configure interface-specific parameters. By default interfaces are activated in PIM based on the **apply-to** command, and do not have to be configured on an individual basis unless the default values must be changed.

The **no** form of this command deletes the PIM interface configuration for this interface. If the **apply-to** command parameter is configured, then the **no interface** form must be saved in the configuration to avoid automatic (re)creation after the next **apply-to** is executed as part of a reboot.

The **shutdown** command can be used to disable an interface without removing the configuration for the interface.

Default Interfaces are activated in PIM based on the apply-to command.

Parameters *ip-int-name* — Specifies the interface name. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>service>vprn>router-advertisement interface)

Full Context configure service vprn router-advertisement interface

Description This command configures router advertisement properties on a specific interface. The interface must already exist in the **config>router>if** context.

Default No interfaces are configured by default.

Parameters *ip-int-name* — Specifies the interface name. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name* [**dual-stack**]

Context **[Tree]** (config>router>ldp>interface-parameters interface)

Full Context configure router ldp interface-parameters interface

Description This command enables LDP on the specified IP interface.

The **no** form of the command deletes the LDP interface and all configuration information associated with the LDP interface.

The LDP interface must be disabled using the **shutdown** command before it can be deleted.

The user can configure different parameters for IPv4 and IPv6 LDP interfaces by entering **ipv4** or **ipv6** as the next command.

Parameters *ip-int-name* — Specifies the name of an existing interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

dual-stack — This optional keyword allows the user to explicitly indicate if this interface should create the IPv4 context automatically or not. With the introduction of LDP IPv6, the creation of the interface does not automatically mean it is to be used for IPv4 like with legacy IPv4 only LDP interface. Thus the dual-stack keyword is an indication to the system that user will manually enable the IPv4, IPv6, or the dual-stack IPv4/IPv6 contexts manually.

The following are some of the key points for this keyword:

- If the keyword is provided, then IPv4 interface context will not be created automatically. If it is not provided, the IPv4 interface context will be created like in the legacy single stack LDP IPv4 interface behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- This new keyword will always show in a configuration.
- When entering an already configured interface, there is no need to provide the keyword, but it will be ignored if provided.
- When deleting a configured interface, the keyword will not be accepted in the **no** version of the **interface** command.

Platforms All

interface

Syntax [**no**] **interface** *interface-name family*

Context **[Tree]** (debug>router>ldp interface)

Full Context debug router ldp interface

Description Use this command for debugging an LDP interface.

Parameters *interface-name* — The name of an existing interface.

family — Specifies the family type.

Values ipv4, ipv6

Platforms All

interface

Syntax **interface** *ip-address* **srlg-group** *group-name* [*group-name*]
no interface *ip-address* [**srlg-group** *group-name*]

Context **[Tree]** (config>router>mpls>srlg-database>router-id interface)

Full Context configure router mpls srlg-database router-id interface

Description This command allows the operator to manually enter the SRLG membership information for any link in the network, including links on this node, into the user SRLG database.

An interface can be associated with up to five SRLG groups for each execution of this command. The operator can associate an interface with up to 64 SRLG groups by executing the command multiple times.

CSPF will not use entered SRLG membership if an interface is not validated as part of a router ID in the routing table.

The **no** form of this command deletes a specific interface entry in this user SRLG database. The *group-name* must already exist in the config>router>if-attribute>srlg-group context.

Parameters *ip-address* — Specifies the IPv4 address in a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

srlg-group *group-name* — Specifies the SRLG group name. Up to 1024 group names can be defined in the config>router>if-attribute context. The SRLG group names must be identical across all routers in a single domain.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>mpls interface)

Full Context configure router mpls interface

Description This command specifies MPLS protocol support on an IP interface. No MPLS commands are executed on an IP interface where MPLS is not enabled. An MPLS interface must be explicitly enabled (**no shutdown**).

The **no** form of this command deletes all MPLS commands such as **label-map** which are defined under the interface. The MPLS interface must be shutdown first in order to delete the interface definition. If the interface is not shutdown, the **no interface** *ip-int-name* command does nothing except issue a warning message on the console indicating that the interface is administratively up.

Default shutdown

Parameters *ip-int-name* — Specifies the name of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Values 1 to 32 alphanumeric characters.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>rsvp interface)

Full Context configure router rsvp interface

Description This command enables RSVP protocol support on an IP interface. No RSVP commands are executed on an IP interface where RSVP is not enabled.

The **no** form of this command deletes all RSVP commands such as **hello-interval** and **subscription**, which are defined for the interface. The RSVP interface must be **shutdown** it can be deleted. If the interface is not shut down, the **no interface** *ip-int-name* command does nothing except issue a warning message on the console indicating that the interface is administratively up.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default shutdown

Parameters *ip-int-name* — Specifies the name of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Values 1 to 32

Platforms All

interface

Syntax **interface** [*ip-int-name* | *mt-int-name* | *ip-address*] [**detail**]
no interface

Context **[Tree]** (debug>router>pim interface)

Full Context debug router pim interface

Description This command enables debugging for PIM interface information.

The **no** form of this command disables PIM interface debugging.

Parameters *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IPv4 or IPv6 interface address

mt-int-name — Debugs the information associated with the specified VPRN ID and group address.

ip-address — Debugs the information associated with the specified IP address.

detail — Debugs detailed IP interface information.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>pim interface)

Full Context configure router pim interface

Description This command creates a PIM interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Interface names are case-sensitive and must be unique within the group of defined IP interfaces defined for **config>router>interface**, **config>service>ies>interface**, and **config>service>ies>subscriber-interface>group-interface**. Interface names must not be in the dotted decimal notation of an IP address. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either the interface names or the IP addresses. Ambiguity can exist if an IP address is used as an IP address and an interface name. Duplicate interface names can exist in different router instances, although this is not recommended because it may be confusing.

By default, no interfaces or names are defined within PIM.

The **no** form of this command removes the IP interface and all the associated configurations.

Parameters *ip-int-name* — Specifies the name of the IP interface, up to 32 characters. Interface names must be unique within the group of defined IP interfaces for **config router interface**, **config service ies interface**, and **config service ies subscriber-interface group-interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on.), the entire string must be enclosed within double quotes.

If the *ip-int-name* already exists, the context is changed to maintain that IP interface. If *ip-int-name* does not exist, the interface is created and the context is changed to that interface for further command processing.

Platforms All

interface

Syntax **interface** *interface-name* [**unnumbered-mpls-tp**]
interface *interface-name* **control-tunnel**
interface *interface-name* **gmpls-loopback**
interface *interface-name* **pdn**
no interface *interface-name*

Context **[Tree]** (config>router interface)

Full Context configure router interface

Description This command creates a logical IP routing or unnumbered MPLS-TP interface. Once created, attributes like IP address, port, or system can be associated with the IP interface.

Interface names are case-sensitive and must be unique within the group of IP interfaces defined for **config router interface** and **config service ies interface**. Interface names must not be in the dotted decimal notation of an IP address.; for example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either the interface names or the IP addresses. Ambiguity can exist if an IP address is used as an IP address and an interface name. Duplicate interface names can exist in different router instances, although this is not recommended because it is confusing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

Although not a keyword, the ip-int-name "**system**" is associated with the network entity (such as a specific router), not a specific interface. The system interface is also referred to as the loopback address.

An unnumbered MPLS-TP interface is a special type of interface that is only intended for MPLS-TP LSPs. IP routing protocols are blocked on interfaces of this type. If an interface is configured as unnumbered-mpls-tp, then it can only be associated with an Ethernet port or VLAN, using the port command, then either a unicast, multicast, or broadcast remote MAC address may be configured. Only static ARP is supported.

A GMPLS loopback interface is a special type of loopback interface that is used as the IP interface for a GMPLS IP Control Channel (IPCC). RSVP and LMP packets associated with GMPLS are associated with this loopback interface. All other IP protocols are blocked on this interface. One **gmpls-loopback** interface is required for each GMPLS peer node.

The control-tunnel parameter creates a loopback interface representing a GRE tunnel. One IP tunnel can be created in this interface.

Only the primary IPv4 interface address and only one IP tunnel per interface are allowed. Multiple tunnels can be configured using up to four controlTunnel loopback interfaces. A static route can take the new controlTunnel interface as a next hop.

The **no** form of this command removes the IP interface and all the associated configurations. The interface must be administratively shut down before issuing the **no interface** command.

Parameters *interface-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Values 1 to 32 alphanumeric characters

If the *ip-int-name* already exists, the context is changed to maintain that IP interface. If *ip-int-name* already exists within another service ID or is an IP interface defined within the **config router** commands, an error will occur and the context will not be changed to that IP interface. If *ip-int-name* does not exist, the interface is created and the context is changed to that interface for further command processing.

unnumbered-mpls-tp — Specifies that an interface is an unnumbered MPLS-TP. An unnumbered MPLS-TP interface is a special type of interface that is only intended for MPLS-TP LSPs. IP routing protocols are blocked on interfaces of this type. If an interface is configured as **unnumbered-mpls-tp**, then it can only be associated with an Ethernet port or VLAN, using the **port** command. A unicast, multicast, or broadcast remote MAC address can be configured using the **static-arp** command. Only static ARP is supported.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gmpls-loopback — Specifies that the interface is a loopback interface for GMPLS control plane packets.

control-tunnel — Specifies that the interface represents a loopback interface for a GRE tunnel to be used for the GMPLS IPCC.

pdn — Specifies that the interface is a PDN.

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>router-advert interface)

Full Context configure router router-advertisement interface

Description This command configures router advertisement properties on a specific interface. The interface must already exist in the **config**>**router**>**if** context.

Parameters *ip-int-name* — Specifies the interface name. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

interface

Syntax [**no**] **interface** *interface-name*

Context **[Tree]** (config>router>pcp-server>server interface)

Full Context configure router pcp-server server interface

Description This command associates an interface.

The **no** form of this command reverts to the default value.

Parameters *interface-name* — Specifies the interface name, up to 32 characters. The interface name must start with a letter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

interface

Syntax [**no**] **interface** [{*ip-int-name* | *ip-address*}]

Context **[Tree]** (debug>router>ip interface)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router ip interface

Description This command displays the router IP interface table sorted by interface index.

Parameters *ip-int-name* — Only displays the interface information associated with the specified IP interface name.

Values 32 characters maximum

ip-address — Only displays the interface information associated with the specified IP address.

Values The following values apply to the 7750 SR and 7950 XRS:

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Values The following values apply to the 7450 ESS:
ipv4-address: a.b.c.d (host bits must be 0)

Platforms All

interface

Syntax [**no**] **interface** *ip-int-name*

Context **[Tree]** (config>router>isis interface)

Full Context configure router isis interface

Description This command creates the context to configure an IS-IS interface.

When an area is defined, the interfaces belong to that area. Interfaces cannot belong to separate areas.

When the interface is a POS channel, the OSINLCP is enabled when the interface is created and removed when the interface is deleted.

The **no** form of this command removes IS-IS from the interface.

The **shutdown** command in the **config>router>isis>interface** context administratively disables IS-IS on the interface without affecting the IS-IS configuration.

Parameters *ip-int-name* — Identify the IP interface name created in the **config>router>interface** context. The IP interface name must already exist.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interface

Syntax **interface** [*ip-int-name* | *ip-address*]
no interface

Context **[Tree]** (debug>router>isis interface)

Full Context debug router isis interface

Description This command enables debugging for IS-IS interface.

The **no** form of the command disables debugging.

Parameters *ip-address* — When specified, only the interface with the specified interface address is debugged.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

ip-int-name — When specified, only the interface with the specified interface name is debugged.

Platforms All

interface

Syntax **interface** *ip-int-name* [**secondary**]
no interface *ip-int-name*

Context **[Tree]** (config>router>ospf>area interface)
[Tree] (config>router>ospf3>area interface)

Full Context configure router ospf area interface
configure router ospf3 area interface

Description This command configures an OSPF interface.

Unless they are explicitly configured, interfaces are not activated, by default, in any interior gateway protocol, such as OSPF.

The **no** form of this command deletes the OSPF interface configuration for this interface. Use the **shutdown** command in the **config**>**router**>**ospf**>**interface** context to disable an interface without removing the configuration for the interface.

Default no interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-int-name* — Specifies the IP interface name. Interface names must be unique within the group of defined IP interfaces for the **configure router interface** and **configure service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string, up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured, an error message is returned.

If the IP interface exists in a different area it is moved to this area.

secondary — Keyword used to allow multiple secondary adjacencies, in addition to the primary adjacency, to be established over a single IP interface. This keyword can also be applied to the system interface and to loopback interfaces to allow them to participate in multiple areas, although no adjacencies are formed over these types of interfaces.

Platforms All

interface

Syntax **interface** [*ip-int-name* | *ip-address*]
interface [**interface-name**]
no interface

Context **[Tree]** (debug>router>ospf interface)
[Tree] (debug>router>ospf3 interface)

Full Context debug router ospf interface
debug router ospf3 interface

Description This command enables debugging for an OSPF and OSPF3 interface.

Parameters *ip-int-name* — Specifies the IP interface name, in the **debug**>**router**>**ospf** context. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

ip-address — Specifies the interface's IP address, in the **debug**>**router**>**ospf** context.

interface-name — Specifies the interface name, in the **debug**>**router**>**ospf3** context.

Platforms All

interface

Syntax **interface** *interface-name*
no interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>policy-options>policy-statement>entry>from interface)

Full Context configure router policy-options policy-statement entry from interface

Description This command specifies the router interface, specified either by name or address, as a filter criterion.

The **no** form of this command removes the criterion from the configuration.

Default no interface

Parameters *ip-int-name* — Specifies the name of the interface as a match criterion for this entry. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

interface

Syntax **interface** *interface-name*
no interface

Context [Tree] (config>router>segment-routing>srv6>inst>loc>func>end-x interface)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-x interface

Description This command configures an interface for the End.X function.

The **no** form of this command removes the interface name from the configuration.

Default no interface

Parameters *interface-name* — Specifies an existing interface name, up to 32 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

13.179 interface-a

interface-a

Syntax **interface-a**

Context [Tree] (config>fwd-path-ext>fpe>srv6 interface-a)

Full Context configure fwd-path-ext fpe srv6 interface-a

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the context to configure the parameters of the network interface-a of the SRv6 FPE.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

13.180 interface-b

interface-b

Syntax **interface-b**

Context **[Tree]** (config>fwd-path-ext>fpe>srv6 interface-b)

Full Context configure fwd-path-ext fpe srv6 interface-b

Description This command enables the context to configure the parameters of the network interface-b of the SRv6 FPE.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

13.181 interface-disable-sample

interface-disable-sample

Syntax [**no**] **interface-disable-sample**

Context **[Tree]** (config>filter>ip-filter>entry interface-disable-sample)
[Tree] (config>filter>ipv6-filter>entry interface-disable-sample)

Full Context configure filter ip-filter entry interface-disable-sample
configure filter ipv6-filter entry interface-disable-sample

Description This command disables cflowd sampling for packets matching this filter entry, for the IP interface set to **cflowd interface** mode. This allows the option to not sample specific types of traffic when interface sampling is enabled.

If the cflowd is either not enabled or set to **cflowd acl** mode, this command is ignored.

The **no** form of this command enables sampling.

Default no interface-disable-sample

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.182 interface-group-handler

interface-group-handler

Syntax [**no**] **interface-group-handler** *index*

Context **[Tree]** (config interface-group-handler)

Full Context configure interface-group-handler

Description This command creates an interface group handler that can be associated with a number of independent IP links. The purpose of the group is to operationally disable all interfaces in a common group if the number of active links drops below the minimum interface threshold.

The **no** form of this command deletes the interface group handler. All members must be removed before the IGH can be deleted.

Parameters *index* — Identifies the specific Interface Group Handler.

Values 1 to 100

Platforms All

13.183 interface-id

interface-id

Syntax **interface-id** [**ascii-tuple**]
interface-id ifindex
interface-id sap-id
interface-id string *string*
no interface-id

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6>option interface-id)
[Tree] (config>service>vprn>if>ipv6>dhcp6>option interface-id)

Full Context configure service ies interface ipv6 dhcp6-relay option interface-id
configure service vprn interface ipv6 dhcp6-relay option interface-id

Description This command enables the sending of interface ID options in the DHCPv6 relay packet.

The **no** form of this command disables the sending of interface ID options in the DHCPv6 relay packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **ascii-tuple** — Specifies that the ASCII-encoded concatenated tuple is used which consists of the access-node-identifier, service-id, and interface-name, separated by "| ".

ifindex — Specifies that the interface index is used. The If Index of a router interface can be displayed using the **show>router>interface>detail** command.

sap-id — Specifies that the SAP identifier is used.

string — Specifies that a string is used.

string — Specifies a string of up to 80 characters long, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

interface-id

Syntax **interface-id** [**ascii-tuple**]
interface-id ifindex
interface-id sap-id
interface-id string *string*
no interface-id

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>option interface-id)

Full Context configure service vprn subscriber-interface group-interface ipv6 dhcp6 option interface-id

Description This command enables the sending of interface ID options in the DHCPv6 relay packet.

The **no** form of this command disables the sending of interface ID options in the DHCPv6 relay packet.

Parameters **ascii-tuple** — Specifies that the ASCII-encoded concatenated tuple is used which consists of the access-node-identifier, service-id, and interface-name, separated by "| ".

ifindex — Specifies that the interface index is used (the If Index of a router interface can be displayed using the command **show>router>if>detail**).

sap-id — Specifies that the SAP identifier is used.

string — Specifies a string, up to 32 characters long, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.184 interface-id-mapping

interface-id-mapping

Syntax [**no**] **interface-id-mapping**

Context **[Tree]** (config>router>dhcp6>server interface-id-mapping)
[Tree] (config>service>vprn>dhcp6>server interface-id-mapping)

Full Context configure router dhcp6 local-dhcp-server interface-id-mapping
configure service vprn dhcp6 local-dhcp-server interface-id-mapping

Description This command enables the behavior where unique /64 prefix is allocated per interface-id, and all clients having the same interface-id get an address allocated out of this /64 prefix for DHCP6. This is relevant for bridged clients behind the same local-loop (and same SAP), where sharing the same prefix allows communication between bridged clients behind the same local-loop to stay local. For SLAAC based assignment, downstream neighbor-discovery is automatically enabled to resolve the assigned address.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.185 interface-list

interface-list

Syntax **interface-list**

Context **[Tree]** (config>cflowd>collector>exp-filter interface-list)

Full Context configure cflowd collector export-filter interface-list

Description Commands in this context allow the administrator to specify which interface's flow data should be exported to the associated collector.

Table 65 describes the cflowd export filter precedence.

Table 65 **Cflowd Export Filter Precedence**

Family Filter	Router Filter	Interface Filter	Export to Collector
0	0	0	export all

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 65 **Cflowd Export Filter Precedence**

Family Filter	Router Filter	Interface Filter	Export to Collector
0	0	1	export if matched interface only
0	1	0	export if matched router only
0	1	1	export if router match *OR* interface match
1	0	0	not exported due to family exclusion filter
1	0	1	not exported due to family exclusion filter
1	1	0	not exported due to family exclusion filter
1	1	1	not exported due to family exclusion filter

Platforms All

13.186 interface-parameters

interface-parameters

Syntax **interface-parameters**

Context **[Tree]** (config>router>ldp interface-parameters)

Full Context configure router ldp interface-parameters

Description Commands in this context configure LDP interfaces and parameters applied to LDP interfaces. The user can configure different default parameters for IPv4 and IPv6 LDP interfaces by entering **ipv4** or **ipv6** as the next command.

Platforms All

13.187 interface-subnets

interface-subnets

Syntax **interface-subnets** [**service** *service-id*] *interface-name* [*interface-name*...**up to 10 max**]
no interface-subnets

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>policy-options>policy-statement>entry>from interface-subnets)

Full Context configure router policy-options policy-statement entry from interface-subnets

Description This command configures the applied router instance and interfaces that are used as matching condition within each policy-statement entry. A maximum of 10 *interface-name* entries is supported, and all entries must belong to the same routing context (either **base** or **service**). The interface subnet policy-statement match criterion is applied to the following unicast use case contexts:

- **export**, when used with OSPFv2, OSPFv3, IS-IS, RIP, RIPng, and BGP
- **route-table-import**, when used with BGP
- **vrf-export**, when used with MP-BGP

The **no** form of this command removes all policies from the configuration.

Default no interface-subnets

Parameters **service** — Specifies the context in which the configured interface exists. By default, the base routing instance is assumed. However, the configured service context is used only when the service is configured.

service-id — Specifies the service ID of the service to match.

Values *service-id* — 1 to 2147483647
svc-name — 64 characters maximum

interface-name — Specifies the interface name, up to 32 characters, to match when exporting the IP address of the associated interface to a routing protocol.

Platforms All

13.188 interface-support-enable

interface-support-enable

Syntax [**no**] **interface-support-enable**

Context [Tree] (config>port>ethernet>eth-cfm>mep>ais-enable interface-support-enable)

Full Context configure port ethernet eth-cfm mep ais-enable interface-support-enable

Description This command enables and disables the generation of AIS PDUs based on the associated endpoint state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interface-support-enable

Syntax [**no**] **interface-support-enable**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>ais interface-support-enable)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>ais interface-support-enable)
[Tree] (config>service>vpls>sap>eth-cfm>mep>ais interface-support-enable)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>ais interface-support-enable)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>ais interface-support-enable)

Full Context configure service epipe sap eth-cfm mep ais-enable interface-support-enable
configure service epipe spoke-sdp eth-cfm mep ais-enable interface-support-enable
configure service vpls mesh-sdp eth-cfm mep ais-enable interface-support-enable
configure service vpls sap eth-cfm mep ais-enable interface-support-enable
configure service vpls spoke-sdp eth-cfm mep ais-enable interface-support-enable

Description This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPs are triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled, then transmission of the AIS PDU is based on either the non-operational state of the entity or on any CCM defect condition. AIS generation ceases if both the operational state is UP and the CCM has no defect conditions. If the MEP is not CCM-enabled then the operational state of the entity is the only consideration, assuming this command is present for the MEP. By default, AIS is not generated or stopped based on the state of the entity on which the DOWN MEP is configured.

The **no** form of this command disables the AIS function to consider the operational state of the entity on which it is configured.

Default no interface-support-enabled

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interface-support-enable

Syntax [**no**] **interface-support-enable**

Context **[Tree]** (config>service>ies>sap>eth-cfm>mep>ais-enable interface-support-enable)
[Tree] (config>service>ies>spoke-sdp>eth-cfm>mep>ais-enable interface-support-enable)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>ais-enable interface-support-enable)

Full Context configure service ies sap eth-cfm mep ais-enable interface-support-enable
configure service ies spoke-sdp eth-cfm mep ais-enable interface-support-enable
configure service ies subscriber-interface group-interface sap eth-cfm mep ais-enable interface-support-enable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPs will be triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled then transmission of the AIS PDU will be based on either the non-operational state of the entity or on any CCM defect condition. AIS generation will cease if BOTH operational state is UP and CCM has no defect conditions. If the MEP is not CCM enabled then the operational state of the entity is the only consideration assuming this command is present for the MEP.

Default no interface-support-enable (AIS will not be generated or stopped based on the state of the entity on which the DOWN MEP is configured).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

interface-support-enable

Syntax [**no**] **interface-support-enable**

Context **[Tree]** (config>service>vprn>sap>eth-cfm>mep>ais-enable interface-support-enable)
[Tree] (config>service>vprn>spoke-sdp>eth-cfm>mep>ais-enable interface-support-enable)

Full Context configure service vprn sap eth-cfm mep ais-enable interface-support-enable
configure service vprn spoke-sdp eth-cfm mep ais-enable interface-support-enable

Description This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPs will be triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled then transmission of the AIS PDU will be based on either the non-operational state of the entity or on ANY CCM defect condition. AIS generation will cease if BOTH operational state is UP and CCM has no defect conditions. If the MEP is not CCM enabled then the operational state of the entity is the only consideration assuming this command is present for the MEP.

The **no** form of this command means that AIS will not be generated or stopped based on the state of the entity on which the DOWN MEP is configured.

Default no interface-support-enable

13.189 interface-type

interface-type

Syntax **interface-type** {**gn** | **s2a** | **s2b** | **s11**}
no interface-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>gtp>peer-profile interface-type)

Full Context configure subscriber-mgmt gtp peer-profile interface-type

Description This command specifies the interface applicable for communications to the peer. If the interface type does not match the given context in an uplink context, the peer setup will fail.

The **no** form of this command reverts to the default value.

Default interface-type s2a

Parameters **gn** — Signaling interface with the peer is Gn as specified in 3GPP TS 29.060.

s2a — Signaling interface with the peer is s2a as specified in 3GPP TS 29.274.

s2b — Signaling interface with the peer is s2b as specified in 3GPP TS 29.274.

s11 — Signaling interface with the peer is s11 as specified in 3GPP TS 29.274.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

interface-type

Syntax **interface-type** {**broadcast** | **point-to-point**}
no interface-type

Context [Tree] (config>service>vprn>isis>if interface-type)

Full Context configure service vprn isis interface interface-type

Description This command configures the IS-IS interface type as either broadcast or point-to-point.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the designated IS-IS overhead if the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to IS-IS and subsequently the IP interface is bound (or moved) to a different interface type, then this command must be entered manually.

The **no** form of this command reverts to the default value.

Default point-to-point — For IP interfaces on SONET channels.

broadcast — For IP interfaces on Ethernet or unknown type physical interfaces.

Special Cases **SONET —** Interfaces on SONET channels default to the point-to-point type.

Ethernet or Unknown — Physical interfaces that are Ethernet or unknown default to the broadcast type.

Parameters **broadcast** — Configures the interface to maintain this link as a broadcast network.

point-to-point — Configures the interface to maintain this link as a point-to-point link.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

interface-type

Syntax **interface-type** {**broadcast** | **point-to-point** | **non-broadcast**}
no interface-type

Context **[Tree]** (config>service>vprn>ospf>area>if interface-type)
[Tree] (config>service>vprn>ospf3>area>if interface-type)

Full Context configure service vprn ospf area interface interface-type
configure service vprn ospf3 area interface interface-type

Description This command configures the interface type to be one of broadcast, point-to-point, or non-broadcast.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the broadcast adjacency maintenance overhead if the Ethernet link provided the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to OSPF and subsequently the IP interface is bound (or moved) to a different interface type, this command must be entered manually.

The **no** form of this command reverts to the default value.

Default point-to-point — If the physical interface is SONET.

broadcast — If the physical interface is Ethernet or unknown.

Special Cases **Virtual-Link —** A virtual link is always regarded as a point-to-point interface and is not configurable.

Parameters **broadcast** — Configures the interface as a broadcast network. To significantly improve adjacency forming and network convergence, configure the network as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.

point-to-point — Configures the interface as a point-to-point link.

non-broadcast — Configures the interface as a non-broadcast network.

Platforms All

interface-type

Syntax **interface-type** {**ds1** [{**esf** | **sf**}] | **e1** [{**pcm30crc** | **pcm31crc**}]}
no interface-type

Context **[Tree]** (config>system>sync-if-timing>bits interface-type)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system sync-if-timing bits interface-type

Description This command configures the Building Integrated Timing Source (BITS) timing reference.

The **no** form of the command reverts to the default configuration.

Default interface-type ds1 esf

Parameters **ds1 esf** — Specifies Extended Super Frame (ESF). This is a framing type used on DS1 circuits that consists of 24 192-bit frames, The 193rd bit provides timing and other functions.

ds1 sf — Specifies Super Frame (SF), also called D4 framing. This is a common framing type used on DS1 circuits. SF consists of 12 192-bit frames. The 193rd bit provides error checking and other functions. ESF supersedes SF.

e1 pcm30crc — Specifies the pulse code modulation (PCM) type. PCM30CRC uses PCM to separate the signal into 30 user channels with CRC protection.

e1 pcm31crc — Specifies the pulse code modulation (PCM) type. PCM31CRC uses PCM to separate the signal into 31 user channels with CRC protection.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interface-type

Syntax **interface-type** {**broadcast** | **point-to-point**}
no interface-type

Context **[Tree]** (config>router>isis>interface interface-type)

Full Context configure router isis interface interface-type

Description This command configures the IS-IS interface type as either broadcast or point-to-point.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the designated IS-IS overhead if the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to IS-IS and subsequently the IP interface is bound (or moved) to a different interface type, then this command must be entered manually.

The **no** form of this command reverts to the default value.

Default interface-type point-to-point — For IP interfaces on SONET channels.

interface-type broadcast — For IP interfaces on Ethernet or unknown type physical interfaces.

Special Cases **SONET —** Interfaces on SONET channels default to the point-to-point type.

Ethernet or Unknown — Physical interfaces that are Ethernet or unknown default to the broadcast type.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **broadcast** — Configures the interface to maintain this link as a broadcast network.

point-to-point — Configures the interface to maintain this link as a point-to-point link.

Platforms All

interface-type

Syntax **interface-type** {**broadcast** | **point-to-point** | **non-broadcast**}
no interface-type

Context **[Tree]** (config>router>ospf>area>interface interface-type)
[Tree] (config>router>ospf3>area>interface interface-type)

Full Context configure router ospf area interface interface-type
configure router ospf3 area interface interface-type

Description This command configures the interface type to be one of broadcast, point-to-point, or non-broadcast.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the broadcast adjacency maintenance overhead of the Ethernet link provided the link is used as point-to-point.

If the interface type is not known at the time the interface is added to OSPF and subsequently the IP interface is bound (or moved) to a different interface type, this command must be entered manually.

The **no** form of this command returns the setting to the default value.

Default interface-type point-to-point (if the physical interface is SONET)

interface-type broadcast (if the physical interface is Ethernet or unknown)

Special Cases **Virtual-Link —** A virtual link is always regarded as a point-to-point interface and not configurable.

Parameters **broadcast** — Configures the interface as a broadcast network. To significantly improve adjacency forming and network convergence, configure a network as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.

point-to-point — Configures the interface as a point-to-point link.

non-broadcast — Configures the interface as a non-broadcast network.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.190 interim-credit

interim-credit

Syntax **interim-credit**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>efh interim-credit)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling interim-credit

Description Commands in this context configure interim credit parameters for Extended Failure Handling (EFH).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.191 interim-update

interim-update

Syntax **interim-update**
interim-update include-counters [**hold-down** *seconds*]
no interim-update

Context **[Tree]** (config>router>wlan-gw>mobility-triggered-acct interim-update)
[Tree] (config>service>vprn>wlan-gw>mobility-triggered-acct interim-update)

Full Context configure router wlan-gw mobility-triggered-acct interim-update
configure service vprn wlan-gw mobility-triggered-acct interim-update

Description This command enables the inclusion of counters with a **hold-down** time option in mobility-triggered interim-updates. When enabled, to disable the inclusion of counters, interim updates must be disabled and then re-enabled without the **include-counters** keyword. By default, the **hold-down** time is not imposed.

The **no** form of this command disables generation of flash interim accounting updates to RADIUS when change in location of the UE is detected.

Default no interim-update

Parameters **include-counters** — Specifies the inclusion of counters in mobility triggered interim-updates.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

seconds — Specifies the time, in seconds, that must elapse after a mobility- triggered interim with counters sent for the next mobility-triggered interim with counters to be sent.

Values 60 to 864000

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.192 interim-update-interval

interim-update-interval

Syntax **interim-update-interval** *minutes*
no interim-update-interval

Context **[Tree]** (config>app-assure>rad-acct-plcy interim-update-interval)

Full Context configure application-assurance radius-accounting-policy interim-update-interval

Description This command configures the interim update interval.

The **no** form of this command reverts to the default.

Default no interim-update-interval

Parameters *minutes* — Specifies the interval at which subscriber accounting data will be updated. If set no value is specified then no interim updates will be sent.

Values 5 to 1080

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.193 interleave

interleave

Syntax [**no**] **interleave**

Context **[Tree]** (config>router>l2tp>group>mlppp interleave)
[Tree] (config>service>vprn>l2tp>group>mlppp interleave)

Full Context configure router l2tp group mlppp interleave
configure service vprn l2tp group mlppp interleave

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is applicable only to LNS. Interleaving is supported only on MLPPPoX bundles that contain a single member link. If more than one link is present in the MLPPPoX bundle, interleaving is automatically disabled and a TRAP/log (tmnxMlpppBundleIndicatorsChange) is generated.

The minimum supported rate of the link on which interleaving is performed is 1 kb/s.

If configured at this level, interleaving is enabled on all tunnels within the group, unless it is explicitly disable per tunnel.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

interleave

Syntax **interleave** {**always** | **never**}
no interleave

Context **[Tree]** (config>router>l2tp>group>tunnel>mlppp interleave)
[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp interleave)

Full Context configure router l2tp group tunnel mlppp interleave
configure service vprn l2tp group tunnel mlppp interleave

Description This command configures the user of link fragmentation and interleaving and is applicable only to LNS. Interleaving is supported only on MLPPPoX bundles that contain a single member link. If more than one link is present in the MLPPPoX bundle, interleaving is automatically disabled and a TRAP/log (tmnxMlpppBundleIndicatorsChange) is generated.

The minimum supported rate of the link on which interleaving is performed is 1 kb/s.

Interleaving configured on this level overwrites the configuration option under the group hierarchy. If the **no** form of this command is configured for interleaving at this level, the interleaving configuration inherits the configuration option configured under the L2TP group.

The **no** form of this command reverts to the default.

Parameters **always** — Always perform interleaving on single linked MLPPPoX sessions within this tunnel, regardless of the configuration option for interleaving under the group level.

never — Never perform interleaving on single linked MLPPPoX sessions within this tunnel, regardless of the configuration option for interleaving under the group level.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

interleave

Syntax [**no**] **interleave**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>epipe>sap>frame-relay>frf.12 interleave)
[Tree] (config>service>ipipe>sap>frame-relay>frf.12 interleave)

Full Context configure service epipe sap frame-relay frf.12 interleave
configure service ipipe sap frame-relay frf.12 interleave

Description This command enables interleaving of high priority frames and low priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non-expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header, among the fragmented frames. In effect, this provides a behavior like in MLPPP Link Fragment Interleaving (LFI).

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. The fragmentation header is however not included when the frame size is smaller than the user configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

The **no** form of this command restores the default mode of operation.

Default no interleave

interleave

Syntax **interleave no interleave**

Context [Tree] (config>service>vpls>sap>frame-relay>frf.12 interleave)

Full Context configure service vpls sap frame-relay frf.12 interleave

Description This command enables interleaving of high priority frames and low priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non-expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header, among the fragmented frames. In effect, this provides a behavior like in MLPPP Link Fragment Interleaving (LFI).

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. The fragmentation header is however not included when the frame size is smaller than the user configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

The **no** form of this command restores the default mode of operation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no interleave

interleave

Syntax [**no**] **interleave**

Context **[Tree]** (config>service>ies>if>sap>frame-relay>frf-12 interleave)

Full Context configure service ies interface sap frame-relay frf-12 interleave

Description This command enables interleaving of high priority frames and low-priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header, among the fragmented frames. In effect, this provides a behavior like in MLPPP Link Fragment Interleaving (LFI).

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. The fragmentation header is however not included when the frame size is smaller than the user configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

The **no** form of this command restores the default mode of operation.

Default no interleave

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interleave

Syntax [**no**] **interleave**

Context **[Tree]** (config>service>vprn>if>sap>frame-relay>frf.12 interleave)

Full Context configure service vprn interface sap frame-relay frf.12 interleave

Description This command enables interleaving of high priority frames and low-priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header, among the fragmented frames. In effect, this provides a behavior like in MLPPP Link Fragment Interleaving (LFI).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. The fragmentation header is however not included when the frame size is smaller than the user configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

The **no** form of this command restores the default mode of operation.

Default no interleave

13.194 interleave-fragments

interleave-fragments

Syntax [**no**] **interleave-fragments**

Context **[Tree]** (config>port>multilink-bundle interleave-fragments)

Full Context configure port multilink-bundle interleave-fragments

Description This command enables Link Fragmentation and Interleaving on the multilink bundle.

The **no** form of this command disables Link Fragmentation and Interleaving on the multilink bundle.

Platforms 7450 ESS, 7750 SR-7/12/12e

13.195 internal-ip4-address

internal-ip4-address

Syntax [**no**] **internal-ip4-address**

Context **[Tree]** (config>ipsec>ike-policy>relay-unsol-attr internal-ip4-address)

Full Context configure ipsec ike-policy relay-unsolicited-cfg-attribute internal-ip4-address

Description This command will return IPv4 address from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip4-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.196 internal-ip4-dns

internal-ip4-dns

Syntax [**no**] **internal-ip4-dns**

Context **[Tree]** (config>ipsec>ike-policy>relay-unsol-attr internal-ip4-dns)

Full Context configure ipsec ike-policy relay-unsolicited-cfg-attribute internal-ip4-dns

Description This command will return IPv4 DNS server address from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip4-dns

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.197 internal-ip4-netmask

internal-ip4-netmask

Syntax [**no**] **internal-ip4-netmask**

Context **[Tree]** (config>ipsec>ike-policy>relay-unsol-attr internal-ip4-netmask)

Full Context configure ipsec ike-policy relay-unsolicited-cfg-attribute internal-ip4-netmask

Description This command will return IPv4 netmask from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip4-netmask

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.198 internal-ip6-address

internal-ip6-address

Syntax [**no**] **internal-ip6-address**

Context **[Tree]** (config>ipsec>ike-policy>relay-unsol-attr internal-ip6-address)

Full Context configure ipsec ike-policy relay-unsolicited-cfg-attribute internal-ip6-address

Description This command will return IPv6 address from source (such as a RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip6-address

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.199 internal-ip6-dns

internal-ip6-dns

Syntax [**no**] **internal-ip6-dns**

Context **[Tree]** (config>ipsec>ike-policy>relay-unsol-attr internal-ip6-dns)

Full Context configure ipsec ike-policy relay-unsolicited-cfg-attribute internal-ip6-dns

Description This command will return IPv6 DNS server address from source (RADIUS server) to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Default no internal-ip6-dns

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.200 internal-lease-ipsec

internal-lease-ipsec

Syntax [**no**] **internal-lease-ipsec**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>dhcp>server>lease-hold-time-for internal-lease-ipsec)
[Tree] (config>router>dhcp6>server>lease-hold-time-for internal-lease-ipsec)
[Tree] (config>service>vprn>dhcp>server>lease-hold-time-for internal-lease-ipsec)
[Tree] (config>service>vprn>dhcp6>server>lease-hold-time-for internal-lease-ipsec)

Full Context configure router dhcp local-dhcp-server lease-hold-time-for internal-lease-ipsec
configure router dhcp6 local-dhcp-server lease-hold-time-for internal-lease-ipsec
configure service vprn dhcp local-dhcp-server lease-hold-time-for internal-lease-ipsec
configure service vprn dhcp6 local-dhcp-server lease-hold-time-for internal-lease-ipsec

Description This command enables the server to hold up the lease of local IPsec clients.

The **no** form of this command disables the ability of the server to hold up the lease of local IPsec clients.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.201 internal-scheduler-weight-mode

internal-scheduler-weight-mode

Syntax **internal-scheduler-weight-mode** {**default** | **force-equal** | **offered-load** | **capped-offered-load**}
no internal-scheduler-weight-mode

Context [Tree] (config>card>virt-sched-adj internal-scheduler-weight-mode)

Full Context configure card virtual-scheduler-adjustment internal-scheduler-weight-mode

Description This command specifies the internal scheduler (tier 0) weight mode for all ingress queues on a LAG on the card on which it is applied.

Default internal-scheduler-weight-mode default

Parameters **default** — Specifies that ingress queues are weighted based on port speed or, if configured, the hash weight.

force-equal — Specifies that the ingress queues are always equally weighted.

offered-load — Specifies that the ingress queues are weighted based on observed offered load.

capped-offered-load — Specifies that the ingress queues are weighted based on observed offered load capped by PIR.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

internal-scheduler-weight-mode

Syntax **internal-scheduler-weight-mode** {**default** | **force-equal** | **offered-load** | **capped-offered-load**}
no internal-scheduler-weight-mode

Context **[Tree]** (config>qos>adv-config-policy>child-control>bandwidth-distribution internal-scheduler-weight-mode)

Full Context configure qos adv-config-policy child-control bandwidth-distribution internal-scheduler-weight-mode

Description This command specifies the internal scheduler (tier 0) weight mode for the queues on a LAG on which the advanced configuration policy is applied.

Default internal-scheduler-weight-mode default

Parameters **default** — Specifies that queues are weighted based on the port speed or, if configured, the hash weight.

force-equal — Specifies that the queues are always equally weighted.

offered-load — Specifies that the queues are weighted based on the observed offered load.

capped-offered-load — Specifies that the queues are weighted based on the observed offered load capped by PIR.

Platforms All

13.202 intersite-shared

intersite-shared

Syntax **intersite-shared** [**persistent-type5-adv**] [**kat-type5-adv-withdraw**]
no intersite-shared

Context **[Tree]** (config>service>vprn>mvpn intersite-shared)

Full Context configure service vprn mvpn intersite-shared

Description This command specifies whether to use inter-site shared C-trees or not. Optional parameters allow enabling additional inter-site shared functionality. Not specifying an optional parameter when executing the command disables that parameter.

Default n/a

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **persistent-type5-adv** — When specified for inter-site shared trees enabled, this parameter ensures that Type 5 SA routes are generated for the multicast source even if no joins are present for that source. When the parameter is not specified, the Type 5 SA routes are withdrawn where the prune from the last receiver is received for the multicast source.

kat-type5-adv-withdraw — When specified for inter-site shared trees, this parameter allows operators to enable KeepAlive Timers (KAT) on source PEs for ng-MVPN inter-site shared deployments. On a multicast source failure, a KAT expiry on source PEs will trigger a withdrawal of Type-5 Source-Active (S-A) route and switch from (C-S,C-G) to (C-*,C-G). When receiver PEs process reflected Type-5 S-A route withdrawals, they will withdraw their Type-7 ng-MVPN routes to the failed multicast source. The following conditions apply:

- KAT must only be enabled on source PEs.
- Functionality is supported with mLDP and RSVP-TE in the P-instance.
- Local receiver per (C-S, C-G) must be configured on source PEs running KAT.

Platforms All

13.203 interval

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>ccrt-replay interval)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy>ccrt-replay interval)

Full Context configure subscriber-mgmt diameter-application-policy gx ccrt-replay interval
configure subscriber-mgmt diameter-application-policy gy ccrt-replay interval

Description This command specifies the interval at which CCR-T messages for Diameter Gx or Gy sessions that belong to the Diameter application policy are replayed, until a valid CCA-t response is received or until the configured **max-lifetime** period expires.

The **no** form of this command resets the interval to the default setting.

Default interval 3600

Parameters *seconds* — Specifies the interval at which the CCR-T messages are replayed for a gx session. The messages are replayed until a valid CCA-t response is received or until a 24 hour period expires, whichever comes first.

Values 60 to 86400

Default 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

interval

Syntax **interval** *seconds*
no interval

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx>ccrt-replay interval)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy>ccrt-replay interval)

Full Context configure subscriber-mgmt diameter-application-policy gx ccrt-replay interval
configure subscriber-mgmt diameter-application-policy gy ccrt-replay interval

Description This command specifies the interval at which CCR-T messages for Diameter Gx or Gy sessions that belong to the Diameter application policy are replayed, until a valid CCA-t response is received or until the configured **max-lifetime** period expires.

The **no** form of this command resets the interval to the default setting.

Default interval 3600

Parameters *seconds* — Specifies the interval at which the CCR-T messages are replayed for a gx session. The messages are replayed until a valid CCA-t response is received or until a 24 hour period expires, whichever comes first.

Values 60 to 86400

Default 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

interval

Syntax **interval** *interval*

Context [Tree] (config>redundancy>mc>peer>mcr>ring>cv interval)
[Tree] (config>redundancy>mc>peer>mc>l3-ring>cv interval)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring cv interval
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify interval

Description This command specifies the polling interval of the ring-node connectivity verification of this ring node.

The **no** form of this command reverts to the default.

Default interval 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *interval* — Specifies the polling interval of the ring-node connectivity verification of this ring node.

Values 1 to 6000

Platforms All

interval

Syntax **interval** *minutes*
no interval

Context **[Tree]** (config>subscr-mgmt>shcv-policy>periodic interval)

Full Context configure subscriber-mgmt shcv-policy periodic interval

Description This command specifies the time interval which all known sources should be verified. The actual rate is dependent on the number of known hosts and intervals.

The **no** form of this command reverts to the default.

Default interval 30 minutes

Parameters *minutes* — Specifies the interval, in minutes, between periodic connectivity checks.

Values 1 to 6000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>health-check>test-account interval)

Full Context configure aaa radius-server-policy servers health-check test-account interval

Description This command specifies the intervals at which the test account will send its access requests to probe the RADIUS servers.

Default interval 3

Parameters *seconds* — Specifies the probing interval.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interval

Syntax **interval** *seconds*

Context **[Tree]** (config>subscr-mgmt>pfcp-association>heartbeat interval)

Full Context configure subscriber-mgmt pfcp-association heartbeat interval

Description This command configures the interval between successive, successful heartbeats.

Default interval 60

Parameters *seconds* — Specifies the time frame, in seconds, between successive, successful heartbeats. This interval must be identical on both the BNG UPF and CPF. For information about the BNG CUPS CPF configuration, refer to the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide*.

Values 60 to 180

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

interval

Syntax **interval** {**1** | **60**}
no interval

Context **[Tree]** (config>port>ethernet>eth-cfm>mep>ais-enable interval)
[Tree] (config>lag>eth-cfm>mep>ais-enable interval)

Full Context configure lag eth-cfm mep ais-enable interval
configure port ethernet eth-cfm mep ais-enable interval

Description This command specifies the transmission interval of AIS messages in seconds.

The **no** form of this command reverts to the default values.

Parameters **1 | 60** — The transmission interval of AIS messages, in seconds.

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** *deci-seconds*
no interval

Context **[Tree]** (config>service>mac-notification interval)

Full Context configure service mac-notification interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls the frequency of subsequent MAC notification messages.

Parameters *deci-seconds* — Specifies the frequency of subsequent MAC notification messages, in deciseconds

Values 1 to 100

Platforms All

interval

Syntax **interval** {**1** | **60**}
no interval

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>ais-enable interval)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>ais-enable interval)

Full Context configure service epipe sap eth-cfm mep ais-enable interval
configure service epipe spoke-sdp eth-cfm ais-enable interval

Description This command specifies the transmission interval of AIS messages in seconds.

Parameters **1 | 60** — Specifies the transmission interval of AIS messages in seconds.

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** *deci-seconds*
no interval

Context **[Tree]** (config>service>vpls>mac-notification interval)

Full Context configure service vpls mac-notification interval

Description This command controls the frequency of subsequent MAC notification messages.

By default, this command inherits the chassis level configuration from **config>service>mac-notification**.

Parameters *deci-seconds* — Specifies the frequency of subsequent MAC notification messages, in deciseconds

Values 1 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interval

Syntax **interval** {**1** | **60**}
no interval

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable interval)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable interval)

Full Context configure service vpls mesh-sdp eth-cfm mep ais-enable interval
configure service vpls spoke-sdp eth-cfm mep ais-enable interval

Description This command specifies the transmission interval of AIS messages in seconds.

Parameters **1 | 60** — The transmission interval of AIS messages in seconds

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>service>vprn>static-route-entry>indirect>cpe-check interval)
[Tree] (config>service>vprn>static-route-entry>next-hop>cpe-check interval)

Full Context configure service vprn static-route-entry indirect cpe-check interval
configure service vprn static-route-entry next-hop cpe-check interval

Description This optional parameter specifies the interval between ICMP pings to the target IP address.

Default interval 1

Parameters *seconds* — An integer interval value.

Values 1 to 255

Platforms All

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>router>mpls>lsp-self-ping interval)

Full Context configure router mpls lsp-self-ping interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the interval at which LSP Self Ping packets are periodically sent on a candidate path of an RSVP LSP. This value is used for all LSPs that have LSP Self Ping enabled.

The **no** form of this command reverts to the default value.

Default interval 1

Parameters *seconds* — Specifies the value, in seconds, used as the fast retry timer for a secondary path.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** {**one-time** | *minimum-interval*}

Context **[Tree]** (config>app-assure>group>http-notif interval)

Full Context configure application-assurance group http-notification interval

Description This command configures the minimum interval in between notification messages. It can be set to **one-time** or a value in minutes from 1 to 1440.

The **no** form of this command removes the interval from the http-notification policy.

Default interval one-time

Parameters *minimum-interval* — Represents the minimum interval value in minutes in between two http notifications.

Values 1 to 1440

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

interval

Syntax **interval** *seconds*

Context **[Tree]** (config>ipsec>tnl-temp>icmp6-gen>pkt-too-big interval)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>icmp6-gen>pkt-too-big interval)
[Tree] (config>router>if>ipsec-tunnel>icmp-gen>pkt-too-big interval)

Full Context configure ipsec tunnel-template icmp6-generation pkt-too-big interval
configure router interface ipsec-tunnel icmp-gen pkt-too-big interval
configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval

Description This command configures the maximum interval during which messages can be sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the maximum interval during which messages can be sent, in seconds.

Values 1 to 60

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec tunnel-template icmp6-generation pkt-too-big interval

VSR

- configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interval

Syntax **interval** *seconds*

Context **[Tree]** (config>ipsec>tnl-temp>icmp6-gen>pkt-too-big interval)
[Tree] (config>router>if>ipsec-tunnel>icmp6-gen>pkt-too-big interval)
[Tree] (config>service>ies>if>ipsec-tunnel>icmp6-gen>pkt-too-big interval)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>icmp6-gen>pkt-too-big interval)
[Tree] (config>service>vprn>if>sap>ipsec-tun>icmp6-gen>pkt-too-big interval)

Full Context configure ipsec tunnel-template icmp6-generation pkt-too-big interval
configure router interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval
configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval
configure service vprn interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval
configure service vprn interface sap ipsec-tunnel icmp6-generation pkt-too-big interval

Description This command configures the interval for sending ICMPv6 Packet Too Big (code 2) messages. The maximum number of messages that can be sent during the interval is configured by the **message-count** command.

The **no** form of the command reverts to the default value.

Default interval 10

Parameters *seconds* — Specifies the time, in seconds, for sending 'message-count' ICMPv6 messages

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel icmp6-generation pkt-too-big interval
- configure ipsec tunnel-template icmp6-generation pkt-too-big interval

VSR

- configure router interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval
- configure service vprn interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval
- configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big interval

interval

Syntax **interval** *minutes*
no interval

Context **[Tree]** (config>test-oam>ldp-treetrace>path-discovery interval)

Full Context configure test-oam ldp-treetrace path-discovery interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the frequency of the LDP ECMP OAM path discovery. Every interval, the node sends LSP trace messages to attempt to discover the entire ECMP path tree for a given destination FEC.

The **no** form of this command removes the value from the configuration.

Default no interval

Parameters *minutes* — Specifies the number of minutes to wait before repeating the LDP tree auto discovery process.

Values 60 to 1440

Platforms All

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>test-oam>icmp>ping-template interval)

Full Context configure test-oam icmp ping-template interval

Description This command configures the packet transmit interval used when the interface is operational and possibly transitioning from up to down, but not down to up, because of the ping-template function.

The **no** form of this command reverts to the default value.

Default interval 60

Parameters *seconds* — Sets the packet transmit interval, in seconds, when the interface is operational.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** *minutes*
no interval

Context **[Tree]** (config>test-oam>ldp-treetrace>path-probing interval)

Full Context configure test-oam ldp-treetrace path-probing interval

Description This command configures the frequency of the LSP Ping messages used in the path probing phase to probe the paths of all LDP FECs discovered by the LDP tree trace path discovery.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command resets the interval to its default value.

Default no interval

Parameters *minutes* — Specifies the number of minutes to probe all active ECMP paths for each LDP FEC.

Values 1 to 60

Platforms All

interval

Syntax **interval** *interval*
no interval

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy interval)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy interval)

Full Context configure saa test type-multi-line lsp-ping sr-policy interval
configure saa test type-multi-line lsp-trace sr-policy interval

Description This command configures the number of seconds to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

The **no** form of this command reverts to the default value.

Default interval 1

Parameters *interval* — Specifies the number of seconds to wait before the next message request is sent.

Values 1 to 10

Default 1

Platforms All

interval

Syntax **interval** *milliseconds*
no interval

Context **[Tree]** (config>oam-pm>session>ethernet>dmm interval)
[Tree] (config>oam-pm>session>ethernet>lmm interval)

Full Context configure oam-pm session ethernet dmm interval
configure oam-pm session ethernet lmm interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the message period or probe spacing for the transmission of the DMM or LMM frame.

The **no** form of this command sets the interval to the default. If an LMM test is in **no shutdown** state, it always has timing parameters, whether default or operator configured.

Parameters *milliseconds* — Specifies the number of milliseconds between the transmission of the DMM or LMM frames. The default value for the DMM or LMM interval is different than the default interval for SLM. This is intentional.

Values 100, 1000, 10000

Default 1000

Platforms All

interval

Syntax **interval** *milliseconds*
no interval

Context **[Tree]** (config>oam-pm>session>ip>twamp-light interval)

Full Context configure oam-pm session ip twamp-light interval

Description This command defines the message period, or probe spacing, for transmitting a TWAMP Light frame.

The **no** form of this command sets the interval to the default value.

Default interval 1000

Parameters *milliseconds* — Specifies the number of milliseconds between TWAMP Light frame transmission.

Values 100, 1000, 10000

Default 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** *milliseconds*
no interval

Context **[Tree]** (config>oam-pm>session>mpls>dm interval)

Full Context configure oam-pm session mpls dm interval

Description This command defines the message period, or probe spacing, to transmit a DM frame.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command sets the interval to the default value.

Parameters *milliseconds* — Specifies the number of milliseconds between DM frame transmissions.

Values 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000, 10000

Default 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

interval

Syntax **interval** [*seconds*]
no interval

Context **[Tree]** (config>filter>redirect-policy>dest>ping-test interval)

Full Context configure filter redirect-policy destination ping-test interval

Description This command specifies the amount of time, in seconds, between consecutive requests sent to the far end host.

Default interval 1

Parameters *seconds* — Specifies the amount of time, in seconds, between consecutive requests sent to the far end host.

Values 1 to 60

Platforms All

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>router>static-route-entry>indirect>cpe-check interval)
[Tree] (config>router>static-route-entry>next-hop>cpe-check interval)

Full Context configure router static-route-entry indirect cpe-check interval
configure router static-route-entry next-hop cpe-check interval

Description This optional parameter specifies the interval between ICMP pings to the target IP address.

Default interval 1

Parameters *seconds* — Specifies the interval value, in seconds.

Values 1 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>vrrp>priority-event>host-unreachable interval)

Full Context configure vrrp priority-event host-unreachable interval

Description This command configures the number of seconds between host unreachable priority event ICMP echo request messages directed to the host IP address.

The **no** form of the command reverts to the default value.

Default interval 1

Parameters *seconds* — Specifies the number of seconds between the ICMP echo request messages sent to the host IP address for the host unreachable priority event.

Values 1 to 60

interval

Syntax **interval** *seconds*
no interval

Context **[Tree]** (config>system>cron>sched interval)

Full Context configure system cron schedule interval

Description This command specifies the interval between runs of an event.

Default no interval

Parameters *seconds* — Specifies the interval, in seconds, between runs of an event.

Values 30 to 42949672

Platforms All

interval

Syntax **interval** *interval*
no interval

Context **[Tree]** (config>system>grpc>tcp-keepalive interval)
[Tree] (config>system>grpc-tunnel>destination-group>tcp-keepalive interval)
[Tree] (config>system>telemetry>destination-group>tcp-keepalive interval)

Full Context configure system grpc tcp-keepalive interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system grpc-tunnel destination-group tcp-keepalive interval
configure system telemetry destination-group tcp-keepalive interval

Description This command configures the amount of time, in seconds, between successive TCP keepalive probes sent by the router.

The **no** form of this command reverts to the default value.

Default interval 15

Parameters *interval* — Specifies the number of seconds between TCP keepalive probes.

Values 1 to 100000

Default 15

Platforms All

interval

Syntax **interval** *seconds*

Context **[Tree]** (config>ipsec>tnl-temp>icmp-gen>frag-required interval)
[Tree] (config>router>if>ipsec>ipsec-tunnel>icmp-generation>frag-required interval)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>icmp-generation>frag-required interval)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>icmp-generation>frag-required interval)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel>icmp-generation>frag-required interval)
[Tree] (config>service>vprn>if>sap>ip-tunnel>icmp-generation>frag-required interval)

Full Context configure ipsec tunnel-template icmp-generation frag-required interval
configure router interface ipsec ipsec-tunnel icmp-generation frag-required interval
configure service ies interface ipsec ipsec-tunnel icmp-generation frag-required interval
configure service vprn interface ipsec ipsec-tunnel icmp-generation frag-required interval
configure service vprn interface sap ip-tunnel icmp-generation frag-required interval
configure service vprn interface sap ipsec-tunnel icmp-generation frag-required interval

Description This command configures the interval for sending ICMP Destination Unreachable "fragmentation needed and DF set" messages (type 3, code 4). The maximum number of messages that can be sent during the interval is configured by the **message-count** command.

The **no** form of the command reverts to the default value.

Default interval 10

Parameters *seconds* — Specifies the time, in seconds, for sending ICMPv6 Destination Unreachable "fragmentation needed and DF set" messages (type 3, code 4).

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure ipsec tunnel-template icmp-generation frag-required interval
- configure service vprn interface sap ip-tunnel icmp-generation frag-required interval
- configure service vprn interface sap ipsec-tunnel icmp-generation frag-required interval

VSR

- configure service vprn interface ipsec ipsec-tunnel icmp-generation frag-required interval
- configure router interface ipsec ipsec-tunnel icmp-generation frag-required interval
- configure service ies interface ipsec ipsec-tunnel icmp-generation frag-required interval

interval

Syntax **interval** *seconds*

Context **[Tree]** (config>test-oam>link-meas>template interval)

Full Context configure test-oam link-measurement measurement-template interval

Description This command configures the length of time between test packet transmission.

Default interval 1

Parameters *seconds* — Specifies the elapsed time between transmission of test packets for the specified template

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.204 intervals-stored

intervals-stored

Syntax **intervals-stored** *intervals*
no intervals-stored

Context **[Tree]** (config>oam-pm>session>meas-interval intervals-stored)

Full Context configure oam-pm session meas-interval intervals-stored

Description This command defines the number of completed measurement intervals per session to be stored in volatile system memory. The entire block of memory is allocated for the measurement interval when the test is active (**no shutdown**) to ensure memory is available. The numbers are increasing from 1 to the configured value + 1. The active pm data is stored in the interval number 1 and older runs are stored, in order, to the upper most number with

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

the oldest rolling off when the number of completed measurement intervals exceeds the configured value+1. As new test measurement intervals complete for the session, the stored intervals are renumbered to maintain the described order. Use caution when setting this value. There must be a balance between completed runs stored in volatile memory and the use of the write-to-flash function of the accounting policy.

The **5-mins** and **15-mins** measurement intervals share the same (1 to 96) retention pool. In the event that both intervals are required, the sum total of both intervals cannot exceed 96. The **1-hour** and **1-day** measurement intervals utilize their own ranges.

If this command is omitted when configuring the measurement interval, the default value is used.

The **no** form of the command reverts to the default.

Default intervals-stored 1

Parameters *intervals* — Specifies the number of measurement intervals.

Values **5-mins**: 1 to 96
15-mins: 1 to 96
1-hour: 1 to 24
1-day: 1

Default **5-mins**: 32
15-mins: 32
1-hour: 8
1-day: 1

Platforms All

13.205 interworking

interworking

Syntax **interworking** *frf-5*
no interworking

Context **[Tree]** (config>service>apipe interworking)

Full Context configure service apipe interworking

Description This command specifies the interworking function that should be applied for packets that ingress or egress SAPs that are part of an Apipe service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Interworking must be configured before adding a Frame-Relay SAP to an Apipe service. Interworking is applicable only when the two endpoints (that is, the two SAPs or the SAP and the spoke SDP) are of different types. Also, there are limitations on the combinations of SAP type, vc-type, and interworking values as shown in Table 66.

Table 66 **SAP Types, VC-Types and Interworking Values**

SAP Type	Allowed VC-Type Value	Allowed Interworking Value
ATM VC	atm-vcc, atm-sdu	—
	fr-dlci	
FR DLCI	fr-dlci	—
	atm-sdu	frf-5

Parameters *frf-5* — Specifies Frame Relay to ATM Network Interworking (FRF.5).

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

13.206 invert-data

invert-data

Syntax [**no**] **invert-data**

Context **[Tree]** (config>port>tdm>ds1 invert-data)
[Tree] (config>port>tdm>e1 invert-data)

Full Context configure port tdm ds1 invert-data
configure port tdm e1 invert-data

Description This command causes all data bits to be inverted, to guarantee ones density. Typically used with AMI line encoding.

Default no invert-data

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.207 iom

iom

Syntax **iom** *slot-number* **type** {[**load-balancer**] [**ue-anchor**]}
no iom *slot-number*

Context **[Tree]** (config>isa>wlan-gw-group iom)

Full Context configure isa wlan-gw-group iom

Description This command designates the specified IOM as a WLAN-GW IOM. Each WLAN-GW IOM must be provisioned with two ISA-BB modules on a hardware chassis and with an ISA-BB module in the first MDA slot in the VSR.

The **no** form of this command removes the IOM from the configuration.

Parameters *slot-number* — Indicates the IOM slot to be used in the WLAN-GW group.

Values 1 to 10

type {[**load-balancer**] [**ue-anchor**]} — This parameter is supported on the VSR only. It determines if an IOM slot is used for load-balancing or UE anchoring and processing, or both. When the **wlan-gw-group** has only a single IOM, it is required to put this IOM in both modes at the same time.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

iom

Syntax **iom** [**detail**]
no iom

Context **[Tree]** (debug>router>mpls>event iom)

Full Context debug router mpls event iom

Description This command reports MPLS debug events originating from the XMA.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about MPLS events originating from the XMA.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.208 ip

ip

Syntax **ip** *address*
no ip

Context **[Tree]** (config>service>vpls>mcr-default-gtw ip)

Full Context configure service vpls mcr-default-gtw ip

Description This command relates to a system configured for Dual Homing in L2-TPSDA. It defines the IP address used when the system sends out a gratuitous ARP on an active SAP after a ring heals or fails in order to attract traffic from subscribers on the ring with connectivity to that SAP.

The **no** form of this command reverts to the default.

Default no ip

Parameters *address* — Specifies the IP address in a.b.c.d. format.

Platforms All

ip

Syntax **ip** *ip-filter-id*
no ip

Context **[Tree]** (config>service>template>epipe-sap-template>egress>filter ip)
[Tree] (config>service>template>epipe-sap-template>ingress>filter ip)

Full Context configure service template epipe-sap-template egress filter ip
configure service template epipe-sap-template ingress filter ip

Description This command associates an existing IP filter policy with the template.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

Parameters *ip-filter-id* — Specifies the IP filter policy ID. The filter ID must already exist within the created IP filters.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip

Syntax **ip** *name*
no ip

Context **[Tree]** (config>service>template>epipe-sap-template>egress>filter-name ip)
[Tree] (config>service>template>epipe-sap-template>ingress>filter-name ip)

Full Context configure service template epipe-sap-template egress filter-name ip
configure service template epipe-sap-template ingress filter-name ip

Description This command associates an existing IP filter policy with the template.

Parameters *name* — Specifies the IP filter policy name, up to 64 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip

Syntax **ip** *name*
no ip

Context **[Tree]** (config>service>template>vpls-sap-template>egress>filter-name ip)
[Tree] (config>service>template>vpls-sap-template>ingress>filter-name ip)

Full Context configure service template vpls-sap-template egress filter-name ip
configure service template vpls-sap-template ingress filter-name ip

Description This command associates an existing IP filter policy with the template.

Parameters *name* — Specifies the IP filter policy name, up to 64 characters.

Platforms All

ip

Syntax [**no**] **ip** *ip-address*

Context **[Tree]** (debug>service>id>arp-host ip)

Full Context debug service id arp-host ip

Description This command displays ARP host events for a particular IP address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip

Syntax [**no**] **ip** *ip-address*

Context **[Tree]** (debug>service>id>host-connectivity-verify ip)

Full Context debug service id host-connectivity-verify ip

Description This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular IP address.

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values ipv4-prefix: a.b.c.d (host bits must be 0)

ipv6-prefix:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF] H
- d: [0 to 255] D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip

Syntax [**no**] **ip** *ip-address*[/*mask*]

Context **[Tree]** (config>app-assure>group>policy>transit-ip-policy>static-aa-sub ip)

Full Context configure application-assurance group policy transit-ip-policy static-aa-sub ip

Description This command configures the /32 IP address for a static transit aa-sub.

The **no** form of this command deletes the ip address assigned to the static transit aa-sub from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the IP address in a.b.c.d form.

Values

ipv6-address/prefix:	ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D prefix-length /32 to /64

ip

Syntax **ip src** *ip-address* **dest** *ip-address*
no ip

Context **[Tree]** (config>mirror>mirror-dest>encap>layer-3-encap>gateway ip)

Full Context configure mirror mirror-dest encap layer-3-encap gateway ip

Description This command configures the source IPv4 address and destination IPv4 address to use in the IPv4 header part of the routable LI encapsulation.

Parameters **src** *ip-address* — Specifies source IP address.

Values a.b.c.d

dest *ip-address* — Specifies destination IP address.

Values a.b.c.d

Platforms All

ip

Syntax **ip**

Context **[Tree]** (config>oam-pm>session ip)

Full Context configure oam-pm session ip

Description Commands in this context configure the IP-specific source and destination information, the priority, and the IP test tools on the launch point.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ip

Syntax [**no**] **ip** *ip-filter-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>system-filter ip)

Full Context configure filter system-filter ip

Description This command activates an IPv4 system filter policy. Once activated, all IPv4 ACL filter policies that chain to the system filter (**config>filter>ip-filter>chain-to-system-filter**) will automatically execute system filter policy rules first.

The **no** form of the command deactivates the system filter policy.

Parameters *ip-filter-id* — Specifies the existing IPv4 filter policy with scope **system**. This parameter can either be expressed as a decimal integer, or as an ASCII string of up to 64 characters.

Values 1 to 65535 or the filter policy name (*filter-name*, 64 char max)

Platforms All

ip

Syntax [**no**] **ip**

Context [Tree] (debug>router ip)

Full Context debug router ip

Description This command configures debugging for IP.

Platforms All

ip

Syntax **ip**

Context [Tree] (config>system ip)

Full Context configure system ip

Description This command configures system-wide IP router parameters.

Platforms All

ip

Syntax **ip** *ip-address netmask*
ip *ip-address/mask*
ip ip-prefix-list *ip-prefix-list-name*
no ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>ip-filter>entry>match ip)

Full Context configure filter ip-filter entry match ip

Description This command configures a destination or source IP address to be used as an IP match criterion.

Parameters *ip-address/mask* — Specifies the IPv4 address and mask.

Values

ip-address	a.b.c.d

netmask — Specifies the name of the IP prefix list, up to 256 characters.

ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.

Platforms All

ip

Syntax **ip** *ipv6-address ipv6-address-mask*
ip *ipv6-address/mask*
ip ipv6-prefix-list *prefix-list-name*
no ip

Context [Tree] (config>filter>ipv6-filter>entry>match ip)

Full Context configure filter ipv6-filter entry match ip

Description This command configures a destination or source IP address to be used as an IP match criterion.

Parameters *ipv6-address/mask* — Specifies the IPv6 address and mask.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

ip-prefix-list-name — Specifies the name of an IPv6 prefix list, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.209 ip-addr-backup

ip-addr-backup

Syntax **ip-addr-backup** *ip-address*[:*port*]
no ip-addr-backup

Context **[Tree]** (config>sflow>receiver ip-addr-backup)

Full Context configure sflow receiver ip-addr-backup

Description This command configures back-up IPv4 or IPv6 destination address for the sFlow agent to send sFlow datagrams to. Optionally a destination port can also be configured (by default port 6343 is used).

The **no** form of this command deletes backup sFlow receiver destination.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address to send the sFlow datagrams to.

Values

a.b.c.d	(IPv4)
x:x:x:x:x:x:x:x	(IPv6)
[x:x:x:x:x:x:x:x]	(IPv6)
x - [0 to FFFF]H	

port — Specifies the UDP destination port to send the sFlow datagrams to.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-s, 7950 XRS

13.210 ip-addr-primary

ip-addr-primary

Syntax **ip-addr-primary** *ip-address*[:*port*]
no ip-addr-primary

Context **[Tree]** (config>sflow>receiver ip-addr-primary)

Full Context configure sflow receiver ip-addr-primary

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures primary IPv4 or IPv6 destination address for the sFlow agent to send sFlow datagrams to. Optionally a destination port can also be configured (by default port 6343 is used).

The **no** form of this command deletes primary sFlow receiver destination.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address to send the sFlow datagrams.

Values

a.b.c.d	(IPv4)
x:x:x:x:x:x:x:x	(IPv6)
[x:x:x:x:x:x:x:x]	(IPv6)
x - [0..FFFF]H	

port — Specifies the UDP destination port to send the sFlow datagrams.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-s, 7950 XRS

13.211 ip-addr1

ip-addr1

Syntax **ip-addr1** {**eq** | **neq**} *ip-address*
no ip-addr1

Context **[Tree]** (debug>app-assure>group>traffic-capture>match ip-addr1)

Full Context debug application-assurance group traffic-capture match ip-addr1

Description This command configures debugging on IP address 1.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.212 ip-addr2

ip-addr2

Syntax **ip-addr2** {**eq** | **neq**} *ip-address*
no ip-addr2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>app-assure>group>traffic-capture>match ip-addr2)

Full Context debug application-assurance group traffic-capture match ip-addr2

Description This command configures debugging on IP address 2.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.213 ip-address

ip-address

Syntax **ip-address** *ip-address*
no ip-address

Context [Tree] (config>aaa>isa-radius-plcy>servers>server ip-address)

Full Context configure aaa isa-radius-policy servers server ip-address

Description This command configures the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Default no ip-address

Parameters *ip-address* — Specifies the IP address of the RADIUS server.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.214 ip-advertise-routes

ip-advertise-routes

Syntax **ip-advertise-routes**

Context [Tree] (config>subscr-mgmt>isa-svc-chain>evpn>export ip-advertise-routes)

Full Context configure subscriber-mgmt isa-service-chaining evpn export ip-advertise-routes

Description Commands in this context configure EVPN routes to be advertised to a BGP EVPN peer participating in service chaining.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.215 ip-assigned

ip-assigned

Syntax [**no**] **ip-assigned**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state ip-assigned)

Full Context configure subscriber-mgmt wlan-gw ue-query state ip-assigned

Description This command enables matching on UEs in an IP-assigned state, meaning that the UE already has an IP assigned but it is not yet authorized. This usually only applies when **auth-on-dhcp** is not configured.

The **no** form of this command disables matching on UEs in an IP-assigned state, unless all state matching is disabled.

Default no ip-assigned

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.216 ip-assigned-authorized

ip-assigned-authorized

Syntax [**no**] **ip-assigned-authorized**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state ip-assigned-authorized)

Full Context configure subscriber-mgmt wlan-gw ue-query state ip-assigned-authorized

Description This command enables matching on UEs in an IP-assigned and authorized state, meaning that the UE already has an IP assigned and is authorized, but is not yet promoted to a final state such as ESM or DSM. This applies to UEs authenticated by distributed RADIUS proxy without **auth-on-dhcp** configured. UEs move to this state upon DHCP completion and continue to a more final state (such as DSM, ESM, or portal) upon receiving the first data packet.

The **no** form of this command disables matching on UEs in an IP-assigned and authorized state, unless all state matching is disabled.

Default no ip-assigned-authorized

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.217 ip-cache

ip-cache

Syntax **ip-cache**

Context **[Tree]** (config>app-assure>group>dns-ip-cache ip-cache)

Full Context configure application-assurance group dns-ip-cache ip-cache

Description This command configures the dns-ip-cache cache parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.218 ip-can-type

ip-can-type

Syntax [**no**] **ip-can-type**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp ip-can-type)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp ip-can-type

Description This command includes the ip-can-type.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.219 ip-criteria

ip-criteria

Syntax [**no**] **ip-criteria**

Context **[Tree]** (config>qos>sap-egress ip-criteria)
[Tree] (config>qos>sap-ingress ip-criteria)

Full Context configure qos sap-egress ip-criteria
configure qos sap-ingress ip-criteria

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description IP criteria-based SAP ingress or egress policies are used to select the appropriate ingress or egress queue or policer and corresponding forwarding class and packet profile for matched traffic.

This command is used to enter the context to create or edit policy entries that specify IP criteria such as IP quintuple lookup or DiffServ code point.

The software implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit.

The **no** form of this command deletes all the entries specified under this node. When IP criteria entries are removed from a SAP ingress or egress policy, the IP criteria is removed from all services where that policy is applied.

Platforms All

ip-criteria

Syntax [**no**] **ip-criteria**

Context **[Tree]** (config>qos>network>ingress ip-criteria)
[Tree] (config>qos>network>egress ip-criteria)

Full Context configure qos network egress ip-criteria
configure qos network ingress ip-criteria

Description IP criteria-based network ingress and egress policies are used to select the appropriate ingress or egress queue or policer, and the corresponding forwarding class and packet profile for matched traffic. This command is used to enter the context to create or edit policy entries that specify IP criteria such as IP quintuple lookup or DSCP.

The 7750 SR OS implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. Entries must be sequenced correctly from most to least explicit.

The ingress classification only applies to the outer IP header of non-tunneled traffic. The only exception is for traffic received on a Draft Rosen tunnel, for which only classification on the outer IP header is supported.

Attempting to apply a network QoS policy containing an **ip-criteria** statement to any object except a network IP interface will result in an error.

The **no** form of this command deletes all entries specified under this node. When IP criteria entries are removed from a network policy, the IP criteria are removed from all network interfaces to which that policy is applied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-criteria

Syntax [**no**] **ip-criteria**

Context **[Tree]** (config>service>apipe>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>cpipe>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>epipe>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>fpipe>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>ies>if>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>ipipe>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>vpls>sap>ingress>criteria-overrides ip-criteria)
[Tree] (config>service>vprn>if>sap>ingress>criteria-overrides ip-criteria)

Full Context configure service apipe sap ingress criteria-overrides ip-criteria
configure service cpipe sap ingress criteria-overrides ip-criteria
configure service epipe sap ingress criteria-overrides ip-criteria
configure service fpipe sap ingress criteria-overrides ip-criteria
configure service ies interface sap ingress criteria-overrides ip-criteria
configure service ipipe sap ingress criteria-overrides ip-criteria
configure service vpls sap ingress criteria-overrides ip-criteria
configure service vprn interface sap ingress criteria-overrides ip-criteria

Description Commands in this context configure IPv4 criteria overrides.

The **no** form of this command removes any existing IPv4 overrides from the SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap ingress criteria-overrides ip-criteria
- configure service fpipe sap ingress criteria-overrides ip-criteria
- configure service cpipe sap ingress criteria-overrides ip-criteria
- configure service vprn interface sap ingress criteria-overrides ip-criteria
- configure service epipe sap ingress criteria-overrides ip-criteria
- configure service ipipe sap ingress criteria-overrides ip-criteria
- configure service vpls sap ingress criteria-overrides ip-criteria

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress criteria-overrides ip-criteria

13.220 ip-exception

ip-exception

Syntax **ip-exception** *filter-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ip-exception

Context [Tree] (config>router>if>ipsec ip-exception)
[Tree] (config>service>ies>if>ipsec ip-exception)
[Tree] (config>service>vprn>if>ipsec ip-exception)

Full Context configure router interface ipsec ip-exception
configure service ies interface ipsec ip-exception
configure service vprn interface ipsec ip-exception

Description This command configures the IP exception filter for the secured interface. All ingress traffic matching by the specified filter bypasses IPsec processing.

The **no** form of this command removes the policy from the configuration.

Default no ip-exception

Parameters *filter-id* — Specifies IP filter policy that will be used to bypass encryption.

Platforms VSR

ip-exception

Syntax **ip-exception** *filter-id* [**create**]
no ip-exception *filter-id*

Context [Tree] (config>filter ip-exception)

Full Context configure filter ip-exception

Description Commands in this context configure the specified IPv4 exception filter.

The **no** form of the command deletes the IPv4 exception filter.

Parameters *filter-id* — Specifies the IPv4 filter policy ID expressed as a decimal integer.

Values 1 to 65535

create — This keyword is required to create the configuration context. Once it is created, the context can be enabled with or without the **create** keyword.

Platforms VSR

ip-exception

Syntax **ip-exception** *filter-id* **direction** {**inbound** | **outbound**}
no ip-exception direction {**inbound** | **outbound**}

Context [Tree] (config>router>if>group-encryption ip-exception)

Full Context configure router interface group-encryption ip-exception

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates an IP exception filter policy with an NGE-enabled router interface to allow packets matching the exception criteria to transit the NGE domain as clear text.

When an exception filter is added for inbound traffic, packets matching the criteria in the IP exception filter policy are allowed to be received in clear text even if an inbound key group is configured. If no inbound key group is configured, then associated inbound IP exception filter policies will be ignored.

When an exception filter is added for outbound traffic, packets matching the criteria in the IP exception filter policy are not encrypted when sent out of the router interface even if an outbound key group is configured. If no outbound key group is configured, then associated outbound IP exception filter policies will be ignored.

The **no** form of this command removes the IP exception filter policy from the specified direction.

Default no ip-exception direction inbound
no ip-exception direction outbound

Parameters *filter-id* — Specifies the IP exception filter policy. The IP exception ID or exception name must have already been created.

Values 1 to 6553, *filter-name* (64 characters maximum)

inbound — Binds the exception filter policy in the inbound direction.

outbound — Binds the exception filter policy in the outbound direction.

Platforms VSR

13.221 ip-fast-reroute

ip-fast-reroute

Syntax [**no**] **ip-fast-reroute**

Context **[Tree]** (config>router ip-fast-reroute)

Full Context configure router ip-fast-reroute

Description This command enables IP Fast-Reroute (FRR) feature on the system.

This feature provides for the use of a Loop-Free Alternate (LFA) backup next-hop for forwarding in-transit and CPM generated IP packets when the primary next-hop is not available. IP FRR is supported on IPv4 and IPv6 OSPF/IS-IS prefixes forwarded in the base router instance to a network IP interface or to an IES SAP interface or spoke interface. It is also supported for VPRN VPN-IPv4 OSPF prefixes and VPN-IPv6 OSPF prefixes forwarded to a VPRN SAP interface or spoke interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IP FRR also provides a LFA backup next-hop for the destination prefix of a GRE tunnel used in an SDP or in VPRN auto-bind.

When any of the following events occurs, IGP instructs in the fast path on the XMAs to enable the LFA backup next-hop:

- OSPF/IS-IS interface goes operationally down: physical or local admin shutdown.
- Timeout of a BFD session to a next-hop when BFD is enabled on the OSPF/IS-IS interface

When the SPF computation determines there is more than one primary next-hop for a prefix, it will not program any LFA next-hop in RTM. Therefore, the IP prefix will resolve to the multiple equal-cost primary next-hops that provide the required protection.

The **no** form of this command disables the IP FRR feature on the system

Default no ip-fast-reroute

Platforms All

13.222 ip-filter

ip-filter

Syntax **ip-filter** *filter-id*
no ip-filter [**force**]

Context **[Tree]** (config>subscr-mgmt>sla-profile>egress ip-filter)
[Tree] (config>subscr-mgmt>sla-profile>ingress ip-filter)

Full Context configure subscriber-mgmt sla-profile egress ip-filter
configure subscriber-mgmt sla-profile ingress ip-filter

Description This command configures an egress or ingress IP filter.

The **no** form of this command reverts to the default.

Parameters *filter-id* — Specifies an existing IP filter policy ID.

Values 1 to 65535, or name, up to 64 characters

force — Forces the exclusion of the IP filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-filter

Syntax **ip-filter** *ip-filter-id* **entry** *entry-id* [*entry-id*]
no ip-filter *ip-filter-id* [**entry** *entry-id*]

Context **[Tree]** (config>mirror>mirror-source ip-filter)

Full Context configure mirror mirror-source ip-filter

Description This command enables mirroring of packets that match specific entries in an existing IP filter.

The **ip-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The IP filter must already exist in order for the command to execute. Filters are configured in the **config>filter** context. If the IP filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IP interface, an error is not generated but mirroring will not be enabled (there are no packets to mirror). Once the IP filter is defined to a SAP or IP interface, mirroring is enabled.

If the IP filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

If the IP filter is defined as egress, only egress packets are mirrored. Egress mirrored packets are mirrored to the mirror destination after all egress packet modifications.

An *entry-id* within an IP filter can only be mirrored to a single mirror destination. If the same *entry-id* is defined multiple times, an error occurs and only the first **mirror-source** definition is in effect.

By default, no packets matching any IP filters are mirrored. Mirroring of IP filter entries must be explicitly defined.

The **no ip-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *ip-filter-id*.

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring of that list of *entry-id*'s is terminated within the *ip-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

Parameters *ip-filter-id* — Specifies the IP filter ID whose entries are mirrored. If the *ip-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *ip-filter-id* is defined on a SAP or IP interface.

Values 1 to 65535
name, up to 64 characters

entry-id — Specifies the IP filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. Multiple *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If an *entry-id* does not exist within the IP filter, an error occurs and the command will not execute.

If the filter's *entry-id* is renumbered within the IP filter definition, the old *entry-id* is removed but the new *entry-id* must be manually added to the configuration to include the new (renumbered) entry's criteria.

Values 1 to 2097151

Platforms All

ip-filter

Syntax [**no**] **ip-filter** *ip-filter-id*

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block ip-filter)

Full Context configure li li-filter-block-reservation li-reserved-block ip-filter

Description This command configures to which normal IPv4 address filters the entry reservation is applied.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

The **no** form of this command removes the IPv4 filter ID from the configuration.

Parameters *ip-filter-id* — Specifies the filter identification identifies the normal IPv4 address filters.

Values {*filter-id* | *filter-name*}

filter-id:	1 to 65535
filter-name:	up to 64 characters (*filter-name* is an alias for input only. The *filter-name* gets replaced with an id automatically by SR OS in the configuration).

Platforms All

ip-filter

Syntax [**no**] **ip-filter** *ip-filter-id*

Context **[Tree]** (config>li>li-filter-assoc>li-ip-fltr ip-filter)

Full Context configure li li-filter-associations li-ip-filter ip-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the IP filter(s) into which the entries from the specified li-ip-filter are to be inserted. The **li-ip-filter** and **ip-filter** must already exist before the association is made. If the normal IP filter is deleted then the association is also removed (and not re-created if the IP filter comes into existence in the future).

The **no** form of this command removes the IP filter name from the configuration.

Parameters *ip-filter-id* — Specifies an existing IP filter policy.

Values *filter-id* — 1 to 65535
filter-name — up to 64 characters

Platforms All

ip-filter

Syntax **ip-filter** *ip-filter-id* **entry** *entry-id* [*entry-id*] [**intercept-id** *intercept-id* [*intercept-id*]] [**session-id** *session-id* [*session-id*]]
no ip-filter *ip-filter-id* [**entry** *entry-id* [*entry-id*]]

Context **[Tree]** (config>li>li-source ip-filter)

Full Context configure li li-source ip-filter

Description This command enables lawful interception (LI) of packets that match specific entries in an existing IP filter.

The **ip-filter** command directs packets which match the defined list of entry IDs to be intercepted to the destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The IP filter must already exist in order for the command to execute. Filters are configured in the **config>filter** context. If the IP filter does not exist, an error occurs. If the filter exists but has not been associated with a SAP or IP interface, an error is not generated but mirroring will not be enabled (there are no packets to mirror). Once the IP filter is defined to a SAP, IP interface or subscriber, mirroring is enabled.

If the IP filter is defined as ingress, only ingress packets are intercepted. Ingress packets are sent to the destination prior to any ingress packet modifications.

If the IP filter is defined as egress, only egress packets are intercepted. Egress packets are sent to the destination after all egress packet modifications.

An *entry-id* within an IP filter can only be intercepted to a single destination. If the same *entry-id* is defined multiple times, an error occurs and only the first definition is in effect.

By default, no packets matching any IP filters are intercepted. Interception of IP filter entries must be explicitly defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, interception of that list of *entry-id*'s is terminated within the *ip-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being intercepted, no error will occur for that *entry-id* and the command will execute normally.

Parameters *ip-filter-id* — Specifies the IP filter ID whose entries are to be intercepted. If the *ip-filter-id* does not exist, an error will occur and the command will not execute. Intercepting packets will commence when the *ip-filter-id* is defined on a SAP or IP interface.

entry-id — Specifies the IP filter entries to use as match criteria for lawful intercept (LI). The **entry** keyword begins a list of *entry-id*'s for interception. Multiple *entry-id* entries can be specified with a single command. Each *entry-id* must be separated by a space. Up to <N><n> 8 entry IDs may be specified in a single command.

If an *entry-id* does not exist within the IP filter, an error occurs and the command will not execute.

If the filter's *entry-id* is renumbered within the IP filter definition, the old *entry-id* is removed but the new *entry-id* must be manually added to the configuration to include the new (renumbered) entry's criteria.

intercept-id — Specifies the intercept ID that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This intercept ID can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, an *intercept-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *intercept-id* configured for an **li-source** entry, then the default value is inserted. When the mirror service is configured with **ip-gre** routable encapsulation, no *intercept-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4294967295 (32b) for **nat li-source** entries that are using a mirror service that is not configured with routable encap

1 to 1073741824 (30b) for all types of **li-source** entries that are using a mirror service with routable ip-udp-shim encap and no direction-bit.

1 to 536870912 (29b) for all types of **li-source** entries that are using a mirror service with routable **ip-udp-shim** encapsulation and with the **direction-bit** enabled.

session-id — Specifies the *session-id* that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This *session-id* can be used (for example by a downstream LI Gateway) to identify the particular LI session to which the packet belongs. The *session-id* is only valid and used for mirror services that are configured with **ip-udp-shim** routable encap (**config>mirror>mirror-dest>encap>ip-udp-shim**). For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-udp-shim routable encap, a *session-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *session-id* configured for an **li-source** entry, then the default value is inserted. When a mirror service is configured with **ip-gre** routable encap, no *session-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4,294,967,295 (32b)

Platforms All

ip-filter

Syntax **ip-filter** *ip-filter-id* **entry** *entry-id* [*entry-id*]
no ip-filter *ip-filter-id* [**entry** *entry-id*]

Context **[Tree]** (debug>mirror-source ip-filter)

Full Context debug mirror-source ip-filter

Description This command enables mirroring of packets that match specific entries in an existing IP filter.

The **ip-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The IP filter must already exist in order for the command to execute. Filters are configured in the **config>filter** context. If the IP filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IP interface, an error is not generated but mirroring will not be enabled (there are no packets to mirror). Once the IP filter is defined to a SAP or IP interface, mirroring is enabled.

If the IP filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

If the IP filter is defined as egress, only egress packets are mirrored. Egress mirrored packets are mirrored to the mirror destination after all egress packet modifications.

An *entry-id* within an IP filter can only be mirrored to a single mirror destination. If the same *entry-id* is defined multiple times, an error occurs and only the first **mirror-source** definition is in effect.

By default, no packets matching any IP filters are mirrored. Mirroring of IP filter entries must be explicitly defined.

The **no ip-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *ip-filter-id*.

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring of that list of *entry-id*'s is terminated within the *ip-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-filter-id* — The IP filter ID whose entries are mirrored. If the *ip-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *ip-filter-id* is defined on a SAP or IP interface.

entry-id — The IP filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. A maximum of eight *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space.

If an *entry-id* does not exist within the IP filter, an error occurs and the command will not execute.

If the filter's *entry-id* is renumbered within the IP filter definition, the old *entry-id* is removed but the new *entry-id* must be manually added to the configuration to include the new (renumbered) entry's criteria.

Platforms All

ip-filter

Syntax **ip-filter** *filter-id* [**name**] [**create**]
no ip-filter {*filter-id* | *filter-name*}

Context **[Tree]** (config>filter ip-filter)

Full Context configure filter ip-filter

Description Commands in this context configure the specified IPv4 filter policy.

The **no** form of the command deletes the IPv4 filter policy. A filter policy cannot be deleted until it is removed from all objects where it is applied.

Default none

Parameters *filter-id* — Specifies the IPv4 filter policy ID expressed as a decimal integer.

Values 1 to 65535

name — Configures an optional filter name, up to 64 characters in length, to a given filter. This filter name can then be used in configuration references, display, and show commands throughout the system. A defined filter name can help the service provider or administrator to identify and manage filters within the SR OS platforms.

To create a filter, you must assign a filter ID, however, after it is created, either the filter ID or filter name can be used to identify and reference a filter.

If a name is not specified at creation time, then SR OS assigns a string version of the *filter-id* as the name.

Filter names may not begin with an integer (0 to 9).

filter-name — Specifies a string, up to 64 characters, uniquely identifying this IPv4 filter policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — This keyword is required to create the configuration context. Once it is created, the context can be enabled with or without the **create** keyword.

Platforms All

ip-filter

Syntax [**no**] **ip-filter**

Context **[Tree]** (config>system>security>mgmt-access-filter ip-filter)

Full Context configure system security management-access-filter ip-filter

Description Commands in this context configure management access IP filter parameters.

Platforms All

ip-filter

Syntax [**no**] **ip-filter**

Context **[Tree]** (config>system>security>cpm-filter ip-filter)

Full Context configure system security cpm-filter ip-filter

Description Commands in this context configure CPM IP filter parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ip-filter

Syntax **ip-filter** *src-filter-id* [**src-entry** *src-entry-id*] **to** *dst-filter-id* [**dst-entry** *dst-entry-id*] [**overwrite**]

Context **[Tree]** (config>filter>copy ip-filter)

Full Context configure filter copy ip-filter

Description This command copies an existing filter entry for a specific filter ID to another filter ID. The command is a configuration level maintenance tool used to create new entries using an existing filter policy. If **overwrite** is not specified, an error will occur if the destination filter entry exists.

Parameters *src-filter-id* — Identifies the source filter policy from which the copy command will attempt to copy. The filter policy must exist within the context of the preceding keyword (**ip-filter**).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dst-filter-id — Identifies the destination filter policy to which the copy command will attempt to copy. If the **overwrite** keyword is not specified, the filter entry ID cannot already exist in the destination filter policy. If the **overwrite** keyword is present, the destination entry ID may or may not exist.

overwrite — Specifies that the destination filter entry may exist. If it does, everything in the existing destination filter entry will be completely overwritten with the contents of the source filter entry. If the destination filter entry exists, either **overwrite** must be specified or an error message will be returned. If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms All

13.223 ip-filter-max-size

ip-filter-max-size

Syntax **ip-filter-max-size** {*value* | **default**}

Context **[Tree]** (config>service>vprn>flowspec ip-filter-max-size)

Full Context configure service vprn flowspec ip-filter-max-size

Description This command configures the maximum number of FlowSpec routes or rules that can be embedded into an ingress IP filter policy for a specified routing instance. FlowSpec filter entries embedded in a filter policy in this routing instance will use filter entries from the range between the embedding offset and “offset + ip-filter-max-size – 1”.

The sum of the **ip-filter-max-size** *value* parameter and the highest offset in any IPv4 filter that embeds IPv4 FlowSpec rules from this routing instance (excluding filters that embed at offset 262143) must not exceed 262143.

The **ip-filter-max-size** configuration can be adjusted up or down at any time. If the number of IPv4 FlowSpec rules that are currently installed is *M*, and the new limit is *N*, where *N*<*M*, then the last set of rules from *N* to *M* (by FlowSpec order) are immediately removed, but are retained in the BGP RIB. If the limit is increased, new rules are programmed only as they are received again in new BGP updates.

Default ip-filter-max-size default

Parameters *value* — The maximum number of FlowSpec routes or rules that can be embedded into an ingress IP filter policy.

Values 0 to 262143

default — Configures the maximum size as 512.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-filter-max-size

Syntax **ip-filter-max-size** {*value* | **default**}

Context **[Tree]** (config>router>flowspec ip-filter-max-size)

Full Context configure router flowspec ip-filter-max-size

Description This command configures the maximum number of FlowSpec routes or rules that can be embedded into the auto-created embedded filter (fSpec-*X*). FlowSpec filter entries embedded in a filter policy in this routing instance will use filter entries from the range between “embedding offset + 1” and “embedding offset + ip-filter-max-size”.

The sum of the **ip-filter-max-size** *value* parameter and the highest offset in any IPv4 filter that embeds IPv4 FlowSpec rules from this routing instance (excluding filters that embed at offset 262143) must not exceed 262143.

The **ip-filter-max-size** configuration can be adjusted up or down at any time. If the number of IPv4 FlowSpec rules that are currently installed is *M*, and the new limit is *N*, where *N*<*M*, then the last set of rules from *N* to *M* (by FlowSpec order) are immediately removed, but are retained in the BGP RIB. If the limit is increased, new rules are programmed only as they are received again in new BGP updates.

Default ip-filter-max-size 512

Parameters *value* — Specifies the maximum number of FlowSpec routes or rules that can be embedded into an ingress IP filter policy.

Values 0 to 262143

default — Keyword to configure the maximum size as 512.

Platforms All

13.224 ip-filter-name

ip-filter-name

Syntax [**no**] **ip-filter-name** *filter-name*

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block ip-filter-name)

Full Context configure li li-filter-block-reservation li-reserved-block ip-filter-name

Description This command configures an IP filter in which the reservation is done through name.

The **no** form of this command removes the IP filter name.

Parameters *filter-name* — Specifies the IP filter name, up to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

ip-filter-name

Syntax [**no**] **ip-filter-name** *filter-name*

Context **[Tree]** (config>li>li-filter-assoc>li-ip-fltr ip-filter-name)

Full Context configure li li-filter-associations li-ip-filter ip-filter-name

Description This command associates an IP filter with a specified LI IP filter through its name.

The **no** form of this command removes the IP filter name.

Parameters *filter-name* — Specifies the IP filter name, up to 64 characters.

Platforms All

13.225 ip-fragmentation

ip-fragmentation

Syntax **ip-fragmentation** {**disabled** | **fragment-ipv6** | **fragment-ipv6-unless-ipv4-df-set**}
no ip-fragmentation

Context **[Tree]** (config>router>nat>inside>dslite>address ip-fragmentation)
[Tree] (config>router>nat>inside>nat64 ip-fragmentation)
[Tree] (config>service>vprn>nat>inside>nat64 ip-fragmentation)
[Tree] (config>service>vprn>nat>inside>dslite>addressip-fragmentation ip-fragmentation)

Full Context configure router nat inside dual-stack-lite address ip-fragmentation
configure router nat inside nat64 ip-fragmentation
configure service vprn nat inside dslite addressip-fragmentation ip-fragmentation
configure service vprn nat inside nat64 ip-fragmentation

Description This command configures downstream IPv6 fragmentation behavior in DS-Lite and NAT64. IPv6 fragmentation is performed in the ISA. IPv4 fragmentation is not affected by this command. If desired, downstream IPv4 packet can be fragmented in the carrier IOM before the packet reaches ISA (and the NAT function). The IPv4 fragmentation in the downstream direction can be set by the **config>router/vprn>nat>outside>mtu** command.

DS-Lite IPv6 Fragmentation in Downstream Direction (IPv4 to IPv6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In case that the length of the received IPv4 packet is larger than the configured tunnel-mtu value while fragmentation is allowed, the resulting IPv6 packet will be fragmented (IPv4 is tunneled within IPv6). The maximum size of the of the fragmented IPv6 packet will be 48bytes larger than the configured tunnel-mtu value. This is due to the size of the tunneling IPv6 header: 40bytes basic IPv6 header + 8 bytes of extended fragmentation IPv6 header.

In case that fragmentation is not allowed while the IPv4 packet size is larger than configured tunnel-mtu size, the IPv4 packet will be dropped and an ICMPv4 Datagram Too Big message will be generated towards the source. The advertised mtu size in that ICMP message will be set to configured tunnel-mtu value.

NAT64 IPv6 Fragmentation in Downstream Direction (IPv4to IPv6)

In contrast to DS-Lite, NAT64 transport is not based on tunneling. Instead, IP headers are translated between IPv4 and IPv6. Consequently, NAT64 fragmentation operates based on the ipv6-mtu, as opposed to tunnel-mtu in DS-Lite which represents the size of the tunnel payload (IPv4 packet).

In case that the length of the translated IPv6 packet exceeds the size of the configured ipv6-mtu value while fragmentation is allowed, the resulting IPv6 packet will be fragmented. The maximum size of the of the fragmented IPv6 packet will be the configured ipv6-mtu value.

In case that fragmentation is not allowed while the translated IPv6 packet size is larger than configured ipv6-mtu size, the IPv4 packet (that is supposed to be translated into IPv6) will be dropped and an ICMPv4 Datagram Too Big message will be generated towards the source. The advertised mtu size in that ICMP message will be set to the ipv6-mtu value minus 28bytes. The 28bytes comes from the size of the IPv6 overhead of the translated packet (20bytes difference between the IP header sizes ? 40bytes in IPv6 vs 20bytes in IPv4; 8 bytes for extended IPv6 fragmentation header).

Default disabled

Parameters **disabled** — IPv6 Fragmentation is disabled. In case that the packet size is larger than what is set by the mtu value (tunnel-mtu or ipv6-mtu) the IPv4 packet will be dropped and ICPMv4 Datagram Too Big messages will be sent back to the source.

fragment-ipv6 — IPv6 fragmentation will be performed in all cases, regardless of the DF bit setting in the tunneled/translated IPv4 packet.

fragment-ipv6-unless-ipv4-df-set — IPv6 Fragmentation will be performed only in cases when DF bit in tunneled/translated IPv4 packet is cleared.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.226 ip-helper-address

ip-helper-address

Syntax **ip-helper-address** *gateway-address*
no ip-helper-address

Context **[Tree]** (config>service>ies>if ip-helper-address)

Full Context configure service ies interface ip-helper-address

Description This command enables broadcast UDP packets received on the associated interface to be redirected to the specified gateway address and then forwarded on to the gateway.

The **no** form of this command removes the gateway address from the interface configuration and stops the UDP broadcast redirect function.

Parameters *gateway-address* — Specifies the IPv4 address of the target UDP broadcast gateway.

Platforms All

ip-helper-address

Syntax **ip-helper-address** *gateway-address*
no ip-helper-address

Context **[Tree]** (config>service>vprn>if ip-helper-address)

Full Context configure service vprn interface ip-helper-address

Description This command enables broadcast UDP packets received on the associated interface to be redirected to the specified gateway address and then forwarded on to the gateway.

The **no** form of this command removes the gateway address from the interface configuration and stops the UDP broadcast redirect function.

Parameters *gateway-address* — Specifies the IPv4 address of the target UDP broadcast gateway.

Platforms All

ip-helper-address

Syntax **ip-helper-address** *gateway-address*
no ip-helper-address

Context **[Tree]** (config>router>if ip-helper-address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface ip-helper-address

Description This command enables broadcast UDP packets received on the associated interface to be redirected to the specified gateway address and then forwarded on to the gateway.

The **no** form of this command removes the gateway address from the interface configuration and stops the UDP broadcast redirect function.

Parameters *gateway-address* — Specifies the IPv4 address of the target UDP broadcast gateway.

Platforms All

13.227 ip-mirror

ip-mirror

Syntax **ip-mirror**

Context **[Tree]** (config>mirror>mirror-dest>sap>egress ip-mirror)

Full Context configure mirror mirror-dest sap egress ip-mirror

Description This command configures IP mirror information.

Platforms All

13.228 ip-mirror-interface

ip-mirror-interface

Syntax **ip-mirror-interface** *ip-int-name* [**create**]
no ip-mirror-interface *ip-int-name*

Context **[Tree]** (config>service>vprn ip-mirror-interface)

Full Context configure service vprn ip-mirror-interface

Description This command is used for remote mirroring, where the mirror source is a separate system then the mirror destination. The mirror source can only be of IP type and is only supported for the following services: IES, VPRN, VPLS and Ipipe. The mirror destination on a remote system will configure an interface on a VPRN as **ip-mirror-interface**. This interface only supports spoke sdp termination. The IP mirror interface requires PBR to determine the next outgoing interface for the mirror packet to be delivered to.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the interface name from the configuration.

Parameters *ip-int-name* — Specifies the name of the IP interface, up to 32 characters. An interface name cannot be in the form of an IP address.

create — Keyword used to create an IP mirror interface.

Platforms All

13.229 ip-mtu

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>service>ies>sub-if>grp-if ip-mtu)
[Tree] (config>service>vprn>sub-if>grp-if ip-mtu)

Full Context configure service ies subscriber-interface group-interface ip-mtu
configure service vprn subscriber-interface group-interface ip-mtu

Description This command specifies the maximum size of IP packets on this group interface. Packets larger than this are fragmented.

The **ip-mtu** applies to all IPoE host types (dhcp, arp, static). For PPP/L2TP sessions, the **ip-mtu** is not considered for the MTU negotiation. The **ppp-mtu** in the **ppp-policy** should be used instead.

The **no** form of this command reverts to the default.

Parameters *octets* — Specifies the largest frame size (in octets) that this interface can handle.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>service>vprn>if ip-mtu)

Full Context configure service vprn interface ip-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the maximum size of IP packets on this group interface. Packets larger than this are fragmented.

The **ip-mtu** applies to all IPoE host types (DHCP, ARP, or static). For PPP/L2TP sessions, the **ip-mtu** is not considered for the MTU negotiation. The **ppp-mtu** in the PPP policy should be used instead.

The **no** form of this command reverts to the default.

Default no ip-mtu

Parameters *octets* — Specifies the largest frame size (in octets) that this interface can handle.

Values 512 to 9000

Platforms All

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>service>ies>if ip-mtu)
[Tree] (config>service>ies>if>sap>ip-tunnel ip-mtu)

Full Context configure service ies interface ip-mtu
configure service ies interface sap ip-tunnel ip-mtu

Description This command configures the IP maximum transmit unit (packet) for this interface.

Because this connects a Layer 2 to a Layer 3 service, this parameter can be adjusted under the IES interface.

The MTU that is advertised from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

By default (for Ethernet network interface) if no ip-mtu is configured it is (1568 - 14) = 1554.

The **no** form of this command returns the default value.

Default no ip-mtu

Parameters *octets* — Specifies the maximum number of octets that can be transmitted.

Values 512 to 9786 (for IES interface)
512 to 9000 (for ip-tunnel interface)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ip-tunnel ip-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service ies interface ip-mtu

ip-mtu

Syntax **ip-mtu** *bytes*
no ip-mtu

Context **[Tree]** (config>router>if>ipsec>ipsec-tunnel ip-mtu)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel ip-mtu)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel ip-mtu)
[Tree] (config>service>vprn>if>sap>ip-tunnel ip-mtu)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel ip-mtu)

Full Context configure router interface ipsec ipsec-tunnel ip-mtu
configure service ies interface ipsec ipsec-tunnel ip-mtu
configure service vprn interface ipsec ipsec-tunnel ip-mtu
configure service vprn interface sap ip-tunnel ip-mtu
configure service vprn interface sap ipsec-tunnel ip-mtu

Description This command configures the IP maximum transmit unit (packet) for this interface.

Because this connects a Layer 2 to a Layer 3 service, this parameter can be adjusted under the IES interface.

The MTU that is advertised from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

By default (for the Ethernet network interface), if no ip-mtu is configured it is (1568 - 14) equals 1554.

The **ip-mtu** command instructs the MS-ISA to perform IP packet fragmentation, prior to IPsec encryption and encapsulation, based on the configured MTU value. In particular:

If the length of a payload IP packet (including its header) exceeds the configured MTU value and the DF flag is clear (due to the presence of the clear-df-bit command or because the original DF value was 0) then the MS-ISA fragments the payload packet as efficiently as possible (i.e. it creates the minimum number of fragments each less than or equal to the configured MTU size); in each created fragment the DF bit shall be 0.

If the length of a payload IP packet (including its header) exceeds the configured MTU value and the DF flag is set (because the original DF value was 1 and the tunnel has no clear-df-bit in its configuration) then the MS-ISA discards the payload packet without sending an ICMP type 3/code 4 message back to the packet’s source address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The effective MTU for packets entering a tunnel is the minimum of the private tunnel SAP interface IP MTU value (used by the IOM) and the tunnel IP MTU value (configured using the above command and used by the MS-ISA). To fragment IP packets larger than X bytes with DF set, rather than discarding them, the tunnel IP MTU should be set to X and the private tunnel SAP interface IP MTU should be set to a value larger than X.

The **no ip-mtu** command, corresponding to the default behavior, disables fragmentation of IP packets by the MS-ISA; all IP packets, regardless of size or DF bit setting, are allowed into the tunnel.

Default no ip-mtu

Parameters *bytes* — Specifies the IP maximum transmit unit (packet) for this interface.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel ip-mtu
- configure service vprn interface sap ip-tunnel ip-mtu

VSR

- configure service ies interface ipsec ipsec-tunnel ip-mtu
- configure service vprn interface ipsec ipsec-tunnel ip-mtu
- configure router interface ipsec ipsec-tunnel ip-mtu

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>service>ies>subscriber-interface ip-mtu)
[Tree] (config>service>vprn>subscriber-interface ip-mtu)

Full Context configure service ies subscriber-interface ip-mtu
configure service vprn subscriber-interface ip-mtu

Description This command specifies the maximum size of frames on this group-interface. Packets larger than this will get fragmented.

The **no** form of this command removes this functionality.

Parameters *octets.* — Specifies the largest frame size (in octets) that this interface can handle.

Values 512 to 9000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>subscr-mgmt>git ip-mtu)

Full Context configure subscriber-mgmt group-interface-template ip-mtu

Description This command configures the maximum size of outgoing IP packets on this group interface. Packets larger than this are fragmented.

The **no** form of this command removes the configuration.

Default no ip-mtu

Parameters *octets* — Specifies the largest frame size (in octets) that this interface can handle.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>service>ies>aarp-interface ip-mtu)

Full Context configure service ies aarp-interface ip-mtu

Description This command configures the IP maximum transmit unit (packet) for this interface.

The **no** form of this command returns the default value.

Default no ip-mtu

By default (for Ethernet network interface) if no ip-mtu is configured it is (1568 - 14) = 1554.

Parameters *octets* — Specifies the maximum number of octets that can be transmitted.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>red-if ip-mtu)

Full Context configure service ies redundant-interface ip-mtu

Description This command configures the IP maximum transmit unit (packet) for the associated router IP interface.

The configured IP-MTU cannot be larger than the calculated IP MTU based on the port MTU configuration.

The MTU that is advertised from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

The **no** form of this command returns the associated IP interfaces MTU to its default value, which is calculated based on the port MTU setting. For Ethernet ports this will typically be 1554.

Default no ip-mtu

Parameters *octets* — Specifies the octets.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*
no up-mtu

Context [Tree] (config>service>vprn>aarp-interface ip-mtu)

Full Context configure service vprn aarp-interface ip-mtu

Description This command configures the IP maximum transmit unit (packet) for this interface.

The **no** form of this command returns the default value. By default (for Ethernet network interface) if no ip-mtu is configured it is (1568 - 14) = 1554.

Default no ip-mtu

Parameters *octets* — Specifies the maximum number of octets that can be transmitted.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ip-mtu

Context [Tree] (config>service>vprn>nw-if ip-mtu)
[Tree] (config>service>vprn>red-if ip-mtu)

Full Context configure service vprn network-interface ip-mtu
configure service vprn redundant-interface ip-mtu

Description This command configures the IP maximum transmit unit (packet) for the associated router IP interface.

The configured IP-MTU cannot be larger than the calculated IP MTU based on the port MTU configuration.

The MTU that is advertised from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

The **no** form of this command returns the associated IP interfaces MTU to its default value, which is calculated based on the port MTU setting. For Ethernet ports this will typically be 1554.

Default no ip-mtu

Parameters *octets* — Specifies the octets.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface ip-mtu

All

- configure service vprn network-interface ip-mtu

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context [Tree] (config>service>ies>aa-interface ip-mtu)
[Tree] (config>service>vprn>aa-interface ip-mtu)

Full Context configure service ies aa-interface ip-mtu
configure service vprn aa-interface ip-mtu

Description This command configures the AA interface IP MTU.

Default no ip-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *octets* — Specifies the MTU value.

Values 512 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (config>ipsec>tnl-temp ip-mtu)

Full Context configure ipsec tunnel-template ip-mtu

Description This command configures the template IP MTU.

Default no ip-mtu

Parameters *octets* — Specifies the maximum size in octets.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *bytes*

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy ip-mtu)

Full Context configure isa nat-group inter-chassis-redundancy ip-mtu

Description This command configures the IP-MTU size that is used to transport flow synchronization records between the ISAs. Multiple flow synchronization events can be packed into a single frame up to the IP-MTU size.

Default ip-mtu 1500

Parameters *bytes* — Specifies the IP-MTU size in bytes.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>router>if ip-mtu)

Full Context configure router interface ip-mtu

Description This command configures the IP maximum transmit unit (packet) for the associated router IP interface.

The operational IP MTU that is used for the interface is determined based on both the configured IP MTU and the port MTU of the port bound to this interface.

The MTU that is used is:

MINIMUM((Port_MTU - EthernetHeaderSize), (configured ip-mtu))

The **no** form of this command returns the associated IP interfaces MTU to its default value, which is calculated based on the port MTU setting. (For Ethernet ports the default IP MTU is 1500 octets.)

Default no ip-mtu

Parameters *octets* — Specifies the IP MTU value associated with the IP interface, specified in octets. If the interface supports IPv6 packets, the IP-MTU must be set to a value greater than or equal to (≥) 1280 in accordance with RFC 2460 *Internet Protocol, Version 6 (IPv6) Specification*.

Values 512 to 9786

Platforms All

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context **[Tree]** (bof ip-mtu)

Full Context bof ip-mtu

Description This command configures the IP maximum transmit unit (packet) for the management router instance.

The operational IP MTU that is used for the interface is determined based on both the configured IP MTU and the port MTU of the port bound to this interface.

The MTU that is used is:

MINIMUM((Port_MTU - EthernetHeaderSize), (configured ip-mtu))

For the management port, the port MTU is fixed at 1514 and the EthernetHeaderSize is 14 so the first element of the equation above is 1500 octets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the associated IP interfaces MTU to its default value, which is calculated based on the port MTU setting. (For the management port the default IP MTU is 1500 octets.)

Default ip-mtu 1500

Parameters *octets* — Specifies the IP MTU value associated with the IP interface, specified in octets. If the interface supports IPv6 packets, the IP-MTU must be set to a value greater than or equal to (≥) 1280 in accordance with RFC 2460 *Internet Protocol, Version 6 (IPv6) Specification*.

Values 512 to 9786

Platforms All

13.230 ip-option

ip-option

Syntax **ip-option** *ip-option-value* [*ip-option-mask*]
no ip-option

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match ip-option)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match ip-option)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match ip-option
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match ip-option

Description This command configures the IP option match condition.

The **no** form of this command reverts to the default.

Parameters *ip-option-value* — Specifies the IP option value as a decimal hex or binary.

Values 0 to 255

ip-option-mask — Specifies the IP option mask as a decimal hex or binary.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip-option

Syntax **ip-option** *ip-option-value* [*ip-option-mask*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ip-option

Context [Tree] (config>filter>ip-filter>entry>match ip-option)

Full Context configure filter ip-filter entry match ip-option

Description This command configures matching packets with a specific IP option or a range of IP options in the first option of the IP header as an IP filter match criterion.

The option-type octet contains 3 fields:

- 1 bit copied flag (copy options in all fragments)
- 2 bits option class
- 5 bits option number

The **no** form of the command removes the match criterion.

Default no ip-option

Parameters *ip-option-value* — Specifies the 8 bit option-type as a decimal integer, binary, or hexadecimal format. The mask is applied as an AND to the option byte, the result is compared with the option-value.

The decimal value entered for the match should be a combined value of the eight bit option type field and not just the option number. Therefore, to match on IP packets that contain the Router Alert option (option number = 20), enter the option type of 148 (10010100).

Values 0 to 255

ip-option-mask — Specifies an optional parameter that can be used when specifying a range of option numbers to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Table 67 **ip-option-mask Formats**

Format Style	Format Syntax	Example
Decimal	DDD	20
Hexadecimal	0xHH	0x14
Binary	0bBBBBBBBB	0b0010100

Default 255 (decimal) (exact match)

Values 1 to 255 (decimal)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-option

Syntax **ip-option** *ip-option-value ip-option-mask*
no ip-option

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match ip-option)

Full Context configure system security cpm-filter ip-filter entry match ip-option

Description This command configures matching packets with a specific IP option or a range of IP options in the IP header as an IP filter match criterion.

The option-type octet contains 3 fields:

- 1 bit copied flag (copy options in all fragments)
- 2 bits option class
- 5 bits option number

The **no** form of this command removes the match criterion.

Default no ip-option

Parameters *ip-option-value* — Enter the 8 bit option-type as a decimal integer. The mask is applied as an AND to the option byte, the result is compared with the option-value.

The decimal value entered for the match should be a combined value of the eight bit option type field and not just the option number. Thus to match on IP packets that contain the Router Alert option (option number =20), enter the option type of 148 (10010100).

Values 0 **to** 255

ip-option-mask — Specifies a range of option numbers to use as the match criteria.

This 8 bit mask can be configured using the formats described in Table 68:

Table 68 **ip-option-mask Formats**

Format Style	Format Syntax	Example
Decimal	DDD	20
Hexadecimal	0xHH	0x14
Binary	0bBBBBBBBB	0b0010100

Default 255 (decimal) (exact match)

Values 1 to 255 (decimal)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.231 ip-prefix

ip-prefix

Syntax **ip-prefix** *ip-prefix/ip-prefix-length*
no ip-prefix

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident ip-prefix)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification ip-prefix

Description This command specifies the source IPv4/IPv6 address/prefix of the data trigger packet as the host identification.

Note: This command is only used when **ip** is configured as one of the **match-list** parameters.

The **no** form of this command removes the IP prefix from the configuration.

Parameters *ip-prefix/ip-prefix-length* — Specifies the IPv4 address, IPv6 address, or IPv6 prefix.

Values	ipv4-prefix	a.b.c.d
	ipv4-prefix-length	0 to 32
	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x to [0 to FFFF]H d to [0 to 255]D
	ipv6-prefix-length	0 to 128

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ip-prefix

Syntax **ip-prefix** *ipv6-prefixIprefix-length*
no ip-prefix

Context **[Tree]** (conf>router>segment-routing>srv6>loc>prefix ip-prefix)

Full Context configure router segment-routing segment-routing-v6 locator prefix ip-prefix

Description This command configures the IPv6 prefix and prefix length for an SRv6 locator.

The locator prefix length is the sum of the lengths of the block field and that of the node ID field.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the IPv6 prefix from this locator.

Default no ip-prefix

Parameters *ipv6-prefix/prefix-length* — Specifies an IPv6 address prefix written as hexadecimalnumbers separated by colons with host bits set to 0.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
ipv6-prefix-length	4 to 96

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

13.232 ip-prefix-list

ip-prefix-list

Syntax **ip-prefix-list** *ip-prefix-list-name* [**create**]
no ip-prefix-list *ip-prefix-list-name*

Context **[Tree]** (config>app-assure>group ip-prefix-list)

Full Context configure application-assurance group ip-prefix-list

Description This command configures an IP prefix list.

Parameters *ip-prefix-list-name* — Specifies the name of the IP prefix list, up to 32 characters.

create — Mandatory keyword used when creating an application profile. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ip-prefix-list

Syntax **ip-prefix-list** *ip-prefix-list-name* [**create**]
no ip-prefix-list *ip-prefix-list-name*

Context **[Tree]** (config>qos>match-list ip-prefix-list)

Full Context configure qos match-list ip-prefix-list

Description This command creates a list of IPv4 prefixes for match criteria in QoS policies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An IP prefix list must contain only IPv4 address prefixes created using the prefix command and cannot be deleted if it is referenced by a QoS policy.

The **no** form of this command deletes the specified list.

Parameters *ip-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The name **default** (case insensitive) is reserved by the system.

Platforms All

ip-prefix-list

Syntax **ip-prefix-list** *ip-prefix-list-name* [**create**]
no ip-prefix-list *ip-prefix-list-name*

Context **[Tree]** (config>filter>match-list ip-prefix-list)

Full Context configure filter match-list ip-prefix-list

Description This command creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

The **no** form of this command deletes the specified list.

Operational Notes:

An **ip-prefix-list** must contain only IPv4 address prefixes.

An IPv4 prefix match list cannot be deleted if it is referenced by a filter policy.

See general description related to match-list usage in filter policies.

Parameters *ip-prefix-list-name* — Specifies a string of up to 32 printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

13.233 ip-prefix-routes

ip-prefix-routes

Syntax **ip-prefix-routes**

Context **[Tree]** (config>service>system>bgp-evpn ip-prefix-routes)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service system bgp-evpn ip-prefix-routes

Description Commands in this context configure attribute uniform propagation and BGP path selection.

Platforms All

13.234 ip-protocol-num

ip-protocol-num

Syntax **ip-protocol-num** {**eq** | **neq**} *protocol-id*
no ip-protocol-num

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry ip-protocol-num)
[Tree] (config>app-assure>group>policy>aqp>entry>match ip-protocol-num)

Full Context configure application-assurance group policy app-filter entry ip-protocol-num
configure application-assurance group policy app-qos-policy entry match ip-protocol-num

Description This command configures the IP protocol to use in the application definition.

The **no** form of this command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).

Default no ip-protocol-num

Parameters **eq** — Specifies that the value configured and the value in the flow must be equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-id — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17).

The **no** form the command removes the protocol from the match criteria.

Values 1 to 255 (Decimal, Hexadecimal, or Binary representation).

Supported IANA IP protocol names:

none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp, tcp, udp, vrrp

* - udp/tcp wildcard

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-protocol-num

Syntax **ip-protocol-num** *ip-protocol number*
no ip-protocol-num

Context **[Tree]** (config>app-assure>group>policy>sess-fltr>entry>match ip-protocol-num)

Full Context configure application-assurance group policy session-filter entry match ip-protocol-num

Description This command configures the IP protocol to use in the application definition.

The **no** form of this command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).

Default no ip-protocol-num

Parameters *ip-protocol-number* — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17).

The **no** form the command removes the protocol from the match criteria.

Values *protocol-number*: 0 to 255 (decimal, hexadecimal, or binary representation)

protocol-name: Supported IANA IP protocol names:

none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, sctp, stp, tcp, udp, vrrp

* - udp/tcp wildcard

ip-protocol-num

Syntax **ip-protocol-num** {**eq** | **neq**} *protocol-id*
no ip-protocol-num

Context **[Tree]** (debug>app-assure>group>traffic-capture>match ip-protocol-num)

Full Context debug application-assurance group traffic-capture match ip-protocol-num

Description This command configures debugging on an IP protocol number.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.235 ip-route-advertisement

ip-route-advertisement

Syntax **ip-route-advertisement** [**incl-host**] [**domain-id** *global-field*:*local-field*]
no ip-route-advertisement

Context **[Tree]** (config>service>vpls>bgp-evpn ip-route-advertisement)

Full Context configure service vpls bgp-evpn ip-route-advertisement

Description This command enables and disables the advertisement of IP prefixes in EVPN. If enabled, any active route in the R-VPLS VPRN route table are advertised in EVPN using the VPLS BGP configuration. The interface host addresses are not advertised in EVPN unless the **ip-route-advertisement incl-host** command is enabled.

The **no** form of this command disables IP prefixes advertisement in EVPN.

Default no ip-route-advertisement

Parameters **incl-host** — Specifies to advertise the interface host addresses in EVPN.

global-field:local-field — Specifies the domain ID.

Values

4byte-GlobalAdminValue:2byte-LocalAdminValue

4byte-GlobalAdminValue:	0 to 4294967295
2byte-LocalAdminValue	0 to 65535

Platforms All

13.236 ip-src

ip-src

Syntax **ip-src** *ip-address*
no ip-src

Context **[Tree]** (config>li>mirror-dest-template>layer-3-encap ip-src)

Full Context configure li mirror-dest-template layer-3-encap ip-src

Description This command configures the source IPv4 address to use in the IPv4 header part of the routable LI encapsulation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the source IPv4 address.

Values a.b.c.d

Platforms All

13.237 ip-ttl

ip-ttl

Syntax **ip-ttl** *hops*
no ip-ttl

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile ip-ttl)

Full Context configure subscriber-mgmt gtp peer-profile ip-ttl

Description This command configures the value to put in the IP header's TTL field for GTP control messages.

The **no** form of this command reverts to the default value.

Default ip-ttl 255

Parameters *hops* — Specifies the IP TTL.

Values 1 to 255

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.238 ip-tunnel

ip-tunnel

Syntax **ip-tunnel** *name* [**create**]
no ip-tunnel *name*

Context **[Tree]** (config>service>ies>if>sap ip-tunnel)
[Tree] (config>service>vprn>if>sap ip-tunnel)

Full Context configure service ies interface sap ip-tunnel
configure service vprn interface sap ip-tunnel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to configure an IP-GRE or IP-IP tunnel and associate it with a private tunnel SAP within an IES or VPRN service.

The **no** form of this command deletes the specified IP/GRE or IP-IP tunnel from the configuration. The tunnel must be administratively shutdown before issuing the **no ip-tunnel** command.

Default no-ip tunnel *name*

Parameters *name* — Specifies the name of the IP tunnel. Tunnel names can be from 1 to 32 alphanumeric characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

Platforms All

ip-tunnel

Syntax **ip-tunnel**

Context **[Tree]** (config>router>if ip-tunnel)

Full Context configure router interface ip-tunnel

Description Commands in this context configure parameters for an IP tunnel on a **control-channel** loopback interface. The default encapsulation is IP/GRE. The local end tunnel IP address will be configured using the interface primary IP address.

The **ip-tunnel** command can only be configured on **control-channel** loopback interfaces.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.239 ipcp

ipcp

Syntax **ipcp**

Context **[Tree]** (config>service>ies>if ipcp)

Full Context configure service ies interface ipcp

Description This command enables access to the IPCP context within the interface configuration. Within this context, IPCP extensions can be configured to define such things as the remote IP address and DNS IP address to be signaled via IPCP on the associated PPP interface. This command is only applicable if the associated SAP or port is a PPP or MLPPP interface.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipcp

Syntax **ipcp**

Context **[Tree]** (config>service>vprn>if ipcp)

Full Context configure service vprn interface ipcp

Description This command creates allows access to the IPCP context within the interface configuration. Within this context, IPCP extensions can be configured to define such things as the remote IP address and DNS IP address to be signaled via IPCP on the associated PPP interface.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface.

Platforms All

13.240 ipcp-subnet-negotiation

ipcp-subnet-negotiation

Syntax **no ipcp-subnet-negotiation**

Context **[Tree]** (config>router>l2tp>group>ppp ipcp-subnet-negotiation)
[Tree] (config>router>l2tp>group>tunnel>ppp ipcp-subnet-negotiation)
[Tree] (config>service>vprn>l2tp>group>ppp ipcp-subnet-negotiation)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp ipcp-subnet-negotiation)

Full Context configure router l2tp group ppp ipcp-subnet-negotiation
configure router l2tp group tunnel ppp ipcp-subnet-negotiation
configure service vprn l2tp group ppp ipcp-subnet-negotiation
configure service vprn l2tp group tunnel ppp ipcp-subnet-negotiation

Description This command configures the IPCP subnet negotiation using PPP IPCP Subnet-Mask option (0x90) if requested by the client. The subnet can be obtained from RADIUS (Framed-IP-Netmask attribute) or local user database. The subnet is installed as a managed route of the PPP session. This requires the anti-spoof type on the SAP to be configured to nh-mac.

By default, an IPCP Config Request with IPCP Subnet-Mask option (0x90) is rejected.

The **no** form of this command reverts to the default value.

Default no ipcp-subnet-negotiation

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipcp-subnet-negotiation

Syntax [**no**] **ipcp-subnet-negotiation**

Context **[Tree]** (config>subscr-mgmt>ppp-policy ipcp-subnet-negotiation)

Full Context configure subscriber-mgmt ppp-policy ipcp-subnet-negotiation

Description This command enables subnet negotiation using PPP IPCP Subnet-Mask option (0x90) if requested by the client. The subnet can be obtained from RADIUS (Framed-IP-Netmask attribute) or local user database. The subnet is installed as a managed route of the PPP session. This requires the anti-spoof type on the SAP to be configured to nh-mac.

By default, an IPCP Config Request with IPCP Subnet-Mask option (0x90) is rejected.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.241 ipfix

ipfix

Syntax **ipfix**

Context **[Tree]** (config>service ipfix)

Full Context configure service ipfix

Description Commands in this context configure IPFIX parameters.

Platforms All

13.242 ipfix-export-policy

ipfix-export-policy

Syntax **ipfix-export-policy** *policy-name*
no ipfix-export-policy

Context **[Tree]** (config>service>nat>nat-policy ipfix-export-policy)
[Tree] (config>service>nat>up-nat-policy ipfix-export-policy)

Full Context configure service nat nat-policy ipfix-export-policy
configure service nat up-nat-policy ipfix-export-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the IP flow information export policy.

The **no** form of the command removes the IP flow information export policy.

Default no ipfix-export-policy

Parameters *policy-name* — Specifies the name of the policy, up to 32 characters. The specified policy must be created in the **config**>**service**>**ipfix ipfix-export-policy** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipfix-export-policy

Syntax **ipfix-export-policy** *policy-name* [**create**]
no ipfix-export-policy *policy-name*

Context **[Tree]** (config>service>ipfix ipfix-export-policy)

Full Context configure service ipfix ipfix-export-policy

Description This command creates an IPFIX export policy with a set of transport parameters that will be used to transmit IPFIX records generated by an application within 7750 SR node to an external collector node. This policy name can be referenced from each application within 7750 SR that requires flow logging.

Default none

Parameters *policy-name* — Specifies the name of the policy that can be referenced within an application in 7750 SR node that requires flow logging.

create — Keyword used to create the policy.

Platforms All

13.243 ipipe

ipipe

Syntax **ipipe** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**vc-switching**] [**name** *name*]
no ipipe *service-id*

Context **[Tree]** (config>service ipipe)

Full Context configure service ipipe

Description This command configures an IP-Pipe service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7450 ESS or 7750 SR on which this service is defined.

Values *service-id*: 1 to 2147483647

svc-name: up to 64 characters

customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

Values 1 to 2147483647

Default null (0)

vc-switching — Specifies if the pseudowire switching signaling is used for the spoke SDPs configured in this service.

create — Keyword used to create the Ipipe service instance. The **create** keyword requirement can be enabled/disabled in the **environment**>**create** context.

name *name* — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Values *name*: up to 64 characters

Platforms All

13.244 ipoe

ipoe

Syntax **ipoe**

Context **[Tree]** (config>subscr-mgmt>loc-user-db ipoe)

Full Context configure subscriber-mgmt local-user-db ipoe

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure IPoE host parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipoe

Syntax **ipoe**

Context **[Tree]** (debug>call-trace ipoe)

Full Context debug call-trace ipoe

Description Commands in this context set up call trace debugging for IP over Ethernet (IPoE) sessions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipoe

Syntax **ipoe** *origin*

Context **[Tree]** (config>li>x-interfaces>correlation-id ipoe)

Full Context configure li x-interfaces correlation-id ipoe

Description This command specifies the type of RADIUS accounting session ID to use for IPoE subscriber correlation.

Default host

Parameters *origin* — Specifies the correlation identifier origin type for IPoE.

Values host, queue, session

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ipoe

Syntax **ipoe** *max-nr-of-sessions*
no ipoe

Context **[Tree]** (config>subscr-mgmt>sla-profile>session-limits ipoe)
[Tree] (config>subscr-mgmt>sub-profile>session-limits ipoe)

Full Context configure subscriber-mgmt sla-profile session-limits ipoe
configure subscriber-mgmt sub-profile session-limits ipoe

Description This command configures the maximum number of IPoE sessions per SLA profile instance or per subscriber.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the maximum number of IPoE sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of IPoE sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.245 ipoe-bridged-mode

ipoe-bridged-mode

Syntax [**no**] **ipoe-bridged-mode**

Context **[Tree]** (config>service>ies>sub-if>ipv6 ipoe-bridged-mode)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 ipoe-bridged-mode)
[Tree] (config>service>vprn>sub-if>ipv6 ipoe-bridged-mode)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 ipoe-bridged-mode)

Full Context configure service ies subscriber-interface group-interface ipv6 ipoe-bridged-mode
configure service ies subscriber-interface ipv6 ipoe-bridged-mode
configure service vprn subscriber-interface group-interface ipv6 ipoe-bridged-mode
configure service vprn subscriber-interface ipv6 ipoe-bridged-mode

Description This command enables IPv6 IPoE bridged mode.

The **no** form of this command disables the IPv6 IPoE bridged mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.246 ipoe-linking

ipoe-linking

Syntax **ipoe-linking**

Context **[Tree]** (config>service>ies>sub-if ipoe-linking)
[Tree] (config>service>vprn>sub-if ipoe-linking)
[Tree] (config>service>ies>sub-if>grp-if ipoe-linking)
[Tree] (config>service>vprn>sub-if>grp-if ipoe-linking)

Full Context configure service ies subscriber-interface group-interface ipoe-linking
configure service ies subscriber-interface ipoe-linking
configure service vprn subscriber-interface group-interface ipoe-linking

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface ipoe-linking

Description Commands in this context configure IPoE host linking.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.247 ipoe-session

ipoe-session

Syntax [**no**] **ipoe-session**

Context **[Tree]** (config>service>vpls>sap ipoe-session)
[Tree] (config>service>ies>sub-if>grp-if ipoe-session)
[Tree] (config>service>vprn>sub-if>grp-if ipoe-session)
[Tree] (config>service>ies>sub-if ipoe-session)
[Tree] (config>service>vprn>sub-if ipoe-session)

Full Context configure service ies subscriber-interface group-interface ipoe-session
configure service ies subscriber-interface ipoe-session
configure service vpls sap ipoe-session
configure service vprn subscriber-interface group-interface ipoe-session
configure service vprn subscriber-interface ipoe-session

Description Commands in this context configure IPoE session parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.248 ipoe-session-policy

ipoe-session-policy

Syntax **ipoe-session-policy** *policy-name* [**create**]
no ipoe-session-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt ipoe-session-policy)

Full Context configure subscriber-mgmt ipoe-session-policy

Description This command configures an IPoE session policy. The policies are referenced from subscriber interfaces, group interfaces and capture SAPs. Multiple IPoE session policies can be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the IPoE policy name up to 32 characters.

create — Keyword required to create the configuration context

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipoe-session-policy

Syntax **ipoe-session-policy** *policy-name*
no ipoe-session-policy

Context **[Tree]** (config>service>vpls>sap>ipoe-session ipoe-session-policy)
[Tree] (config>service>ies>sub-if>grp-if>ipoe-session ipoe-session-policy)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session ipoe-session-policy)

Full Context configure service ies subscriber-interface group-interface ipoe-session ipoe-session-policy
configure service vpls sap ipoe-session ipoe-session-policy
configure service vprn subscriber-interface group-interface ipoe-session ipoe-session-policy

Description This command specifies the IPoE session policy applicable for this group interface or capture SAP.

On WLAN GW group interfaces, it is not possible to change this value.

The **no** form of this command reverts to the default.

Default no ipoe-session-policy ipoe-session-policy default on WLAN GW group interfaces

Parameters *policy-name* — Specifies the IPoE session policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.249 ipoe-sub-id-key

ipoe-sub-id-key

Syntax **ipoe-sub-id-key** *sub-id-key* [*sub-id-key*]
no ipoe-sub-id-key

Context **[Tree]** (config>subscr-mgmt>auto-sub-id-key ipoe-sub-id-key)

Full Context configure subscriber-mgmt auto-sub-id-key ipoe-sub-id-key

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables certain fields to become the base for auto-generation of the default sub-id name. The sub-id name is auto generated if there is not a more specific method available. Such more specific methods would be a default sub-id name as a sap-id, a preconfigured static string or explicit mappings based on RADIUS/LUDB returned strings.

In case that a more specific sub-id name generation method is not available and the auto-id keyword is defined under the def-sub-id hierarchy, the sub-id name is generated by concatenating fields defined in this command separated by a "|" character.

The maximum *sub-id* name length is 32 characters while the concatenation of subscriber identification fields can easily exceed 32 characters. Subscriber host instantiation fails if the *sub-id* name is based on subscriber identification fields whose concatenated length exceeds 32 characters. Failing the host creation rather than truncating *sub-id* name on a 32 character boundary prevents collision of sub-ids (subscriber name duplication).

If the more specific *sub-id* name generation method is not available and the **auto-id** keyword is not defined under the **def-sub-id** hierarchy, the *sub-id* name is a random 10 character encoded string based on the fields defined under this command.

There is only one set of identification fields allowed per host type (IPoE or PPP) per chassis.

The **no** form of this command reverts to the default.

Default ipoe-sub-id-key mac sap-id

Parameters *sub-id-key* — Specifies the auto-generated sub-id keys for IPoE hosts.

Values **mac** — Specifies that the MAC address can be combined with other subscriber host identification fields (circuit-id, remote-id, session-id, sap-id, or service-name) to form a sub-id name in a user readable format or as a random 10 character encoded value.

In case that the mac address is used as a concatenation field in the sub-id name, then its format becomes a string xx:xx:xx:xx:xx:xx with the length 17B.

The MAC address as the subscriber host identification field is not applicable to static hosts.

circuit-id — Specifies that the circuit-id can be combined with other subscriber host identification fields (mac, remote-id, session-id, sap-id, or service-name) to form a sub-id name in a user readable format or as a random 10 character encoded value.

In case that the circuit-id is used as a concatenation field in the sub-id name, then its format becomes access-node-id eth slot/port:[vlan-id] or access-node-id atm slot/port:vpi.vci with a variable length.

Note: If circuit-id contains any non-printable ASCII characters, the entire circuit-id string is formatted in hex in the sub-id name output. Otherwise all characters in circuit-id is converted to ASCII. ASCII printable characters contain bytes in range 0x20 to 0x7E.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The circuit-id as the subscriber identification field is not applicable to ARP hosts or static hosts.

remote-id — Specifies that the remote-id can be combined with other subscriber host identification fields (mac, circuit-id, session-id, sap-id, or service-name) to form a sub-id name in a user readable format or as a random 10 character encoded value.

In case that the remote-id is used as a concatenation field in the sub-id name, then its format becomes a remote-id string with a variable length.

Note: If remote-id contains any non-printable ASCII characters, the entire remote-id string is formatted in hex in the sub-id name output. Otherwise all characters in remote-id is converted to ASCII. ASCII printable characters contain bytes in range 0x20 to 0x7E.

The remote-id as the subscriber identification field is not applicable to ARP hosts or static hosts.

sap-id — Specifies that the sap-id can be combined with other subscriber host identification fields (mac, circuit-id, remote-id, session-id, or service-name) to form a sub-id name in a user readable format or as a random 10 character encoded value.

If a circuit-id is used as a concatenation field in the sub-id name, then its format becomes: slot/mda:[outer-vlan].[inner-vlan] with a variable length.

The sap-id as the subscriber identification field is applicable to all hosts types with exception of static hosts.

dual-stack-remote-id — Specifies that the dual stack remote ID is used as the base for the auto-generated subscriber identification

service-name — Specifies that the service name that terminates the subscriber is used as the base for auto-generated subscriber identification.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.250 ipsec

ipsec

Syntax **ipsec**

Context **[Tree]** (admin ipsec)

Full Context admin ipsec

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context perform Internet Protocol Security (IPsec) operations. IPsec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipsec

Syntax [**no**] **ipsec**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync ipsec)

Full Context configure redundancy multi-chassis peer sync ipsec

Description This command enables multi-chassis synchronization of IPsec states on system level.

Default no ipsec

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipsec

Syntax **ipsec**

Context **[Tree]** (config ipsec)

Full Context configure ipsec

Description Commands in this context configure Internet Protocol Security (IPsec) parameters. IPsec is a structure of open standards to ensure private, secure communications over Internet Protocol (IP) networks by using cryptographic security services.

Platforms All

ipsec

Syntax **ipsec** [**tunnel-group** *ipsec-group-id*] [**public-sap** *public-sap*]
no ipsec

Context **[Tree]** (config>service>ies ipsec)
[Tree] (config>service>ies>if ipsec)
[Tree] (config>service>vprn ipsec)
[Tree] (config>router>if ipsec)

Full Context configure router interface ipsec
configure service ies interface ipsec
configure service ies ipsec

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ipsec

Description Commands in this context configure IPsec policies on a VSR.

Parameters *ipsec-group-id* — Specifies the IPsec group ID used for the IPsec tunnels configured under this context.

Values 1 to 16

public-sap — Specifies the public SAP ID used for the IPsec tunnels configured under this context.

Values 0 to 4096

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec

VSR

- configure router interface ipsec
- configure service ies interface ipsec

13.251 ipsec-auth

ipsec-auth

Syntax **ipsec-auth**

Context **[Tree]** (config>test-oam>build-packet>header ipsec-auth)
[Tree] (debug>oam>build-packet>packet>field-override>header ipsec-auth)

Full Context configure test-oam build-packet header ipsec-auth
debug oam build-packet packet field-override header ipsec-auth

Description This command causes the associated header to be defined as an IPsec header template and enters the context to define the IPsec parameters. This same context can be used for IPv4 and IPv6 packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.252 ipsec-gw

ipsec-gw

Syntax **ipsec-gw** *name*
no ipsec-gw

Context **[Tree]** (config>service>ies>if>sap ipsec-gw)
[Tree] (config>service>vprn>if>sap ipsec-gw)

Full Context configure service ies interface sap ipsec-gw
configure service vprn interface sap ipsec-gw

Description This command configures an IPsec gateway.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.253 ipsec-lifetime

ipsec-lifetime

Syntax **ipsec-lifetime** *ipsec-lifetime*
no ipsec-lifetime

Context **[Tree]** (config>ipsec>ike-policy ipsec-lifetime)

Full Context configure ipsec ike-policy ipsec-lifetime

Description This command specifies the lifetime of the Phase 2 IKE key.

The **no** form of this command reverts to the default, which is 3600 seconds.

Default no ipsec-lifetime

Parameters *ipsec-lifetime* — Specifies the Phase 2 lifetime for this IKE policy in seconds.

Values 1200 to 31536000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipsec-lifetime

Syntax **ipsec-lifetime** *seconds*
ipsec-lifetime inherit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>ipsec-transform ipsec-lifetime)

Full Context configure ipsec ipsec-transform ipsec-lifetime

Description This command specifies the CHILD_SA. If the **inherit** parameter is specified, then the system uses the IPsec lifetime configuration in the corresponding IKE policy configured in the same IPsec gateway or IPsec tunnel.

Default ipsec-lifetime inherit

Parameters *seconds* — Specifies the lifetime of the Phase 2 IKE key in seconds.

Values 1200 to 31536000

inherit — Specifies that the system uses the **ipsec-lifetime** configuration in the corresponding IKE policy that is configured for the same IPsec gateway or IPsec tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.254 ipsec-responder-only

ipsec-responder-only

Syntax [**no**] **ipsec-responder-only**

Context [Tree] (config>isa>tunnel-group ipsec-responder-only)

Full Context configure isa tunnel-group ipsec-responder-only

Description With this command configured, system will only act as IKE responder except for the automatic CHILD_SA re-key upon MC-IPsec switchover.

Default no ipsec-responder-only

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.255 ipsec-transform

ipsec-transform

Syntax **ipsec-transform** *transform-id* [**create**]
no ipsec-transform *transform-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec ipsec-transform)

Full Context configure ipsec ipsec-transform

Description Commands in this context create an **ipsec-transform** policy. IPsec transforms policies can be shared. A change to the ipsec-transform is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

IPsec transform policy assignments to a tunnel require the tunnel to be shutdown.

The **no** form of this command removes the ID from the configuration.

Parameters *transform-id* — Specifies a policy ID value to identify the IPsec transform policy.

Values 1 to 2048

create — This keyword is mandatory when creating an ipsec-transform policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.256 ipsec-transport-mode-profile

ipsec-transport-mode-profile

Syntax **ipsec-transport-mode-profile** *name* [**create**]
no ipsec-transport-mode-profile *name*

Context [Tree] (config>ipsec ipsec-transport-mode-profile)

Full Context configure ipsec ipsec-transport-mode-profile

Description Commands in this context configure an IPsec transport mode profile.

The **no** form of this command removes the name from the configuration.

Parameters *name* — Specifies the name of the IPsec transport mode profile, up to 32 characters.

create — Keyword used to create the IPsec transport mode profile instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipsec-transport-mode-profile

Syntax **ipsec-transport-mode-profile** *name*
no ipsec-transport-mode-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>ip-tunnel ipsec-transport-mode-profile)
[Tree] (config>service>vprn>if>sap>ip-tunnel ipsec-transport-mode-profile)

Full Context configure service ies interface sap ip-tunnel ipsec-transport-mode-profile
configure service vprn interface sap ip-tunnel ipsec-transport-mode-profile

Description This command specifies an IPsec transport mode profile name to the SAP.

The **no** form of this command removes the profile name from the service configuration.

Parameters *name* — Specifies the name of an existing IPsec transport mode profile, up to 32 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.257 ipsec-tunnel

ipsec-tunnel

Syntax **ipsec-tunnel** *ipsec-tunnel-name*
no ipsec-tunnel [*ipsec-tunnel-name*]

Context [Tree] (config>service>vprn>static-route-entry ipsec-tunnel)

Full Context configure service vprn static-route-entry ipsec-tunnel

Description This command creates a static route in a VPRN service context that points to the global routing context (base router). This is primarily used to allow traffic that ingress through a VPRN service to be routed out of the global routing context.

This **next-hop** type cannot be used in conjunction with any other next-hop types.

Default no ipsec-tunnel

Parameters *ipsec-tunnel-name* — IPsec tunnel name; maximum length up to 32 characters.

Platforms All

ipsec-tunnel

Syntax **ipsec-tunnel** *name* [**private-sap** [*0..4094*]] [**private-service-name** *private-service-name*] [**create**]
no ipsec-tunnel *ipsec-tunnel-name*

Context [Tree] (config>router>if>ipsec ipsec-tunnel)
[Tree] (config>service>ies>if>ipsec ipsec-tunnel)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>sap ipsec-tunnel)

Full Context configure router interface ipsec ipsec-tunnel
configure service ies interface ipsec ipsec-tunnel
configure service vprn interface sap ipsec-tunnel

Description This command configures a secured interfrace IPsec tunnel. If the **private-service-name** is not specified, the private service is the secured interface service.

The **no** form of this command removes the IPsec tunnel from the configuration.

Parameters *name* — Specifies the name of the IPsec tunnel.

private-sap — Specifies the private SAP ID.

Values 0 to 4094

private-service-name — Specifies the private service name.

create — Keyword used to create the IPsec tunnel instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel

VSR

- configure service ies interface ipsec ipsec-tunnel
- configure router interface ipsec ipsec-tunnel

13.258 ipv4

ipv4

Syntax **ipv4**

Context [Tree] (config>subscr-mgmt>git ipv4)

Full Context configure subscriber-mgmt group-interface-template ipv4

Description Commands in this context configure IPv4 parameters.

Default ipv4

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4

Syntax **ipv4**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>to-client-options ipv4)

Full Context configure subscriber-mgmt local-user-db ipoe host to-client-options ipv4

Description Commands in this context configure DHCPv4 options.

Default ipv4

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv4

Syntax **ipv4** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no ipv4

Context **[Tree]** (config>service>vprn>bgp>multi-path ipv4)

Full Context configure service vprn bgp multi-path ipv4

Description This command sets ECMP multipath parameters that apply only to the (unlabeled) IPv4 unicast address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

To qualify as a multipath, a non-best route must meet the following criteria (some criteria are controlled by this command):

- The multi-path route must be the same type of route as the best path (same AFI/SAFI and, in some cases, same next-hop resolution method).
- The multi-path route must be tied with the best path for all criteria of greater significance than next-hop cost, except for criteria that are configured to be ignored.
- If the best path selection reaches the next-hop cost comparison, the multi-path route must have the same next-hop cost as the best route unless the **unequal-cost** option is configured.
- The multi-path route must not have the same BGP next-hop as the best path or any other multi-path route.
- The multi-path route must not cause the ECMP limit of the routing instance to be exceeded (configured using the **ecmp** command with a value in the range 1 to 64).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The multi-path route must not cause the applicable *max-paths* limit to be exceeded. If the best path is an EBGP learned route and the **ebgp** option is used, the *ebgp-max-paths* limit overrides the *max-paths* limit. If the best path is an IBGP-learned route and the **ibgp** option is used, the *ibgp-max-paths* limit overrides the *max-paths* limit. All path limits are configurable up to a maximum of 64. Multi-path is effectively disabled if a value is set to 1.
- The multi-path route must have the same neighbor AS in its AS path as the best path if the **restrict same-neighbor-as** option is configured. By default, any path with the same AS path length as the best path (regardless of neighbor AS) is eligible for multi-path.
- The route must have the same AS path as the best path if the **restrict exact-as-path** option is configured. By default, any path with the same AS path length as the best path (regardless of the actual AS numbers) is eligible for multi-path.

The **no** form of this command removes IPv4-specific overrides.

Default no ipv4

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

egp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path-as — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

ipv4

Syntax **ipv4**

Context **[Tree]** (config>router>ldp>if-params>if ipv4)

Full Context configure router ldp interface-parameters interface ipv4

Description Commands in this context configure LDP interfaces and parameters applied to an IPv4 LDP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

ipv4

Syntax [**no**] **ipv4**

Context **[Tree]** (config>router>ldp>if-params ipv4)

Full Context configure router ldp interface-parameters ipv4

Description Commands in this context configure IPv4 LDP parameters applied to the interface.

Platforms All

ipv4

Syntax **ipv4**

Context **[Tree]** (config>router>ldp>targeted-session ipv4)

Full Context configure router ldp targeted-session ipv4

Description Commands in this context configure parameters applied to targeted sessions to all IPv4 LDP peers.

Platforms All

ipv4

Syntax **ipv4**

Context **[Tree]** (config>router>ldp>targeted-session>auto-tx ipv4)
[Tree] (config>router>ldp>targeted-session>auto-rx ipv4)

Full Context configure router ldp targeted-session auto-rx ipv4
configure router ldp targeted-session auto-tx ipv4

Description Commands in this context configure IPv4 parameters of an automatic targeted LDP session.

Platforms All

ipv4

Syntax **ipv4**

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>lcl-addr-assign ipv4)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign ipv4)

Full Context configure service ies interface sap ipsec-gw local-address-assignment ipv4
configure service vprn interface sap ipsec-gw local-address-assignment ipv4

Description Commands in this context configure IPv4 local address assignment parameters for the IPsec gateway.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipv4

Syntax **ipv4**

Context **[Tree]** (config>test-oam>build-packet>header ipv4)
[Tree] (debug>oam>build-packet>packet>field-override>header ipv4)

Full Context configure test-oam build-packet header ipv4
debug oam build-packet packet field-override header ipv4

Description This command causes the associated header to be defined as an IPv4 header template and enables the context to define the IPv4 parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ipv4

Syntax [**no**] **ipv4**

Context **[Tree]** (config>cflowd>collector>export-filter>family ipv4)

Full Context configure cflowd collector export-filter family ipv4

Description This command filters IPv4 flow data from being sent to the associated collector.

The **no** form of this command removes the filter, allowing IPv4 flow data to be sent to the associated collector.

Default no ipv4

Platforms All

ipv4

Syntax **ipv4**

Context **[Tree]** (config>filter>gre-tun-tmp ipv4)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter gre-tunnel-template ipv4

Description Commands in this context configure GRE tunnel template IPv4 parameters.

Platforms All

ipv4

Syntax **ipv4**

Context **[Tree]** (bof>autoconfigure ipv4)

Full Context bof autoconfigure ipv4

Description Commands in this context autoconfigure the IPv4 DHCP client.

Platforms 7450 ESS-7, 7750 SR-1, 7750 SR-1e, 7750 SR-7, 7750 SR-s

ipv4

Syntax **ipv4** *ip-address*
ipv4 auto-generate [**vendor-id-value** *vendor-id-value*]
no ipv4

Context **[Tree]** (config>system>ned>prof>neip ipv4)

Full Context configure system network-element-discovery profile neip ipv4

Description This command configures the IPv4 NEIP for this profile. The NEIP can be configured manually or set to be automatically generated using the NEID. If the NEID option is set, the first most significant byte of the IPv4 NEIP is set to 140 and the remaining 3 bytes are set to the NEID value. The NEID can be configured with a vendor ID value, in which case the first most significant byte of the IPv4 NEIP is set to this vendor ID value.

The **no** form of this command removes the IPv4 address association for this profile.

Default no ipv4

Parameters *ip-address* — Specifies the IPv4 address of the NEIP.

auto-generate — Specifies that the NEIP is automatically generated using the NEID.

vendor-id-value — Specifies the vendor ID value.

Values 1 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4

Syntax **ipv4 send** *send-limit* **receive** [**none**]
ipv4 send *send-limit*
no ipv4

Context **[Tree]** (config>router>bgp>add-paths ipv4)
[Tree] (config>router>bgp>group>add-paths ipv4)
[Tree] (config>router>bgp>group>neighbor>add-paths ipv4)

Full Context configure router bgp add-paths ipv4
configure router bgp group add-paths ipv4
configure router bgp group neighbor add-paths ipv4

Description This command configures the add-paths capability for unlabeled IPv4 unicast routes. By default, add-paths is not enabled for unlabeled IPv4 unicast routes.

The maximum number of unlabeled unicast paths per IPv4 prefix to send is the configured send limit, which is a mandatory parameter. The capability to receive multiple unlabeled IPv4 unicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command the receive capability is enabled by default.

The **no** form of this command disables add-paths support for unlabeled IPv4 unicast routes, causing sessions established using add-paths for unlabeled IPv4 unicast to go down and come back up without the add-paths capability.

Default no ipv4

Parameters *send-limit* — Specifies the maximum number of paths per unlabeled IPv4 unicast prefix that are allowed to be advertised to add-paths peers, the actual number of advertised routes may be less. If the value is **none**, the router does not negotiate the send capability with respect to IPv4 AFI/SAFI. If the value is **multipaths**, then BGP advertises all of the used BGP multipaths for each IPv4 NLRI if the peer has signaled support to receive multiple add-paths.

Values 1 to 16, none, multipaths

receive — Specifies that the router negotiates to receive multiple unlabeled unicast routes per IPv4 prefix.

none — Specifies that the router does not negotiate to receive multiple unlabeled unicast routes per IPv4 prefix.

Platforms All

ipv4

Syntax **ipv4** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ipv4

Context [Tree] (config>router>bgp>multi-path ipv4)

Full Context configure router bgp multi-path ipv4

Description This command sets ECMP multipath parameters that apply only to the (unlabeled) IPv4 unicast address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

The **no** form of this command removes IPv4-specific overrides.

Default no ipv4

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

ebgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

ipv4

Syntax **ipv4**

Context [Tree] (config>router>if>if-attr>delay>dyn>twamp ipv4)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv4

Description Commands in this context select, enable, and specify the IPv4 addressing used to carry the TWAMP Light test packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.259 ipv4-address

ipv4-address

Syntax **ipv4-address** *ip-address*
no ipv4-address

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query ipv4-address)

Full Context configure subscriber-mgmt wlan-gw ue-query ipv4-address

Description This command enables matching on UEs with the specified IPv4 address.

The **no** form of this command disables matching on the IPv4 address.

Default no ipv4-address

Parameters *ip-address* — Specifies the IPv4 address.

Values a.b.c.d

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.260 ipv4-adjacency-sid

ipv4-adjacency-sid

Syntax **ipv4-adjacency-sid label** *value*
no ipv4-adjacency-sid

Context **[Tree]** (config>router>isis>interface ipv4-adjacency-sid)

Full Context configure router isis interface ipv4-adjacency-sid

Description This command allows a static value to be assigned to an IPv4 adjacency SID in IS-IS segment routing.

The **label** option specifies that the value is assigned to an MPLS label.

The **no** form of this command removes the adjacency SID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the adjacency SID label.

Values 18432 to 5248 | 1048575 (FP4 only)

Platforms All

13.261 ipv4-arp

ipv4-arp

Syntax **ipv4-arp** *max-nr-of-hosts*
no ipv4-arp

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv4-arp)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv4-arp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv4-arp
configure subscriber-mgmt sub-profile host-limits ipv4-arp

Description This command configures the maximum number of IPv4 ARP hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv4 ARP hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv4 ARP hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.262 ipv4-dhcp

ipv4-dhcp

Syntax **ipv4-dhcp** *max-nr-of-hosts*
no ipv4-dhcp

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv4-dhcp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv4-dhcp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv4-dhcp
configure subscriber-mgmt sub-profile host-limits ipv4-dhcp

Description This command limits the number of IPv4 DHCP hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv4 DHCP hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv4 DHCP hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.263 ipv4-mtu

ipv4-mtu

Syntax **ipv4-mtu** *bytes*
no ipv4-mtu

Context [Tree] (config>subscr-mgmt>gtp>peer-profile ipv4-mtu)

Full Context configure subscriber-mgmt gtp peer-profile ipv4-mtu

Description This command configures the value of the IPv4-MTU PCO sent in S11 GTP messages. This is the MTU a device should honor when sending data toward the SGW/PGW. For IPv6, this value is signaled in the RA message and which can be configured in the **grp-if> ipv6>rtr-adv>mtu** context.

The **no** form of this command resets the signaled IPv4 MTU to the default.

Default ipv4-mtu 1400

Parameters *bytes* — Specifies the MTU value in bytes.

Values 512 to 9000

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.264 ipv4-multicast

ipv4-multicast

Syntax [**no**] **ipv4-multicast**

Context **[Tree]** (config>service>vprn>isis>multi-topology ipv4-multicast)

Full Context configure service vprn isis multi-topology ipv4-multicast

Description This command enables support for the IPv4 topology (MT3) within the associate IS-IS instance.

The **no** form of this command disables support for the IPv4 topology (MT3) within the associated IS-IS instance.

Default no ipv4-multicast

Platforms All

ipv4-multicast

Syntax [**no**] **ipv4-multicast**

Context **[Tree]** (config>router>isis>multi-topology ipv4-multicast)

Full Context configure router isis multi-topology ipv4-multicast

Description This command enables support for the IPv4 topology (MT3) within the associate IS-IS instance.

The **no** form of this command disables support for the IPv4 topology (MT3) within the associated IS-IS instance.

Default no ipv4-multicast

Platforms All

13.265 ipv4-multicast-disable

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>service>vpls>pim-snooping ipv4-multicast-disable)

Full Context configure service vpls pim-snooping ipv4-multicast-disable

Description This command disables PIM snooping for IPv4 multicast traffic within a VPLS service.

The **no** form of this command enables PIM snooping for IPv4 multicast traffic within a VPLS service. To fully remove PIM snooping from a VPLS service it is necessary to issue the no pim-snooping command.

Default no ipv4-multicast-disable

Platforms All

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

Context **[Tree]** (config>service>vprn>isis>if ipv4-multicast-disable)

Full Context configure service vprn isis interface ipv4-multicast-disable

Description This command administratively disables/enables ISIS operation for IPv4.

Default no ipv4-multicast-disable

Platforms All

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

Context **[Tree]** (config>service>vprn>pim ipv4-multicast-disable)
[Tree] (config>service>vprn>pim>if ipv4-multicast-disable)

Full Context configure service vprn pim interface ipv4-multicast-disable
configure service vprn pim ipv4-multicast-disable

Description This command administratively disables/enables PIM operation for IPv4.

Default no ipv4-multicast-disable

Platforms All

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>pim ipv4-multicast-disable)
[Tree] (config>router>pim>interface ipv4-multicast-disable)

Full Context configure router pim interface ipv4-multicast-disable
configure router pim ipv4-multicast-disable

Description This command administratively enables PIM operation for IPv4.

IPv4 multicast must be enabled to enable MLDP in-band signaling for IPv4 PIM joins; see **config>router>pim>interface p2mp-ldp-tree-join**.

The **no** form of this command disables the PIM operation for IPv4.

Default no ipv4-multicast-disable

Platforms All

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

Context [Tree] (config>router>isis>interface ipv4-multicast-disable)

Full Context configure router isis interface ipv4-multicast-disable

Description This command disables IS-IS IPv4 multicast routing for the interface.

The **no** form of this command enables IS-IS IPv4 multicast routing for the interface.

Platforms All

13.266 ipv4-multicast-metric

ipv4-multicast-metric

Syntax **ipv4-multicast-metric** *metric*
no ipv4-multicast-metric

Context [Tree] (config>service>vprn>isis>if>level ipv4-multicast-metric)

Full Context configure service vprn isis interface level ipv4-multicast-metric

Description This command configures IS-IS interface metric for IPv4 multicast for the VPRN instance.

The **no** form of this command removes the metric from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — Specifies the IS-IS interface metric for IPv4 multicast.

Values 1 to 16777215

Platforms All

ipv4-multicast-metric

Syntax **ipv4-multicast-metric** *metric*
no ipv4-multicast-metric

Context **[Tree]** (config>router>isis>if>level ipv4-multicast-metric)

Full Context configure router isis interface level ipv4-multicast-metric

Description This command configures the IS-IS interface metric for IPv4 multicast.

The **no** form of this command removes the metric from the configuration.

Parameters *metric* — Specifies the IS-IS interface metric for IPv4 multicast.

Values 1 to 16777215

Platforms All

13.267 ipv4-multicast-metric-offset

ipv4-multicast-metric-offset

Syntax **ipv4-multicast-metric-offset** *offset-value*
no ipv4-multicast-metric-offset

Context **[Tree]** (config>service>vprn>isis>link-group>level ipv4-multicast-metric-offset)

Full Context configure service vprn isis link-group level ipv4-multicast-metric-offset

Description This command sets the offset value for the IPv4 multicast address family. If the number of operational links drops below the oper-members threshold, the configured offset is applied to the interface metric for the IPv4 multicast topology

The **no** form of this command reverts the offset value to 0.

Default no ipv4-multicast-metric-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold.

Values 0 to 6777215

Platforms All

ipv4-multicast-metric-offset

Syntax **ipv4-multicast-metric-offset** *offset-value*
no ipv4-multicast-metric-offset

Context **[Tree]** (config>router>isis>link-group>level ipv4-multicast-metric-offset)

Full Context configure router isis link-group level ipv4-multicast-metric-offset

Description This command sets the offset value for the IPv4 multicast address family. If the number of operational links drops below the oper-members threshold, the configured offset is applied to the interface metric for the IPv4 multicast topology.

The **no** form of this command reverts the offset value to 0.

Default no ipv4-multicast-metric-offset

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold

Values 0 to 6777215

Platforms All

13.268 ipv4-multicast-routing

ipv4-multicast-routing

Syntax **ipv4-multicast-routing** {**native** | **mt**}
[**no**] **ipv4-multicast-routing**

Context **[Tree]** (config>service>vprn>isis ipv4-multicast-routing)

Full Context configure service vprn isis ipv4-multicast-routing

Description The multicast RTM is used for Reverse Path Forwarding checks. This command controls which IS-IS topology is used to populate the IPv4 multicast RTM.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** ipv4-multicast-routing form of this command results in none of the IS-IS routes being populated in the IPv4 multicast RTM and would be used if multicast is configured to use the unicast RTM for the RPF check.

Default ipv4-multicast-routing native

Parameters **native** — Causes IPv4 routes from the MT0 topology to be added to the multicast RTM for RPF checks.

mt — Causes IPv4 routes from the MT3 topology to be added to the multicast RTM for RPF checks.

Platforms All

ipv4-multicast-routing

Syntax **ipv4-multicast-routing** {**native** | **mt**}
[**no**] **ipv4-multicast-routing**

Context **[Tree]** (config>router>isis ipv4-multicast-routing)

Full Context configure router isis ipv4-multicast-routing

Description The multicast RTM is used for Reverse Path Forwarding checks. This command controls which IS-IS topology is used to populate the IPv4 multicast RTM.

The **no** form of this command results in none of the IS-IS routes being populated in the IPv4 multicast RTM and would be used if multicast is configured to use the unicast RTM for the RPF check.

Default ipv4-multicast-routing native

Parameters **native** — Causes IPv4 routes from the MT0 topology to be added to the multicast RTM for RPF checks.

mt — Causes IPv4 routes from the MT3 topology to be added to the multicast RTM for RPF checks.

Platforms All

13.269 ipv4-node-sid

ipv4-node-sid

Syntax **ipv4-node-sid index** *index-value* [**clear-n-flag**]
ipv4-node-sid label *label-value* [**clear-n-flag**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ipv4-node-sid

Context [Tree] (config>router>isis>interface ipv4-node-sid)

Full Context configure router isis interface ipv4-node-sid

Description This command assigns a node SID index or label value to the prefix representing the primary address of an IPv4 network interface of **type loopback**. Only a single node SID can be assigned to an interface. The secondary address of an IPv4 interface cannot be assigned a node SID index and does not inherit the SID of the primary IPv4 address.

The command fails if the network interface is not of **type loopback** or if the interface is defined in an IES or a VPRN context. Also, assigning the same SID index or label value to the same interface in two different IGP instances is not allowed within the same node.

The value of the label or index SID is taken from the range configured for this IGP instance. When using the global mode of operation, a new segment routing module checks that the same index or label value cannot be assigned to more than one loopback interface address. When using the per-instance mode of operation, this check is not required since the index and thus label ranges of the various IGP instance are not allowed to overlap.

The **clear-n-flag** option allows the user to clear the N-flag (node-sid flag) in an IS-IS prefix SID sub-TLV originated for the IPv4 prefix of a loopback interface on the system.

By default, the prefix SID sub-TLV for the prefix of a loopback interface is tagged as a node SID, meaning that it belongs to this node only. However, when the user wants to configure and advertise an anycast SID using the same loopback interface prefix on multiple nodes, you must clear the N-flag to assure interoperability with third party implementations, which may perform a strict check on the receiving end and drop duplicate prefix SID sub-TLVs when the N-flag is set.

The SR OS implementation is relaxed on the receiving end and accepts duplicate prefix SIDs with the N-flag set or cleared. SR OS will resolve to the closest owner, or owners if ECMP is configured, of the prefix SID according to its cost.

Default no ipv4-node-sid

Parameters **index** *index-value* — Specifies the index value.

Values 0 to 4294967295

label *label-value* — Specifies the label value.

Values 0 to 4294967295

clear-n-flag — Clears the node SID flag.

Default no clear-n-flag

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.270 ipv4-overall

ipv4-overall

Syntax **ipv4-overall** *max-nr-of-hosts*
no ipv4-overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv4-overall)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv4-overall)

Full Context configure subscriber-mgmt sla-profile host-limits ipv4-overall
configure subscriber-mgmt sub-profile host-limits ipv4-overall

Description This command configures the maximum number of IPv4 hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv4 hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv4 hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.271 ipv4-ppp

ipv4-ppp

Syntax **ipv4-ppp** *max-nr-of-hosts*
no ipv4-ppp

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv4-ppp)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv4-ppp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv4-ppp
configure subscriber-mgmt sub-profile host-limits ipv4-ppp

Description This command configures the maximum number of IPv4 PPP hosts per SLA profile instance or per subscriber.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the maximum number of IPv4 PPP hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv4 PPP hosts.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.272 ipv4-prefix

ipv4-prefix

Syntax **ipv4-prefix** *ipv4-prefix*
no ipv4-prefix

Context **[Tree]** (config>service>nat>map-domain>mapping-rule ipv4-prefix)

Full Context configure service nat map-domain mapping-rule ipv4-prefix

Description This command configures an IPv4 MAP rule prefix.

Parameters *ipv4-prefix* — Specifies the IPv4 MAP prefix.

Values <*ipv4-prefix*>/<*ipv4-prefix-length*>
<*ipv4-prefix*> : a.b.c.d (host bits must be 0)
<*ipv4-prefix-length*> : [0..32]

Platforms VSR

ipv4-prefix

Syntax [**no**] **ipv4-prefix**

Context **[Tree]** (debug>router>rpki-session>packet ipv4-prefix)

Full Context debug router rpki-session packet ipv4-prefix

Description This command enables debugging for IPv4 prefix RPKI packets.

The **no** form of this command disables debugging for IPv4 prefix RPKI packets.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.273 ipv4-routing

ipv4-routing

Syntax [**no**] **ipv4-routing**

Context **[Tree]** (config>service>vprn>isis ipv4-routing)

Full Context configure service vprn isis ipv4-routing

Description This command specifies whether this IS-IS instance supports IPv4.

The **no** form of this command disables IPv4 on the IS-IS instance.

Default ipv4-routing

Platforms All

ipv4-routing

Syntax [**no**] **ipv4-routing**

Context **[Tree]** (config>router>isis ipv4-routing)

Full Context configure router isis ipv4-routing

Description This command specifies whether this IS-IS instance supports IPv4.

The **no** form of this command disables IPv4 on the IS-IS instance.

Default ipv4-routing

Platforms All

13.274 ipv4-sid

ipv4-sid

Syntax **ipv4-sid index** *index-id*
ipv4-sid label *label-id*
no ipv4-sid

Context **[Tree]** (config>router>segment-routing>sr-mpls>prefix-sids ipv4-sid)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router segment-routing sr-mpls prefix-sids ipv4-sid

Description This command is used to configure the IPv4 segment routing SID associated with the primary IPv4 address of the loopback or system interface.

The **no** form of this command removes the configuration of the IPv4 segment routing SID associated with the primary IPv4 interface address.

Default no ipv4-sid

Parameters **index** *index-id* — Specifies the node SID index for this interface.

Values 0 to 4294967295

label *label-id* — Specifies the label value for the node SID.

Values 32 to 1048575

Platforms All

13.275 ipv4-source-address

ipv4-source-address

Syntax **ipv4-source-address** *ipv4-address*
no ipv4-source-address

Context **[Tree]** (config>service>vprn>dns ipv4-source-address)

Full Context configure service vprn dns ipv4-source-address

Description This command configures the IPv4 address of the default secondary DNS server for the subscribers using this interface. Subscribers that cannot obtain an IPv4 DNS server address by other means, can use this for DNS name resolution.

The ipv4-address value can only be set to a nonzero value if the value of VPRN type is set to **subscriber-split-horizon**.

The **no** form of this command reverts to the default.

Parameters *ipv4-address* — Specifies the IPv4 address of the default secondary DNS server.

Values ipv4-address - a.b.c.d

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-source-address

Syntax **ipv4-source-address** *ip-address*
no ipv4-source-address

Context **[Tree]** (config>system>file-trans-prof ipv4-source-address)

Full Context configure system file-transmission-profile ipv4-source-address

Description This command specifies the IPv4 source address used for transport protocol.

The **no** form of this command uses the default source address which typically is the address of the egress interface.

Default no ipv4-source-address

Parameters *ip-address* — Specifies a unicast v4 address. This should be a local interface address.

Platforms All

ipv4-source-address

Syntax **ipv4-source-address** *ip-address*
no ipv4-source-address

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>collector ipv4-source-address)

Full Context configure service nat syslog syslog-export-policy collector ipv4-source-address

Description This command configures the IPv4 source address from which the UDP streams containing syslog flow records are sourced.

The **no** form of the command removes the IPv4 address from the configuration.

Parameters *ip-address* — Specifies the source IPv4 address from which UDP streams are sent.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.276 ipv4-unicast-metric-offset

ipv4-unicast-metric-offset

Syntax **ipv4-unicast-metric-offset** *offset-value*
no ipv4-unicast-metric-offset

Context **[Tree]** (config>service>vprn>isis>link-group>level ipv4-unicast-metric-offset)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn isis link-group level ipv4-unicast-metric-offset

Description This command sets the offset value for the IPv4 unicast address family. If the number of operational links drops below the oper-members threshold, the configured offset is applied to the interface metric.

The **no** form of this command reverts the offset value to 0.

Default no ipv4-unicast-metric-offset

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold.

Values 0 to 6777215

Platforms All

ipv4-unicast-metric-offset

Syntax **ipv4-unicast-metric-offset** *offset-value*
no ipv4-unicast-metric-offset

Context **[Tree]** (config>router>isis>link-group>level ipv4-unicast-metric-offset)

Full Context configure router isis link-group level ipv4-unicast-metric-offset

Description This command sets the offset value for the IPv4 unicast address family. If the number of operational links drops below the oper-members threshold, the configured offset is applied to the interface metric.

The **no** form of this command reverts the offset value to 0.

Default no ipv4-unicast-metric-offset

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold.

Values 0 to 6777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.277 ipv6

ipv6

Syntax **[no] ipv6**

Context [Tree] (config>service>ies>if ipv6)
[Tree] (config>service>ies>sub-if ipv6)
[Tree] (config>service>ies>sub-if>grp-if ipv6)
[Tree] (config>service>ies>sub-if>lcl-addr-assign ipv6)
[Tree] (config>service>vprn>if ipv6)
[Tree] (config>service>vprn>sub-if ipv6)
[Tree] (config>service>vprn>sub-if>grp-if ipv6)
[Tree] (config>service>vprn>sub-if>lcl-addr-assign ipv6)

Full Context configure service ies interface ipv6
configure service ies subscriber-interface group-interface ipv6
configure service ies subscriber-interface ipv6
configure service ies subscriber-interface local-address-assignment ipv6
configure service vprn interface ipv6
configure service vprn subscriber-interface group-interface ipv6
configure service vprn subscriber-interface ipv6
configure service vprn subscriber-interface local-address-assignment ipv6

Description Commands in this context configure IPv6 parameters for the interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface ipv6
- configure service vprn subscriber-interface ipv6
- configure service ies subscriber-interface ipv6
- configure service vprn subscriber-interface local-address-assignment ipv6
- configure service ies subscriber-interface group-interface ipv6
- configure service ies subscriber-interface local-address-assignment ipv6

All

- configure service ies interface ipv6
- configure service vprn interface ipv6

ipv6

Syntax **ipv6** *ipv6-filter-id*
no ipv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>template>epipe-sap-template>egress>filter ipv6)
[Tree] (config>service>template>epipe-sap-template>ingress>filter ipv6)

Full Context configure service template epipe-sap-template egress filter ipv6
configure service template epipe-sap-template ingress filter ipv6

Description This command associates an existing IPv6 filter policy with the template.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

Parameters *ipv6-filter-id* — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipv6

Syntax **ipv6** *name*
no ipv6

Context [Tree] (config>service>template>epipe-sap-template>egress>filter-name ipv6)
[Tree] (config>service>template>epipe-sap-template>ingress>filter-name ipv6)

Full Context configure service template epipe-sap-template egress filter-name ipv6
configure service template epipe-sap-template ingress filter-name ipv6

Description This command associates an existing IP filter policy with the template.

Parameters *name* — Specifies the IPv6 filter policy name, up to 64 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipv6

Syntax **ipv6** *name*
no ipv6

Context [Tree] (config>service>template>vpls-sap-template>egress>filter-name ipv6)
[Tree] (config>service>template>vpls-sap-template>ingress>filter-name ipv6)

Full Context configure service template vpls-sap-template egress filter-name ipv6
configure service template vpls-sap-template ingress filter-name ipv6

Description This command associates an existing IP filter policy with the template.

Parameters *name* — Specifies the IPv6 filter policy name, up to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

ipv6

Syntax **ipv6 max-paths** [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no ipv6

Context **[Tree]** (config>service>vprn>bgp>multi-path ipv6)

Full Context configure service vprn bgp multi-path ipv6

Description This command sets ECMP multipath parameters that apply only to the (unlabeled) IPv6 unicast address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

To qualify as a multipath, a non-best route must meet the following criteria (some criteria are controlled by this command):

- The multi-path route must be the same type of route as the best path (same AFI/SAFI and, in some cases, same next-hop resolution method).
- The multi-path route must be tied with the best path for all criteria of greater significance than next-hop cost, except for criteria that are configured to be ignored.
- If the best path selection reaches the next-hop cost comparison, the multi-path route must have the same next-hop cost as the best route unless the **unequal-cost** option is configured.
- The multi-path route must not have the same BGP next-hop as the best path or any other multi-path route.
- The multi-path route must not cause the ECMP limit of the routing instance to be exceeded (configured using the **ecmp** command with a value in the range 1 to 64)
- The multi-path route must not cause the applicable *max-paths* limit to be exceeded. If the best path is an EBGP learned route and the **ebgp** option is used, the *ebgp-max-paths* limit overrides the *max-paths* limit. If the best path is an IBGP-learned route and the **ibgp** option is used, the *ibgp-max-paths* limit overrides the *max-paths* limit. All path limits are configurable up to a maximum of 64. Multi-path is effectively disabled if a value is set to 1.
- The multi-path route must have the same neighbor AS in its AS path as the best path if the **restrict same-neighbor-as** option is configured. By default, any path with the same AS path length as the best path (regardless of neighbor AS) is eligible for multi-path.
- The route must have the same AS path as the best path if the **restrict exact-as-path** option is configured. By default, any path with the same AS path length as the best path (regardless of the actual AS numbers) is eligible for multi-path.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes IPv6-specific overrides.

Default no ipv6

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

egp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path-as — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

When enabled, the Alc-App-Prof-Str VSA is ignored in a radius Accept that enables portal redirection using this redirect policy. AA functionality will be disabled during portal authentication.

The **no** version of this command allows an Alc-App-Prof-Str to be present and will enable Application Assurance during portal authentication. In this case redirection rules defined in this policy are bypassed and it is assumed the AA function is configured for portal redirection.

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>to-client-options ipv6)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>to-server-options ipv6)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>to-client-options ipv6)

Full Context configure subscriber-mgmt local-user-db ipoe host to-client-options ipv6
configure subscriber-mgmt local-user-db ipoe host to-server-options ipv6
configure subscriber-mgmt local-user-db ppp host to-client-options ipv6

Description This command enables the context to configure DHCPv6 options.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6

Syntax **ipv6**

Context **[Tree]** (config>subscr-mgmt>isa-filter ipv6)

Full Context configure subscriber-mgmt isa-filter ipv6

Description Commands in this context configure IPv6 parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6

Syntax **ipv6**

Context **[Tree]** (config>service>vprn>mvpn>red-source-list ipv6)

Full Context configure service vprn mvpn red-source-list ipv6

Description This command enables context to configure list of redundant IPv6 source prefixes for preferred source selection.

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (config>service>vprn>pim>rp ipv6)

Full Context configure service vprn pim rp ipv6

Description This command enables access to the context to configure the rendezvous point (RP) of a PIM IPv6 protocol instance.

A Nokia IPv6 PIM router acting as an RP must respond to an IPv6 PIM register message specifying an SSM multicast group address by sending to the first hop router stop register message(s). It does not build an (S, G) shortest path tree toward the first hop router. An SSM multicast group address can be either from the SSM default range or from a multicast group address range that was explicitly configured for SSM.

Default ipv6 RP enabled when IPv6 PIM is enabled.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6

Syntax [**no**] **ipv6**

Context **[Tree]** (config>router>ldp>if-params>if ipv6)

Full Context configure router ldp interface-parameters interface ipv6

Description Commands in this context configure IPv6 LDP parameters applied to the interface.

This command is not supported on the 7450 ESS.

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (config>router>ldp>if-params ipv6)

Full Context configure router ldp interface-parameters ipv6

Description Commands in this context configure LDP interfaces and parameters applied to an IPv6 LDP interface.

This command is not supported on the 7450 ESS.

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (config>router>ldp>targeted-session ipv6)

Full Context configure router ldp targeted-session ipv6

Description Commands in this context configure parameters applied to targeted sessions to all IPv6 LDP peers.

This command is not supported on the 7450 ESS.

Platforms All

ipv6

Syntax **ipv6**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>ipsec-gw>lcl-addr-assign ipv6)
[Tree] (config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign ipv6)

Full Context configure service ies interface sap ipsec-gw local-address-assignment ipv6
configure service vprn interface sap ipsec-gw local-address-assignment ipv6

Description Commands in this context configure IPv6 local address assignment parameters for the IPsec gateway.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipv6

Syntax **ipv6**

Context [Tree] (config>router>pim>rp ipv6)

Full Context configure router pim rp ipv6

Description Commands in this context configure IPv6 parameters.

Platforms All

ipv6

Syntax **ipv6**

Context [Tree] (config>test-oam>build-packet>header ipv6)
[Tree] (debug>oam>build-packet>packet>field-override>header ipv6)

Full Context configure test-oam build-packet header ipv6
debug oam build-packet packet field-override header ipv6

Description This command causes the associated header to be defined as an IPv6 header template and enters the context to define the IPv6 parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ipv6

Syntax [**no**] **ipv6**

Context [Tree] (config>cflowd>collector>export-filter>family ipv6)

Full Context configure cflowd collector export-filter family ipv6

Description This command filters IPv6 flow data from being sent to the associated collector.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the filter, allowing IPv6 flow data to be sent to the associated collector.

Default no ipv6

Platforms All

ipv6

Syntax [**no**] **ipv6** *ipv6-filter-id*

Context **[Tree]** (config>filter>system-filter ipv6)

Full Context configure filter system-filter ipv6

Description This command activates an IPv6 system filter policy. Once activated, all IPv6 ACL filter policies that chain to the system filter (**config>filter>ipv6-filter>chain-to-system-filter**) will automatically execute system filter policy rules first.

The **no** form of the command deactivates the system filter policy.

Parameters *ipv6-filter-id* — Specifies the existing IPv6 filter policy with scope **system**. This parameter can either be expressed as a decimal integer, or as an ASCII string of up to 64 characters in length.

Values 1 to 65535 or the filter policy name

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (config>router ipv6)

Full Context configure router ipv6

Description Commands in this context configure the IPv6 interface of the router.

Default ipv6

Platforms All

ipv6

Syntax [**no**] **ipv6**

Context **[Tree]** (config>router>if ipv6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface ipv6

Description This command configures IPv6 for a router interface.

The **no** form of this command disables IPv6 on the interface.

Default no ipv6

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (bof>autoconfigure ipv6)

Full Context bof autoconfigure ipv6

Description Commands in this context autoconfigure the IPv6 DHCP client.

Platforms 7450 ESS-7, 7750 SR-1, 7750 SR-1e, 7750 SR-7, 7750 SR-s

ipv6

Syntax **ipv6** *ipv6-address*
ipv6 auto-generate [**vendor-id-value** *vendor-id*]
no ipv6

Context **[Tree]** (config>system>ned>prof>neip ipv6)

Full Context configure system network-element-discovery profile neip ipv6

Description This command configures the IPv6 NEIP for this profile. The NEIP can be configured manually or set to be automatically generated. If the NEIP is set to be automatically generated, the NEID is used for the subnet and host portion of the IPv6 address and the vendor ID value is set to 140 by default. The vendor ID value can be configured.

The **no** form of this command removes the IPv6 address association for this profile.

Default no ipv6

Parameters *ipv6-address* — Specifies the IPv6 address of the NEIP.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0..FFFF]H d: [0..255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

auto-generate — Specifies that the NEIP is automatically generated using the NEID.

vendor-id-value — Specifies the vendor ID value.

Values 1 to 255

Platforms All

ipv6

Syntax **ipv6 send** *send-limit* **receive** [**none**]
ipv6 send *send-limit*
no ipv6

Context **[Tree]** (config>router>bgp>add-paths ipv6)
[Tree] (config>router>bgp>group>add-paths ipv6)
[Tree] (config>router>bgp>group>neighbor>add-paths ipv6)

Full Context configure router bgp add-paths ipv6
configure router bgp group add-paths ipv6
configure router bgp group neighbor add-paths ipv6

Description This command configures the add-paths capability for unlabeled IPv6 unicast routes. By default, add-paths is not enabled for unlabeled IPv6 unicast routes.

The maximum number of unlabeled unicast paths per IPv6 prefix to send is the configured send limit, which is a mandatory parameter. The capability to receive multiple unlabeled IPv6 unicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command the receive capability is enabled by default.

The **no** form of this command disables add-paths support for unlabeled IPv6 unicast routes, causing sessions established using add-paths for unlabeled IPv6 unicast to go down and come back up without the add-paths capability.

Default no ipv6

Parameters **send** *send-limit* — Specifies the maximum number of paths per unlabeled IPv6 unicast prefix that are allowed to be advertised to add-paths peers. (The actual number of advertised routes may be less.) If the value is **none**, the router does not negotiate the send capability with respect to IPv6 AFI/SAFI. If the value is **multipaths**, then BGP advertises all the used BGP multipaths for each IPv6 NLRI if the peer has signaled support to receive multiple add-paths.

Values 1 to 16, none, multipaths

receive — Specifies the router negotiates to receive multiple unlabeled unicast routes per IPv6 prefix.

none — Specifies the router does not negotiate to receive multiple unlabeled unicast routes per IPv6 prefix.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

ipv6

Syntax **ipv6** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no ipv6

Context **[Tree]** (config>router>bgp>multi-path ipv6)

Full Context configure router bgp multi-path ipv6

Description This command sets ECMP multipath parameters that apply only to the (unlabeled) IPv6 unicast address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

The **no** form of this command removes IPv6-specific overrides.

Default no ipv6

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

ebgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6

Syntax [**no**] **ipv6**

Context **[Tree]** (config>router>isis>traffic-engineering-options ipv6)

Full Context configure router isis traffic-engineering-options ipv6

Description This command enables the advertisement of IPv6 TE in the IS-IS instance. When this command is enabled, traffic engineering behavior with IPv6 TE links is enabled. This IS-IS instance automatically begins advertising the new RFC 6119 IPv6 and TE TLVs and sub-TLVs.

The **no** form of this command disables IPv6 TE in this ISIS instance.

Default no ipv6

Platforms All

ipv6

Syntax **ipv6**

Context **[Tree]** (config>router>if>if-attr>delay>dyn>twamp ipv6)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv6

Description Commands in this context select, enable, and specify the IPv6 addressing used to carry the TWAMP Light test packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.278 ipv6-address

ipv6-address

Syntax **ipv6-address** *ipv6-address*
no ipv6-address

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-address)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-address)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-address
configure subscriber-mgmt local-user-db ppp host ipv6-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures static DHCPv6 IA-NA address for the host. This address is delegated to the client as /128 via DHCPv6 proxy function within the router. This IP address must not be part of any DHCP pool within internal DHCP server.

The **no** form of this command removes the IPv6 address from the host configuration.

Parameters *ipv6-address* — Specifies the IPv6 address.

Values

ipv6-address: ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0 to FFFF]H
d [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6-address

Syntax **ipv6-address** *ipv6-address*
no ipv6-address

Context **[Tree]** (config>service>vprn>radius-proxy>server>wlan-gw ipv6-address)
[Tree] (config>router>radius-proxy>server>wlan-gw ipv6-address)

Full Context configure router radius-proxy server wlan-gw ipv6-address
configure service vprn radius-proxy server wlan-gw ipv6-address

Description This command configures the IPv6 address of the distributed RADIUS proxy server for use by the access points.

The **no** form of this command removes the address from the configuration.

Parameters *ipv6-address* — Specifies the destination IPv6 address of the RADIUS proxy server.

Values

ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0 to FFFF]H
d [0 to 255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipv6-address

Syntax [**no**] **framed-ipv6-address**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute ipv6-address)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute ipv6-address

Description This command enables the generation of the **ipv6-address** RADIUS attribute.

The **no** form of this command disables the generation of the **ipv6-address** RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6-address

Syntax [**no**] **ipv6-address**

Context [Tree] (config>aaa>isa-radius-plcy>auth-include-attributes ipv6-address)

Full Context configure aaa isa-radius-policy auth-include-attributes ipv6-address

Description This attribute defines if the ipv6 address of the UE is present during authentication if the datatrigger packet is IPv6.

Default no ipv6-address

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ipv6-address

Syntax [**no**] **ipv6-address**

Context [Tree] (config>aaa>isa-radius-plcy>acct-include-attributes ipv6-address)

Full Context configure aaa isa-radius-policy acct-include-attributes ipv6-address

Description If an active IA_NA lease exists, this attribute defines if the IA_NA address of the UE is present in accounting.

Default no ipv6-address

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.279 ipv6-address-prefix-length

ipv6-address-prefix-length

Syntax **ipv6-address-prefix-length** *IPv6-prefix-length*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ipv6-address-prefix-length

Context [Tree] (config>app-assure>group>transit-ip-policy ipv6-address-prefix-length)

Full Context configure application-assurance group transit-ip-policy ipv6-address-prefix-length

Description This command configures a transit IP policy IPv6 address prefix length.

Default no ipv6-address-prefix-length

Parameters *IPv6-prefix-length* — Specifies the prefix length of IPv6 addresses in this policy for both static and dynamic transits.

Values 32 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.280 ipv6-adjacency-sid

ipv6-adjacency-sid

Syntax **ipv6-adjacency-sid label** *value*
no ipv6-adjacency-sid

Context [Tree] (config>router>isis>interface ipv6-adjacency-sid)

Full Context configure router isis interface ipv6-adjacency-sid

Description This command allows a static value to be assigned to an IPv6 adjacency SID in IS-IS segment routing.

The **label** option specifies that the value is assigned to an MPLS label.

The **no** form of this command removes the adjacency SID.

Parameters *value* — Specifies the adjacency SID label.

Values 18432 to 5248, 1048575 (FP4 only)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.281 ipv6-criteria

ipv6-criteria

Syntax [**no**] **ipv6-criteria**

Context **[Tree]** (config>qos>sap-egress ipv6-criteria)
[Tree] (config>qos>sap-ingress ipv6-criteria)

Full Context configure qos sap-egress ipv6-criteria
configure qos sap-ingress ipv6-criteria

Description IPv6 criteria-based SAP egress or ingress policies are used to select the appropriate ingress or egress queue or policer and corresponding forwarding class and packet profile for matched traffic.

This command is used to enter the node to create or edit policy entries that specify IPv6 criteria such as IP quintuple lookup or DiffServ code point.

The OS implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit.

The **no** form of this command deletes all the entries specified under this node. When ipv6-criteria entries are removed from a SAP ingress policy, the ipv6-criteria is removed from all services where that policy is applied.

Platforms All

ipv6-criteria

Syntax [**no**] **ipv6-criteria**

Context **[Tree]** (config>qos>network>ingress ipv6-criteria)
[Tree] (config>qos>network>egress ipv6-criteria)

Full Context configure qos network egress ipv6-criteria
configure qos network ingress ipv6-criteria

Description IPv6 criteria-based network ingress and egress policies are used to select the appropriate ingress or egress queue or policer, and the corresponding forwarding class and packet profile for matched traffic. This command is used to enter the context to create or edit policy entries that specify IPv6 criteria such as IP quintuple lookup or DSCP.

The 7750 SR OS implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. Entries must be sequenced correctly from most to least explicit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The ingress classification only applies to the outer IPv6 header of non-tunneled traffic.

Attempting to apply a network QoS policy containing an **ipv6-criteria** statement to any object except a network IP interface will result in an error.

The **no** form of this command deletes all entries specified under this node. When IP criteria entries are removed from a network policy, the IPv6 criteria are removed from all network interfaces to which that policy is applied.

Platforms All

ipv6-criteria

Syntax [**no**] **ipv6-criteria**

Context **[Tree]** (config>service>apipe>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>cpipe>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>epipe>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>fpipe>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>ies>if>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>ipipe>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>vpls>sap>ingress>criteria-overrides ipv6-criteria)
[Tree] (config>service>vprn>if>sap>ingress>criteria-overrides ipv6-criteria)

Full Context configure service apipe sap ingress criteria-overrides ipv6-criteria
configure service cpipe sap ingress criteria-overrides ipv6-criteria
configure service epipe sap ingress criteria-overrides ipv6-criteria
configure service fpipe sap ingress criteria-overrides ipv6-criteria
configure service ies interface sap ingress criteria-overrides ipv6-criteria
configure service ipipe sap ingress criteria-overrides ipv6-criteria
configure service vpls sap ingress criteria-overrides ipv6-criteria
configure service vprn interface sap ingress criteria-overrides ipv6-criteria

Description Commands in this context configure IPv6 criteria overrides.

The **no** form of this command removes any existing IPv6 overrides from the SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress criteria-overrides ipv6-criteria
- configure service ies interface sap ingress criteria-overrides ipv6-criteria
- configure service fpipe sap ingress criteria-overrides ipv6-criteria
- configure service epipe sap ingress criteria-overrides ipv6-criteria
- configure service vpls sap ingress criteria-overrides ipv6-criteria
- configure service ipipe sap ingress criteria-overrides ipv6-criteria
- configure service vprn interface sap ingress criteria-overrides ipv6-criteria

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe sap ingress criteria-overrides ipv6-criteria

13.282 ipv6-delegated-prefix

ipv6-delegated-prefix

Syntax **ipv6-delegated-prefix** *ipv6-prefix/prefix-length*
no ipv6-delegated-prefix

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-delegated-prefix)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-delegated-prefix)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-delegated-prefix
configure subscriber-mgmt local-user-db ppp host ipv6-delegated-prefix

Description This command configures static DHCPv6 IA-PD prefix for the host. This prefix can be further delegated by the host itself to its clients. The prefix length is restricted to 48 to 64 bits. This prefix must not be part of any DHCP pool within internal DHCP server.

Parameters *ipv6-address* — Specifies the IPv6 address.

Values

ipv6-address:	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x [0 to FFFF]H
		d [0 to 255]D
prefix-length	48 to 64	

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.283 ipv6-delegated-prefix-length

ipv6-delegated-prefix-length

Syntax **ipv6-delegated-prefix-length** *bits*
no ipv6-delegated-prefix-length

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-delegated-prefix-length)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-delegated-prefix-length)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-delegated-prefix-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt local-user-db ppp host ipv6-delegated-prefix-length

Description This command allows configuration of delegated prefix length via local user database.

The **no** form of this command reverts to the default.

Parameters *bits* — Specifies the delegated prefix length, in bits.

Values 48 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.284 ipv6-delegated-prefix-pool

ipv6-delegated-prefix-pool

Syntax **ipv6-delegated-prefix-pool** *pool-name*
no ipv6-delegated-prefix-pool

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-delegated-prefix-pool)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-delegated-prefix-pool)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-delegated-prefix-pool
configure subscriber-mgmt local-user-db ppp host ipv6-delegated-prefix-pool

Description This command configures the pool name that is used in DHCPv6 server for DHCPv6 IA-PD prefix selection.

The **no** form of this command removes the pool name from the configuration.

Parameters *pool-name* — Specifies the pool name, up to 32 characters, to be assigned to the delegated prefix pool.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.285 ipv6-eh

ipv6-eh

Syntax **ipv6-eh** {**max** | **limited**}
no ipv6-eh

Context **[Tree]** (config>system>ip ipv6-eh)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system ip ipv6-eh

Description This command defines the maximum number of IPv6 extension headers parsed in the line cards. The system parses up to six extension headers when **ipv6-eh max** is configured.

When the **ipv6-eh limited** command is configured, the system does not parse IPv6 extension headers and provides consistent ipv6-filter matches for the next-header value found in the IPv6 packet header. LAG and ECMP hashing of IPv6 packets with extension headers is limited to Layer 3 IP addresses. Layer 4 ports, TEID, and SPI values are not available for hashing. MLD snooping on Layer 2 services is also not supported in this mode.

The **no** form of this command reverts to the default value.

Default ipv6-eh max

Parameters **max** — Specifies that the maximum number of IPv6 extension headers is parsed in the line cards.

limited — Specifies that the system does not parse IPv6 extension headers and provides consistent ipv6-filter matches for the next-header value found in the IPv6 packet header.

Platforms All

13.286 ipv6-error

ipv6-error

Syntax [**no**] **ipv6-error**

Context **[Tree]** (debug>router>ip>event ipv6-error)

Full Context debug router ip event ipv6-error

Description This command enables debugging for IPv6 error events.

The **no** form of this command disables debugging for IPv6 error events

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.287 ipv6-exception

ipv6-exception

Syntax **ipv6-exception** *exception*
no ipv6-exception

Context **[Tree]** (config>router>if>ipsec ipv6-exception)
[Tree] (config>service>ies>if>ipsec ipv6-exception)
[Tree] (config>service>vprn>if>ipsec ipv6-exception)

Full Context configure router interface ipsec ipv6-exception
configure service ies interface ipsec ipv6-exception
configure service vprn interface ipsec ipv6-exception

Description This command configures the IPv6 filter exception for an IPsec-secured IPv6 interface. When an IPv6 filter exception is added, clear text packets that match the exception criteria in the IPv6 filter exception policy can ingress the interface, even when IPsec is enabled on that interface.

The **no** form of this command removes the IPv6 filter exception.

Default no ipv6-exception

Parameters *exception* — Specifies the IPv6 filter exception that is used to bypass encryption.

Values *exception-id*: 1 to 65535
exception-name: An existing IPv6 filter exception name up to 64 characters.

Platforms VSR

ipv6-exception

Syntax **ipv6-exception** *exception-id* [**name** *exception-name*] [**create**]
no ipv6-exception {*exception-id* | *exception-name*}

Context **[Tree]** (config>filter ipv6-exception)

Full Context configure filter ipv6-exception

Description Commands in this context configure the specified IPv6 exception filter.

The **no** form of the command deletes the IPv6 exception filter.

Parameters *exception-id* — Specifies the IPv6 filter exception ID expressed as a decimal integer.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name *exception-name* — Specifies the IPv6 filter exception as a name, up to 64 characters.

create — This keyword is required to create the configuration context. Once it is created, the context can be enabled with or without the **create** keyword.

Platforms VSR

13.288 ipv6-filter

ipv6-filter

Syntax **ipv6-filter** *ipv6-filter-id*
no ipv6-filter [**force**]

Context **[Tree]** (config>subscr-mgmt>sla-profile>egress ipv6-filter)
[Tree] (config>subscr-mgmt>sla-profile>ingress ipv6-filter)

Full Context configure subscriber-mgmt sla-profile egress ipv6-filter
configure subscriber-mgmt sla-profile ingress ipv6-filter

Description This command configures an egress or ingress IPv6 filter.

The **no** form of this command reverts to the default.

Parameters *ipv6-filter-id* — Specifies an existing IPv6 filter policy ID.

Values 1 to 65535, or name, up to 64 characters

force — Forces the exclusion of the IPv6 filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6-filter

Syntax **ipv6-filter** *ipv6-filter-id* **entry** *entry-id* [*entry-id*]
no ipv6-filter *ipv6-filter-id* [**entry** *entry-id*]

Context **[Tree]** (config>mirror>mirror-source ipv6-filter)

Full Context configure mirror mirror-source ipv6-filter

Description This command enables mirroring of packets that match specific entries in an existing IPv6 filter.

The **ipv6-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IPv6 filter must already exist in order for the command to execute. Filters are configured in the **config>filter** context. If the IPv6 filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IPv6 interface, an error is not generated but mirroring will not be enabled (there are no packets to mirror). Once the IPv6 filter is defined to a SAP or IPv6 interface, mirroring is enabled.

If the IPv6 filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

If the IPv6 filter is defined as egress, only egress packets are mirrored. Egress mirrored packets are mirrored to the mirror destination after all egress packet modifications.

An *entry-id* within an IPv6 filter can only be mirrored to a single mirror destination. If the same *entry-id* is defined multiple times, an error occurs and only the first **mirror-source** definition is in effect.

By default, no packets matching any IPv6 filters are mirrored. Mirroring of IPv6 filter entries must be explicitly defined.

The **no ipv6-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *ip-filter-id*.

When the **no** form of this command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring that *entry-id* list is terminated within the *ip-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

Parameters *ipv6-filter-id* — Specifies the IPv6 filter ID whose entries are mirrored. If the *ipv6-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *ipv6-filter-id* is defined on a SAP or IPv6 interface.

entry-id — Specifies the IP filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. Multiple *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space.

If an *entry-id* does not exist within the IP filter, an error occurs and the command will not execute.

If the filter's *entry-id* is renumbered within the IP filter definition, the old *entry-id* is removed but the new *entry-id* must be manually added to the configuration to include the new (renumbered) entry's criteria.

Platforms All

ipv6-filter

Syntax [**no**] **ipv6-filter** *ipv6-filter-id*

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block ipv6-filter)

Full Context configure li li-filter-block-reservation li-reserved-block ipv6-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures to which normal IPv6 address filters the entry reservation is applied.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

The **no** form of this command removes the IPv6 filter ID from the configuration.

Parameters *ipv6-filter-id* — Specifies the filter identification identifies the normal IPv6 address filters.

Values {*filter-id* | *filter-name*}

filter-id:	1 to 65535
filter-name:	up to 64 characters (*filter-name* is an alias for input only. The *filter-name* gets replaced with an id automatically by SR OS in the configuration).

Platforms All

ipv6-filter

Syntax [**no**] **ipv6-filter** *ipv6-filter-id*

Context **[Tree]** (config>li>li-fltr-assoc>li-ipv6-fltr ipv6-filter)

Full Context configure li li-filter-associations li-ipv6-filter ipv6-filter

Description This command specifies the IP filter(s) into which the entries from the specified **li-ipv6-filter** are to be inserted. The **li-ipv6-filter** and **ipv6-filter** must already exist before the association is made. If the normal IPv6 filter is deleted then the association is also removed (and not re-created if the IPv6 filter comes into existence in the future).

The **no** form of this command removes the IPv6 filter ID from the configuration.

Parameters *ipv6-filter-id* — Specifies an existing IPv6 filter policy.

Values *filter-id* — 1 to 65535
filter-name — up to 64 characters

Platforms All

ipv6-filter

Syntax **ipv6-filter** *ipv6-filter-id* **entry** *entry-id* [*entry-id*] [**intercept-id** *intercept-id* [*intercept-id*]] [**session-id** *session-id* [*session-id*]]
no ipv6-filter *ipv6-filter-id* [**entry** *entry-id* [*entry-id*]]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>li>li-source ipv6-filter)

Full Context configure li li-source ipv6-filter

Description This command enables lawful interception (LI) of packets that match specific entries in an existing IPv6 filter.

The **ipv6-filter** command directs packets which match the defined list of entry IDs to be intercepted to the destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The IPv6 filter must already exist in order for the command to execute. Filters are configured in the **config>filter** context. If the IPv6 filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IPv6 interface, an error is not generated but mirroring will not be enabled (there are no packets to mirror). Once the IPv6 filter is defined to a SAP, IPv6 interface or subscriber, mirroring is enabled (subscriber mirroring applies only to the 7750 SR).

If the IPv6 filter is defined as ingress, only ingress packets are intercepted. Ingress packets are sent to the destination prior to any ingress packet modifications.

If the IPv6 filter is defined as egress, only egress packets are intercepted. Egress packets are sent to the destination after all egress packet modifications.

An *entry-id* within an IPv6 filter can only be intercepted to a single destination. If the same *entry-id* is defined multiple times, an error occurs and only the first definition is in effect.

By default, no packets matching any IPv6 filters are intercepted. Interception of IPv6 filter entries must be explicitly defined.

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, interception of that list of *entry-id*'s is terminated within the *ipv6-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being intercepted, no error will occur for that *entry-id* and the command will execute normally.

Parameters *ipv6-filter-id* — Specifies the IPv6 filter ID whose entries are to be intercepted. If the *ipv6-filter-id* does not exist, an error will occur and the command will not execute. Intercepting packets will commence when the *ipv6-filter-id* is defined on a SAP or IPv6 interface.

entry-id — Specifies the IPv6 filter entries to use as match criteria for lawful intercept (LI). The **entry** keyword begins a list of *entry-id*'s for interception. Multiple *entry-id* entries can be specified with a single command. Each *entry-id* must be separated by a space. Up to <N><n> 8 entry IDs may be specified in a single command.

If an *entry-id* does not exist within the IPv6 filter, an error occurs and the command will not execute.

If the filter's *entry-id* is renumbered within the IPv6 filter definition, the old *entry-id* is removed but the new *entry-id* must be manually added to the configuration to include the new (renumbered) entry's criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

intercept-id — Specifies the intercept ID that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This intercept ID can be used (for example by a downstream LI Gateway) to identify the particular LI session to which the packet belongs. For all types of **li-source** entries (**filter**, **nat**, **sap**, **subscriber**), when the mirror service is configured with **ip-udp-shim** routable encap, an *intercept-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no intercept ID configured for an **li-source** entry, then the default value will be inserted. When the mirror service is configured with **ip-gre** routable encapsulation, no *intercept-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4294967295 (32b) For nat li-source entries that are using a mirror service that is not configured with routable encap

Values 1t o 1,073,741,824 (30b) For all types of li-source entries that are using a mirror service with routable ip-udp-shim encap and no direction-bit.

Values 1 to 536,870,912 (29b) For all types of li-source entries that are using a mirror service with routable ip-udp-shim encap and with the direction-bit enabled.

session-id — Specifies the *session-id* that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This *session-id* can be used (for example by a downstream LI Gateway) to identify the particular LI session to which the packet belongs. The *session-id* is only valid and used for mirror services that are configured with **ip-udp-shim** routable encap (**config>mirror>mirror-dest>encap>ip-udp-shim**). For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encapsulation, a *session-id* field (as part of the routable encapsulation) is always present in the mirrored packets. If there is no *session-id* configured for an **li-source** entry, then the default value will be inserted. When a mirror service is configured with **ip-gre** routable encap, no *session-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4,294,967,295 (32b)

Platforms All

ipv6-filter

Syntax **ipv6-filter** *filter-id* [**name** *filter-name*] [**create**]
no ipv6-filter {*filter-id* | *filter-name*}

Context **[Tree]** (config>filter ipv6-filter)

Full Context configure filter ipv6-filter

Description Commands in this context configure the specified IPv6 filter policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command deletes the IPv6 filter policy. A filter policy cannot be deleted until it is removed from all objects where it is applied.

Parameters *filter-id* — Specifies the IPv6 filter policy ID expressed as a decimal integer.

Values 1 to 65535

name — Configures an optional filter name, up to 64 characters in length, to a given filter. This filter name can then be used in configuration references, display, and show commands throughout the system. A defined filter name can help the service provider or administrator to identify and manage filters within the SR OS platforms.

To create a filter, you must assign a filter ID, however, after it is created, either the filter ID or filter name can be used to identify and reference a filter.

If a name is not specified at creation time, then SR OS assigns a string version of the *filter-id* as the name.

Filter names may not begin with an integer (0 to 9).

Values *name*: 64 characters maximum

filter-name — Specifies a string of up to 64 characters uniquely identifying this IPv6 filter policy.

create — This keyword is required to create the configuration context. Once it is created, the context can be enabled with or without the **create** keyword.

Platforms All

ipv6-filter

Syntax [**no**] **ipv6-filter**

Context **[Tree]** (config>system>security>mgmt-access-filter ipv6-filter)

Full Context configure system security management-access-filter ipv6-filter

Description Commands in this context configure management access IPv6 filter parameters. This command only applies to the 7750 SR and 7950 XRS.

Platforms All

ipv6-filter

Syntax [**no**] **ipv6-filter**

Context **[Tree]** (config>system>security>cpm-filter ipv6-filter)

Full Context configure system security cpm-filter ipv6-filter

Description Commands in this context configure CPM IPv6 filter parameters. This command applies only to the 7750 SR and 7950 XRS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ipv6-filter

Syntax **ipv6-filter** *src-filter-id* [**src-entry** *src-entry-id*] **to** *dst-filter-id* [**dst-entry** *dst-entry-id*] [**overwrite**]

Context **[Tree]** (config>filter>copy ipv6-filter)

Full Context configure filter copy ipv6-filter

Description This command copies an existing filter entry for a specific filter ID to another filter ID. The command is a configuration level maintenance tool used to create new entries using an existing filter policy. If **overwrite** is not specified, an error will occur if the destination filter entry exists.

Parameters *src-filter-id* — Identifies the source filter policy from which the copy command will attempt to copy. The filter policy must exist within the context of the preceding keyword (**ipv6-filter**).

dst-filter-id — Identifies the destination filter policy to which the copy command will attempt to copy. If the **overwrite** keyword is not specified, the filter entry ID cannot already exist in the destination filter policy. If the **overwrite** keyword is present, the destination entry ID may or may not exist.

overwrite — Specifies that the destination filter entry may exist. If it does, everything in the existing destination filter entry will be completely overwritten with the contents of the source filter entry. If the destination filter entry exists, either **overwrite** must be specified or an error message will be returned. If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms All

13.289 ipv6-filter-max-size

ipv6-filter-max-size

Syntax **ipv6-filter-max-size** {*value* | **default**}

Context **[Tree]** (config>service>vprn>flowspec ipv6-filter-max-size)

Full Context configure service vprn flowspec ipv6-filter-max-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of IPv6 FlowSpec routes or rules that can be embedded into an ingress IPv6 filter policy for a specified routing instance. Flowspec filter entries embedded in a filter policy in this routing instance will use filter entries from the range between the embedding offset and “offset + ip-filter-max-size – 1”.

The sum of the **ip-filter-max-size** *value* parameter and the highest offset in any IPv6 filter that embeds IPv6 FlowSpec rules from this routing instance (excluding filters that embed at offset 262143) must not exceed 262143.

The **ip-filter-max-size** configuration can be adjusted up or down at any time. If the number of IPv6 FlowSpec rules that are currently installed is *M*, and the new limit is *N*, where *N*<*M*, then the last set of rules from *N* to *M* (by FlowSpec order) are immediately removed, but are retained in the BGP RIB. If the limit is increased, new rules are programmed only as they are received again in new BGP updates.

Default ipv6-filter-max-size default

Parameters *value* — The maximum number of FlowSpec routes or rules that can be embedded into an ingress IP filter policy.

Values 0 to 262143

default — Configures the maximum size as 512.

Platforms All

ipv6-filter-max-size

Syntax **ipv6-filter-max-size** {*value* | **default**}

Context **[Tree]** (config>router>flowspec ipv6-filter-max-size)

Full Context configure router flowspec ipv6-filter-max-size

Description This command configures the maximum number of IPv6 FlowSpec routes or rules that can be embedded into the auto-created embedded filter (fSpec-*X*). FlowSpec filter entries embedded in a filter policy in this routing instance will use filter entries from the range between “embedding offset + 1” and “embedding offset + ip-filter-max-size”.

The sum of the **ipv6-filter-max-size** *value* parameter and the highest offset in any IPv6 filter that embeds IPv6 FlowSpec rules from this routing instance (excluding filters that embed at offset 262143) must not exceed 262143.

The **ipv6-filter-max-size** configuration can be adjusted up or down at any time. If the number of IPv6 FlowSpec rules that are currently installed is *M*, and the new limit is *N*, where *N*<*M*, then the last set of rules from *N* to *M* (by FlowSpec order) are immediately removed, but are retained in the BGP RIB. If the limit is increased, new rules are programmed only as they are received again in new BGP updates.

Default ipv6-filter-max-size 512

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the maximum number of FlowSpec routes or rules that can be embedded into an ingress IP filter policy.

Values 0 to 262143

default — Keyword to configure the maximum size as 512.

Platforms All

13.290 ipv6-filter-name

ipv6-filter-name

Syntax [**no**] **ipv6-filter-name** *filter-name*

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block ipv6-filter-name)

Full Context configure li li-filter-block-reservation li-reserved-block ipv6-filter-name

Description This command configures an IPv6 filter in which the reservation is done through name.

The **no** form of this command removes the IPv6 filter name.

Parameters *filter-name* — Specifies the IPv6 filter name, up to 64 characters.

Platforms All

ipv6-filter-name

Syntax [**no**] **ipv6-filter-name** *filter-name*

Context **[Tree]** (config>li>li-fltr-assoc>li-ipv6-fltr ipv6-filter-name)

Full Context configure li li-filter-associations li-ipv6-filter ipv6-filter-name

Description This command associates an IPv6 filter with a specified LI IPv6 filter through its name.

The **no** form of this command removes the IPv6 filter name.

Parameters *filter-name* — Specifies the IPv6 filter name, up to 64 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.291 ipv6-fragment

ipv6-fragment

Syntax **ipv6-fragment**

Context **[Tree]** (config>test-oam>build-packet>header ipv6-fragment)

Full Context configure test-oam build-packet header ipv6-fragment

Description This command causes the associated header to be defined as an IPv6 fragment header template.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

13.292 ipv6-lease-times

ipv6-lease-times

Syntax [**no**] **ipv6-lease-times**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-lease-times)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-lease-times)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-lease-times
configure subscriber-mgmt local-user-db ppp host ipv6-lease-times

Description Commands in this context configure lease times for DHCPv6.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.293 ipv6-mtu

ipv6-mtu

Syntax **ipv6-mtu** *ipv6-mtu*
no ipv6-mtu

Context **[Tree]** (config>service>vprn>nat>inside>nat64 ipv6-mtu)
[Tree] (config>router>nat>inside>nat64 ipv6-mtu)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router nat inside nat64 ipv6-mtu
configure service vprn nat inside nat64 ipv6-mtu

Description This command sets the size of the IPv6 downstream packet in NAT64. This packet is translated from IPv4.

The **no** form of the command reverts to the default.

Default ipv6-mtu 1520

Parameters *ipv6-mtu* — Specifies the IPv6 MTU.

Values 1280 to 9212

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.294 ipv6-multicast

ipv6-multicast

Syntax [**no**] **ipv6-multicast**

Context **[Tree]** (config>router>isis>multi-topology ipv6-multicast)

Full Context configure router isis multi-topology ipv6-multicast

Description This command enables support for the IPv6 topology (MT4) within the associate IS-IS instance.

The **no** form of this command disables support for the IPv6 topology (MT4) within the associated IS-IS instance.

Default no ipv6-multicast

Platforms All

13.295 ipv6-multicast-disable

ipv6-multicast-disable

Syntax [**no**] **ipv6-multicast-disable**

Context **[Tree]** (config>service>vpls>pim-snooping ipv6-multicast-disable)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls pim-snooping ipv6-multicast-disable

Description This command disables PIM snooping for IPv6 multicast traffic within a VPLS service.

The **no** form of this command enables PIM snooping for IPv6 multicast traffic within a VPLS service. To fully remove PIM snooping from a VPLS service it is necessary to issue the no pim-snooping command.

Default ipv6-multicast-disable

Platforms All

ipv6-multicast-disable

Syntax **ipv6-multicast-disable**

Context **[Tree]** (config>service>vprn>pim ipv6-multicast-disable)
[Tree] (config>service>vprn>pim>if ipv6-multicast-disable)

Full Context configure service vprn pim interface ipv6-multicast-disable
configure service vprn pim ipv6-multicast-disable

Description This command administratively disables/enables PIM operation for IPv6.

Default ipv6-multicast-disable (config>service>vprn>pim)

no ipv6-multicast-disable (config>service>vprn>pim>if)

Platforms All

ipv6-multicast-disable

Syntax [**no**] **ipv6-multicast-disable**

Context **[Tree]** (config>router>pim ipv6-multicast-disable)
[Tree] (config>router>pim>interface ipv6-multicast-disable)

Full Context configure router pim interface ipv6-multicast-disable
configure router pim ipv6-multicast-disable

Description This command administratively enables PIM operation for IPv6.

IPv6 multicast must be enabled to enable MLDP in-band signaling for IPv6 PIM joins; see **config>router>pim>interface p2mp-ldp-tree-join**.

The **no** form of this command disables the PIM operation for IPv6.

Default ipv6-multicast-disable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-multicast-disable

Syntax [**no**] **ipv6-multicast-disable**

Context **[Tree]** (config>router>isis>interface ipv6-multicast-disable)

Full Context configure router isis interface ipv6-multicast-disable

Description This command disables IS-IS IPv6 multicast routing for the interface.

The **no** form of this command enables IS-IS IPv6 multicast routing for the interface.

Platforms All

13.296 ipv6-multicast-metric

ipv6-multicast-metric

Syntax **ipv6-multicast-metric** *metric*
no ipv6-multicast-metric

Context **[Tree]** (config>router>isis>if>level ipv6-multicast-metric)

Full Context configure router isis interface level ipv6-multicast-metric

Description This command configures the IS-IS interface metric for IPv6 multicast.

The **no** form of this command removes the metric from the configuration.

Default no ipv6-multicast-metric

Parameters *metric* — Specifies the IS-IS interface metric for IPv6 multicast.

Values 1 to 16777215

Platforms All

13.297 ipv6-multicast-metric-offset

ipv6-multicast-metric-offset

Syntax **ipv6-multicast-metric-offset** *offset-value*
no ipv6-multicast-metric-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis>link-group>level ipv6-multicast-metric-offset)

Full Context configure router isis link-group level ipv6-multicast-metric-offset

Description This command sets the offset value for the IPv6 multicast address family. If the number of operational links drops below the oper-members threshold, the configured offset is applied to the interface metric for the IPv6 multicast topology.

The **no** form of this command reverts the offset value to 0.

Default no ipv6-multicast-metric-offset

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold

Values 0 to 6777215

Platforms All

13.298 ipv6-multicast-routing

ipv6-multicast-routing

Syntax **ipv6-multicast-routing** {**native** | **mt**}
[**no**] **ipv6-multicast-routing**

Context [Tree] (config>router>isis ipv6-multicast-routing)

Full Context configure router isis ipv6-multicast-routing

Description The multicast RTM is used for Reverse Path Forwarding checks. This command controls which IS-IS topology is used to populate the IPv6 multicast RTM.

The **no** form of this command results in none of the IS-IS routes being populated in the IPv4 multicast RTM and would be used if multicast is configured to use the unicast RTM for the RPF check.

Default ipv6-multicast-routing native

Parameters **native** — Causes IPv6 routes from the MT0 topology to be added to the multicast RTM for RPF checks.

mt — Causes IPv6 routes from the MT3 topology to be added to the multicast RTM for RPF checks.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.299 ipv6-node-sid

ipv6-node-sid

Syntax **ipv6-node-sid index** *index-value* [**clear-n-flag**]
ipv6-node-sid label *label-value* [**clear-n-flag**]
no ipv6-node-sid

Context **[Tree]** (config>router>isis>interface ipv6-node-sid)

Full Context configure router isis interface ipv6-node-sid

Description This command assigns a node SID index or label value to the prefix representing the primary address of an IPv6 network interface of type loopback. Only a single node SID can be assigned to an IPv6 interface. When an IPv6 interface has multiple global addresses, the primary address is always the first one in the list, as displayed by the **interface info** command.

The command fails if the network interface is not of loopback type or if the interface is defined in an IES or a VPRN context. Assigning the same SID index/label value to the same interface in two different IGP instances is not allowed within the same node.

The value of the label or index SID is taken from the range configured for this IGP instance. When using the global mode of operation, a new segment routing module checks that the same index or label value cannot be assigned to more than one loopback interface address. When using the per-instance mode of operation, this check is not required since the index and thus label ranges of the various IGP instance are not allowed to overlap.

The **clear-n-flag** option allows the user to clear the N-flag (node-sid flag) in an IS-IS prefix SID sub-TLV originated for the IPv6 prefix of a loopback interface on the system.

By default, the prefix SID sub-TLV for the prefix of a loopback interface is tagged as a node SID, meaning that it belongs to this node only. However, when the user wants to configure and advertise an anycast SID using the same loopback interface prefix on multiple nodes, you must clear the N-flag to assure interoperability with third-party implementations, which may perform a strict check on the receiving end and drop duplicate prefix SID sub-TLVs when the N-flag is set.

The SR OS implementation is relaxed on the receiving end and accepts duplicate prefix SIDs with the N-flag set or cleared. SR OS will resolve to the closest owner, or owners if ECMP is configured, of the prefix SID according to its cost.

Default no ipv6-node-sid

Parameters *index-value* — Specifies the index value.

Values 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

label-value — Specifies the label value.

Values 0 to 4294967295

clear-n-flag — Clears the node SID flag.

Default no clear-n-flag

Platforms All

13.300 ipv6-overall

ipv6-overall

Syntax **ipv6-overall** *max-nr-of-hosts*
no ipv6-overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-overall)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-overall)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-overall
configure subscriber-mgmt sub-profile host-limits ipv6-overall

Description This command configures the maximum number of IPv6 hosts per SLA profile instance or subscriber.

The **no** form of this command removes the maximum number of IPv6 hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.301 ipv6-pd-ipoe-dhcp

ipv6-pd-ipoe-dhcp

Syntax **ipv6-pd-ipoe-dhcp** *max-nr-of-hosts*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ipv6-pd-ipoe-dhcp

Context [Tree] (config>subscr-mgmt>sla-profile>host-limits ipv6-pd-ipoe-dhcp)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-pd-ipoe-dhcp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-pd-ipoe-dhcp
configure subscriber-mgmt sub-profile host-limits ipv6-pd-ipoe-dhcp

Description This command configures the maximum number of IPv6 IPoE DHCP Prefix Delegation hosts (IA-PD) per SLA profile instance or per subscriber.

Note: Prefix delegation hosts that are modeled as a managed route do not count against this limit.

The **no** form of this command removes the maximum number of IPv6 IPoE DHCP Prefix Delegation hosts (IA-PD) limit.

Parameters *max-nr-of-hosts* — Specifies the total number of IPv6 IPoE DHCP Prefix Delegation hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.302 ipv6-pd-overall

ipv6-pd-overall

Syntax **ipv6-pd-overall** max-nr-of-hosts
no ipv6-pd-overall

Context [Tree] (config>subscr-mgmt>sla-profile>host-limits ipv6-pd-overall)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-pd-overall)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-pd-overall
configure subscriber-mgmt sub-profile host-limits ipv6-pd-overall

Description This command configures the maximum number of IPv6 DHCP Prefix Delegation hosts (IA-PD) per SLA profile instance or per subscriber.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: Prefix delegation hosts that are modeled as a managed route do not count against this limit.

The **no** form of this command removes the maximum number of IPv6 Prefix Delegation hosts (IA-PD) limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 Prefix Delegation hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.303 ipv6-pd-ppp-dhcp

ipv6-pd-ppp-dhcp

Syntax **ipv6-pd-ppp-dhcp** *max-nr-of-hosts*
no ipv6-pd-ppp-dhcp

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-pd-ppp-dhcp)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-pd-ppp-dhcp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-pd-ppp-dhcp
configure subscriber-mgmt sub-profile host-limits ipv6-pd-ppp-dhcp

Description This command configures the maximum number of IPv6 PPPoE DHCP Prefix Delegation hosts (IA-PD) per SLA profile instance or per subscriber.

Note: Prefix delegation hosts that are modeled as a managed route do not count against this limit.

The **no** form of this command removes the maximum number of IPv6 PPPoE DHCP Prefix Delegation hosts (IA-PD) limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 PPPoE DHCP Prefix Delegation hosts.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.304 ipv6-prefix

ipv6-prefix

Syntax [**no**] **ipv6-prefix**

Context **[Tree]** (debug>router>rpki-session>packet ipv6-prefix)

Full Context debug router rpki-session packet ipv6-prefix

Description This command enables debugging for IPv6 prefix RPKI packets.

The **no** form of this command disables debugging for IPv6 prefix RPKI packets.

Platforms All

13.305 ipv6-prefix-list

ipv6-prefix-list

Syntax **ipv6-prefix-list** *ipv6-prefix-list-name* [**create**]
no ipv6-prefix-list *ipv6-prefix-list-name*

Context **[Tree]** (config>qos>match-list ipv6-prefix-list)

Full Context configure qos match-list ipv6-prefix-list

Description This command creates a list of IPv6 prefixes for match criteria in QoS policies. An ipv6-prefix-list must contain only IPv6 address prefixes created using the **prefix** command and cannot be deleted if it is referenced by a QoS policy.

The **no** form of this command deletes the specified list.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used (#, $, spaces, and so on), the string must be enclosed within double quotes. The name **default** (case insensitive) is reserved by the system.

create — Creates IPv6 prefixes for match criteria in QoS policies.

Platforms All

ipv6-prefix-list

Syntax **ipv6-prefix-list** *ipv6-prefix-list-name* [**create**]
no ipv6-prefix-list *ipv6-prefix-list-name*

Context **[Tree]** (config>filter>match-list ipv6-prefix-list)

Full Context configure filter match-list ipv6-prefix-list

Description This command creates a list of IPv6 prefixes for match criteria in ACL and CPM IPv6 filter policies.

The **no** form of this command deletes the specified list.

Operational Notes:

An IPv6 prefix list must contain only IPv6 address prefixes.

An IPv6 prefix list cannot be deleted if it is referenced by a filter policy.

See general description related to match-list usage in filter policies.

Parameters *ipv6-prefix-list-name* — Specifies a string of up to 32 printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

13.306 ipv6-routing

ipv6-routing

Syntax [**no**] **ipv6-routing** {**native** | **mt**}

Context **[Tree]** (config>service>vprn>isis ipv6-routing)

Full Context configure service vprn isis ipv6-routing

Description This command enables IPv6 routing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables support for IS-IS IPv6 TLVs for IPv6 routing.

Default no ipv6-routing

Parameters **native** — Enables IS-IS IPv6 TLVs for IPv6 routing and enables support for native IPv6 TLVs.

mt — Enables IS-IS multi-topology TLVs for IPv6 routing. When this parameter is specified, the support for native IPv6 TLVs is disabled.

Platforms All

ipv6-routing

Syntax [**no**] **ipv6-routing** {**native** | **mt**}

Context **[Tree]** (config>router>isis ipv6-routing)

Full Context configure router isis ipv6-routing

Description This command enables IPv6 routing.

The **no** form of this command disables support for IS-IS IPv6 TLVs for IPv6 routing.

Default no ipv6-routing

Parameters **native** — Enables IS-IS IPv6 TLVs for IPv6 routing and enables support for native IPv6 TLVs.

mt — Enables IS-IS multi-topology TLVs for IPv6 routing. When this parameter is specified, the support for native IPv6 TLVs is disabled.

Platforms All

13.307 ipv6-sid

ipv6-sid

Syntax **ipv6-sid index** *index-id*
ipv6-sid label *label-id*
no ipv6-sid

Context **[Tree]** (config>router>segment-routing>sr-mpls>prefix-sids ipv6-sid)

Full Context configure router segment-routing sr-mpls prefix-sids ipv6-sid

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to configure the IPv6 segment routing SID associated with the primary IPv6 address of the loopback or system interface.

The **no** form of this command removes the configuration of the IPv6 segment routing SID associated with the primary IPv6 interface address.

Default no ipv6-sid

Parameters **index** *index-id* — Specifies the node SID index for this interface.

Values 0 to 4294967295

label *label-id* — Specifies the label value for the node SID.

Values 32 to 1048575

Platforms All

13.308 ipv6-slaac-prefix

ipv6-slaac-prefix

Syntax **ipv6-slaac-prefix** *ipv6-prefix/prefix-length*
no ipv6-slaac-prefix

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host ipv6-slaac-prefix)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-slaac-prefix)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-slaac-prefix
configure subscriber-mgmt local-user-db ppp host ipv6-slaac-prefix

Description This command configures static IPv6 SLAAC prefix (PIO) for the host. The host will assign an IPv6 address to itself based on this prefix. The prefix length is 64 bits.

The **no** form of this command removes the static IPv6 SLAAC prefix (PIO) for the host from the configuration.

Default no ipv6-slaac-prefix

Parameters *ipv6-prefix/prefix-length* — Specifies the IPv6 address and prefix length.

Values

ipv6-prefix/prefix-length : ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D
prefix-length	64

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.309 ipv6-slaac-prefix-pool

ipv6-slaac-prefix-pool

Syntax **ipv6-slaac-prefix-pool** *pool*
no ipv6-slaac-prefix-pool

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-slaac-prefix-pool)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-slaac-prefix-pool)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-slaac-prefix-pool
configure subscriber-mgmt local-user-db ppp host ipv6-slaac-prefix-pool

Description This command configures the IPv6 SLAAC prefix pool of this host.

The **no** form of this command reverts to the default.

Parameters *pool* — Specifies the pool name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.310 ipv6-source-address

ipv6-source-address

Syntax **ipv6-source-address** *ipv6-address*
no ipv6-source-address

Context **[Tree]** (config>aaa>diam-peer-plcy ipv6-source-address)

Full Context configure aaa diameter-peer-policy ipv6-source-address

Description This command configures IPv6 source address that the SR OS node will use for its peering connection.

The **no** form of this command removes the IPv6 source address from the configuration.

Parameters *ipv6-address* — Specifies the source IPv6 address to use for outgoing diameter messages to an IPv6-reachable peer.

Values
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6-source-address

Syntax **ipv6-source-address** *ipv6-address* [**allow-connections**]
no ipv6-source-address

Context **[Tree]** (config>aaa>diam>node ipv6-source-address)

Full Context configure aaa diameter node ipv6-source-address

Description This command configures IPv6 source address that the SR OS node will use for its peering connection.

The **no** form of this command removes the IPv6 source address from the configuration.

Parameters *ipv6-address* — Specifies the source IPv6 address to use for outgoing diameter messages to an IPv6-reachable peer.

Values
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

allow-connections — Specifies to accept peering connections on the configured source IPv6 address. The peer initiating the connection can only be an inter-chassis peer.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6-source-address

Syntax **ipv6-source-address** *ipv6-address*
no ipv6-source-address

Context **[Tree]** (config>aaa>radius-srv-plcy>servers ipv6-source-address)

Full Context configure aaa radius-server-policy servers ipv6-source-address

Description This command configures the source address of an IPv6 RADIUS packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When no ipv6-source-address is configured, the system IPv6 address (inband RADIUS server connection) or Boot Option File (BOF) IPv6 address (outband RADIUS server connection) must be configured in order for the RADIUS client to work with an IPv6 RADIUS server.

This address is also used in the NAS-IPv6-Address attribute.

The **no** form of this command reverts to the default value.

Parameters *ipv6-address* — Specifies the source address of an IPv6 RADIUS packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ipv6-source-address

Syntax **ipv6-source-address** *ipv6-address*
no ipv6-source-address

Context **[Tree]** (config>service>vprn>dns ipv6-source-address)

Full Context configure service vprn dns ipv6-source-address

Description This command configures the IPv6 address of the default secondary DNS server for the subscribers using this interface. Subscribers that cannot obtain an IPv6 DNS server address by other means, can use this for DNS name resolution.

The ipv6-address value can only be set to a nonzero value if the value of VPRN type is set to **subscriber-split-horizon**.

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the IPv6 address of the default secondary DNS server.

Values ipv6-address - a.b.c.d

Platforms All

ipv6-source-address

Syntax **ipv6-source-address** *ipv6-address*
no ipv6-source-address

Context **[Tree]** (config>system>file-trans-prof ipv6-source-address)

Full Context configure system file-transmission-profile ipv6-source-address

Description This command specifies the IPv6 source address used for transport protocol.

The **no** form of this command uses the default source address which typically is the address of egress interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no ipv6-source-address

Parameters *Ipv6-address* — Specifies a unicast v6 address. This should be a local interface address.

Platforms All

13.311 ipv6-tcp-mss-adjust

ipv6-tcp-mss-adjust

Syntax **ipv6-tcp-mss-adjust** *segment-size*
no ipv6-tcp-mss-adjust

Context **[Tree]** (config>router>wlan-gw>dsm ipv6-tcp-mss-adjust)
[Tree] (config>service>vprn>wlan-gw>dsm ipv6-tcp-mss-adjust)

Full Context configure router wlan-gw distributed-sub-mgmt ipv6-tcp-mss-adjust
configure service vprn wlan-gw distributed-sub-mgmt ipv6-tcp-mss-adjust

Description This command specifies the value used for TCP-MSS-adjust in the IPv6 upstream direction for DSM. The downstream direction for both IPv4 and IPv6 are both configured under the group-interface. The upstream direction for IPv4 NAT hosts is configured under the NAT policy.

The defined segment size is inserted in a TCP SYN message if there is no existing MSS option or the value in the MSS option is bigger than the configured value.

The **no** form of this command disables upstream TCP MSS adjust for IPv6 DSM.

Default no ipv6-tcp-mss-adjust

Parameters *segment-size* — Specifies the segment size to be inserted.

Values 160 to 10240

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.312 ipv6-te-router-id

ipv6-te-router-id

Syntax **ipv6-te-router-id interface** *interface-name*
no ipv6-te-router-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router ipv6-te-router-id)

Full Context configure router ipv6-te-router-id

Description This command configures the IPv6 TE Router ID. The IPv6 TE Router ID, when configured, uniquely identifies the router as being IPv6 TE capable to other routers in an IGP TE domain.

IS-IS advertises this information using the IPv6 TE Router ID TLV.

If this command is not configured, the IPv6 TE Router ID will use the global unicast address of the system interface by default. The user can specify the system interface using this command to achieve the same result. If a different interface is specified, the preferred primary global unicast address of that interface is used instead

The **no** form of this command reverts the IPv6 TE Router ID to the default value.

Parameters **interface** *interface-name* — Specifies the name of the interface to be added or removed. Only system and loopback interfaces are accepted.

Platforms All

13.313 ipv6-unicast

ipv6-unicast

Syntax [**no**] **ipv6-unicast**

Context [Tree] (config>service>vprn>isis>multi-topology ipv6-unicast)

Full Context configure service vprn isis multi-topology ipv6-unicast

Description This command enables multi-topology TLVs.

The **no** form of this command disables multi-topology TLVs.

Platforms All

ipv6-unicast

Syntax [**no**] **ipv6-unicast**

Context [Tree] (config>router>isis>multi-topology ipv6-unicast)

Full Context configure router isis multi-topology ipv6-unicast

Description This command enables multi-topology TLVs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables multi-topology TLVs.

Default no ipv6-unicast

Platforms All

13.314 ipv6-unicast-disable

ipv6-unicast-disable

Syntax [**no**] **ipv6-unicast-disable**

Context **[Tree]** (config>router>isis>if ipv6-unicast-disable)
[Tree] (config>service>vprn>isis>if ipv6-unicast-disable)

Full Context configure router isis interface ipv6-unicast-disable
configure service vprn isis interface ipv6-unicast-disable

Description This command disables IS-IS IPv6 unicast routing for the interface.

By default IPv6 unicast on all interfaces is enabled. However, IPv6 unicast routing on IS-IS is in effect when the **config>router>isis>ipv6-routing mt** command is configured.

The **no** form of this command enables IS-IS IPv6 unicast routing for the interface.

Platforms All

13.315 ipv6-unicast-metric

ipv6-unicast-metric

Syntax **ipv6-unicast-metric** *metric*
no ipv6-unicast-metric

Context **[Tree]** (config>service>vprn>isis>if>level ipv6-unicast-metric)

Full Context configure service vprn isis interface level ipv6-unicast-metric

Description This command configures IS-IS interface metric for IPv6 unicast.

The **no** form of this command removes the metric from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — Specifies the IS-IS interface metric for IPv6 unicast.

Values 1 to 16777215

Platforms All

ipv6-unicast-metric

Syntax **ipv6-unicast-metric** *metric*
no ipv6-unicast-metric

Context **[Tree]** (config>router>isis>if>level ipv6-unicast-metric)

Full Context configure router isis interface level ipv6-unicast-metric

Description This command configures the IS-IS interface metric for IPv6 unicast.

The **no** form of this command removes the metric from the configuration.

Default no ipv6-unicast-metric

Parameters *metric* — Specifies the IS-IS interface metric for IPv6 unicast.

Values 1 to 16777215

Platforms All

13.316 ipv6-unicast-metric-offset

ipv6-unicast-metric-offset

Syntax **ipv6-unicast-metric-offset** *offset-value*
no ipv6-unicast-metric-offset

Context **[Tree]** (config>service>vprn>isis>link-group>level ipv6-unicast-metric-offset)

Full Context configure service vprn isis link-group level ipv6-unicast-metric-offset

Description This command sets the offset value for the IPv6 unicast address family. If the number of operational links drops below the **oper-members** threshold, the configured offset is applied to the interface metric for the IPv6 topology.

The **no** form of this command reverts the offset value to 0.

Default no ipv6-unicast-metric-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold.

Values 0 to 6777215

Platforms All

ipv6-unicast-metric-offset

Syntax **ipv6-unicast-metric-offset** *offset-value*
no ipv6-unicast-metric-offset

Context **[Tree]** (config>router>isis>link-group>level ipv6-unicast-metric-offset)

Full Context configure router isis link-group level ipv6-unicast-metric-offset

Description This command sets the offset value for the IPv6 unicast address family. If the number of operational links drops below the **oper-members** threshold, the configured offset is applied to the interface metric for the IPv6 topology.

The **no** form of this command reverts the offset value to 0.

Default no ipv6-unicast-metric-offset

Parameters *offset-value* — Specifies the amount the interface metric for the associated address family is to be increased if the number of operational members in the associated link-group drops below the oper-members threshold.

Values 0 to 6777215

Platforms All

13.317 ipv6-wan-address-pool

ipv6-wan-address-pool

Syntax **ipv6-wan-address-pool** *pool-name*
no ipv6-wan-address-pool

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host ipv6-wan-address-pool)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host ipv6-wan-address-pool)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-wan-address-pool
configure subscriber-mgmt local-user-db ppp host ipv6-wan-address-pool

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the pool name that is used in the DHCPv6 server for DHCPv6 IA-PA address selection.

The **no** form of this command removes the pool name from the configuration.

Parameters *pool-name* — Specifies the WAN address pool, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.318 ipv6-wan-ipoe-dhcp

ipv6-wan-ipoe-dhcp

Syntax **ipv6-wan-ipoe-dhcp** *max-nr-of-hosts*
no ipv6-wan-ipoe-dhcp

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-wan-ipoe-dhcp)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-wan-ipoe-dhcp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-wan-ipoe-dhcp
configure subscriber-mgmt sub-profile host-limits ipv6-wan-ipoe-dhcp

Description This command configures the maximum number of IPv6 IPoE DHCP WAN hosts (IA-NA) per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv6 IPoE DHCP WAN hosts (IA-NA) limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 IPoE DHCP WAN hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.319 ipv6-wan-ipoe-slaac

ipv6-wan-ipoe-slaac

Syntax **ipv6-wan-ipoe-slaac** *max-nr-of-hosts*
no ipv6-wan-ipoe-slaac

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-wan-ipoe-slaac)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-wan-ipoe-slaac)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-wan-ipoe-slaac
configure subscriber-mgmt sub-profile host-limits ipv6-wan-ipoe-slaac

Description This command configures the maximum number of IPv6 IPoE SLAAC WAN hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv6 IPoE SLAAC WAN hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 IPoE SLAAC WAN hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.320 ipv6-wan-overall

ipv6-wan-overall

Syntax **ipv6-wan-overall** *max-nr-of-hosts*
no ipv6-wan-overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-wan-overall)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-wan-overall)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-wan-overall
configure subscriber-mgmt sub-profile host-limits ipv6-wan-overall

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of IPv6 WAN hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPV6 WAN hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 WAN hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.321 ipv6-wan-ppp-dhcp

ipv6-wan-ppp-dhcp

Syntax **ipv6-wan-ppp-dhcp** *max-nr-of-hosts*
no ipv6-wan-ppp-dhcp

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-wan-ppp-dhcp)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-wan-ppp-dhcp)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-wan-ppp-dhcp
configure subscriber-mgmt sub-profile host-limits ipv6-wan-ppp-dhcp

Description This command configures the maximum number of IPv6 PPPoE DHCP WAN hosts (IA-NA) per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv6 PPPoE DHCP WAN hosts (IA-NA) limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 PPPoE DHCP WAN hosts (IA-NA).

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.322 ipv6-wan-ppp-slaac

ipv6-wan-ppp-slaac

Syntax **ipv6-wan-ppp-slaac** *max-nr-of-hosts*
no ipv6-wan-ppp-slaac

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits ipv6-wan-ppp-slaac)
[Tree] (config>subscr-mgmt>sub-profile>host-limits ipv6-wan-ppp-slaac)

Full Context configure subscriber-mgmt sla-profile host-limits ipv6-wan-ppp-slaac
configure subscriber-mgmt sub-profile host-limits ipv6-wan-ppp-slaac

Description This command configures the maximum number of IPv6 PPPoE SLAAC WAN hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of IPv6 PPPoE SLAAC WAN hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of IPv6 PPPoE SLAAC WAN hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.323 isa

isa

Syntax **isa**

Context **[Tree]** (config isa)

Full Context configure isa

Description Commands in this context configure Integrated Services Adapter (ISA) parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.324 isa-aa-group

isa-aa-group

Syntax **isa-aa-group** *aa-group-id*
no isa-aa-group

Context **[Tree]** (config>isa>wlan-gw-group>distributed-sub-mgmt isa-aa-group)

Full Context configure isa wlan-gw-group distributed-sub-mgmt isa-aa-group

Description This command configures an ISA application assurance group for WLAN gateway DSM subscribers.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

isa-aa-group

Syntax **isa-aa-group** *isa-aa-group-id* {**all** | **unknown**}
no isa-aa-group *isa-aa-group-id*

Context **[Tree]** (debug>mirror-source isa-aa-group)

Full Context debug mirror-source isa-aa-group

Description This command configures AA ISA group as a mirror source for this mirror service. Traffic is mirrored after AA processing takes place on AA ISAs of the group, therefore, any packets dropped as part of that AA processing are not mirrored.

Parameters *isa-aa-group-id* — Specifies the ISA ISA-AA group ID.

Values 1 to 255

all — Specifies that all traffic after AA processing will be mirrored.

unknown — Specifies that all traffic during the identification phase (may match policy entry or entries that have mirror action configured) and traffic that had been identified as unknown_tcp or unknown_udp after AA processing will be mirrored.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.325 isa-aa-oversubscription-factor

isa-aa-oversubscription-factor

Syntax **isa-aa-oversubscription-factor** *factor*
no isa-aa-oversubscription-factor

Context **[Tree]** (config>isa>wlan-gw-group>distributed-sub-mgmt isa-aa-oversubscription-factor)

Full Context configure isa wlan-gw-group distributed-sub-mgmt isa-aa-oversubscription-factor

Description This command specifies by how much an AA ISA is oversubscribed when linked to a WLAN-GW group. A factor of 1 indicates that each AA ISA is linked to a single WLAN-GW ISA, while a factor of 10 indicates that each AA ISA is linked to up to 10 WLAN-GW ISAs. The factor must be an integer but poses an oversubscription limit, not an exact ratio. For example, for 2 AA ISAs and 5 WLAN-GW ISAs, a factor of 3 or higher is valid. Additional standby ISAs can be added until the oversubscription limit is reached.

The **no** form of this command resets the configuration to the default value.

Default isa-aa-oversubscription-factor 1

Parameters *factor* — The number of WLAN GW ISAs that can be served by a single AA ISA.

Values 1 to 10

Platforms 7750 SR, 7750 SR-e, 7750 SR-s

13.326 isa-capacity-cost-high-threshold

isa-capacity-cost-high-threshold

Syntax **isa-capacity-cost-high-threshold** *threshold*
no isa-capacity-cost-high-threshold

Context **[Tree]** (config>isa>aa-grp isa-capacity-cost-high-threshold)

Full Context configure isa application-assurance-group isa-capacity-cost-high-threshold

Description This command configures the ISA-AA capacity cost high threshold.

The **no** form of this command reverts the threshold to the default value.

Default isa-capacity-cost-high-threshold 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *threshold* — Specifies the capacity cost high threshold for the ISA-AA group.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.327 isa-capacity-cost-low-threshold

isa-capacity-cost-low-threshold

Syntax **isa-capacity-cost-low-threshold** *threshold*
no isa-capacity-cost-low-threshold

Context **[Tree]** (config>isa>aa-grp isa-capacity-cost-low-threshold)

Full Context configure isa application-assurance-group isa-capacity-cost-low-threshold

Description This command configures the ISA-AA capacity cost low threshold.

The **no** form of this command reverts the threshold to the default value.

Default isa-capacity-cost-low-threshold 0

Parameters *threshold* — Specifies the capacity cost low threshold for the ISA-AA group.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.328 isa-dp-cpu-usage

isa-dp-cpu-usage

Syntax [**no**] **isa-dp-cpu-usage**

Context **[Tree]** (config>isa>tunnel-grp>stats-collection isa-dp-cpu-usage)

Full Context configure isa tunnel-group stats-collection isa-dp-cpu-usage

Description This command enables the system to collect statistics used to derive ISA CPU data plane usage. When enabled, this command impacts the ISA performance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.329 isa-filter

isa-filter

Syntax **isa-filter** *name* [**type** {**dsm**}] [**create**]
no isa-filter *name*

Context **[Tree]** (config>subscr-mgmt isa-filter)

Full Context configure subscriber-mgmt isa-filter

Description Commands in this context configure ISA filter parameters.

Parameters *name* — Specifies the name of the filter.

type dsm — Selects DSM as the type.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.330 isa-overload-cut-through

isa-overload-cut-through

Syntax [**no**] **isa-overload-cut-through**

Context **[Tree]** (config>isa>aa-grp isa-overload-cut-through)

Full Context configure isa application-assurance-group isa-overload-cut-through

Description This command configures the ISA group to enable cut-through of traffic if an overload event occurs, triggered when the IOM weighted average queues depth exceeds the **wa-shared-high-wmark**. In this ISA state, packets are cut-through from application analysis but retain subscriber context with default subscriber policy applied.

The **no** form of this command disables cut-through processing on overload.

Default no isa-overload-cut-through

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

13.331 isa-policer

isa-policer

Syntax **isa-policer** *policer-name* [**type** *policer-type*] [**create**]
no isa-policer *policer-name*

Context **[Tree]** (config>subscr-mgmt isa-policer)

Full Context configure subscriber-mgmt isa-policer

Description This command creates the context to configure an ISA policer. When creating a policer for the first time, both the **create** and **type** parameters are required.

The **no** form of this command reverts to the default.

Parameters *policer-name* — Specifies the name by which this policer is referenced up to 32 characters.

policer-type — Specifies the policer type. The dual-bucket-bandwidth policer applies both a CIR and PIR.

Values single-bucket-bandwidth, dual-bucket-bandwidth

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

13.332 isa-radius-policy

isa-radius-policy

Syntax **isa-radius-policy** *name* [**create**]
no isa-radius-policy *name*

Context **[Tree]** (config>aaa isa-radius-policy)

Full Context configure aaa isa-radius-policy

Description This command creates a policy template related to transport of accounting messages from the BB-ISA card to the accounting server. It also defines accounting attributes that will be included in accounting messages. The policy template will be instantiated once it is applied to the BB-ISA cards in the nat-group.

The **no** form of the command removes the policy name from the configuration.

Default none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the name of the ISA RADIUS policy that can be referenced by a NAT application.

create — Keyword used to create the policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.333 isa-service-chaining

isa-service-chaining

Syntax [**no**] **isa-service-chaining**

Context **[Tree]** (config>router isa-service-chaining)

Full Context configure router isa-service-chaining

Description Commands in this context configure ISA service chaining parameters.

The **no** form of this command disables ISA service chaining parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

isa-service-chaining

Syntax **isa-service-chaining**

Context **[Tree]** (config>subscr-mgmt isa-service-chaining)

Full Context configure subscriber-mgmt isa-service-chaining

Description Commands in this context configure ISA-based service chaining for subscribers with L2-Aware NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.334 isakmp-lifetime

isakmp-lifetime

Syntax **isakmp-lifetime** *seconds*

Context **[Tree]** (config>ipsec>ike-transform isakmp-lifetime)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure ipsec ike-transform isakmp-lifetime

Description This command specifies the lifetime of the IKE SA.

Default isakmp-lifetime 86400

Parameters *seconds* — Specifies the Phase 1 life time for this IKE transform.

Values 1200 to 31536000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

13.335 isid

isid

Syntax **isid** *start* [**to** *to*]
no isid *start*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>service-carving>manual isid)

Full Context configure service system bgp-evpn ethernet-segment service-carving manual isid

Description This command configures the ISID ranges for which the PE is primary, or uses the lowest preference algorithm.

Note: Multiple individual ISID values and ranges are allowed.

The following service-carving manual algorithms are supported for DF election:

- Manual non-preference

  A **preference** command is not configured for this algorithm. The primary PE for the configured ISIDs is determined by the ISID range. The manual non-preference algorithm only supports two PEs in the Ethernet Segment
- Manual preference-based

  If a **preference** command is configured, the algorithm uses the configured value to determine the DF election. For ISIDs not defined in the range, the highest-preference algorithm is used. For configured ISIDs, the lowest-preference algorithm is used.

Parameters *start* — Specifies the initial **isid** value of the range.

Values 1 to 16777215

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

to — Specifies the end **isid** value of the range. If not configured, only the individual start value is considered.

Values 1 to 16777215

Platforms All

isid

Syntax **isid** *value* [**to** *higher-value*]
no isid

Context **[Tree]** (config>filter>mac-filter>entry>match isid)

Full Context configure filter mac-filter entry match isid

Description This command configures an ISID value or a range of ISID values to be matched by the mac-filter parent. The pbb-etype value for the related SAP (inherited from the ethernet port configuration) or for the related SDP binding (inherited from SDP configuration) will be used to identify the ISID tag.

The **no** form of this command removes the ISID match criterion.

Default no isid

Parameters *value* — Specifies the ISID value, 24 bits as a decimal integer. When just one present identifies a specific ISID to be used for matching.

Values 0 to 16777215

to *higher-value* — Identifies a range of ISIDs to be used as matching criteria.

Platforms All

isid

Syntax **isid** *value* [**to** *higher-value*]
no isid
no isid *value* [**to** *higher-value*]

Context **[Tree]** (config>serv>mrp>mrp-policy>entry>match isid)

Full Context configure service mrp mrp-policy entry match isid

Description This command configures an ISID value or a range of ISID values to be matched by the mrp-policy parent when looking at the related MMRP attributes (Group B-MACs). The pbb-etype value for the related SAP (inherited from the ethernet port configuration) or for the related SDP binding (inherited from SDP configuration) will be used to identify the ISID tag.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Multiple ISID statements are allowed under a match node. The following rules govern the usage of multiple ISID statements:

- Overlapping values are allowed:
  - isid from 1 to 10
  - isid from 5 to 15
  - isid 16
- The minimum and maximum values from overlapping ranges are considered and displayed. The above entries will be equivalent with the “isid from 1 to 16” statement.
- There is no consistency check with the content of ISID statements from other entries. The entries are evaluated in the order of their IDs and the first match causes the implementation to execute the associated action for that entry and then to exit the mrp-policy.
- If there are no ISID statements under a match criteria but the **mac-filter** type is **isid** the following behaviors apply for different actions:
  - For **end-station**, it treats any ISID value as no match and goes to next entry or default action which must be “block” in this case
  - For **allow**, it treats any ISID value as a match and allows it
  - For **block**, it treats any ISID value as a match and blocks it

The **no** form of the command can be used in two ways:

no isid removes all the previous statements under one match node.

no isid *value* | **from** *value* **to** *higher-value* removes a specific ISID value or range. It must match a previously used positive statement: for example if the command **isid 16 to 100** was used using **no isid 16 to 50** will not work but **no isid 16 to 100** will be successful.

Default no isid

Parameters *value or higher-value* — Specifies the ISID value in 24 bits. When just one value is present, it identifies a particular ISID to be used for matching.

Values 0 to 16777215

from value to higher-value — Identifies a range of ISIDs to be used as matching criteria.

Platforms All

13.336 isid-policy

isid-policy

Syntax **isid-policy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls isid-policy)

Full Context configure service vpls isid-policy

Description This command configures ISID policies for individual ISIDs or ISID ranges in a B-VPLS using SPBM. The ISIDs may belong to I-VPLS services or may be static-isids defined on this node. Multiple entry statements are allowed under a **isid-policy**. ISIDs that are declared as static do not require and **isid-policy** unless the ISIDs are not to be advertised.

isid-policy allows finer control of ISID multicast but is not typically required for SPBM operation. Use of ISID policies can cause additional flooding of multicast traffic.

Platforms All

13.337 isid-range

isid-range

Syntax **isid-range** *from* [**to** *to*] {**auto-rt** | **route-target** *rt*}
no isid-range *from*

Context [Tree] (config>service>vpls>bgp-evpn>isid-route-target isid-range)

Full Context configure service vpls bgp-evpn isid-route-target isid-range

Description This command creates a range of ISIDs associated with a specified route-target that is advertised with BMAC-ISID and IMET-ISID routes for the ISID. The route-target can be explicitly configured or automatically assigned by the system if the **auto-rt** option is configured. Auto routes assignment is based on RFC 7623 as follows:

<2-byte-as-number>:<4-byte-value>, where 4-byte-value = 0x30+ISID

The **no** form of the command deletes the **isid-range** and its association with the **route-target**.

The **no** form is the default action, which advertises the BMAC-ISID and IMET-ISID routes with the B-VPLS configured route-target.

Default no isid-range

Parameters *from* — Specifies the start of the ISID range.

Values 1 to 16777215

to — Specifies the end of the ISID range. If it is not configured, the range is comprised of (only) the ISID specified in the *to* option.

Values 1 to 16777215

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

auto-rt — Automatically generates an ISID-derived **route-target** in the format: AS_number:0x30+ISID.

route-target — Specifies an explicit route target.

Values rt - target:{<ip-addr:comm-val>| <2byte-as-number:extcomm-val>| <4byte-asnumber:comm-val>}

ip-addr: a.b.c.d

comm-val: [0 to 65535]

2byte-as-number: [0 to 65535]

ext-comm-val: [0 to 4294967295]

4byte-asnumber: [0 to 4294967295]

Platforms All

13.338 isid-route-target

isid-route-target

Syntax **isid-route-target**

Context **[Tree]** (config>service>vpls>bgp-evpn isid-route-target)

Full Context configure service vpls bgp-evpn isid-route-target

Description Commands in this context configure the isid-range to route-target associations.

Platforms All

13.339 isis

isis

Syntax [**no**] **isis** *isis-instance*

Context **[Tree]** (config>service>vprn isis)

Full Context configure service vprn isis

Description Commands in this context configure the Intermediate-System-to-Intermediate-System (IS-IS) protocol instance in the VPRN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IS-IS protocol instance is enabled with the **no shutdown** command in the **config>service>vprn>isis** context. Alternatively, the IS-IS protocol instance is disabled with the **shutdown** command in the **config>service>vprn>isis** context.

IS-IS instances are **shutdown** when created, so that all parameters can be configured prior to the instance being enabled.

The **no** form of this command disables the ISIS protocol instance from the given VPRN service.

Default 0

Parameters *isis-instance* — Specifies the instance ID for an IS-IS instance.

Values 0 to 127

Platforms All

isis

Syntax [**no**] **isis** [*isis-instance*]

Context **[Tree]** (config>router isis)

Full Context configure router isis

Description Commands in this context configure the Intermediate-System-to-Intermediate-System (IS-IS) protocol instance.

The IS-IS protocol instance is enabled with the **no shutdown** command in the **config>router>isis** context. Alternatively, the IS-IS protocol instance is disabled with the **shutdown** command in the **config>router>isis** context.

IS-IS instances are shutdown when created, so that all parameters can be configured prior to the instance being enabled.

The **no** form of this command deletes the IS-IS protocol instance. Deleting the protocol instance removes all configuration parameters for this IS-IS instance.

Parameters *isis-instance* — Specifies the instance ID for an IS-IS instance.

Values 0 to 127

Platforms All

isis

Syntax **isis** [*isis-instance*]

Context **[Tree]** (debug>router isis)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router isis

Description Commands in this context debug IS-IS protocol entities.

Parameters *isis-instance* — Specifies the IS-IS instance.

Values 0 to 127

Output The following output is an example of the debugging information.

Sample Output

```
*A:Dut-C# /tools dump router isis sr-database  prefix 10.20.1.5 detail
===============================================================================
Rtr Base ISIS Instance 0 SR Database
===============================================================================
103   474390 10.20.1.5       LfaNhops  1   0  15      1000    1    1
  1492   1500    1500   0 0  1  1   0100.2000.1005 SR_ERR_OK
       IP:10.10.5.5 gifId:3 ifId:4 protectId:7 numLabels:1 outLbl:474390 isAdv:1 is
LfaX:0
       IP:10.10.12.2 gifId:5 ifId:6 protectId:0 numLabels:2 outLbl1:474389 outLbl2:
474390 numLfaNhops:1 isAdv:0
-------------------------------------------------------------------------------
D = duplicate pending
xL = exclude from LFA
rL = remote LFA
Act = tunnel active
LDP = LDP FEC is the SID NH for SR-LDP stitching
===============================================================================

*A:Dut-C# /tools dump router isis sr-database nh-type ldp  detail
===============================================================================
Rtr Base ISIS Instance 0 SR Database
===============================================================================
SID   Label  Prefix          Last-act  Lev MT TnlPref Metric  IpNh SrNh
  Mtu    MtuPrim MtuBk  D xL rL Act AdvSystemId    SrErr
-------------------------------------------------------------------------------
1000  475287 10.20.1.4       AddTnl    1   0  15      0       1    1
  0      0       0      0 0  0  1   0100.2000.1004 SR_ERR_OK
       LDP: IP:10.20.1.4 tnlId:65546 tnlTyp:2
1001  475288 10.20.1.5       AddTnl    1   0  15      0       1    1
  0      0       0      0 0  0  1   0100.2000.1005 SR_ERR_OK
       LDP: IP:10.20.1.5 tnlId:65548 tnlTyp:2
1002  475289 10.20.1.6       AddTnl    1   0  15      0       1    1
  0      0       0      0 0  0  1   0100.2000.1006 SR_ERR_OK
       LDP: IP:10.20.1.6 tnlId:65549 tnlTyp:2
-------------------------------------------------------------------------------
D = duplicate pending
xL = exclude from LFA
rL = remote LFA
Act = tunnel active
LDP = LDP FEC is the SID NH for SR-LDP stitching
===============================================================================
```

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

14 j Commands

14.1 jitter-event

jitter-event

Syntax **jitter-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
no jitter-event

Context **[Tree]** (config>saa>test jitter-event)

Full Context configure saa test jitter-event

Description This command specifies that at the termination of an SAA test probe, the calculated jitter value is evaluated against the configured rising and falling jitter thresholds. SAA threshold events are generated as required.

Once the threshold (rising/falling) is crossed, it is disabled from generating additional events until the opposite threshold is crossed. If a **falling-threshold** is not supplied, the **rising-threshold** is re-enabled when it falls below the threshold after the initial crossing that generated the event.

The configuration of jitter event thresholds is optional.

The **no** form of the command disables the jitter event.

Parameters **rising-threshold** *threshold* — Specifies a rising threshold jitter value, in milliseconds. When the test run is completed, the calculated jitter value is compared to the configured jitter rising threshold. If the test run jitter value is greater than the configured rising threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Values 0 to 2147483

Default 0

falling-threshold *threshold* — Specifies a falling threshold jitter value, in milliseconds. When the test run is completed, the calculated jitter value is compared to the configured jitter falling threshold. If the test run jitter value is greater than the configured falling threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Values 0 to 2147483

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

direction — Specifies the direction for OAM ping responses received for an OAM ping test run.

Values **inbound** — Monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run.

outbound — Monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run.

roundtrip — Monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run.

Default roundtrip

Platforms All

14.2 join-time

join-time

Syntax **join-time** *value*
no join-time

Context **[Tree]** (config>service>vpls>sap>mrp join-time)
[Tree] (config>service>vpls>spoke-sdp>mrp join-time)
[Tree] (config>service>vpls>mesh-sdp>mrp join-time)

Full Context configure service vpls mesh-sdp mrp join-time
configure service vpls sap mrp join-time
configure service vpls spoke-sdp mrp join-time

Description This command controls the interval between transmit opportunities that are applied to the Applicant state machine. An instance of this Join Period Timer is required on a per-Port, per-MRP Participant basis. For additional information, refer to IEEE 802.1ak-2007 section 10.7.4.1.

Default join-time 2

Parameters *value* — The interval between transmit opportunities, in tenths of a second.

Values 1 to 10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

14.3 join-tlv-packing-disable

join-tlv-packing-disable

Syntax [**no**] **join-tlv-packing-disable**

Context **[Tree]** (config>service>vprn>mvpn>pt>selective join-tlv-packing-disable)

Full Context configure service vprn mvpn provider-tunnel selective join-tlv-packing-disable

Description This command enables packing of MDT join TLVs into a single PDU to improve efficiency, if multiple join TLVs are available at the time of transmission.

The **no** form of this command disables packing of MDT join TLVs into a single PDU.

Default no join-tlv-packing-disable

Platforms All

14.4 jp

jp

Syntax **jp** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no jp

Context **[Tree]** (debug>service>id>pim-snooping jp)

Full Context debug service id pim-snooping jp

Description This command enables or disables debugging for the PIM Join-Prune mechanism.

Parameters *grp-ip-address* — Debugs information associated with the specified Join-Prune mechanism.

Values multicast group address (ipv4 or ipv6) or zero

ip-address — Debugs information associated with the specified Join-Prune mechanism

Values source IP address (IPv4 or IPv6)

detail — Debugs detailed Join-Prune mechanism information

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

jp

Syntax **jp** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no jp

Context **[Tree]** (debug>router>pim jp)

Full Context debug router pim jp

Description This command enables debugging for PIM join and prune mechanisms.

The **no** form of this command disables PIM join and prune mechanisms debugging.

Parameters *grp-ip-address* — Debugs information associated with the specified Join-Prune mechanism.

Values multicast group address (ipv4, ipv6) or zero

ip-address — Debugs information associated with the specified Join-Prune mechanism.

Values source address (ipv4, ipv6)

detail — Debugs detailed Join-Prune mechanism information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

15 k Commands

15.1 kb-memory-use-alarm

kb-memory-use-alarm

Syntax **kb-memory-use-alarm rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no kb-memory-use-warn

Context **[Tree]** (config>system>thresholds kb-memory-use-alarm)

Full Context configure system thresholds kb-memory-use-alarm

Description This command configures memory use, in kilobytes, alarm thresholds.

The **no** form of the command removes the parameters from the configuration.

Parameters **rising-threshold** *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

The threshold value represents units of kilobytes.

Values -2147483648 to 2147483647

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

The threshold value represents units of kilobytes.

Values -2147483648 to 2147483647

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence. This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

startup-alarm *alarm-type* — Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Platforms All

15.2 kb-memory-use-warn

kb-memory-use-warn

Syntax **kb-memory-use-warn rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no kb-memory-use-warn

Context **[Tree]** (config>system>thresholds kb-memory-use-warn)

Full Context configure system thresholds kb-memory-use-warn

Description This command configures memory usage, in kilobytes, for warning thresholds

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **rising-threshold** *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

The threshold value represents units of kilobytes.

Values -2147483648 to 2147483647

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

The threshold value represents units of kilobytes.

Values -2147483648 to 2147483647

Default 0

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the show>system>thresholds CLI command.

trap — An SR OSS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

alarm-type — Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Platforms All

15.3 keep-alive

keep-alive

Syntax **keep-alive** [**interval** *seconds*] [**retry-count** *value*] [**timeout** *retry-seconds*]
no keep-alive

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile keep-alive)

Full Context configure subscriber-mgmt gtp peer-profile keep-alive

Description This command configures Echo-Request messages.

The **no** form of this command reverts to the default values.

Default keep-alive interval 60 retry-count 4 timeout 5

Parameters *seconds* — Specifies, in seconds, the interval between keep-alive Echo-Request messages towards the same peer.

Values 0, 60 to 180

Default 60

value — Specifies, in seconds, the interval between keep-alive Echo-Request messages towards the same peer.

Values 1 to 15

Default 4

retry-seconds — Specifies the retry timeout, in seconds.

Values 1 to 20

Default 5

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

keep-alive

Syntax **keep-alive** *timer*
no keep-alive

Context **[Tree]** (config>port>ethernet>dwl keep-alive)

Full Context configure port ethernet down-when-looped keep-alive

Description This command configures the time interval between keep-alive PDUs.

Default no keep-alive

Parameters *timer* — Specifies the time interval, in seconds, between keep-alive PDUs.

Values 1 to 120

Platforms All

keep-alive

Syntax **keep-alive** [**poll-frequency** *seconds*] [**poll-count** *value*] [**test-frequency** *seconds*]
no keep-alive

Context **[Tree]** (config>port>sonet-sdh>path>atm>ilmi keep-alive)

Full Context configure port sonet-sdh path atm ilmi keep-alive

Description This command configures keepalive parameters to monitor ILMI link connectivity.

The **no** form of this command resets the default values on an ILMI link.

Parameters **poll-frequency** *seconds* — Specifies the amount of time, in seconds, between successive transmissions of ILMI messages on this interface for the purpose of detecting the establishment of ILMI connectivity.

Values 1 to 255

value — Specifies the number of consecutive polls on this interface for which no ILMI response message is received before ILMI connectivity is declared lost.

Values 1 to 255

test-frequency *seconds* — Specifies the frequency for testing for connectivity when the link is establishing before polling begins.

Values 0 to 255

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

keep-alive

Syntax **keep-alive** *seconds*

Context [Tree] (config>li>x-interfaces>x2>timeouts keep-alive)
[Tree] (config>li>x-interfaces>x3>timeouts keep-alive)

Full Context configure li x-interfaces x2 timeouts keep-alive
configure li x-interfaces x3 timeouts keep-alive

Description This command configures the X2 and X3 keep-alive timeout.

Parameters *seconds* — Specifies the maximum time to wait for a LIC reply to a keep alive request. The system retries up to three more times, and if no reply is received, the system declares a connection fault and logs the failure event.

Values 300 to 600

Default 300

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

keep-alive

Syntax **keep-alive**

Context [Tree] (config>service>sdp keep-alive)

Full Context configure service sdp keep-alive

Description This command enables the context to configure SDP connectivity monitoring keepalive messages for the SDP ID.

SDP ID keepalive messages use SDP Echo Request and Reply messages to monitor SDP connectivity. The operating state of the SDP is affected by the keepalive state on the SDP ID. SDP Echo Request messages are only sent when the SDP ID is completely configured and administratively up. If the SDP ID is administratively down, keepalives for that SDP ID are disabled. SDP Echo Requests (when sent for keepalive messages) are always sent with the *originator-sdp-id*. All SDP ID keepalive SDP Echo Replies are sent using generic IP/GRE OAM encapsulation.

When a keepalive response is received that indicates an error condition, the SDP ID will immediately be brought operationally down. Once a response is received that indicates the error has cleared and the **hold-down-time** interval has expired, the SDP ID will be eligible to be put into the operationally up state. If no other condition prevents the operational change, the SDP ID will enter the operational state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A set of event counters track the number of keepalive requests sent, the size of the message sent, non-error replies received and error replies received. A keepalive state value is kept indicating the last response event. A keepalive state timestamp value is kept indicating the time of the last event. With each keepalive event change, a log message is generated indicating the event type and the timestamp value.

Table 69 describes the keepalive interpretation of SDP echo reply response conditions and the effect on the SDP ID operational status.

Table 69 **Keepalive Interpretation and Effect of SDP Echo Reply**

Result of Request	Stored Response State	Operational State
keepalive request timeout without reply	Request Timeout	Down
keepalive request not sent due to non-existent *orig-sdp-id* (This condition should not occur)	Orig-SDP Non-Existent	Down
keepalive request not sent due to administratively down *orig-sdp-id*	Orig-SDP Admin-Down	Down
keepalive reply received, invalid origination-id	Far End: Originator-ID Invalid	Down
keepalive reply received, invalid responder-id	Far End: Responder-ID Error	Down
keepalive reply received, No Error	Success	Up (If no other condition prevents)

Platforms All

15.4 keep-alive-interval

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-lag keep-alive-interval)

Full Context configure redundancy multi-chassis peer mc-lag keep-alive-interval

Description This command sets the interval at which keep-alive messages are exchanged between two systems participating in MC-LAG. These keep-alive messages are used to determine remote-node failure and the interval is set in deciseconds.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command sets the interval to default value.

Default keep-alive-interval 10

Parameters *interval* — The time interval expressed in tenths of a second.

Values 5 to 500

Platforms All

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp keep-alive-interval)
[Tree] (config>service>vprn>sub-if>grp-if>srrp keep-alive-interval)

Full Context configure service ies subscriber-interface group-interface srrp keep-alive-interval
configure service vprn subscriber-interface group-interface srrp keep-alive-interval

Description This command defines the interval between SRRP advertisement messages sent when operating in the master state. The interval is also the basis for setting the master-down timer used to determine when the master is no longer sending. The system uses three times the keep-alive interval to set the timer. Every time an SRRP advertisement is seen that is better than the local priority, the timer is reset. If the timer expires, the SRRP instance assumes that a master does not exist and initiates the attempt to become master.

When in backup state, the SRRP instance takes the keep-alive interval of the master as represented in the masters SRRP advertisement message. Once in master state, the SRRP instance uses its own configured keep-alive interval.

The keep-alive-interval may be changed at any time, but will have no effect until the SRRP instance is in the master state.

The **no** form of this command restores the default interval.

Default keep-alive-interval 10

Parameters *interval* — Specifies the interval, in deciseconds, between SRRP advertisement messages sent when operating in the master state.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

keep-alive-interval

Syntax **keep-alive-interval** *interval*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no keep-alive-interval

Context [Tree] (config>redundancy>multi-chassis>peer>mc-ep keep-alive-interval)

Full Context configure redundancy multi-chassis peer mc-endpoint keep-alive-interval

Description This command sets the interval at which keep-alive messages are exchanged between two systems participating in MC-EP when bfd is not enabled or is down. These fast keep-alive messages are used to determine remote-node failure and the interval is set in deciseconds.

The **no** form of this command sets the interval to default value

Default no keep-alive-interval

Parameters *interval* — The time interval expressed in tenths of a second.

Values 5 to 500

Platforms All

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context [Tree] (config>redundancy>multi-chassis>peer>mc-ipsec keep-alive-interval)

Full Context configure redundancy multi-chassis peer mc-ipsec keep-alive-interval

Description This command specifies the time interval of the mastership election protocol sending keep-alive packet.

The **no** form of this command reverts to the default.

Default keep-alive-interval 10

Parameters *interval* — Specifies the keep alive interval in tenths of seconds.

Values 5 to 500

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

15.5 keep-count

keep-count

Syntax **keep-count** *count*
no keep-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>bmp>station>connection>tcp-keepalive keep-count)

Full Context configure bmp station connection tcp-keepalive keep-count

Description This command configures the number of missed keepalives before the TCP connection is declared down.

The **no** form of this command reverts to the default.

Default keep-count 4

Parameters *count* — Specifies the number of missed keepalives before the TCP connection is declared down.

Values 3 to 100

Platforms All

15.6 keep-idle

keep-idle

Syntax **keep-idle** *idle*
no keep-idle

Context [Tree] (config>bmp>station>connection>tcp-keepalive keep-idle)

Full Context configure bmp station connection tcp-keepalive keep-idle

Description This command configures the time until the first TCP keepalive probe is sent.

The **no** form of this command reverts to the default.

Default keep-idle 600

Parameters *idle* — Specifies the time, in seconds, until the first TCP keepalive probe is sent.

Values 1 to 100000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

15.7 keep-interval

keep-interval

Syntax **keep-interval** *interval*
no keep-interval

Context **[Tree]** (config>bmp>station>connection>tcp-keepalive keep-interval)

Full Context configure bmp station connection tcp-keepalive keep-interval

Description This command configures the time between two TCP keepalives probes.

The **no** form of this command reverts to the default.

Default keep-interval 15

Parameters *interval* — Specifies the time, in seconds, between two TCP keepalives probes.

Values 1 to 100000

Platforms All

15.8 keep-multiplier

keep-multiplier

Syntax **keep-multiplier** *number*
no keep-multiplier

Context **[Tree]** (config>router>gmpls keep-multiplier)

Full Context configure router gmpls keep-multiplier

Description This command configures the integer used by RSVP to declare that a reservation is down or the neighbor is down.

The **no** form of this command resets the configuration to the default value.

Default keep-multiplier 3

Parameters *number* — Specifies the keep multiplier value.

Values 1 to 255

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

keep-multiplier

Syntax [**no**] **keep-multiplier** *number*
no keep-multiplier

Context **[Tree]** (config>router>rsvp keep-multiplier)

Full Context configure router rsvp keep-multiplier

Description The **keep-multiplier** *number* is an integer used by RSVP to declare that a reservation is down or the neighbor is down.

The **no** form of this command reverts to the default value.

Default keep-multiplier 3

Parameters *number* — Specifies the **keep-multiplier** value.

Values 1 to 255

Platforms All

15.9 keepalive

keepalive

Syntax **keepalive** *seconds* [**hold-up-multiplier** *multiplier*]
no keepalive

Context **[Tree]** (config>router>l2tp>group>ppp keepalive)
[Tree] (config>router>l2tp>group>tunnel>ppp keepalive)
[Tree] (config>service>vprn>l2tp>group>ppp keepalive)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp keepalive)

Full Context configure router l2tp group ppp keepalive
configure router l2tp group tunnel ppp keepalive
configure service vprn l2tp group ppp keepalive
configure service vprn l2tp group tunnel ppp keepalive

Description This command configures the PPP keepalive interval and multiplier.

Default keepalive 30 hold-up-multiplier 3

Parameters *seconds* — Specifies in seconds the interval.

Values 10 to 300

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multiplier — Specifies the multiplier.

Values 1 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

keepalive

Syntax **keepalive** *seconds* [**hold-up-multiplier** *multiplier*]
no keepalive

Context **[Tree]** (config>subscr-mgmt>ppp-policy keepalive)

Full Context configure subscriber-mgmt ppp-policy keepalive

Description This command defines the keepalive interval and the number of keepalives that can be missed before the session is declared down for this PPP policy.

The **no** form of this command reverts to the default value.

Default keepalive 30 hold-up-multiplier 3

Parameters *seconds* — Specifies the keepalive interval in seconds.

Values 4 to 300

hold-up-multiplier *multiplier* — Specifies the number of keepalives that can be missed.

Values 1 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

keepalive

Syntax **keepalive** *seconds*
no keepalive

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy keepalive)

Full Context configure subscriber-mgmt bgp-peering-policy keepalive

Description This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires.

The keepalive value is generally one-third of the hold-time interval. Even though the OS implementation allows the keepalive value and the hold-time interval to be independently set, under the following circumstances, the configured keepalive value is overridden by the hold-time value:

If the specified keepalive value is greater than the configured hold-time, then the specified value is ignored, and the keepalive is set to one third of the current hold-time value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the specified hold-time interval is less than the configured keepalive value, then the keepalive value is reset to one third of the specified hold-time interval.

If the hold-time interval is set to zero, then the configured value of the keepalive value is ignored. This means that the connection with the peer is up permanently and no keepalive packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

Default keepalive 30

Parameters *seconds* — Specifies the keepalive timer in seconds, expressed as a decimal integer.

Values 0 to 21845

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

keepalive

Syntax **keepalive** *seconds*
no keepalive

Context **[Tree]** (config>service>vpls>gsmp>group keepalive)
[Tree] (config>service>vprn>gsmp>group keepalive)

Full Context configure service vpls gsmp group keepalive
configure service vprn gsmp group keepalive

Description This command configures keepalive values for the GSMP connections in this group.

The **no** form of this command reverts to the default.

Default no keepalive

Parameters *seconds* — Specifies the GSMP keepalive timer value in seconds.

Values 1 to 25

Platforms All

keepalive

Syntax **keepalive** *seconds* [**hold-up-multiplier** *multiplier*]
no keepalive

Context **[Tree]** (config>subscr-mgmt>pppoe-client-policy keepalive)

Full Context configure subscriber-mgmt pppoe-client-policy keepalive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the **keepalive** interval and the number of times the **keepalive** can be missed before the session is declared down for this PPPoE client policy.

The **no** form of this command reverts to the default.

Default keepalive 30 hold-up-multiplier 3

Parameters *seconds* — Specifies the **keepalive** interval in seconds.

Values 10 to 300

multiplier — Specifies the number times **keepalive** can be missed.

Values 1 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

keepalive

Syntax **keepalive** *time-interval* [**dropcount** *drop-count*]
no keepalive

Context **[Tree]** (config>port>sonet-sdh>path>ppp keepalive)
[Tree] (config>port>tdm>ds1>channel-group>ppp keepalive)
[Tree] (config>port>tdm>ds3>ppp keepalive)
[Tree] (config>port>tdm>e1>channel-group>ppp keepalive)
[Tree] (config>port>tdm>e3>ppp keepalive)

Full Context configure port sonet-sdh path ppp keepalive
configure port tdm ds1 channel-group ppp keepalive
configure port tdm ds3 ppp keepalive
configure port tdm e1 channel-group ppp keepalive
configure port tdm e3 ppp keepalive

Description This command sets the keepalive interval.

The **no** form of this command returns the interval to the default value.

Default keepalive 10

Parameters *time-interval* — Specifies the time, in seconds, between keepalive messages, expressed as a decimal integer.

Values 1 to 60

drop-count — Specifies the number of consecutive keepalive failed request attempts or remote replies that can be missed after which the port is operationally downed.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path ppp keepalive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 ppp keepalive
- configure port tdm ds3 ppp keepalive
- configure port tdm e1 channel-group ppp keepalive
- configure port tdm ds1 channel-group ppp keepalive

keepalive

Syntax **keepalive** *time-interval*
no keepalive

Context **[Tree]** (config>port>sonet-sdh>path>cisco-hdlc keepalive)
[Tree] (config>port>tdm>ds1>channel-group>cisco-hdlc keepalive)
[Tree] (config>port>tdm>ds3>cisco-hdlc keepalive)
[Tree] (config>port>tdm>e1>channel-group>cisco-hdlc keepalive)
[Tree] (config>port>tdm>e3>cisco-hdlc keepalive)

Full Context configure port sonet-sdh path cisco-hdlc keepalive
configure port tdm ds1 channel-group cisco-hdlc keepalive
configure port tdm ds3 cisco-hdlc keepalive
configure port tdm e1 channel-group cisco-hdlc keepalive
configure port tdm e3 cisco-hdlc keepalive

Description This command specifies the interval, in seconds, used to send periodic keepalive packets. The receiver process expects to receive a keepalive packet every “keepalive interval”. The link is declared down if the receiver process does not receive a keepalive within the “timeout interval”. The link is declared up once the number of continual keepalive packets received equals to the up-count. The nodes at the two endpoints of the cHDLC link should be provisioned with the same values. A keepalive value of 0 means no keepalive packets are sent.

Default keepalive 10

Parameters *time-interval* — Specifies the interval used to send periodic keepalive packets.

Values 0 to 300

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path cisco-hdlc keepalive

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 cisco-hdlc keepalive
- configure port tdm e1 channel-group cisco-hdlc keepalive
- configure port tdm ds1 channel-group cisco-hdlc keepalive
- configure port tdm e3 cisco-hdlc keepalive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

keepalive

Syntax **keepalive** *seconds*
no keepalive

Context **[Tree]** (config>service>vprn>bgp keepalive)
[Tree] (config>service>vprn>bgp>group keepalive)
[Tree] (config>service>vprn>bgp>group>neighbor keepalive)

Full Context configure service vprn bgp group keepalive
configure service vprn bgp group neighbor keepalive
configure service vprn bgp keepalive

Description This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires. The **seconds** parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **keepalive** value is generally one-third of the **hold-time** interval. Even though the OS implementation allows the **keepalive** value and the **hold-time** interval to be independently set, under the following circumstances, the configured **keepalive** value is overridden by the **hold-time** value:

If the specified **keepalive** value is greater than the configured **hold-time**, then the specified value is ignored, and the **keepalive** is set to one third of the current **hold-time** value.

If the specified **hold-time** interval is less than the configured **hold-time** value, then the **keepalive** value is reset to one third of the specified **hold-time** interval.

If the **hold-time** interval is set to zero, then the configured value of the **keepalive** value is ignored. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default keepalive 30

Parameters *seconds* — The keepalive timer in seconds, expressed as a decimal integer.

Values 0 to 21845

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

keepalive

Syntax **keepalive** *timeout factor*
no keepalive

Context **[Tree]** (config>router>ldp>if-params>if>ipv4 keepalive)
[Tree] (config>router>ldp>if-params>if>ipv6 keepalive)
[Tree] (config>router>ldp>if-params>ipv4 keepalive)
[Tree] (config>router>ldp>if-params>ipv6 keepalive)
[Tree] (config>router>ldp>targ-session>ipv4 keepalive)
[Tree] (config>router>ldp>targ-session>ipv6 keepalive)
[Tree] (config>router>ldp>targ-session>peer keepalive)
[Tree] (config>router>ldp>targ-session>peer-template keepalive)

Full Context configure router ldp interface-parameters interface ipv4 keepalive
configure router ldp interface-parameters interface ipv6 keepalive
configure router ldp interface-parameters ipv4 keepalive
configure router ldp interface-parameters ipv6 keepalive
configure router ldp targeted-session ipv4 keepalive
configure router ldp targeted-session ipv6 keepalive
configure router ldp targeted-session peer keepalive
configure router ldp targeted-session peer-template keepalive

Description This command configures the time interval (in s), that LDP waits before tearing down the session. The **factor** parameter derives the keepalive interval.

The **config**>**router**>**ldp**>**if-params**>**ipv6**>**keepalive** and **config**>**router**>**ldp**>**targ-session**>**ipv6**>**keepalive** commands are not supported on the 7450 ESS.

If no LDP messages are exchanged for the configured time interval, the LDP session is torn down. Keepalive timeout is usually three times the keepalive interval. To maintain the session permanently, regardless of the activity, set the value to zero.

When LDP session is being set up, the keepalive timeout is negotiated to the lower of the two peers. Once an operational value is agreed upon, the keepalive factor is used to derive the value of the keepalive interval.

The **no** form of the command at the interface-parameters and targeted-session levels sets the **keepalive timeout** and the **keepalive factor** to the default value.

The **no** form of this command, at the interface level, sets the **keepalive timeout** and the **keepalive factor** to the value defined under the **interface-parameters** level.

The **no** form of this command, at the peer level, sets the **keepalive timeout** and the **keepalive factor** to the value defined under the **targeted-session** level.

The session must be flapped for the new settings to operate.

Default Table 70 lists the default values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 70 **Timeout Factor Defaults**

Context	Timeout	Factor
config>router>ldp>if-params	30	3
config>router>ldp>targ-session	40	4
config>router>ldp>if-params>if	Inherits values from interface-parameters context.	
config>router>ldp>targ-session>peer	Inherits values from targeted-session context.	

Parameters *timeout* — Configures the time interval, in seconds, that LDP waits before tearing down the session.

Values 1 to 65535

factor — Specifies the number of keepalive messages, expressed as a decimal integer, that should be sent on an idle LDP session in the keepalive timeout interval.

Values 1 to 255

Platforms All

keepalive

Syntax [**no**] **keepalive**

Context **[Tree]** (debug>router>ldp>peer>packet keepalive)

Full Context debug router ldp peer packet keepalive

Description This command enables debugging for LDP Keepalive packets.

The **no** form of the command disables the debugging output.

Platforms All

keepalive

Syntax **keepalive** *seconds*
no keepalive

Context **[Tree]** (config>router>pcep>pcc keepalive)
[Tree] (config>router>pcep>pce keepalive)

Full Context configure router pcep pcc keepalive
configure router pcep pce keepalive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the PCEP session keep-alive value. A PCEP speaker (PCC or PCE) must send a keep-alive message if no other PCEP message is sent to the peer at the expiry of this timer. This timer is restarted every time a PCEP message or keep-alive message is sent.

The keep-alive mechanism is asymmetric, meaning that each peer can use a different keep-alive timer value at its end.

The **no** form of the command returns the keep-alive timer to the default value.

Default keepalive 30

Parameters *seconds* — the keep-alive value, in seconds

Values 1 to 255

Platforms All

keepalive

Syntax **keepalive** *deciseconds* **dropcount** *count*

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy keepalive)

Full Context configure isa nat-group inter-chassis-redundancy keepalive

Description This command configures keepalives between the CPMs residing on different chassis. The keepalives are used to detect the presence of the peering node. If the redundant peer connectivity is lost beyond the limit defined by keepalives, then each node in the redundant pair transitions into a standalone mode. Keepalives use UDP transport.

Default keepalive 30 dropcount 2

Parameters *deciseconds* — Specifies the number of keepalives that are transported periodically at intervals defined by this parameter.

Values 2 to 250

count — Specifies the drop count. If the number of consecutive keepalives defined by this parameter is lost, then the peer is considered unreachable and the node transitions into a standalone mode of operation.

Values 2 to 20

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

keepalive

Syntax **keepalive** *seconds*
no keepalive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>router>bgp keepalive)
[Tree] (config>router>bgp>group keepalive)
[Tree] (config>router>bgp>group>neighbor keepalive)

Full Context configure router bgp group keepalive
configure router bgp group neighbor keepalive
configure router bgp keepalive

Description This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires.

The **keepalive** parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **keepalive** value is generally one-third of the **hold-time** interval. Even though the implementation allows the **keepalive** value and the **hold-time** interval to be independently set, under the following circumstances, the configured **keepalive** value is overridden by the **hold-time** value:

- If the specified **keepalive** value is greater than the configured **hold-time**, then the specified value is ignored and the **keepalive** is set to one third of the current **hold-time** value.
- If the specified **hold-time** interval is less than the configured **keepalive** value, then the **keepalive** value is reset to one third of the specified **hold-time** interval.
- If the **hold-time** interval is set to zero, then the configured value of the **keepalive** value is ignored. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default keepalive 30

Parameters *seconds* — Specifies the keepalive timer, in seconds, expressed as a decimal integer.

Values 0 to 21845

Platforms All

keepalive

Syntax **keepalive** [**neighbor** *ip-addr* | **group** *name*]
no keepalive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>router>bgp keepalive)

Full Context debug router bgp keepalive

Description This command decodes and logs all sent and received keepalive messages in the debug log.

The **no** form of this command disables the debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

15.10 keepalive-override

keepalive-override

Syntax **keepalive-override** *keepalive-timer*
no keepalive-override

Context [Tree] (config>mcast-mgmt>mcast-info-policy>bundle keepalive-override)
[Tree] (config>mcast-mgmt>mcast-info-policy>bundle>channel keepalive-override)
[Tree] (config>mcast-mgmt>mcast-info-policy>bundle>channel>source-override keepalive-override)

Full Context configure mcast-management mcast-info-policy bundle channel keepalive-override
configure mcast-management mcast-info-policy bundle channel source-override keepalive-override
configure mcast-management mcast-info-policy bundle keepalive-override

Description This command configures the keepalive timer override. The PIM (S,G) Keepalive Timer (KAT) is used to maintain the (S,G) state when (S,G) join is not received. Expiry of the KAT causes the (S,G) entry to be removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The KAT override configuration is performed with a multicast information policy, which must be applied to the related PIM routing instance. When a KAT override is configured under a channel (a group or a group range), it applies to all (S,G) entries that fall under it, except when the source-override is configured and a KAT override is also configured under the source-override. In this scenario, the specific KAT override must be used for the (S,G) entries that fall under the source-override, while other (S,G) entries under the bundle use the KAT override configured under the channel.

Parameters *keepalive-timer* — Specifies the keepalive timer override, in seconds.

Values 10 to 86000

15.11 kernel

kernel

Syntax **kernel password** *password*
no kernel

Context **[Tree]** (environment kernel)

Full Context environment kernel

Description This command enables and disables the kernel.

Parameters *password* — Specifies the password to access the kernel, up to 256 characters.

Platforms All

15.12 kex

kex

Syntax **kex** *index* **name** *kex-name*
no kex *index*

Context **[Tree]** (config>system>security>ssh>client-kex-list kex)
[Tree] (config>system>security>ssh>server-kex-list kex)

Full Context configure system security ssh client-kex-list kex
configure system security ssh server-kex-list kex

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the user to configure phase 1 SSH v2 KEX algorithms for SR OS as an SSH server or an SSH client. By default, the client and server lists are empty. If the user configures this list, SSH uses the hard-coded list with the first-listed algorithm having the highest priority and so on. An empty server or client list is the default list and contains the following algorithms:

diffie-hellman-group16-sha512

diffie-hellman-group14-sha256

diffie-hellman-group14-sha1

diffie-hellman-group14-sha1

diffie-hellman-group1-sha1

The **no** form of this command removes the specified KEX index. If all KEX indexes are removed, the default list is used again.

Parameters *index* — Specifies the index of the algorithm in the list. The lowest index in the list is negotiated first on the SSH negotiation list, while the highest index is at the bottom of the SSH negotiation list.

Values 1 to 255

kex-name — Specifies the KEX algorithm for computing the shared secret key.

Values diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1

Platforms All

15.13 key

key

Syntax **key packet-type** {**accept** | **request**} **attribute-type** *attribute-type* [**vendor** *vendor-id*]
no key

Context **[Tree]** (config>router>radius-proxy>server>cache key)
[Tree] (config>service>vprn>radius-proxy>server>cache key)

Full Context configure router radius-proxy server cache key
configure service vprn radius-proxy server cache key

Description This command specifies the RADIUS cache key that is used to match the information in subsequent DHCP requests for authorization.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **packet-type** — Specifies the packet type of the RADIUS messages to use to generate the key for the cache of this RADIUS proxy server.

Values accept, request

attribute-type — Specifies the RADIUS attribute type to cache for this RADIUS proxy. server.

Values 1 to 255

vendor-id — Specifies the RADIUS vendor ID.

Values 1 to 16777215, nokia

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

key

Syntax **key** *key-filename*
no key

Context **[Tree]** (config>ipsec>cert-profile>entry key)

Full Context configure ipsec cert-profile entry key

Description This command specifies the filename of an imported key for the **cert-profile entry**.

The **no** form of this command removes the key filename from the entry configuration.

Default no key

Parameters *key-filename* — Specifies the filename of an imported key.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

key

Syntax **key** *password* [**hash** | **hash2** | **custom**] **reference** *reference-number*
no key reference *reference-number*

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2>key-list key)

Full Context configure system security pki ca-profile cmpv2 key-list key

Description This command specifies a pre-shared key used for CMPv2 initial registration. Multiples of key commands are allowed to be configured under this context.

The password and reference-number is distributed by the CA via out-of-band means.

The configured password is stored in configuration file in an encrypted form by using SR OS hash2 algorithm.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the parameters from the configuration.

Parameters *password* — Specifies a printable ASCII string, up to 64 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

reference *reference-number* — Specifies a printable ASCII string, up to 64 characters in length.

Platforms All

key

Syntax **key** *key-filename*
no key

Context **[Tree]** (config>system>security>tls>cert-profile>entry key)

Full Context configure system security tls cert-profile entry key

Description This command specifies the file name of an imported key for the **cert-profile** entry.

The **no** form of the command removes the key.

Default no key

Parameters *key-filename* — Specifies the file name of the key.

Platforms All

15.14 key-list

key-list

Syntax **key-list**

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 key-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security pki ca-profile cmpv2 key-list

Description This command enables the context to configure pre-shared key list parameters.

Platforms All

15.15 key-re-exchange

key-re-exchange

Syntax **key-re-exchange**

Context **[Tree]** (config>system>security>ssh key-re-exchange)

Full Context configure system security ssh key-re-exchange

Description This command enables the key re-exchange context.

Platforms All

15.16 key-rollover-interval

key-rollover-interval

Syntax **key-rollover-interval** *key-rollover-interval*

Context **[Tree]** (config>service>vprn>ospf3>area key-rollover-interval)

Full Context configure service vprn ospf3 area key-rollover-interval

Description This command configures the key rollover interval.

The **no** form of this command reverts to the default.

Default key-rollover-interval 10

Parameters *key-rollover-interval* — Specifies the time, in seconds, after which a key rollover will start.

Values 10 to 300

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

key-rollover-interval

Syntax **key-rollover-interval** *seconds*

Context **[Tree]** (config>router>ospf3>area key-rollover-interval)

Full Context configure router ospf3 area key-rollover-interval

Description This command configures the key rollover interval.

Default key-rollover-interval 10

Parameters *seconds* — Specifies the time, in seconds, after which a key rollover will start.

Values 10 to 300

Platforms All

15.17 key-update

key-update

Syntax **key-update ca** *ca-profile-name* **newkey** *key-filename* **oldkey** *key-filename* **oldcert** *cert-filename* [**hash-alg** *hash-algorithm*] **save-as** *save-path-of-result-cert*

Context **[Tree]** (admin>certificate>cmpv2 key-update)

Full Context admin certificate cmpv2 key-update

Description This command requests a new certificate from the CA to update an existing certificate due to reasons such as **key refresh** or **replacing compromised key**.

In some cases, the CA may not return certificate immediately, due to reasons such as request processing need manual intervention. In such cases, the admin certificate cmpv2 poll command can be used to poll the status of the request.

Parameters *ca-profile-name* — Specifies a ca-profile name which includes CMP server information, up to 32 characters.

newkey *key-filename* — Specifies the key file of the requesting certificate, up to 95 characters.

oldkey *key-filename* — Specifies the key to be replaced, up to 95 characters.

cert-filename — Specifies the file name of an imported certificate to be replaced, up to 95 characters.

hash-algorithm — Specifies the hash algorithm for RSA key.

Values md5,sha1,sha224,sha256,sha384,sha512

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

save-path-of-result-cert — Specifies the save full path name of saving the result certificate, up to 200 characters.

Platforms All

15.18 key-value

key-value

Syntax **key-value** *public-key-value*
no key-value

Context **[Tree]** (config>system>security>user>public-keys>ecdsa>ecdsa-key key-value)
[Tree] (config>system>security>user>public-keys>rsa>rsa-key key-value)

Full Context configure system security user public-keys ecdsa ecdsa-key key-value
configure system security user public-keys rsa rsa-key key-value

Description This command configures a value for the RSA or ECDSA public key. The public key must be enclosed in quotation marks. For RSA, the key is between 768 and 4096 bits. For ECDSA, the key is between 1 and 1024 bits.

Default no key-value

Parameters *public-key-value* — Specifies the public key value, up to 800 characters for RSA and up to 255 characters for ECDSA.

Platforms All

15.19 keychain

keychain

Syntax [**no**] **keychain** *keychain-name*

Context **[Tree]** (config>system>security keychain)

Full Context configure system security keychain

Description This command enables the context to configure keychain parameters. A keychain must be configured on the system before it can be applied to a session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the keychain nodal context and everything under it from the configuration. If the keychain to be removed is in use when the no keychain command is entered, the command will not be accepted and an error indicating that the keychain is in use will be printed.

Parameters *keychain-name* — Specifies a keychain name which identifies this particular keychain entry.

Values An ASCII string up to 32 characters.

Platforms All

15.20 keygroup-name

keygroup-name

Syntax **keygroup-name** *keygroup-name*
no keygroup-name

Context **[Tree]** (config>grp-encryp>encryp-keygrp keygroup-name)

Full Context configure group-encryption encryption-keygroup keygroup-name

Description This command is used to name the key group. The key group name can be used to reference a key group when configuring services or displaying information.

The **no** form of the command reverts to the default value.

Parameters *keygroup-name* — The name of the key group, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

15.21 kill-session

kill-session

Syntax [**no**] **kill-session**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization kill-session)

Full Context configure system security profile netconf base-op-authorization kill-session

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command authorizes a user associated with the profile to send a NETCONF <kill-session> operation. This kill session operation allows a NETCONF client to kill another NETCONF session, but not the session in which the operation is requested.

The **no** form of the command denies the user from requesting a kill-session.

Default no kill-session

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16 I Commands

16.1 l2

l2

Syntax [**no**] **l2**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>type l2)

Full Context configure subscriber-mgmt wlan-gw tunnel-query type l2

Description This command enables matching on Layer 2 tunnels.

The **no** form of this command disables matching on Layer 2 access points, unless no other tunnel type specifier is configured.

Default no l2

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

l2

Syntax [**no**] **l2**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state l2)

Full Context configure subscriber-mgmt wlan-gw ue-query state l2

Description This command enables matching on UEs in a Layer 2 wholesale state.

The **no** form of this command disables matching on UEs in a Layer 2 wholesale state, unless all state matching is disabled.

Default no l2

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.2 l2-access-id-alias

l2-access-id-alias

Syntax **l2-access-id-alias** *string*
no l2-access-id-alias

Context **[Tree]** (config>service>vpls>sap>pfcp l2-access-id-alias)

Full Context configure service vpls sap pfcp l2-access-id-alias

Description This command defines a Layer 2 access ID alias for the capture SAP. It replaces the default underlying port-based or LAG-based Layer 2 access ID. Different capture SAPs on the same underlying port or LAG can have different Layer 2 access ID aliases.

The **no** form of the command removes the configuration.

Parameters *string* — Specifies the Layer 2 access ID alias, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.3 l2-access-points

l2-access-points

Syntax **l2-access-points**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw l2-access-points)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw l2-access-points)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-access-points
configure service vprn subscriber-interface group-interface wlan-gw l2-access-points

Description Commands in this context configure Layer 2 access points in WLAN gateway group interfaces.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.4 l2-ap

l2-ap

Syntax **l2-ap** *sap-id* [**create**]
no l2-ap *sap-id*

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>l2-access-points l2-ap)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>l2-access-points l2-ap)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-access-points l2-ap
configure service vprn subscriber-interface group-interface wlan-gw l2-access-points l2-ap

Description This command adds a specific SAP where Layer 2 WLAN gateway aggregation is performed. The following SAPs are supported:

- Ethernet
- LAG
- MPLS pseudowire SDPs

This command can be repeated multiple times to create multiple Layer 2 access points.

The **no** form of this command removes the Layer 2 access point. This is only allowed if the Layer 2 access point SAP is shutdown.

Parameters *sap-id* — Specifies SAP to be created.

create — Keyword used to create the Layer 2 WLAN gateway aggregation instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.5 l2-ap-auto-sub-id-fmt

l2-ap-auto-sub-id-fmt

Syntax **l2-ap-auto-sub-id-fmt** {**include-ap-tags** | **sap-only**}

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw l2-ap-auto-sub-id-fmt)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw l2-ap-auto-sub-id-fmt)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-ap-auto-sub-id-fmt
configure service vprn subscriber-interface group-interface wlan-gw l2-ap-auto-sub-id-fmt

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the contents of the auto-generated subscriber ID when the **ipoe-sub-id-key** command is set to include **sap-id** and the **def-sub-id** command is configured with **use-auto-id**. The VLANs must be configured so that the subscriber ID length is not exceeded.

This command can include either the SAP or the SAP + AP delimiting tags.

The **no** form of this command reverts to the default configuration.

Default l2-ap-auto-sub-id-fmt include-ap-tags

Parameters **include-ap-tags** — Specifies that the SAP + AP delimiting tags is used.

sap-only — Specifies that the SAP only is used.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.6 l2-ap-encap-type

l2-ap-encap-type

Syntax **l2-ap-encap-type** {**null** | **dot1q** | **qinq**}

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw l2-ap-encap-type)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw l2-ap-encap-type)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-ap-encap-type
configure service vprn subscriber-interface group-interface wlan-gw l2-ap-encap-type

Description This parameter specifies the number of AP identifying VLAN tags for an AP. This is the default value that can be overridden per SAP. This value must be at least equal to the number of VLANs configured in the SAP or enabling a SAP will fail.

A SAP VLAN is explicitly configured, for example **l2-ap 1/1/1:25**. Other VLANs on the same port can still be used in other contexts.

The number of VLAN tags Epiped to the WLAN gateway IOM equals the **l2-ap-encap-type** minus the encaps of the SAP. Upon receipt of a packet, these VLANs are stored as a Layer 2 tunnel identifier, and are only used in context of WLAN gateway.

The **no** form of this command sets the default value.

Default l2-ap-encap-type null

Parameters **null** — Both the SAP and the AP are not VLAN-tagged.

dot1q — Either the AP or the SAP uses one VLAN tag.

qinq — Up to two VLAN tags are used by the AP or SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.7 l2-aware

l2-aware

Syntax **l2-aware**

Context **[Tree]** (config>service>vprn>nat>inside l2-aware)

Full Context configure service vprn nat inside l2-aware

Description Commands in this context configure parameters specific to Layer2-Aware NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

l2-aware

Syntax **l2-aware**

Context **[Tree]** (config>router>nat>inside l2-aware)

Full Context configure router nat inside l2-aware

Description Commands in this context configure Layer2-Aware NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

l2-aware

Syntax **l2-aware subscriber** *sub-ident-string* **ip** *ip-address* **protocol** {**tcp** | **udp**} [**port** *port*] [**outside-ip** *ip-address*] [**outside-port** *port*] [**nat-policy** *policy-name*] [**member** *member-id*] [**port-range-start** *port*]
no l2-aware subscriber *sub-ident-string* **ip** *ip-address* **protocol** {**tcp** | **udp port** *port*

Context **[Tree]** (config>service>nat>fwd l2-aware)

Full Context configure service nat port-forwarding l2-aware

Description This command creates NAT static port forwards for Layer2-Aware subscribers. The ESM subscriber must be present in the system before this command is executed. The **no** form of the command deletes NAT static port forwards for Layer2-Aware subscribers.

Default none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **subscriber** *sub-ident-string* — This mandatory parameter specifies the ESM subscriber for which the SPF is to be created; ESM subscriber must be present in the system before the SPF can be created.

ip *ip-address* — This mandatory parameter specifies the source IPv4/IPv6 address for which SPF will be created.

protocol {**tcp** | **udp**} — This mandatory parameter specifies the protocol to use, either TCP or UDP.

port *port* — This optional parameter specifies a source port.

Values 1 to 65535

outside-ip *ipv4-address* — This mandatory parameter specifies the outside IPv4 address. If the outside IPv4 address is specified, then all other optional parameters become mandatory.

outside-port *port* — This optional parameter specifies the outside port.

nat-policy *policy-name* — If multiple NAT policies are used inside the routing context, then the NAT policy should be specified in the SPF request so the SPF is created in the correct NAT pool. Otherwise, the default NAT policy from the inside routing context will be used.

member *member-id* — This optional parameter should not be used by the operator. It is used only if the command is replayed via the **exec** command or at **boot-config**. The member ID indicates the identifier of the NAT ISA group member associated with this NAT subscriber.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.8 l2-aware-ip-address

l2-aware-ip-address

Syntax **l2-aware-ip-address** *ip-address*
l2-aware-ip-address from-pool
no l2-aware-ip-address

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp l2-aware-ip-address)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp l2-aware-ip-address)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp l2-aware-ip-address
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp l2-aware-ip-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Layer2-Aware NAT inside IP address to be assigned via DHCP on the WLAN-GW ISA.

If the **from-pool** parameter is specified instead of an IPv4 address, a unique address is allocated to each UE. The pool used is managed by the dhcpv4-nat pool manager, configured under the same subscriber interface. This option is only available when **auth-on-dhcp** is also configured.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the Layer2-Aware NAT inside IP address.

from-pool — Specifies that the Layer2-Aware IP address is allocated from a pool.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.9 l2-aware-nat-bypass

l2-aware-nat-bypass

Syntax [**no**] **l2-aware-nat-bypass**

Context **[Tree]** (config>filter>ip-filter>entry>action l2-aware-nat-bypass)

Full Context configure filter ip-filter entry action l2-aware-nat-bypass

Description This command enables bypassing NAT for packets pertaining to L2-Aware hosts and matching this entry. This action is only applicable to L2-Aware NAT subscribers and it must be configured together with **action forward**. Traffic identified in the match condition bypasses L2-Aware NAT. A common use case is to bypass NAT for on-net destinations (within the customer network).

Traffic that is not classified for bypass is automatically diverted to L2-Aware NAT, unless it is explicitly configured in the IP filter to be dropped.

For selective NAT bypass to take effect, in addition to the IP filter configuration, the L2-Aware NAT subscriber must be specifically enabled for selective bypass via the **nat-allow-bypass** configuration option in the NAT CLI node in the SLA profile.

The **no** form of this command automatically diverts traffic to L2-Aware NAT, unless it is explicitly configured in the IP filter to be dropped.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.10 l2-aware-sub

l2-aware-sub

Syntax [**no**] **l2-aware-sub** *sub-ident-string*

Context **[Tree]** (config>li>li-source>nat l2-aware-sub)

Full Context configure li li-source nat l2-aware-sub

Description This command configures a Layer-2-Aware subscriber source.

The **no** form of this command removes the values from the configuration.

Parameters *sub-ident-string* — Specifies a source name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.11 l2-inner-vlan

l2-inner-vlan

Syntax **l2-inner-vlan** *q-tag*
no l2-inner-vlan

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query l2-inner-vlan)

Full Context configure subscriber-mgmt wlan-gw tunnel-query l2-inner-vlan

Description This command enables matching on a Layer 2 access point with a specified C-VLAN.

The **no** form of this command disables matching on a C-VLAN.

Default no l2-inner-vlan

Parameters *q-tag* — Specifies the *q-tag* for the C-VLAN.

Values 0 to 4095

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.12 l2-ip

l2-ip

Syntax [**no**] **l2-ip**

Context **[Tree]** (config>cflowd>collector>export-filter>family l2-ip)

Full Context configure cflowd collector export-filter family l2-ip

Description This command filters Layer 2 IP flow data from being sent to the associated collector.

The **no** form of this command removes the filter, allowing Layer 2 IP flow data to be sent to the associated collector.

Default no l2-ip

Platforms All

16.13 l2-outer-vlan

l2-outer-vlan

Syntax **l2-outer-vlan** *q-tag*
no l2-outer-vlan

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query l2-outer-vlan)

Full Context configure subscriber-mgmt wlan-gw tunnel-query l2-outer-vlan

Description This command enables matching on a Layer 2 access point with a specified S-VLAN.

The **no** form of this command disables matching on an S-VLAN.

Default no l2-outer-vlan

Parameters *q-tag* — Specifies the *q-tag* for the S-VLAN.

Values 0 to 4095

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.14 l2-outside

l2-outside

Syntax **l2-outside**
no l2-outside

Context **[Tree]** (config>service>nat>nat-policy l2-outside)
[Tree] (config>service>nat>firewall-policy l2-outside)

Full Context configure service nat firewall-policy l2-outside
configure service nat nat-policy l2-outside

Description This command configures a NAT policy to be used with a Layer 2 outside service instead of a Layer 3 outside service. This command and the **pool** command are mutually exclusive.

Default no l2-outside

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy l2-outside

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy l2-outside

16.15 l2-sap

l2-sap

Syntax **l2-sap** *sap-id*
no l2-sap

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query l2-sap)

Full Context configure subscriber-mgmt wlan-gw tunnel-query l2-sap

Description This command enables matching on Layer 2 access points active on the specified SAP.

The **no** form of this command disables matching on the SAP.

Default no l2-sap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sap-id* — Specifies the SAP ID. For details on SAP ID parameter values, refer to section *Monitor CLI Commands* in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.16 l2-service

l2-service

Syntax **l2-service** *service-id*
no l2-service

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range l2-service)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range l2-service)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range l2-service
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range l2-service

Description This command specifies the VPLS service used for L2 wholesale. When such a service is configured no other configuration is allowed under the vlan-range.

The **no** form of this command removes the L2 wholesale service, this is only allowed if the l2-service node is shut down.

Parameters *service-id* — Specifies the VPLS service ID to use for Layer 2 wholesale.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.17 l2pt-termination

l2pt-termination

Syntax **l2pt-termination** [**cdp**] [**dtp**] [**pagp**] [**stp**] [**udld**] [**vtp**]
no l2pt-termination

Context **[Tree]** (config>service>vpls>sap l2pt-termination)
[Tree] (config>service>template>vpls-sap-template l2pt-termination)
[Tree] (config>service>vpls>spoke-sdp l2pt-termination)

Full Context configure service template vpls-sap-template l2pt-termination

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap l2pt-termination
configure service vpls spoke-sdp l2pt-termination

Description This command enables Layer 2 Protocol Tunneling (L2PT) termination on a specified SAP or spoke-SDP. L2PT termination is supported only for STP BPDUs. PDUs of other protocols are discarded.

This feature can be enabled only if STP is disabled in the context of the specified VPLS service.

The **no** form of this command reverts to the default.

Default no l2pt-termination

Parameters **cdp** — Specifies the Cisco discovery protocol

dtp — Specifies the dynamic trunking protocol

pagp — Specifies the port aggregation protocol

stp — Specifies all spanning tree protocols: stp, rstp, mstp, pvst (default)

udld — Specifies unidirectional link detection

vtp — Specifies the virtual trunk protocol

Platforms All

l2pt-termination

Syntax **l2pt-termination** [**cdp**] [**dtp**] [**pagp**] [**stp**] [**udld**] [**vtp**]
no l2pt-termination

Context **[Tree]** (config>service>pw-template l2pt-termination)

Full Context configure service pw-template l2pt-termination

Description This command enables Layer 2 Protocol Tunneling (L2PT) termination on a given SAP or spoke SDP. L2PT termination will be supported only for STP BPDUs. PDUs of other protocols will be discarded.

This feature can be enabled only if STP is disabled in the context of the given VPLS service.

Default no l2pt-termination

Parameters **cdp** — Specifies the Cisco discovery protocol.

dtp — Specifies the dynamic trunking protocol.

pagp — Specifies the port aggregation protocol.

stp — Specifies all spanning tree protocols: stp, rstp, mstp, pvst (default).

udld — Specifies unidirectional link detection.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vtp — Specifies the virtual trunk protocol.

Platforms All

16.18 l2tp

l2tp

Syntax **l2tp**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host l2tp)

Full Context configure subscriber-mgmt local-user-db ppp host l2tp

Description Commands in this context configure L2TP parameters for the host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

l2tp

Syntax **l2tp**

Context **[Tree]** (config>router l2tp)

Full Context configure router l2tp

Description Commands in this context configure L2TP parameters. L2TP extends the PPP model by allowing Layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

l2tp

Syntax [**no**] **l2tp**

Context **[Tree]** (debug>router l2tp)
[Tree] (debug>router>l2tp>assignment-id>packet l2tp)
[Tree] (debug>router>l2tp>group>packet l2tp)
[Tree] (debug>router>l2tp>packet l2tp)
[Tree] (debug>router>l2tp>peer>packet l2tp)

Full Context debug router l2tp
debug router l2tp assignment-id packet l2tp
debug router l2tp group packet l2tp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router l2tp packet l2tp
debug router l2tp peer packet l2tp

Description This command sets debugging for L2TP packets.

The **no** form of this command removes the settings of debugging for L2TP packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

l2tp

Syntax [**no**] **l2tp**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync l2tp)

Full Context configure redundancy multi-chassis peer sync l2tp

Description This command enables L2TP.

The **no** form of this command disables L2TP.

Platforms All

l2tp

Syntax **l2tp** [**terminate-only**]
no l2tp

Context **[Tree]** (debug>service>id>ppp>event l2tp)

Full Context debug service id ppp event l2tp

Description This command enables PPP L2TP event debug.

Parameters **terminate-only** — Enables debug for local terminated PPP session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

l2tp

Syntax [**no**] **l2tp**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>type l2tp)

Full Context configure subscriber-mgmt wlan-gw tunnel-query type l2tp

Description This command enables matching on L2TP tunnels.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables matching on L2TP tunnels, unless no other tunnel type specifier is configured.

Default no l2tp

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

l2tp

Syntax [**no**] **l2tp**

Context **[Tree]** (config>service>vprn l2tp)

Full Context configure service vprn l2tp

Description Commands in this context configure L2TP parameters. L2TP extends the PPP model by allowing Layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

l2tp

Syntax **l2tp**

Context **[Tree]** (config>test-oam>build-packet>header l2tp)
[Tree] (debug>oam>build-packet>packet>field-override>header l2tp)

Full Context configure test-oam build-packet header l2tp
debug oam build-packet packet field-override header l2tp

Description This command causes the associated header to be defined as an L2TP header template and enables the context to define the L2TP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.19 l2tp-accounting-policy

l2tp-accounting-policy

Syntax **l2tp-accounting-policy** *policy-name* [**create**]
no l2tp-accounting-policy *policy-name*

Context **[Tree]** (config>aaa l2tp-accounting-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa l2tp-accounting-policy

Description This command configures an L2TP accounting policy.

The **no** form of this command removes the policy-name from the configuration.

Parameters *policy-name* — Specifies a policy name.

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.20 l2tp-lns

l2tp-lns

Syntax **l2tp-lns** *max-nr-of-sessions*
no l2tp-lns

Context **[Tree]** (config>subscr-mgmt>sla-profile>session-limits l2tp-lns)
[Tree] (config>subscr-mgmt>sub-profile>session-limits l2tp-lns)

Full Context configure subscriber-mgmt sla-profile session-limits l2tp-lns
configure subscriber-mgmt sub-profile session-limits l2tp-lns

Description This command configures the maximum number of L2TP LNS sessions per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of L2TP LNS sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of L2TP LNS sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.21 l2tp-load-balancing

l2tp-load-balancing

Syntax [**no**] **l2tp-load-balancing**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>load-balancing l2tp-load-balancing)

Full Context configure system load-balancing l2tp-load-balancing

Description This command enables the inclusion of the L2TPv2 session ID into the load-balancing hash algorithm to induce more variation and better load distribution over available links and next-hops.

The **no** form of this command disables the inclusion of the session-id.

Platforms All

16.22 l2tp-lts

l2tp-lts

Syntax **l2tp-lts** *max-nr-of-sessions*
no l2tp-lts

Context [Tree] (config>subscr-mgmt>sla-profile>session-limits l2tp-lts)
[Tree] (config>subscr-mgmt>sub-profile>session-limits l2tp-lts)

Full Context configure subscriber-mgmt sla-profile session-limits l2tp-lts
configure subscriber-mgmt sub-profile session-limits l2tp-lts

Description This command configures the maximum number of L2TP LTS sessions per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of L2TP LTS sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of L2TP LTS sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.23 l2tp-overall

l2tp-overall

Syntax **l2tp-overall** *max-nr-of-sessions*
no l2tp-overall

Context [Tree] (config>subscr-mgmt>sla-profile>session-limits l2tp-overall)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>subscr-mgmt>sub-profile>session-limits l2tp-overall)

Full Context configure subscriber-mgmt sla-profile session-limits l2tp-overall
configure subscriber-mgmt sub-profile session-limits l2tp-overall

Description This command configures the maximum number of L2TP sessions per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of L2TP sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of L2TP sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.24 l2tp-tunnel-id-range

l2tp-tunnel-id-range

Syntax **l2tp-tunnel-id-range start** *l2tp-tunnel-id* **end** *l2tp-tunnel-id*
no l2tp-tunnel-id-range

Context [Tree] (config>redundancy>multi-chassis>peer>sync>track-srrp-instances>track-srrp l2tp-tunnel-id-range)

Full Context configure redundancy multi-chassis peer sync track-srrp-instances track-srrp l2tp-tunnel-id-range

Description This command sets the tunnel-id range that is used to allocate a new tunnel-id for a tunnel for which multi-chassis redundancy is configured to this MCS peer.

The **no** form of this command reverts to the default.

Parameters **start** *l2tp-tunnel-id* — Specifies the start of the range of L2TP tunnel identifiers that can be allocated by L2TP on this system, to be synchronized with Multi Chassis Redundancy Synchronization (MCS).

Values 1 to 16383

end *l2tp-tunnel-id* — Specifies the end of the range of L2TP tunnel identifiers that can be allocated by L2TP on this system, to be synchronized with Multi Chassis Redundancy Synchronization (MCS).

Values 1 to 16383

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.25 l2tpv3

l2tpv3

Syntax **l2tpv3**

Context **[Tree]** (config>router>l2tp l2tpv3)
[Tree] (config>router>l2tp>group l2tpv3)
[Tree] (config>router>l2tp>group>tunnel l2tpv3)
[Tree] (config>service>vprn>l2tp l2tpv3)
[Tree] (config>service>vprn>l2tp>group l2tpv3)
[Tree] (config>service>vprn>l2tp>group>tunnel l2tpv3)

Full Context configure router l2tp group l2tpv3
configure router l2tp group tunnel l2tpv3
configure router l2tp l2tpv3
configure service vprn l2tp group l2tpv3
configure service vprn l2tp group tunnel l2tpv3
configure service vprn l2tp l2tpv3

Description Commands in this context configure L2TPv3 parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

l2tpv3

Syntax **l2tpv3**

Context **[Tree]** (config>service>epipe>spoke-sdp>egress l2tpv3)
[Tree] (config>service>epipe>spoke-sdp>ingress l2tpv3)

Full Context configure service epipe spoke-sdp egress l2tpv3
configure service epipe spoke-sdp ingress l2tpv3

Description Commands in this context configure L2TPv3 spoke SDPs for Epipe services.

Platforms All

l2tpv3

Syntax **l2tpv3**

Context **[Tree]** (config>mirror>mirror-dest>spoke-sdp>egress l2tpv3)
[Tree] (config>mirror>mirror-dest>spoke-sdp>ingress l2tpv3)
[Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp>ingress l2tpv3)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure mirror mirror-dest remote-source spoke-sdp ingress l2tpv3
configure mirror mirror-dest spoke-sdp egress l2tpv3
configure mirror mirror-dest spoke-sdp ingress l2tpv3

Description Commands in this context configure an RX/TX cookie for L2TPv3 egress spoke SDP or for the remote-source ingress spoke SDP.

Platforms All

16.26 l2tpv3-session

l2tpv3-session

Syntax **l2tpv3-session** [**create**]
no l2tpv3-session

Context **[Tree]** (config>service>epipe>sap l2tpv3-session)
[Tree] (config>service>vpls>sap l2tpv3-session)

Full Context configure service epipe sap l2tpv3-session
configure service vpls sap l2tpv3-session

Description This command creates the configuration context to define the L2TPv3 tunnel parameters.

The **no** form of this command deletes the L2TPv3 configuration context.

Parameters **create** — This keyword is mandatory while creating a L2TPv3 session.

Platforms All

16.27 l2w

l2w

Syntax [**no**] **l2w**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>ue-state l2w)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ue-state l2w

Description This command enables matching on tunnels with L2W UEs.

The **no** form of this command disables matching on L2W UEs, unless UE state matching is disabled altogether.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no l2w

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.28 l3-ring

l3-ring

Syntax **l3-ring** *name* [**create**]
no l3-ring name

Context **[Tree]** (config>redundancy>mc>peer>mcr l3-ring)

Full Context configure redundancy multi-chassis peer mc-ring l3-ring

Description This command configures a Layer 3 multi-chassis ring.

The **no** form of this command reverts to the default.

Platforms All

16.29 l4-load-balancing

l4-load-balancing

Syntax [**no**] **l4-load-balancing**

Context **[Tree]** (config>system>load-balancing l4-load-balancing)

Full Context configure system load-balancing l4-load-balancing

Description This command configures system-wide Layer 4 load balancing. The configuration at the system level can enable or disable load balancing based on Layer 4 fields. If enabled, the Layer 4 source and destination port fields will be included in hashing calculation for TCP/UDP packets.

The hashing algorithm addresses finer spraying granularity where many hosts are connected to the network.

To address more efficient traffic distribution between network links (forming a LAG group), a hashing algorithm extension takes into account L4 information (that is, src/dst L4-protocol port).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The hashing index can be calculated according to the following algorithm:

```
If [(TCP or UDP traffic) & enabled]
  hash (TCP/UDP ports, IP addresses)
else if (IP traffic)
  hash (IP addresses)
else
  hash (MAC addresses)
endif
```

This algorithm will be used in all cases where IP information in per-packet hashing is included (refer to "Traffic Load Balancing Options" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*). However, the Layer 4 information (TCP/UDP ports) will not be used for fragmented packets.

Default no l4-load-balancing

Platforms All

16.30 l4-src-port

l4-src-port

Syntax **l4-src-port** *port* [*mask*]
no l4-src-port

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry l4-src-port)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry l4-src-port)

Full Context configure system security management-access-filter ip-filter entry l4-src-port
configure system security management-access-filter ipv6-filter entry l4-src-port

Description This command configures a destination TCP or UDP port number or port range for a management access filter match criterion.

The **no** form of this command reverts to the default values.

Default no l4-src-port

Parameters *port* — Specifies the destination TCP or UDP port number as a match criterion.

Values 1 to 65535

Default 6 (exact match)

mask — Specifies the mask used to select a range of source port numbers. Table 71 lists the format styles to configure the 16-bit mask.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 71 **Format Styles to Configure Mask**

Format Style	Format Syntax	Example
Decimal	DDDDD	63488
Hexadecimal	0xHHHH	0xF800
Binary	0bBBBBBBBBBBBBBBB	0b1111100000000000

To select a range from 1024 up to 2047, specify 1024 and 0xFC00 for port and maskrespectively.

Values 1 to 65535 (decimal)

Default 65535 (exact match)

Platforms All

16.31 label

label

Syntax **label** [**detail**]
no label

Context **[Tree]** (debug>router>ldp>peer>packet label)

Full Context debug router ldp peer packet label

Description This command enables debugging for LDP Label packets.

The **no** form of the command disables the debugging output.

Parameters **detail** — Displays detailed information.

Platforms All

label

Syntax **label** *label*
no label

Context **[Tree]** (config>test-oam>build-packet>header>mpls label)
[Tree] (debug>oam>build-packet>packet>field-override>header>mpls label)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure test-oam build-packet header mpls label
debug oam build-packet packet field-override header mpls label

Description This command defines the MPLS value to be used in the MPLS header.

The **no** form of this command removes the label value.

Default label 0

Parameters *label* — Specifies the MPLS label to be used in the MPLS header.

Values 0 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

label

Syntax [**no**] **label** *label*

Context **[Tree]** (debug>router>rib-api label)

Full Context debug router rib-api label

Description This command enables debugging for the specified RIB-API label.

Parameters *label* — Specifies the label of the specified RIB-API entry.

Values 32 to 1048575

Platforms All

16.32 label-allocation

label-allocation

Syntax **label-allocation**

Context **[Tree]** (config>router>bgp label-allocation)

Full Context configure router bgp label-allocation

Description This commands enables the context to configure the allocation of MPLS labels to specific BGP routes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.33 label-block

label-block

Syntax **label-block** *name*
no label-block

Context **[Tree]** (conf>router>segment-routing>srv6>loc>static-function label-block)

Full Context configure router segment-routing segment-routing-v6 locator static-function label-block

Description This command configures a reserved label block name to be used in the termination of services on the SRv6 FPE.

Static values of the service SID function are mapped to label values drawn from this reserved label block. A static function value of 1 maps to the first label in this label block and so on.

Dynamic values of service SID function are mapped to label values drawn from the dynamic label range.

An End or End.X function does not map to a label value.

The **no** form of this command removes the label block name from the configuration.

Default no label-block

Parameters *name* — Specifies a reserved label block name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

16.34 label-ipv4

label-ipv4

Syntax **label-ipv4 max-paths** [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no label-ipv4

Context **[Tree]** (config>service>vprn>bgp>multi-path label-ipv4)

Full Context configure service vprn bgp multi-path label-ipv4

Description This command sets ECMP multipath parameters that apply only to the label IPv4 unicast address family. These settings override the values set by the **maximum-paths** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

To qualify as a multipath, a non-best route must meet the following criteria (some criteria are controlled by this command):

- The multi-path route must be the same type of route as the best path (same AFI/SAFI and, in some cases, same next-hop resolution method).
- The multi-path route must be tied with the best path for all criteria of greater significance than next-hop cost, except for criteria that are configured to be ignored.
- If the best path selection reaches the next-hop cost comparison, the multi-path route must have the same next-hop cost as the best route unless the **unequal-cost** option is configured.
- The multi-path route must not have the same BGP next-hop as the best path or any other multi-path route.
- The multi-path route must not cause the ECMP limit of the routing instance to be exceeded (configured using the **ecmp** command with a value in the range 1 to 64).
- The multi-path route must not cause the applicable *max-paths* limit to be exceeded. If the best path is an EBGP learned route and the **ebgp** option is used, the *ebgp-max-paths* limit overrides the *max-paths* limit. If the best path is an IBGP-learned route and the **ibgp** option is used, the *ibgp-max-paths* limit overrides the *max-paths* limit. All path limits are configurable up to a maximum of 64. Multi-path is effectively disabled if a value is set to 1.
- The multi-path route must have the same neighbor AS in its AS path as the best path if the **restrict same-neighbor-as** option is configured. By default, any path with the same AS path length as the best path (regardless of neighbor AS) is eligible for multi-path.
- The route must have the same AS path as the best path if the **restrict exact-as-path** option is configured. By default, any path with the same AS path length as the best path (regardless of the actual AS numbers) is eligible for multi-path.

The **no** form of this command removes label-IPv4-specific overrides.

Default no label-ipv4

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

egp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path-as — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

label-ipv4

Syntax **label-ipv4 send** *send-limit*
label-ipv4 send *send-limit* **receive** [**none**]
no label-ipv4

Context **[Tree]** (config>router>bgp>add-paths label-ipv4)
[Tree] (config>router>bgp>group>add-paths label-ipv4)
[Tree] (config>router>bgp>group>neighbor>add-paths label-ipv4)

Full Context configure router bgp add-paths label-ipv4
configure router bgp group add-paths label-ipv4
configure router bgp group neighbor add-paths label-ipv4

Description This command configures the add-paths capability for labeled-unicast IPv4 routes. By default, add-paths is not enabled for labeled-unicast IPv4 routes.

The maximum number of labeled-unicast paths per IPv4 prefix to send is the configured *send-limit*, which is a mandatory parameter. The capability to receive multiple labeled-unicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command, receive capability is enabled by default.

The **no** form of this command disables add-paths support for labeled-unicast IPv4 routes, causing sessions established using add-paths for labeled-unicast IPv4 to go down and come back up without the add-paths capability.

Default no label-ipv4

Parameters *send-limit* — Specifies the maximum number of paths per labeled-unicast IPv4 prefix that are allowed to be advertised to add-paths peers. (The actual number of advertised routes may be less.) If the value is none, the router does not negotiate the send capability with respect to label-IPv4 AFI/SAFI. If the value is **multipaths**, then BGP advertises all the used BGP multipaths for each IPv4 NLRI if the peer has signaled support to receive multiple add paths.

Values 1 to 16, none, multipaths

receive — Specifies the router negotiates to receive multiple labeled-unicast routes per IPv4 prefix.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

none — Specifies that the router does not negotiate to receive multiple labeled-unicast routes per IPv4 prefix.

Platforms All

label-ipv4

Syntax **label-ipv4** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no label-ipv4

Context **[Tree]** (config>router>bgp>multi-path label-ipv4)

Full Context configure router bgp multi-path label-ipv4

Description This command sets ECMP multipath parameters that apply only to the label IPv4 unicast address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

The **no** form of this command removes label-IPv4-specific overrides.

Default no label-ipv4

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

ebgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.35 label-ipv6

label-ipv6

Syntax **label-ipv6 max-paths** [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no label-ipv6

Context **[Tree]** (config>service>vprn>bgp>multi-path label-ipv6)

Full Context configure service vprn bgp multi-path label-ipv6

Description This command sets ECMP multipath parameters that apply only to the label unicast IPv6 address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

To qualify as a multipath, a non-best route must meet the following criteria (some criteria are controlled by this command):

- The multi-path route must be the same type of route as the best path (same AFI/SAFI and, in some cases, same next-hop resolution method).
- The multi-path route must be tied with the best path for all criteria of greater significance than next-hop cost, except for criteria that are configured to be ignored.
- If the best path selection reaches the next-hop cost comparison, the multi-path route must have the same next-hop cost as the best route unless the **unequal-cost** option is configured.
- The multi-path route must not have the same BGP next-hop as the best path or any other multi-path route.
- The multi-path route must not cause the ECMP limit of the routing instance to be exceeded (configured using the **ecmp** command with a value in the range 1 to 64)
- The multi-path route must not cause the applicable *max-paths* limit to be exceeded. If the best path is an EBGP learned route and the **ebgp** option is used, the *ebgp-max-paths* limit overrides the *max-paths* limit. If the best path is an IBGP-learned route and the **ibgp** option is used, the *ibgp-max-paths* limit overrides the *max-paths* limit. All path limits are configurable up to a maximum of 64. Multi-path is effectively disabled if a value is set to 1.
- The multi-path route must have the same neighbor AS in its AS path as the best path if the **restrict same-neighbor-as** option is configured. By default, any path with the same AS path length as the best path (regardless of neighbor AS) is eligible for multi-path.
- The route must have the same AS path as the best path if the **restrict exact-as-path** option is configured. By default, any path with the same AS path length as the best path (regardless of the actual AS numbers) is eligible for multi-path.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes label-IPv6-specific overrides.

Default no label-ipv6

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

egp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path-as — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

label-ipv6

Syntax **label-ipv6 send** *send-limit*
label-ipv6 send *send-limit* **receive** [**none**]
no label-ipv6

Context **[Tree]** (config>router>bgp>add-paths label-ipv6)
[Tree] (config>router>bgp>group>add-paths label-ipv6)
[Tree] (config>router>bgp>group>neighbor>add-paths label-ipv6)

Full Context configure router bgp add-paths label-ipv6
configure router bgp group add-paths label-ipv6
configure router bgp group neighbor add-paths label-ipv6

Description This command configures the add-paths capability for labeled-unicast IPv6 routes. By default, add-paths is not enabled for labeled-unicast IPv6 routes.

The maximum number of labeled-unicast paths per IPv6 prefix to send is the configured *send-limit*, which is a mandatory parameter. The capability to receive multiple labeled-unicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command, receive capability is enabled by default.

The **no** form of this command disables add-paths support for labeled-unicast IPv6 routes, causing sessions established using add-paths for labeled-unicast IPv6 to go down and come back up without the add-paths capability.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no label-ipv6

Parameters *send-limit* — Specifies the maximum number of paths per labeled-unicast IPv6 prefix that are allowed to be advertised to add-paths peers. (The actual number of advertised routes may be less.) If the value is none, the router does not negotiate the send capability with respect to label-IPv6 AFI/SAFI. If the value is **multipaths**, then BGP advertises all the used BGP multipaths for each IPv6 NLRI if the peer has signaled support to receive multiple add paths.

Values 1 to 16, none, multipaths

receive — Specifies that the router negotiates to receive multiple labeled-unicast routes per IPv6 prefix.

none — Specifies that the router does not negotiate to receive multiple labeled-unicast routes per IPv6 prefix.

Platforms All

label-ipv6

Syntax **label-ipv6** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no label-ipv6

Context **[Tree]** (config>router>bgp>multi-path label-ipv6)

Full Context configure router bgp multi-path label-ipv6

Description This command sets ECMP multipath parameters that apply only to the label unicast IPv6 address family. These settings override the values set by the **maximum-paths** command.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

The **no** form of this command removes label-IPv6-specific overrides.

Default no label-ipv6

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

ebgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

label-ipv6

Syntax **label-ipv6**

Context **[Tree]** (config>router>bgp>label-allocation label-ipv6)

Full Context configure router bgp label-allocation label-ipv6

Description Commands in this context configure advertised label IPv6 programming rules.

Platforms All

label-ipv6

Syntax **label-ipv6**

Context **[Tree]** (config>service>vprn>bgp>rib-management label-ipv6)

Full Context configure service vprn bgp rib-management label-ipv6

Description Commands in this context configure labeled IPv6 RIB.

Platforms All

16.36 label-ipv6-explicit-null

label-ipv6-explicit-null

Syntax [**no**] **label-ipv6-explicit-null**

Context **[Tree]** (config>router>bgp>next-hop-res>lbl-routes>use-bgp-routes label-ipv6-explicit-null)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bgp next-hop-resolution labeled-routes use-bgp-routes label-ipv6-explicit-null

Description This command allows a labelled IPv6 route with the explicit-null label to be resolved by other labelled IPv6 routes with the explicit-null label, and also by unlabeled IPv4 routes and unlabeled IPv6 routes that are resolved by static routes, interface routes, or tunnels. Up to four levels of recursive resolution are supported when the top route is a labelled IPv6 route with an explicit-null label.

Regardless of setting, a labelled IPv6 route with a regular label (other than explicit-null) is never resolved by other labelled IPv6 routes.

The **no** form of this command disables the label-ipv6-explicit-null functionality. When disabled, a labeled IPv6 route cannot be resolved by other labeled IPv6 routes.

Default no label-ipv6-explicit-null

Platforms All

16.37 label-map

label-map

Syntax [**no**] **label-map** *in-label*

Context **[Tree]** (config>router>mpls>interface label-map)

Full Context configure router mpls interface label-map

Description This command is used on transit routers when a static LSP is defined. The static LSP on the ingress router is initiated using the **config router mpls static-lsp** *lsp-name* command. An *in-label* can be associated with either a **pop** or a **swap** action, but not both. If both actions are specified, the last action specified takes effect.

The **no** form of this command deletes the static LSP configuration associated with the *in-label*.

Parameters *in-label* — Specifies the incoming MPLS label on which to match.

Values 32 to 1023

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.38 label-mode

label-mode

Syntax **label-mode** {**vrf** | **next-hop**}
no label-mode

Context **[Tree]** (config>service>vprn label-mode)

Full Context configure service vprn label-mode

Description This command controls the method by which service labels are allocated to routes exported by the VPRN as BGP-VPN routes. The **vrf** option selects service label per VRF mode while the **next-hop** option selects service label per next-hop mode.

The **no** form of this command sets the mode to the default mode of service label per VRF.

Default no label-mode

Parameters **vrf** — Selects service label per VRF mode.

next-hop — Selects service label per next-hop mode.

Platforms All

16.39 label-preference

label-preference

Syntax **label-preference** *value*
no label-preference

Context **[Tree]** (config>service>vprn>bgp label-preference)
[Tree] (config>service>vprn>bgp>group label-preference)
[Tree] (config>service>vprn>bgp>group>neighbor label-preference)

Full Context configure service vprn bgp group label-preference
configure service vprn bgp group neighbor label-preference
configure service vprn bgp label-preference

Description This command configures the route preference for routes learned from labeled-unicast peers.

This command can be configured at three levels:

- Global level — applies to all peers

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Group level — applies to all peers in the peer-group
- Neighbor level — applies only to the specified peer

The most specific value is used.

The lower the preference, the higher the chance of the route being the active route.

The **no** form of this command used at the global level reverts to the default *value* of 170.

The **no** form of this command used at the group level reverts to the *value* defined at the global level.

The **no** form of this command used at the neighbor level reverts to the *value* defined at the group level.

Default no label-preference

Parameters *value* — Specifies the route preference value.

Values 1 to 255

Platforms All

label-preference

Syntax **label-preference** *value*
no label-preference

Context **[Tree]** (config>router>bgp label-preference)
[Tree] (config>router>bgp>group label-preference)
[Tree] (config>router>bgp>group>neighbor label-preference)

Full Context configure router bgp group label-preference
configure router bgp group neighbor label-preference
configure router bgp label-preference

Description This command configures the route preference for routes learned from labeled-unicast peers.

This command can be configured at three levels:

- Global level — applies to all peers
- Group level — applies to all peers in the peer-group
- Neighbor level — applies only to the specified peer

The most specific value is used.

The lower the preference, the higher the chance of the route being the active route.

The **no** form of this command used at the global level reverts to the default *value* of 170.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no label-preference

Parameters *value* — Specifies the route preference value.

Values 1 to 255

Platforms All

16.40 label-route-local

label-route-local

Syntax **label-route-local** [{**none** | **all**}]

Context **[Tree]** (config>router>ttl-propagate label-route-local)

Full Context configure router ttl-propagate label-route-local

Description This command configures the TTL propagation for locally generated packets which are forwarded over a BGP label route in the Global Routing Table (GRT) context.

For IPv4 and IPv6 packets forwarded using a RFC 3107 label route in the global routing instance, including 6PE, the all value of the command enables TTL propagation from the IP header into all labels in the transport label stack. The none value reverts to the default mode which disables TTL propagation from the IP header to the labels in the transport label stack. This command does not have a no version.

The TTL of the IP packet is always propagated into the RFC 3107 label itself, and this command only controls the propagation into the transport labels, for example, labels of the RSVP or LDP LSP to which the BGP label route resolves and which are pushed on top of the BGP label.

If the BGP peer advertised the implicit-null label value for the BGP label route, the TTL propagation will not follow the configuration described, but will follow the configuration to which the BGP label route resolves:

RSVP LSP shortcut:

- configure router mpls shortcut-local-ttl-propagate

LDP LSP shortcut:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router ldp shortcut-local-ttl-propagate

This feature does not impact packets forwarded over BGP shortcuts. The ingress LER operates in uniform mode by default and can be changed into pipe mode using the configuration of TTL propagation for RSVP or LDP LSP shortcut listed.

Default label-route-local none

Parameters **none** — Specifies that the TTL of the IP packet is not propagated into the transport label stack.

all — Specifies that the TTL of the IP packet is propagated into all labels of the transport label stack.

Platforms All

16.41 label-route-transit

label-route-transit

Syntax **label-route-transit** [{**none** | **all**}]

Context **[Tree]** (config>router>ttl-propagate label-route-transit)

Full Context configure router ttl-propagate label-route-transit

Description This command configures the TTL propagation for transit packets which are forwarded over a BGP label route in the Global Routing Table (GRT) context.

For IPv4 and IPv6 packets forwarded using a RFC 3107 label route in the global routing instance, including 6PE, the all value of the command enables TTL propagation from the IP header into all labels in the transport label stack. The none value reverts to the default mode which disables TTL propagation from the IP header to the labels in the transport label stack. This command does not have a no version.

The TTL of the IP packet is always propagated into the RFC 3107 label itself, and this command only controls the propagation into the transport labels, for example, labels of the RSVP or LDP LSP to which the BGP label route resolves and which are pushed on top of the BGP label.

If the BGP peer advertised the implicit-null label value for the BGP label route, the TTL propagation will not follow the configuration described, but will follow the configuration to which the BGP label route resolves.

RSVP LSP shortcut:

- configure router mpls shortcut-transit-ttl-propagate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

LDP LSP shortcut:

- configure router ldp shortcut-transit-ttl-propagate

This feature does not impact packets forwarded over BGP shortcuts. The ingress LER operates in uniform mode by default and can be changed into pipe mode using the configuration of TTL propagation for the listed RSVP or LDP LSP shortcut.

Default label-route-transit none

Parameters **none** — Specifies that the TTL of the IP packet is not propagated into the transport label stack.

all — Specifies that the TTL of the IP packet is propagated into all labels of the transport label stack.

Platforms All

16.42 label-stack-reduction

label-stack-reduction

Syntax [**no**] **label-stack-reduction**

Context **[Tree]** (config>router>mpls>lsp label-stack-reduction)
[Tree] (config>router>mpls>lsp-template label-stack-reduction)

Full Context configure router mpls lsp label-stack-reduction
configure router mpls lsp-template label-stack-reduction

Description This command enables the label stack size reduction for a SR-TE LSP or SR-TE LSP template.

At a high level, the label stack reduction algorithm attempts to replace a segment of a computed SR-TE LSP path with the farthest node SID on that path that results in using ECMP paths with links which still comply to the TE constraints of the LSP path.

The **no** form of this command returns the command to its default value.

Default no label-stack-reduction

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.43 label-stack-statistics-count

label-stack-statistics-count

Syntax **label-stack-statistics-count** *label-stack-statistics-count*
no label-stack-statistics-count

Context **[Tree]** (config>system>ip>mpls label-stack-statistics-count)

Full Context configure system ip mpls label-stack-statistics-count

Description This command enables the system to collect traffic statistics on the specified number of labels of the MPLS label stack.

The **no** form of this command disables the collecting of traffic statistics.

Default label-stack-statistics-count 1

Parameters *label-stack-statistics-count* — Specifies the number of labels on which the system can collect statistics.

Values 1, 2

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.44 label-withdrawal-delay

label-withdrawal-delay

Syntax **label-withdrawal-delay** *seconds*
no label-withdrawal-delay

Context **[Tree]** (config>router>ldp label-withdrawal-delay)

Full Context configure router ldp label-withdrawal-delay

Description This command specifies configures the time interval (in s), LDP will delay for the withdrawal of FEC-label binding it distributed to its neighbors when FEC is de-activated. When the timer expires, LDP then sends a label withdrawal for the FEC to all its neighbors. This is applicable only to LDP IPv4 prefix FECs and is not applicable to pseudowires (service FECs).

When there is an upper layer (user of LDP) which depends of LDP control plane for failover detection then label withdrawal delay and tunnel-down-damp-time options must be set to 0.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An example is PW redundancy where the primary PW doesn't have its own fast failover detection mechanism and the node depends on LDP tunnel down event to activate the standby PW.

Default no label-withdrawal-delay

Parameters *seconds* — Specifies the time that LDP delays the withdrawal of FEC-label binding it distributed to its neighbors when FEC is de-activated.

Values 3 to 120

Platforms All

16.45 labeled-routes

labeled-routes

Syntax **labeled-routes**

Context **[Tree]** (config>router>bgp>next-hop-res labeled-routes)

Full Context configure router bgp next-hop-resolution labeled-routes

Description Commands in this context configure labeled route options for next-hop resolution.

Platforms All

16.46 lac-overall

lac-overall

Syntax **lac-overall** *max-nr-of-hosts*
no lac-overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits lac-overall)
[Tree] (config>subscr-mgmt>sub-profile>host-limits lac-overall)

Full Context configure subscriber-mgmt sla-profile host-limits lac-overall
configure subscriber-mgmt sub-profile host-limits lac-overall

Description This command configures the maximum number of L2TP LAC hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of L2TP LAC hosts limit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *max-nr-of-hosts* — Specifies the maximum number of L2TP LAC hosts.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.47 lacp

lacp

Syntax **lacp** [**mode**] [**administrative-key** *admin-key*] [**system-id** *system-id*] [**system-priority** *priority*]
no lacp

Context **[Tree]** (config>lag lacp)

Full Context configure lag lacp

Description This command enables the LACP protocol. Per the IEEE 802.1ax standard, the Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner.

If any of the parameters are omitted, the existing configuration is preserved. The default parameter values are used if a parameter is never explicitly configured.

Default no lacp

Parameters **mode** — Specifies the mode in which LACP will operate.

Values **passive** — Starts transmitting LACP packets only after receiving packets.

active — Initiates the transmission of LACP packets.

admin-key — Specifies an administrative key value to identify the channel group on each port configured to use LACP. A random key is assigned by default if a value is not specified when using classic CLI only.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

system-id — Specifies the 48-bit system ID in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff, where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Values 1 to 65535

Default 32768

priority — Specifies the system priority.

Values 0 to 65535

Default 32768

Platforms All

16.48 lacp-mux-control

lacp-mux-control

Syntax **lacp-mux-control** {**coupled** | **independent**}
no lacp-mux-control

Context **[Tree]** (config>lag lacp-mux-control)

Full Context configure lag lacp-mux-control

Description This command configures the type of multiplexing machine control to be used in a LAG with LACP in active/passive modes.

The **no** form of this command disables multiplexing machine control.

Default lacp-mux-control coupled

Parameters **coupled** — Specifies that TX and RX activate together.

independent — Specifies that RX activates independent of TX.

Platforms All

16.49 lacp-system-priority

lacp-system-priority

Syntax **lacp-system-priority** *lacp-system-priority*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no lacp-system-priority

Context [Tree] (config>system lacp-system-priority)

Full Context configure system lacp-system-priority

Description This command configures the Link Aggregation Control Protocol (LACP) system priority on aggregated Ethernet interfaces. LACP allows the operator to aggregate multiple physical interfaces to form one logical interface.

Default lacp-system-priority 32768

Parameters *lacp-system-priority* — Specifies the LACP system priority.

Values 1 to 65535

Platforms All

16.50 lacp-tunnel

lacp-tunnel

Syntax [**no**] **lacp-tunnel**

Context [Tree] (config>port>ethernet lacp-tunnel)

Full Context configure port ethernet lacp-tunnel

Description This command enables LACP packet tunneling for the Ethernet port. When tunneling is enabled, the port will not process any LACP packets but will tunnel them instead. The port cannot be added as a member to a LAG group.

In this context, the **lacp-tunnel** command is supported for Epipe and VPLS services only.

The **no** form of this command disables LACP packet tunneling for the Ethernet port.

Default no lacp-tunnel

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.51 lacp-xmit-interval

lacp-xmit-interval

Syntax **lacp-xmit-interval** {**slow** | **fast**}
no lacp-xmit-interval

Context **[Tree]** (config>lag lacp-xmit-interval)

Full Context configure lag lacp-xmit-interval

Description This command specifies the interval signaled to the peer and tells the peer at which rate it should transmit.

Default lacp-xmit-interval fast

Parameters **slow** — Transmits packets every 30 seconds.

fast — Transmits packets every second.

Platforms All

16.52 lacp-xmit-stdby

lacp-xmit-stdby

Syntax [**no**] **lacp-xmit-stdby**

Context **[Tree]** (config>lag lacp-xmit-stdby)

Full Context configure lag lacp-xmit-stdby

Description This command enables LACP message transmission on standby links.

The **no** form of this command disables LACP message transmission. This command should be disabled for compatibility when using active/standby groups. This forces a timeout of the standby links by the peer. Use the **no** form if the peer does not implement the correct behavior regarding the lacp sync bit.

Default lacp-xmit-stdby

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.53 lag

lag

Syntax **lag** *lag-id* **lacp-key** *admin-key* **system-id** *system-id* [**remote-lag** *remote-lag-id*] **system-priority** *system-priority* **source-bmac-lsb use-lacp-key**
lag *lag-id* **lacp-key** *admin-key* **system-id** *system-id* [**remote-lag** *remote-lag-id*] **system-priority** *system-priority* **source-bmac-lsb** *MAC-Lsb*
lag *lag-id* **lacp-key** *admin-key* **system-id** *system-id* [**remote-lag** *remote-lag-id*] **system-priority** *system-priority*
lag *lag-id* [**remote-lag** *remote-lag-id*]
no lag *lag-id*

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-lag lag)

Full Context configure redundancy multi-chassis peer mc-lag lag

Description This command defines a LAG which is forming a redundant-pair for MC-LAG with a LAG configured on the given peer. The same LAG group can be defined only in the scope of 1 peer. In order MC-LAG to become operational, all parameters (**lacp-key**, **system-id**, **system-priority**) must be configured the same on both nodes of the same redundant pair.

The partner system (the system connected to all links forming MC-LAG) will consider all ports using the same **lacp-key**, **system-id**, **system-priority** as the part of the same LAG. In order to achieve this in MC operation, both redundant-pair nodes have to be configured with the same values. In case of the mismatch, MC-LAG is kept in oper-down status.

Note that the correct CLI command to enable MC LAG for a LAG in **standby-signaling power-off mode** is **lag** *lag-id* [**remote-lag** *remote-lag-id*]. In the CLI help output, the first three forms are used to enable MC LAG for a LAG in LACP mode. MC LAG is disabled (regardless of the mode) for a given LAG with **no lag** *lag-id.*

Parameters *lag-id* — The LAG identifier, expressed as an integer. Specifying the *lag-id* allows the mismatch between lag-id on redundant-pair. If no **lag-id** is specified it is assumed that neighbor system uses the same *lag-id* as a part of the given MC-LAG. If no matching MC-LAG group can be found between neighbor systems, the individual LAGs will operate as usual (no MC-LAG operation is established).

Values 1 to 800

admin-key — Specifies a 16 bit key that needs to be configured in the same manner on both sides of the MC-LAG in order for the MC-LAG to come up.

Values 1 to 65535

system-id — Specifies a 6 byte value expressed in the same notation as MAC address.

Values xx:xx:xx:xx:xx:xx - xx [00 to FF]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-lag-id — Specifies the LAG ID on the remote system.

Values 1 to 800

system-priority — Specifies the system priority to be used in the context of the MC-LAG. The partner system will consider all ports using the same **lacp-key**, **system-id**, and **system-priority** as part of the same LAG.

Values 1 to 65535

MAC-Lsb — Configures the last 16 bit of the MAC address to be used for all traffic ingressing the MC-LAG link(s) or if use-lacp-key option is used, it will only copy the value of lacp-key (redundancy multi-chassis mc-lag lag lacp-key admin-key). The command will fail if the *value* is the same with any of the following configured attributes:

- Source-bmac-lsb assigned to other MC-LAG ports.
- lsb 16 bits value for the source-bmac configured at chassis or BVPLS level

  The first 32 bits will be copied from the source B-MAC of the BVPLS associated with the IVPLS for a specific IVPLS SAP mapped to the MC-LAG. The BVPLS source B-MAC can be provisioned for each BVPLS or can be inherited from the chassis PBB configuration.

Values 1 to 65535 or xx-xx or xx:xx

Platforms All

lag

Syntax **lag** *lag-id* [**name** *lag-name*]
no lag *lag-id*

Context **[Tree]** (config lag)

Full Context configure lag

Description Commands in this context configure Link Aggregation Group (LAG) attributes.

A LAG is used to group multiple ports into one logical link. The aggregation of multiple physical links allows for load sharing and offers seamless redundancy. If one link fails, traffic is redistributed over the remaining links.

Note: For all ports in a LAG group, autonegotiation must be set to “limited” or “off”.

There are three possible settings for autonegotiation, as follows:

- “on” or enabled with full port capabilities advertised
- “off” or disabled where there is no autonegotiation advertisements

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- “limited” where a single speed/duplex is advertised.

When autonegotiation is enabled on a port, the link attempts to automatically negotiate the link speed and duplex parameters; the configured duplex and speed parameters are ignored.

When autonegotiation is disabled on a port, the port does not attempt to autonegotiate and will only operate at the **speed** and **duplex** settings configured for the port.

Note: Disabling autonegotiation on gigabit ports is not allowed. This is in accordance with the IEEE 802.3 specification for gigabit Ethernet, which requires gigabyte to be enabled for far end fault indication.

If the **config**>**port**>**ethernet autonegotiate limited** keyword option is specified, the port will autonegotiate but only advertise the **speed** and **duplex** settings configured for the port. Use the **limited** mode on multi-speed gigabit ports to force gigabit operation while keeping autonegotiation is enabled for compliance with IEEE 801.3.

The system requires autonegotiation to be disabled or limited for ports in a LAG to guarantee a specific port speed.

The **no** form of this command deletes the LAG from the configuration. A LAG can only be deleted while the LAG is administratively shut down. Any dependencies, such as IP-Interface configurations, must be removed from the configuration before the **no lag** command is issued.

Parameters *lag-id* — Specifies the LAG identifier, expressed as an integer.

The LAG ID ranging from 1 to 64 supports up to 64 LAG members and LAG ID above 64 supports 32 LAG members.

Values 1 to 800

lag-name — Specifies an optional LAG name, up to 27 characters.

In model-driven interfaces, the LAG name is used for configuration references and **show** commands. A service provider or administrator can use the defined LAG name to identify and manage LAGs within the SR OS platforms.

In the classic CLI interface, the user must assign a LAG ID to create the LAG. The LAG name is optional and, if specified, must always start with “lag-”. If a name is not specified, SR OS automatically assigns a string version of the LAG ID as “lag-<lag-id>”.

Values lag-<23 chars max>

Platforms All

lag

Syntax **lag** [**lag-id** *lag-id* [**port** *port-id*]] [**all**]
lag [**lag-id** *lag-id* [**port** *port-id*]] [**sm**] [**pkt**] [**cfg**] [**red**] [**iom-upd**] [**port-state**] [**timers**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[**sel-logic**] [**mc**] [**mc-pkt**]
no lag [**lag-id** *lag-id*]

Context [Tree] (debug lag)

Full Context debug lag

Description This command enables debugging for LAG.

Parameters *lag-id* — Specifies the link aggregation group ID.

Values 1 to 800

port-id — Specifies the physical port ID.

Values *slot*/*mda*/*port*

all — Specifies to display all LAG information.

sm — Specifies to display trace LACP state machine.

pkt — Specifies to display trace LACP packets.

cfg — Specifies to display trace LAG configuration.

red — Specifies to display trace LAG high availability.

iom-upd — Specifies to display trace LAG IOM updates.

port-state — Specifies to display trace LAG port state transitions.

timers — Specifies to display trace LAG timers.

sel-logic — Specifies to display trace LACP selection logic.

mc — Specifies to display multi-chassis parameters.

mc-packet — Specifies to display the MC-LAG control packets with valid authentication were received on this system.

Platforms All

lag

Syntax **lag** *lag-id*
no lag

Context [Tree] (config>service>system>bgp-evpn>eth-seg lag)

Full Context configure service system bgp-evpn ethernet-segment lag

Description This command configures a lag-id associated to the Ethernet-Segment. When the Ethernet-Segment is configured as **all-active,** then only a lag or PW port can be associated to the Ethernet-Segment. When the Ethernet-Segment is configured as **single-active**, then a lag, port or sdp can be associated to the Ethernet-Segment. In either case, only one of the four objects can be configured in the Ethernet-Segment. A specified lag can be part of only one Ethernet-Segment.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no lag

Parameters *lag-id* — Specifies the lag-id associated with the Ethernet-Segment.

Values 1 to 800

Platforms All

lag

Syntax **lag** *lag-id*[**:***encap-val*]
no lag

Context **[Tree]** (config>service>vprn>nw-if lag)

Full Context configure service vprn network-interface lag

Description This command binds the interface to a Link Aggregation Group (LAG)

The **no** form of this command removes the LAG id from the configuration.

Parameters *lag-id[:encap-val]* — Specifies the LAG ID.

Values

lag-id	1 to 800
encap-val	0 (for null) 0 to 4094 (for dot1q)

Platforms All

16.54 lag-emulation

lag-emulation

Syntax **lag-emulation**

Context **[Tree]** (config>eth-tunnel lag-emulation)

Full Context configure eth-tunnel lag-emulation

Description Commands in this context configure eth-tunnel loadsharing parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.55 lag-link-map-profile

lag-link-map-profile

Syntax **lag-link-map-profile** *link-map-profile-id*
no lag-link-map-profile

Context **[Tree]** (config>subscr-mgmt>msap-policy lag-link-map-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap lag-link-map-profile)

Full Context configure service vprn subscriber-interface group-interface sap lag-link-map-profile
configure subscriber-mgmt msap-policy lag-link-map-profile

Description This command assigns a pre-configured lag link map profile to a SAP or network interface configured on a LAG or a PW port that exists on a LAG. Once assigned or de-assigned, the SAP or network interface egress traffic is re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Parameters *link-map-profile-id* — Defines a unique LAG link map profile on which the LAG the SAP/network interface exist.

Default 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

lag-link-map-profile

Syntax **lag-link-map-profile** *link-map-profile-id*
no lag-link-map-profile

Context **[Tree]** (config>service>epipe>sap lag-link-map-profile)
[Tree] (config>service>ipipe>sap lag-link-map-profile)

Full Context configure service epipe sap lag-link-map-profile
configure service ipipe sap lag-link-map-profile

Description This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP's/network interface's egress traffic will be re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Default no lag-link-map-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *link-map-profile-id* — An integer from 1 to 64 that defines a unique lag link map profile on the LAG the SAP/network interface exists on.

Platforms All

lag-link-map-profile

Syntax **lag-link-map-profile** *link-map-profile-id*
no lag-link-map-profile

Context **[Tree]** (config>service>vpls>sap lag-link-map-profile)

Full Context configure service vpls sap lag-link-map-profile

Description This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/unassigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Default no lag-link-map-profile

Parameters *link-map-profile-id* — An integer from 1 to 64 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

Platforms All

lag-link-map-profile

Syntax **lag-link-map-profile** *lag-link-map-profile-id*
no lag-link-map-profile

Context **[Tree]** (config>service>ies>if>sap lag-link-map-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap lag-link-map-profile)

Full Context configure service ies interface sap lag-link-map-profile
configure service ies subscriber-interface group-interface sap lag-link-map-profile

Description This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Default no lag-link-map-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *lag-link-map-profile-id* — An integer from 1 to 64 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap lag-link-map-profile

All

- configure service ies interface sap lag-link-map-profile

lag-link-map-profile

Syntax **lag-link-map-profile** *link-map-profile-id*
no lag-link-map-profile

Context **[Tree]** (config>service>vprn>if>sap lag-link-map-profile)

Full Context configure service vprn interface sap lag-link-map-profile

Description This command assigns a pre-configured LAG link map profile to a SAP or network interface configured on a LAG or a PW port that exists on a LAG. Once assigned, the SAP or network interface egress traffic will be re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP or network interface to use per-flow, service or link hash as configured for the service or LAG.

Default no lag-link-map-profile

Parameters *link-map-profile-id* — An integer from 1 to 64 that defines a unique LAG link map profile on which the LAG the SAP or network interface exist.

Platforms All

lag-link-map-profile

Syntax **lag-link-map-profile** *link-map-profile-id*
no lag-link-map-profile

Context **[Tree]** (config>router>if lag-link-map-profile)

Full Context configure router interface lag-link-map-profile

Description This command assigns a preconfigured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/unassigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Default no lag-link-map-profile

Parameters *link-map-profile-id* — An integer from 1 to 32 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

Platforms All

16.56 lag-per-link-hash

lag-per-link-hash

Syntax **lag-per-link-hash class** {*class*} **weight** *weight*
no lag-per-link-hash

Context **[Tree]** (config>subscr-mgmt>sub-profile>egress lag-per-link-hash)

Full Context configure subscriber-mgmt sub-profile egress lag-per-link-hash

Description This command configures weight and class to be used on LAG egress when the LAG uses weighted per-link-hash by subscribers with the profile assigned. Subscribers using profile with lag-per-link-hash default configuration, inherit weight and class from the SAP configuration (1 and 1 respectively if none configured under SAP).

The **no** form of this command restores default configuration.

Parameters *class* — Specifies the class to be used to select a LAG link.

Values 1, 2, 3

Default 1

weight — Specifies the weight to be associated with this SAP when selecting a LAG link.

Values 1 to 1024

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

lag-per-link-hash

Syntax **lag-per-link-hash class** {**1** | **2** | **3**} **weight** [*weight*]
no lag-per-link-hash

Context **[Tree]** (config>service>epipe>sap lag-per-link-hash)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ipipe>sap lag-per-link-hash)
[Tree] (config>service>vpls>sap lag-per-link-hash)

Full Context configure service epipe sap lag-per-link-hash
configure service ipipe sap lag-per-link-hash
configure service vpls sap lag-per-link-hash

Description This command configures weight and class to this SAP to be used on LAG egress when the LAG uses weighted per-link-hash.

The **no** form of this command restores default configuration.

Default no lag-per-link-hash (equivalent to weight 1 class 1)

Platforms All

lag-per-link-hash

Syntax **lag-per-link-hash class** {**1** | **2** | **3**} **weight** *weight*
no lag-per-link-hash

Context [Tree] (config>service>ies>if>sap lag-per-link-hash)
[Tree] (config>service>ies>sub-if>grp-if>sap lag-per-link-hash)

Full Context configure service ies interface sap lag-per-link-hash
configure service ies subscriber-interface group-interface sap lag-per-link-hash

Description This command configures weight and class to this SAP to be used on LAG egress when the LAG uses weighted per-link-hash.

The **no** form of this command restores default configuration.

Default no lag-per-link-hash (equivalent to weight 1 class 1)

Parameters **class** — Specifies the class.

Values 1, 2, 3

weight — Specifies the weight.

Values 1 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap lag-per-link-hash

All

- configure service ies interface sap lag-per-link-hash

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lag-per-link-hash

Syntax **lag-per-link-hash class** {**1** | **2** | **3**} **weight** [**1 to 1024**]
no per-link-hash

Context **[Tree]** (config>service>vprn>nw-if lag-per-link-hash)
[Tree] (config>service>vprn>if>sap lag-per-link-hash)

Full Context configure service vprn interface sap lag-per-link-hash
configure service vprn network-interface lag-per-link-hash

Description This command configures weight and class to this SAP to be used on LAG egress when the LAG uses weighted per-link-hash.

The **no** form of this command restores the default configuration.

Default no lag-per-link-hash (equivalent to weight 1 class 1)

Platforms All

lag-per-link-hash

Syntax **lag-per-link-hash class** *class* **weight** [*weight*]
no lag-per-link-hash

Context **[Tree]** (config>router>if lag-per-link-hash)

Full Context configure router interface lag-per-link-hash

Description This command configures weight and class to this interface to be used on LAG egress when the LAG uses weighted per-link-hash.

The **no** form of this command restores the default configuration (weight 1 class 1).

Default no lag-per-link-hash

Parameters *class* — Specifies the class.

Values 1, 2, 3

weight — Specifies the weight.

Values 1 to 1024

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.57 lag-port-down

lag-port-down

Syntax **lag-port-down** *lag-id* **number-down** *number-lag-port-down* **level** *level-id*
no lag-port-down *lag-id* **number-down** *number-lag-port-down*

Context **[Tree]** (config>router>mcac>policy>bundle>mc-constraints lag-port-down)

Full Context configure router mcac policy bundle mc-constraints lag-port-down

Description This command configures the bandwidth available both at the interface and bundle level when a specific number of ports in a LAG group fail.

The **no** form of this command removes the values from the configuration.

Parameters *lag-id* — Specifies the LAG ID. When the number of ports available in the LAG link is reduced by the number of ports configured in this context then the *level-id* specified here must be applied.

number-lag-port-down — If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

Values 1 to 64 (for 64-link LAG) 1 to 32 (for other LAGs)

level-id — Specifies the amount of bandwidth available within a given bundle for MC traffic for a specified level.

Values 1 to 8

Platforms All

lag-port-down

Syntax [**no**] **lag-port-down** *lag-id*

Context **[Tree]** (config>vrrp>policy>priority-event lag-port-down)

Full Context configure vrrp policy priority-event lag-port-down

Description This command creates the context to configure Link Aggregation Group (LAG) priority control events that monitor the operational state of the links in the LAG.

The **lag-port-down** command configures a priority control event. The event monitors the operational state of each port in the specified LAG. When one or more of the ports enter the operational down state, the event is considered to be set. When all the ports enter the operational up state, the event is considered to be clear. As ports enter the operational up state, any previous set threshold that represents more down ports is considered cleared, while the event is considered to be set.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Multiple unique **lag-port-down** event nodes can be configured within the **priority-event** node up to the maximum of 32 events.

The **lag-port-down** command can reference an arbitrary LAG. The *lag-id* does have to already exist within the system. The operational state of the **lag-port-down** event will indicate:

- Set – non-existent
- Set – one port down
- Set – two ports down
- Set – three ports down
- Set – four ports down
- Set – five ports down
- Set – six ports down
- Set – seven ports down
- Set – eight ports down
- Cleared – all ports up

When the *lag-id* is created, or a port in *lag-id* becomes operationally up or down, the event operational state must be updated appropriately.

When one or more of the LAG composite ports enters the operationally down state or the *lag-id* is deleted or does not exist, the event is considered to be set. When an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instances in-use priority value. As the event transitions from clear to set, a hold-set timer is loaded with the value configured by the events **hold-set** command. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the **hold-set** value, extending the time before another clear can take effect.

The **lag-port-down** event is considered to have a tiered event set state. While the priority impact per number of ports down is totally configurable, as more ports go down, the effect on the associated virtual router instances in-use priority is expected to increase (lowering the priority). When each configured threshold is crossed, any higher thresholds are considered further event sets and are processed immediately with the hold-set timer reset to the configured value of the **hold-set** command. As the thresholds are crossed in the opposite direction (fewer ports down then previously), the priority effect of the event is not processed until the hold-set timer expires. If the number of ports down threshold again increases before the hold-set timer expires, the timer is only reset to the **hold-set** value if the number of ports down is equal to or greater than the threshold that set the timer.

The event contains **number-down** nodes that define the priority delta or explicit value to be used based on the number of LAG composite ports that are in the operationally down state. These nodes represent the event set thresholds. Not all port down thresholds must be configured. As the number of down ports increase, the **number-down** *ports-down* node that expresses a value equal to or less than the number of down ports describes the delta or explicit priority value to be applied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command deletes the specific LAG monitoring event. The event can be removed at anytime. When the event is removed, the in-use priority of all associated virtual router instances must be reevaluated. The events **hold-set** timer has no effect on the removal procedure.

Default no lag-port-down — No LAG priority control events are created.

Parameters *lag-id* — The LAG ID that the specific event is to monitor expressed as a decimal integer. The *lag-id* can only be monitored by a single event in this policy. The LAG may be monitored by multiple VRRP priority control policies. A port within the LAG and the LAG ID itself are considered to be separate entities. A composite port may be monitored with the **port-down** event while the *lag-id* the port is in is monitored by a **lag-port-down** event in the same policy.

Values 1 to 800 (apply to the 7750 SR and 7950 XRS)
1 to 200 (apply to the 7450 ESS)

Platforms All

16.58 lag-usage-optimization

lag-usage-optimization

Syntax [**no**] **lag-usage-optimization**

Context **[Tree]** (config>router>pim lag-usage-optimization)

Full Context configure router pim lag-usage-optimization

Description This command enables the router's usage of the LAG so traffic for a given multicast stream destined to an IP interface using the LAG is sent only to the forwarding complex that owns the LAG link on which it will actually be forwarded.

Changing the value causes the PIM protocol to be restarted.

If this optimization is disabled, the traffic is sent to all forwarding complexes that own at least one link in the LAG.

The **no** form of this command causes the traffic to be sent to all the forwarding complexes that own at least one link in the LAG.

Note: Changes made for multicast hashing cause Layer 4 multicast traffic to not be hashed. This is independent of if **lag-usage-optimization** is enabled or disabled.

Using this command and the **mc-ecmp-hashing-enabled** command on mixed port speed LAGs is not recommended, because some groups may be forwarded incorrectly.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no lag-usage-optimization

Platforms All

16.59 lanext

lanext

Syntax [**no**] **lanext**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw lanext)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw lanext)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext

Description Commands in this context configure HLE parameters.

The **no** form of this command disables the vRGW parameters enabled in this context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

lanext

Syntax [**no**] **lanext**

Context **[Tree]** (config>router>vrgw lanext)

Full Context configure router vrgw lanext

Description Commands in this context configure HLE parameters.

The **no** form of this command disables the context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

lanext

Syntax [**no**] **lanext**

Context **[Tree]** (config>subscr-mgmt>vrgw lanext)

Full Context configure subscriber-mgmt vrgw lanext

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure subscriber management vRGW home HLE parameters.

The **no** form of this command disables the context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.60 lanext-bridge-id

lanext-bridge-id

Syntax [**no**] **lanext-bridge-id**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include lanext-bridge-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute lanext-bridge-id

Description This command enables the system to include the HLE service's bridge ID (Alc-Bridge-Id) in RADIUS accounting packets.

The **no** form of this command excludes the HLE service's bridge ID (Alc-Bridge-Id) from RADIUS accounting packets.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.61 lanext-device-type

lanext-device-type

Syntax [**no**] **lanext-device-type**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include lanext-device-type)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute lanext-device-type

Description This command enables the system to include the HLE host's device type (Alc-HLE-Device-Type) in RADIUS accounting packets.

The **no** form of this command excludes the HLE host's device type (Alc-HLE-Device-Type) from RADIUS accounting packets.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.62 lanext-route-distinguisher

lanext-route-distinguisher

Syntax [**no**] **lanext-route-distinguisher**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include lanext-route-distinguisher)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute lanext-route-distinguisher

Description This command enables the system to include the HLE service's EVPN route distinguisher (Alc-RD) in RADIUS accounting packets.

The **no** form of this command excludes the HLE service's EVPN route distinguisher (Alc-RD) from RADIUS accounting packets.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.63 lanext-route-target

lanext-route-target

Syntax [**no**] **lanext-route-target**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include lanext-route-target)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute lanext-route-target

Description This command enables the system to include the HLE service's EVPN route target (Alc-RT) in RADIUS accounting packets.

The **no** form of this command excludes the HLE service's EVPN route target (Alc-RT) from RADIUS accounting packets.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.64 lanext-vni

lanext-vni

Syntax [**no**] **lanext-vni**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include lanext-vni)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute lanext-vni

Description This command enables the system to include the HLE service's EVPN VXLAN VNI (Alc-Vxlan-VNI) in RADIUS accounting packets.

The **no** form of this command excludes the HLE service's EVPN VXLAN VNI (Alc-Vxlan-VNI) from RADIUS accounting packets.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.65 last-member-query-interval

last-member-query-interval

Syntax **last-member-query-interval** *tenths-of-seconds*
no last-member-query-interval

Context **[Tree]** (config>service>vpls>sap>igmp-snooping last-member-query-interval)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping last-member-query-interval)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping last-member-query-interval)
[Tree] (config>service>vpls>sap>mld-snooping last-member-query-interval)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping last-member-query-interval)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping last-member-query-interval)

Full Context configure service vpls mesh-sdp igmp-snooping last-member-query-interval
configure service vpls mesh-sdp mld-snooping last-member-query-interval
configure service vpls sap igmp-snooping last-member-query-interval
configure service vpls sap mld-snooping last-member-query-interval
configure service vpls spoke-sdp igmp-snooping last-member-query-interval
configure service vpls spoke-sdp mld-snooping last-member-query-interval

Description This command configures the maximum response time used in group-specific queries sent in response to 'leave' messages, and is also the amount of time between two consecutive group-specific queries. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured **last-member-query-interval** is ignored when fast leave is enabled on the SAP or SDP.

The **no** form of this command reverts to the default value.

Default last-member-query-interval 10

Parameters *tenths-of-seconds* — Specifies the frequency, in tenths of a second, at which query messages are sent.

Values 1 to 50

Platforms All

last-member-query-interval

Syntax **last-member-query-interval** *tenths-of-seconds*
no last-member-query-interval

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp last-member-query-interval)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping last-member-query-interval

Description This command configures the maximum response time used in group-specific queries sent in response to leave messages, and is also the amount of time between two consecutive group-specific queries. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

The configured interval is ignored when fast-leave is enabled on the SAP or SDP.

The **no** form of this command reverts to the default.

Default last-member-query-interval 10

Parameters *seconds* — Specifies the frequency, in tenths of seconds, at which query messages are sent.

Values 1 to 50

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

last-member-query-interval

Syntax **last-member-query-interval** *interval*
no last-member-query-interval

Context **[Tree]** (config>service>pw-template>igmp-snooping last-member-query-interval)

Full Context configure service pw-template igmp-snooping last-member-query-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum response time used in group-specific queries sent in response to 'leave' messages, and is also the amount of time between 2 consecutive group-specific queries. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

The configured last-member-query-interval is ignored when fast-leave is enabled on the SAP or SDP.

Default last-member-query-interval 10

Parameters *interval* — Specifies the frequency, in tenths of seconds, at which query messages are sent.

Values 1 to 50

Platforms All

16.66 last-reported-delay-hold

last-reported-delay-hold

Syntax **last-reported-delay-hold** *seconds*
no last-reported-delay-hold

Context **[Tree]** (config>test-oam>link-meas>template last-reported-delay-hold)

Full Context configure test-oam link-measurement measurement-template last-reported-delay-hold

Description This command configures the timer that specifies the wait time before the last reported delay measurement is flushed after a link measurement test enters the operationally down state. The aging timer delays the flushing of the last reported delay metric to the routing engine.

This timer starts a countdown to zero when an administrative function causes the operational state of the test on that specific interface to transition from up to down. If the timer expires before the operational state transitions to up, the previously reported value is flushed. The Delay Measurement Last Reported indicates "Cleared". The timestamp indicates the time of the clear event. The Triggered By indicates "Expired". If the administrative state recovers to operationally up before the expiration of the timer, the previous reported value is not flushed.

The aging timer does not apply to failure conditions that do not affect the administrative state of the interface, for example interface failure or routing changes.

The **no** form of this command reverts to the default value.

Default last-reported-delay-hold 86400

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the delay measurement retention time, in seconds, after the interface on which it was collected is administratively disabled. If the configured value is reached, the last reported measurement is cleared.

A configured value of 0 indicates that the previous reported value is cleared without additional wait time.

Values 0 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.67 latency-event

latency-event

Syntax **latency-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
no latency-event

Context **[Tree]** (config>saa>test latency-event)

Full Context configure saa test latency-event

Description Specifies that at the termination of an SAA test probe, the calculated latency event value is evaluated against the configured rising and falling latency event thresholds. SAA threshold events are generated as required.

Once the threshold (rising/falling) is crossed, it is disabled from generating additional events until the opposite threshold is crossed. If a **falling-threshold** is not supplied, the **rising-threshold** is re-enabled when it falls below the threshold after the initial crossing that generated the event.

The configuration of latency event thresholds is optional.

The **no** form of this command disables the latency event.

Parameters **rising-threshold** *threshold* — Specifies a rising threshold latency value, in milliseconds. When the test run is completed, the calculated latency value is compared to the configured latency rising threshold. If the test run latency value is greater than the configured rising threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Values 0 to 2147483

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

falling-threshold *threshold* — Specifies a falling threshold latency value, in milliseconds. When the test run is completed, the calculated latency value is compared to the configured latency falling threshold. If the test run latency value is greater than the configured falling threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Values 0 to 2147483

Default 0

direction — Specifies the direction for OAM ping responses received for an OAM ping test run.

Values **inbound** — Monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run.

outbound — Monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run.

roundtrip — Monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run.

Default roundtrip

Platforms All

16.68 layer-3

layer-3

Syntax **layer-3**

Context **[Tree]** (config>subscr-mgmt>shcv-policy layer-3)

Full Context configure subscriber-mgmt shcv-policy layer-3

Description Commands in this context configure SHCV behavior parameters for IES and VPRN services.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.69 layer-3-encap

layer-3-encap

Syntax **layer-3-encap** [{**ip-udp-shim** | **ip-gre** | **ip-udp-shim-sampled**}] [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no layer-3-encap

Context [Tree] (config>mirror>mirror-dest>encap layer-3-encap)

Full Context configure mirror mirror-dest encap layer-3-encap

Description This command specifies the format of the routable encapsulation to add to each copied packet. Layer 3 encapsulation takes precedence over Ethernet encapsulation configuration in an LI source. No changes are allowed to the Layer 3 encapsulation once a gateway is configured.

The **no** form of this command removes the routable encapsulation.

Default no layer-3-encap

Parameters **ip-udp-shim** — Specifies that the type of Layer 3 encapsulation is an IPv4 header, UDP header, and LI shim header added to the mirrored packets.

ip-gre — Specifies that the type of Layer 3 encapsulation is an IPv4 header and GRE header added to the mirrored packets. This encapsulation type is only supported with *mirror-type ip-only*.

ip-udp-shim-sampled — Specifies that the type of Layer 3 encapsulation is an IPv4 header, UDP header, and a mirror shim header added to the mirrored packets providing direction, mirror type, filter action, interface type, and interface value.

create — Creates a Layer 3 encapsulation.

Platforms All

layer-3-encap

Syntax **layer-3-encap** [**ip-udp-shim** | **ip-gre**]
no layer-3-encap

Context [Tree] (config>li>mirror-dest-template layer-3-encap)

Full Context configure li mirror-dest-template layer-3-encap

Description This command specifies the format of the routable encapsulation to add to each copied packet. Layer 3 encapsulation takes precedence over Ethernet encapsulation configuration in an LI source. No changes are allowed to the Layer 3 encapsulation after a gateway is configured.

The **no** form of this command disables Layer 3 encapsulation.

Parameters **ip-udp-shim** — Specifies that the type of Layer 3 encapsulation is an IPv4 header, UDP header, and LI-Shim.

ip-gre — Specifies that the type of Layer 3 encapsulation is an IPv4 GRE.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.70 lbl-eth-or-ip-l4-teid

lbl-eth-or-ip-l4-teid

Syntax **lbl-eth-or-ip-l4-teid**
no lbl-eth-or-ip-l4-teid

Context **[Tree]** (config>service>epipe>load-balancing lbl-eth-or-ip-l4-teid)
[Tree] (config>service>vpls>load-balancing lbl-eth-or-ip-l4-teid)

Full Context configure service epipe load-balancing lbl-eth-or-ip-l4-teid
configure service vpls load-balancing lbl-eth-or-ip-l4-teid

Description This command enables hashing of MPLS Ethernet and MPLS IP packets received on the Epipe and VPLS service SAP using the MPLS labels, the inner IP addresses, the port numbers, and the GTP TEID field, if read by the system. This capability is supported on FP4-based line cards.

The **no** form of this command disables hashing.

Default no lbl-eth-or-ip-l4-teid

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.71 lbm-svc-act-responder

lbm-svc-act-responder

Syntax [**no**] **lbm-svc-act-responder**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep lbm-svc-act-responder)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep lbm-svc-act-responder)

Full Context configure service epipe sap eth-cfm mep lbm-svc-act-responder
configure service epipe spoke-sdp eth-cfm mep lbm-svc-act-responder

Description This command enables the MEP to process service activation streams encapsulated in ETH-CFM LBM frames that are directed to the MEP. The MEP will be allocated additional resources to rapidly respond to a high-speed stream of LBM messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A MEP created with this option will not validate any TLVs, will not validate the ETH-LBM MAC Address, and will not increment or compute any loopback statistics. Statistical computation and reporting is the responsibility of the test head-end. The ETH-CFM level of the high speed ETH-LBM stream must match the level of a MEP configured with this command. The high-speed stream must not target an ETH-CFM level that is not explicitly configured with this option. MEPs act as boundaries for lower levels, below the configured MEP level values. Those boundary levels do not inherit this function.

When the service activation test is complete, the MEP may be returned to standard processing by removing this command. If there is available bandwidth, the MEP will respond to other ETH-CFM PDUs, such as ETH-DMM marker packets, using standard processing.

The interaction between this command and the **tools perform service id** *service-id* **loopback eth** command must be carefully considered. It is recommended that either the **lbm-svc-act-responder** or the **tools perform service id** *service-id* **loopback eth** command be used at any given time within a service. If both commands must be configured, and the target reflection point is the MAC Swap Loopback function, the inbound stream of data must not include ETH-CFM traffic that is equal to or lower than the domain level of any configured MEP which would otherwise extract and process the ETH-CFM message. If the reflection target is a MEP configured with the **lbm-svc-act-responder** option, the mode (ingress or egress) of the SAP or SDP specified with this tools command and the MEP **direction** (up or down) must match when the functions are enabled on the same reflection point, and the domain level of the inbound ETH-LBM must be the same as that of the MEP configured with the **lbm-svc-act-responder** option. At no time should the two functions be conflicting with each other along the path of the stream. This conflict would lead to unpredictable and possibly destabilizing situations.

The **no** form of this command reverts to MEP LBM standard processing.

Default no lbm-svc-act-responder

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

lbm-svc-act-responder

Syntax [**no**] **lbm-svc-act-responder**

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>mep lbm-svc-act-responder)
[Tree] (config>service>vpls>sap>eth-cfm>mep lbm-svc-act-responder)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep lbm-svc-act-responder)

Full Context configure service vpls mesh-sdp eth-cfm mep lbm-svc-act-responder
configure service vpls sap eth-cfm mep lbm-svc-act-responder
configure service vpls spoke-sdp eth-cfm mep lbm-svc-act-responder

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the MEP to process service activation streams encapsulated in ETH-CFM LBM frames that are directed to the MEP. The MEP will be allocated additional resources to rapidly respond to a high-speed stream of LBM messages. A MEP created with this option will not validate any TLVs, will not validate the ETH-LBM MAC Address, and will not increment or compute any loopback statistics. Statistical computation and reporting is the responsibility of the test head-end. The ETH-CFM level of the high speed ETH-LBM stream must match the level of a MEP configured with this command. It must not target any lower ETH-CFM level the MEP will terminate. When the service activation test is complete, the MEP may be returned to standard processing by removing this command. If there is available bandwidth, the MEP will respond to other ETH-CFM PDUs, such as ETH-DMM marker packets, using standard processing.

The interaction between this command and the **tools perform service id** *service-id* **loopback eth** command must be carefully considered. It is recommended that either the **lbm-svc-act-responder** or the **tools perform service id** *service-id* **loopback eth** command be used at any given time within a service. If both commands must be configured, and the target reflection point is the MAC Swap Loopback function, the inbound stream of data must not include ETH-CFM traffic that is equal to or lower than the domain level of any configured MEP which would otherwise extract and process the ETH-CFM message. If the reflection target is a MEP configured with the **lbm-svc-act-responder** option, the mode (ingress or egress) of the SAP or SDP specified with this tools command and the MEP **direction** (up or down) must match when the functions are enabled on the same reflection point, and the domain level of the inbound ETH-LBM must be the same as that of the MEP configured with the **lbm-svc-act-responder** option. At no time should the two functions be conflicting with each other along the path of the stream. This conflict would lead to unpredictable and possibly destabilizing situations.

The **no** form of this command reverts to MEP LBM standard processing.

Default no lbm-svc-act-responder

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

lbm-svc-act-responder

Syntax [**no**] **lbm-svc-act-responder**

Context **[Tree]** (config>router>if>eth-cfm>mep lbm-svc-act-responder)

Full Context configure router interface eth-cfm mep lbm-svc-act-responder

Description This command enables the MEP to process service activation streams encapsulated in ETH-CFM LBM frames that are directed to the MEP. The MEP will be allocated additional resources to rapidly respond to a high-speed stream of LBM messages. A MEP created with this option will not validate any TLVs, will not validate the ETH-LBM MAC Address, and will not increment or compute any loopback statistics. Statistical computation and reporting is the responsibility of the test head-end. The ETH-CFM level of the high speed ETH-LBM stream

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

must match the level of a MEP configured with this command. It must not target any lower ETH-CFM level the MEP will terminate. When the service activation test is complete, the MEP may be returned to standard processing by removing this command. If there is available bandwidth, the MEP will respond to other ETH-CFM PDUs, such as ETH-DMM marker packets, using standard processing.

The interaction between this command and the **tools perform service id** *service-id* **loopback eth** command must be carefully considered. It is recommended that either the **lbm-svc-act-responder** or the **tools perform service id** *service-id* **loopback eth** command be used at any given time within a service. If both commands must be configured, and the target reflection point is the MAC Swap Loopback function, the inbound stream of data must not include ETH-CFM traffic that is equal to or lower than the domain level of any configured MEP which would otherwise extract and process the ETH-CFM message. If the reflection target is a MEP configured with the **lbm-svc-act-responder** option, the mode (ingress or egress) of the SAP or SDP specified with this tools command and the MEP **direction** (up or down) must match when the functions are enabled on the same reflection point, and the domain level of the inbound ETH-LBM must be the same as that of the MEP configured with the **lbm-svc-act-responder** option. At no time should the two functions be conflicting with each other along the path of the stream. This conflict would lead to unpredictable and possibly destabilizing situations.

The **no** form of this command reverts to MEP LBM standard processing.

Default no lbm-svc-act-responder

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.72 lbo

lbo

Syntax **lbo** [**0dB** | **-7.5dB** | **-15.0dB** | **-22.5dB**]

Context **[Tree]** (config>port>tdm lbo)

Full Context configure port tdm lbo

Description This command applies only to a DS-1 port configured with a 'long' buildout (see the **buildout** command). Specify the number of decibels the transmission signal decreases over the line.

For 'short' buildout the following values are valid:

lboNotApplicable — Not applicable

For 'long' buildout the following values are valid:

lbo0dB For 0 dB

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lboNeg7p5dB	For -7.5 dB
lboNeg15p0dB	For -15.0 dB
lboNeg22p5dB	For -22.5 dB

The default for 'short' build out is 'NotApplicable' while the default for 'long' buildout is 'lbo0dB'.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

16.73 lcp-force-ack-accm

lcp-force-ack-accm

Syntax **lcp-force-ack-accm** {**always** | **never**}
no lcp-force-ack-accm

Context **[Tree]** (config>router>l2tp>group>ppp lcp-force-ack-accm)
[Tree] (config>router>l2tp>group>tunnel>ppp lcp-force-ack-accm)
[Tree] (config>service>vprn>l2tp>group>ppp lcp-force-ack-accm)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp lcp-force-ack-accm)

Full Context configure router l2tp group ppp lcp-force-ack-accm
configure router l2tp group tunnel ppp lcp-force-ack-accm
configure service vprn l2tp group ppp lcp-force-ack-accm
configure service vprn l2tp group tunnel ppp lcp-force-ack-accm

Description This command enables the LCP Asynchronous Control Character Map (ACCM) configuration option. When enabled, the LCP ACCM configuration option is acknowledged during LCP negotiation between the LNS and the PPP client. The option is then ignored and no ACCM mapping is done.

By default, an L2TP tunnel inherits the configuration from the L2TP group CLI context.

The **no** form of this command disables the LCP ACCM configuration option.

Parameters **always** — Specifies to acknowledge the LCP ACCM configuration option, but not to perform ACCM mapping. This option overrides the group level configuration.

never — Specifies to reject the LCP ACCM configuration option. This option overrides the group level configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.74 lcp-ignore-identifier

lcp-ignore-identifier

Syntax [**no**] **lcp-ignore-identifier**

Context **[Tree]** (config>subscr-mgmt>ppp-policy lcp-ignore-identifier)

Full Context configure subscriber-mgmt ppp-policy lcp-ignore-identifier

Description This command instructs BNG to ignore identifier values in Link Control Protocol (LCP) Echo Reply packets and keep the PPP session up.

The **no** form of this command instructs BNG not to ignore the identifier values, in which case, incorrect messages are discarded and the PPP session terminates because of echo timeout.

Default lcp-ignore-identifier

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.75 lcp-ignore-magic-numbers

lcp-ignore-magic-numbers

Syntax **lcp-ignore-magic-numbers** {**always** | **never**}
no lcp-ignore-magic-numbers

Context **[Tree]** (config>router>l2tp>group>ppp lcp-ignore-magic-numbers)
[Tree] (config>router>l2tp>group>tunnel>ppp lcp-ignore-magic-numbers)
[Tree] (config>service>vprn>l2tp>group>ppp lcp-ignore-magic-numbers)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp lcp-ignore-magic-numbers)

Full Context configure router l2tp group ppp lcp-ignore-magic-numbers
configure router l2tp group tunnel ppp lcp-ignore-magic-numbers
configure service vprn l2tp group ppp lcp-ignore-magic-numbers
configure service vprn l2tp group tunnel ppp lcp-ignore-magic-numbers

Description This command configures checking the magic number field in LCP Echo-Request and LCP Echo-Reply messages.

The **no** form of this command reverts to the default value.

Default no lcp-ignore-magic-numbers

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lcp-ignore-magic-numbers

Syntax [**no**] **lcp-ignore-magic-numbers**

Context **[Tree]** (config>subscr-mgmt>ppp-policy lcp-ignore-magic-numbers)

Full Context configure subscriber-mgmt ppp-policy lcp-ignore-magic-numbers

Description This command enables the PPP session to stay established when an LCP peer magic number mismatch is detected.

By default, the PPP session is terminated when an LCP peer magic number mismatch is detected.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.76 ldap

ldap

Syntax [**no**] **ldap**

Context **[Tree]** (config>system>security ldap)

Full Context configure system security ldap

Description This command configures LDAP authentication parameters for the system.

The **no** form of this command de-configures the LDAP client from the SR OS.

Platforms All

16.77 ldap-server

ldap-server

Syntax **ldap-server** *server-name*
no ldap-server

Context **[Tree]** (config>system>security>ldap>server ldap-server)

Full Context configure system security ldap server ldap-server

Description This command enables the LDAP server name or description.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the LDAP server name.

Parameters *server-name* — Specifies the name of the server, up to 32 characters.

Platforms All

16.78 ldp

ldp

Syntax [**no**] **ldp**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter ldp)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter ldp)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter ldp)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter ldp)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter ldp
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter ldp
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter ldp
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter ldp

Description This command enables LDP for the auto-bind tunnel resolution filter.

This command instructs BGP to search for an LDP LSP with a FEC prefix corresponding to the address of the BGP next hop.

The **no** form of this command removes the configuration.

Default no ldp

Platforms All

ldp

Syntax [**no**] **ldp**

Context **[Tree]** (config>router ldp)

Full Context configure router ldp

Description Commands in this context configure an LDP parameters. LDP is not enabled by default and must be explicitly enabled (**no shutdown**).

To suspend the LDP protocol, use the **shutdown** command. Configuration parameters are not affected.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command deletes the LDP protocol instance, removing all associated configuration parameters. The LDP instance must first be disabled with the **shutdown** command before being deleted.

Platforms All

ldp

Syntax [**no**] **ldp**

Context **[Tree]** (debug>router ldp)

Full Context debug router ldp

Description Use this command to configure LDP debugging.

Platforms All

ldp

Syntax [**no**] **ldp**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter ldp)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter ldp

Description This command enables the use of LDP-sourced tunnel entries in the TTM to resolve the associated static route next-hop.

The **no** form of this command disables the use of LDP-sourced tunnel entries to resolve static route next hops.

Default no ldp

Platforms All

ldp

Syntax [**no**] **ldp**

Context **[Tree]** (config>service>sdp ldp)

Full Context configure service sdp ldp

Description This command enables LDP-signaled LSPs on MPLS-encapsulated SDPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In MPLS SDP configurations *either* one or more LSP names can be specified *or* LDP can be enabled. The SDP **ldp** and **lsp** commands are mutually exclusive except if the mixed-lsp-mode option is also enabled. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the **no lsp** *lsp-name* command or the mixed-lsp-mode option is also enabled.

Alternatively, if LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. To specify an LSP on the SDP, the LDP must be disabled. The LSP must have already been created in the **config>router>mpls** context with a valid far-end IP address. The above rules are relaxed when the **mixed-lsp** option is enabled on the SDP.

Default no ldp (disabled)

Platforms All

ldp

Syntax [**no**] **ldp**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter ldp)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter ldp)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter ldp
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter ldp

Description This command enables LDP tunneling for next-hop resolution and specifies the LDP tunnels in the tunnel table corresponding to /32 IPv4 FECs and /128 IPv6 FECs.

The **no** form of this command disables LDP tunneling for next-hop resolution.

Platforms All

16.79 ldp-over-rsvp

ldp-over-rsvp

Syntax **ldp-over-rsvp** [**include** | **exclude**]

Context **[Tree]** (config>router>mpls>lsp ldp-over-rsvp)
[Tree] (config>router>mpls>lsp-template ldp-over-rsvp)

Full Context configure router mpls lsp ldp-over-rsvp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls lsp-template ldp-over-rsvp

Description This command configures an LSP so that it can be used by the IGP to calculate its SPF tree.

When the **ldp-over-rsvp** option is also enabled in ISIS or OSPF, the IGP provides LDP with all ECMP IP next-hops and tunnel endpoints that it considers to be the lowest cost path to its destination.

IGP provides only the endpoints which are the closest to the destination in terms of IGP cost for each IP next-hop of a prefix. If this results in more endpoints than the ECMP value configured on the router, it will further prune the endpoints based on the lowest router-id and for the same router-id, it will select lowest interface-index first.

LDP then looks up the tunnel table to select the actual tunnels to the endpoint provided by IGP and further limits the endpoint selection to the ones which are the closest to destination across all the IP next-hops provided by IGP for a prefix. For each remaining endpoint, LDP selects a tunnel in a round-robin fashion until the router ECMP value is reached. For each endpoint, only tunnels with the same lowest metric are candidates. If more than one tunnel qualifies, the selection begins with the lowest tunnel-id.

Default ldp-over-rsvp include

Platforms All

ldp-over-rsvp

Syntax [**no**] **ldp-over-rsvp**

Context **[Tree]** (config>router>isis ldp-over-rsvp)

Full Context configure router isis ldp-over-rsvp

Description This command allows LDP over RSVP processing in IS-IS.

The **no** form of this command disables LDP over RSVP processing.

Default no ldp-over-rsvp

Platforms All

ldp-over-rsvp

Syntax [**no**] **ldp-over-rsvp**

Context **[Tree]** (config>router>ospf ldp-over-rsvp)

Full Context configure router ospf ldp-over-rsvp

Description This command allows LDP-over-RSVP processing in this OSPF instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no ldp-over-rsvp

Platforms All

16.80 ldp-shortcut

ldp-shortcut

Syntax [**no**] **ldp-shortcut**

Context **[Tree]** (config>router ldp-shortcut)

Full Context configure router ldp-shortcut

Description This command enables the resolution of IGP routes using LDP LSP across all network interfaces participating in the IS-IS and OSPF routing protocol in the system.

When LDP shortcut is enabled, LDP populates the routing table with next-hop entries corresponding to all prefixes for which it activated an LDP FEC. For a given prefix, two route entries are populated in the system routing table. One corresponds to the LDP shortcut next-hop and has an owner of LDP. The other one is the regular IP next-hop. The LDP shortcut next-hop always has preference over the regular IP next-hop for forwarding user packets and specified control packets over a given outgoing interface to the route next-hop.

All user and specified control packets for which the longest prefix match in RTM yields the FEC prefix will be forwarded over the LDP LSP.

When an IPv4 packet is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the lookup of the packet by the ingress forwarding engine will result in the packet being sent labeled with the label stack corresponding to the NHLFE of the LDP LSP when the preferred RTM entry corresponds to an LDP shortcut.

If the preferred RTM entry corresponds to an IP next-hop, the IPv4 packet is forwarded without a label.

When ECMP is enabled and multiple equal-cost next-hops exit for the IGP route, the ingress forwarding engine will spray the packets for this route based on hashing routine currently supported for IPv4 packets. When the preferred RTM entry corresponds to an LDP shortcut route, spraying will be performed across the multiple next-hops for the LDP FEC. The FEC next-hops can either be direct link LDP neighbors or T-LDP neighbors reachable over RSVP LSPs in the case of LDP-over-RSVP but not both.

When the preferred RTM entry corresponds to a regular IP route, spraying will be performed across regular IP next-hops for the prefix.

The **no** form of this command disables the resolution of IGP routes using LDP shortcuts.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no ldp-shortcut

Platforms All

16.81 ldp-sync

ldp-sync

Syntax [**no**] **ldp-sync**

Context **[Tree]** (config>service>vprn>static-route-entry>indirect ldp-sync)

Full Context configure service vprn static-route-entry indirect ldp-sync

Description This command extends the LDP synchronization feature to a static route. When an interface comes back up, it is possible that a preferred static route using the interface as next-hop for a given prefix is enabled before the LDP adjacency to the peer LSR comes up on this interface. In this case, traffic on an SDP that uses the static route for the far-end address would be black-holed until the LDP session comes up and the FECs exchanged.

This option when enabled delays the activation of the static route until the LDP session comes up over the interface and the ldp-sync-timer configured on that interface has expired

Default no ldp-sync

ldp-sync

Syntax [**no**] **ldp-sync**

Context **[Tree]** (config>router>static-route-entry>next-hop ldp-sync)

Full Context configure router static-route-entry next-hop ldp-sync

Description This command extends the LDP synchronization feature to a static route. When an interface comes back up, it is possible that a preferred static route using the interface as next-hop for a given prefix is enabled before the LDP adjacency to the peer LSR comes up on this interface. In this case, traffic on an SDP that uses the static route for the far-end address would be black-holed until the LDP session comes up and the FECs exchanged.

This option when enabled delays the activation of the static route until the LDP session comes up over the interface and the ldp-sync-timer configured on that interface has expired

Default no ldp-sync

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.82 ldp-sync-timer

ldp-sync-timer

Syntax **ldp-sync-timer** *seconds* [**end-of-lib**]
no ldp-sync-timer

Context **[Tree]** (config>router>if ldp-sync-timer)

Full Context configure router interface ldp-sync-timer

Description This command enables synchronization of an IGP and LDP. When a link is restored after a failure, the IGP sets the link cost to infinity and advertises it. The actual value advertised in OSPF is 0xFFFF (65535). The actual value advertised in IS-IS regular metric is 0x3F (63) and in IS-IS wide-metric is 0xFFFFFE (16777214). This feature is not supported on RIP interfaces.

If an interface belongs to both IS-IS and OSPF, a physical failure will cause both IGPs to advertise an infinite metric and to follow the IGP-LDP synchronization procedures. If only one IGP bounces on this interface or on the system, then only the affected IGP advertises the infinite metric and follows the IGP-LDP synchronization procedures.

Next, an LDP Hello adjacency is brought up with the neighbor. The LDP synchronization timer is started by the IGP when the LDP session to the neighbor is up over the interface. This is to allow time for the label-FEC bindings to be exchanged.

When the LDP synchronization timer expires, the link cost is restored and is readvertised. The IGP will announce a new best next hop and LDP will use it if the label binding for the neighbor's FEC is available.

If the user changes the cost of an interface, the new value is advertised at the next flooding of link attributes by the IGP. However, if the LDP synchronization timer is still running, the new cost value will only be advertised after the timer expires. The new cost value will also be advertised after the user executes any of the following commands:

- **tools>perform>router>isis>ldp-sync-exit**
- **tools>perform>router>ospf>ldp-sync-exit**
- **config>router>if>no ldp-sync-timer**
- **config>router>ospf>disable-ldp-sync**
- **router>isis>disable-ldp-sync**

If the user changes the value of the LDP synchronization timer parameter, the new value will take effect at the next synchronization event. If the timer is still running, it will continue to use the previous value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If parallel links exist to the same neighbor, then the bindings and services should remain up as long as there is one interface that is up. However, the user-configured LDP synchronization timer still applies on the interface that failed and was restored. In this case, the router will only consider this interface for forwarding after the IGP re-advertises its actual cost value.

The LDP Sync Timer State is not always synchronized across to the standby CPM. Therefore, after an activity switch, the timer state might not be same as it was on the previously active CPM.

If the **end-of-lib** option is configured, then the system will start the LDP synchronization timer as usual. If the LDP End of LIB Typed Wildcard FEC messages are received for every FEC type negotiated for a given session to an LDP peer for that IGP interface, the **ldp-sync-timer** is terminated early and the IGP link cost is restored. If the **ldp-sync-timer** expires before the LDP End of LIB messages are received for every negotiated FEC type, then the system will restore the IGP link cost. The **end-of-lib** option is disabled by default.

The **no** form of this command disables IGP-LDP synchronization and deletes the configuration.

Default no ldp-sync-timer

Parameters *seconds* — Specifies the time interval for the IGP-LDP synchronization timer.

Values 1 to 1800

end-of-lib — Specifies that the system should terminate the **ldp-sync-timer** early if the LDP End of LIB Typed Wildcard FEC messages are received for every FEC type negotiated for a given session to an LDP peer for that IGP interface.

Platforms All

16.83 ldp-treetrace

ldp-treetrace

Syntax **ldp-treetrace** {**prefix** *ip-prefix*/*mask*} [**downstream-map-tlv** {**dsmap** | **ddmap**}] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**max-path** *max-paths*] [**max-ttl** *ttl-value*] [**retry-count** *retry-count*] [**timeout** *timeout*]

Context **[Tree]** (oam ldp-treetrace)

Full Context oam ldp-treetrace

Description This command allows the user to perform a single run of the LDP ECMP OAM tree trace to discover all ECMP paths of an LDP FEC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix/mask* — Specifies the address prefix and subnet mask of the target BGP IPv4 label route.

Values ip-prefix: a.b.c.dmask, the value must be 32

downstream-map-tlv {dsmap | ddmap} — Specifies which format of the downstream mapping TLV to use in the LSP trace packet. The DSMAP TLV is the original format in RFC 4379 (obsoleted by RFC 8029). The DDMAP is the new enhanced format specified in RFC 6424 and RFC 8029.

Default Inherited from global configuration of downstream mapping TLV in option **mpls-echo-request-downstream-map** {**dsmap** | **ddmap**}.

fc-name — Specifies the FC and profile parameters are used to indicate the forwarding class and profile of the MPLS echo request packet.

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified FC and profile parameter values. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface.

When the MPLS echo request packet is received on the responding node, The FC and profile parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the FC and profile parameter values determined by the classification of the echo request packet, which is being replied to, at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. The ToS byte is not modified. Table 72 summarizes this behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 72 **ldp-treetrace Request Packet and Behavior**

CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • pkt queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet {tos=1, fc2, profile2}
Outgoing interface (responder node)	Echo reply packet: • pkt queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile state of the MPLS echo request packet.

Values in, out

Default out

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-paths — Specifies the maximum number of paths for a ldp-treetrace test, expressed as a decimal integer.

Values 1 to 255

Default 128

ttl-value — Specifies the maximum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Values 1 to 255

Default 30

retry-count — Specifies the maximum number of consecutive MPLS echo requests, expressed as a decimal integer that do not receive a reply before the trace operation fails for a given TTL.

Values 1 to 255

Default 5

timeout — Specifies the time, in seconds, used to override the default time out value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded.

Values 1 to 60

Default 3

Output The following is an example of treetrace prefix information.

Sample Output

```
*A:Dut-A# oam ldp-treetrace prefix 10.20.1.6/32

ldp-treetrace for Prefix 10.20.1.6/32:

         127.0.0.1, ttl =   3 dst =      127.1.0.255 rc = EgressRtr status = Done
    Hops:         127.0.0.1         127.0.0.1

         127.0.0.1, ttl =   3 dst =      127.2.0.255 rc = EgressRtr status = Done
    Hops:         127.0.0.1         127.0.0.1

ldp-treetrace discovery state: Done
ldp-treetrace discovery status: ' OK '
Total number of discovered paths: 2
Total number of failed traces: 0
```

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ldp-treetrace

Syntax [**no**] **ldp-treetrace**

Context **[Tree]** (config>test-oam ldp-treetrace)

Full Context configure test-oam ldp-treetrace

Description This command creates the context to configure the LDP ECMP OAM tree trace which consists of an LDP ECMP path discovery and an LDP ECMP path probing features.

The **no** form of this command deletes the configuration for the LDP ECMP OAM tree discovery and path probing under this context.

Output The following is an example LDP treetrace information.

Sample Output Over a Numbered IP Interface

```
*A:Dut-B# oam ldp-treetrace prefix 10.20.1.5/32

ldp-treetrace for Prefix 10.20.1.5/32:

       10.10.131.2, ttl =   2 dst =      127.1.0.253 rc = EgressRtr status = Done
    Hops:          11.1.0.2

       10.10.132.2, ttl =   2 dst =      127.1.0.255 rc = EgressRtr status = Done
    Hops:          11.1.0.2

       10.10.131.2, ttl =   2 dst =      127.2.0.255 rc = EgressRtr status = Done
    Hops:          11.2.0.2

       10.10.132.2, ttl =   2 dst =      127.2.0.253 rc = EgressRtr status = Done
    Hops:          11.2.0.2

ldp-treetrace discovery state: Done
ldp-treetrace discovery status: ' OK '
Total number of discovered paths: 4
Total number of failed traces: 0
```

Sample Output Over an Unnumbered IP Interface

```
*A:Dut-A# oam ldp-treetrace prefix 10.20.1.6/32 downstream-map-tlv dsmap

ldp-treetrace for Prefix 10.20.1.6/32:

         127.0.0.1, ttl =   3 dst =      127.1.0.255 rc = EgressRtr status = Done
    Hops:         127.0.0.1         127.0.0.1

         127.0.0.1, ttl =   3 dst =      127.2.0.255 rc = EgressRtr status = Done
    Hops:         127.0.0.1         127.0.0.1

ldp-treetrace discovery state: Done
ldp-treetrace discovery status: ' OK '
Total number of discovered paths: 2
Total number of failed traces: 0
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

ldp-treetrace

Syntax [**no**] **ldp-treetrace**

Context **[Tree]** (debug>oam ldp-treetrace)

Full Context debug oam ldp-treetrace

Description This command enables debugging for OAM LDP treetrace.

The **no** form of this command disables the debugging.

Platforms All

16.84 leak

leak

Syntax **leak** [*ip-address*]
no leak

Context **[Tree]** (debug>router>isis leak)

Full Context debug router isis leak

Description This command enables debugging for IS-IS leaks.

The **no** form of the command disables debugging.

Parameters *ip-address* — When specified, only the specified address is debugged for IS-IS leaks.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

leak

Syntax **leak** [*ip-address*]
no leak

Context **[Tree]** (debug>router>ospf leak)
[Tree] (debug>router>ospf3 leak)

Full Context debug router ospf leak
debug router ospf3 leak

Description This command enables debugging for OSPF leaks.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address to debug OSPF leaks.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

16.85 leak-export

leak-export

Syntax **leak-export** *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]]
no leak-export

Context **[Tree]** (config>router leak-export)

Full Context configure router leak-export

Description This command associates up to four policies to control the leaking of GRT routes into the associated VPRN.

If a route is being evaluated and the action is accepted, then that route is subject leaking into an associated VPRN instance assuming the route is fully resolved and active.

This process creates the pool of routes that can be leaked. Within each VPRN a corresponding **import-grt** policy must be configured to import select routes into that specific VPRN instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes all route leaking policy associations and effectively disables the leaking of GRT routes into associated VPRNs.

Parameters *plcy-or-long-expr* — Specifies the route policy name, up to 64 characters or a policy logical expression, up to 255 characters.

Values *plcy-or-long-expr*: *policy-name* | *long-expr*
policy-name: up to 64 characters
long-expr: up to 255 characters

plcy-or-expr — Specifies the route policy name, up to 64 characters or a policy logical expression, up to 64 characters long. A maximum of four policy names or policy logical expressions can be specified in a single statement.

Values *plcy-or-expr*: *policy-name* | expr
policy-name: up to 64 characters
expr: up to 64 characters

Platforms All

16.86 leak-export-limit

leak-export-limit

Syntax [**no**] **leak-export-limit** [*value*]

Context **[Tree]** (config>router leak-export-limit)

Full Context configure router leak-export-limit

Description This command sets a maximum limit on the number of GRT routes that can be leaked into VPRNs.

The **no** form of this command resets the **leak-export-limit** to its default value of 5.

Default leak-export-limit 5

Parameters *value* — Specifies the maximum number of GRT routes that are eligible to be leaked into VPRN instances.

Values 1 to 10000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.87 leak-import

leak-import

Syntax **leak-import** *plcy-or-long-expr* [*plcy-or-expr*]
no leak-import

Context **[Tree]** (config>service>vprn>bgp>rib-management>ipv4 leak-import)
[Tree] (config>service>vprn>bgp>rib-management>label-ipv4 leak-import)
[Tree] (config>service>vprn>bgp>rib-management>ipv6 leak-import)
[Tree] (config>service>vprn>bgp>rib-management>label-ipv6 leak-import)

Full Context configure service vprn bgp rib-management ipv4 leak-import
configure service vprn bgp rib-management ipv6 leak-import
configure service vprn bgp rib-management label-ipv4 leak-import
configure service vprn bgp rib-management label-ipv6 leak-import

Description This command configures route policies that control the importation of leak-eligible routes from the BGP RIB of another routing instance into the unlabeled-IPv4, unlabeled-IPv6, labeled-IPv4, or labeled-IPv6 RIB of the VPRN instance. To leak a route from one routing instance to another, the origin and destination RIB types must be the same; for example, it is not possible to leak a route from an unlabeled-IPv4 RIB of a VPRN into the labeled-IPv4 RIB of the base router.

The **leak-import** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine the final action to accept or reject the route.

Only one of the 15 objects referenced by the **leak-import** command can be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters while the remaining 14 objects have a maximum length of 64 characters each.

When a **leak-import** policy is not specified, no BGP routes from other routing instances are leaked into the VPRN BGP RIB.

The **no** form of this command removes the policy association.

Default no leak-import

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Allowed values are any string of characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

plcy-or-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Allowed values are any string of characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

leak-import

Syntax **leak-import** *plcy-or-long-expr* [*plcy-or-expr*]
no leak-import

Context **[Tree]** (config>router>bgp>rib-management>ipv4 leak-import)
[Tree] (config>router>bgp>rib-management>label-ipv4 leak-import)
[Tree] (config>router>bgp>rib-management>ipv6 leak-import)

Full Context configure router bgp rib-management ipv4 leak-import
configure router bgp rib-management ipv6 leak-import
configure router bgp rib-management label-ipv4 leak-import

Description This command configures the router to specify route policies that control the importation of leak-eligible routes from the BGP RIB of another routing instance into the unlabeled-IPv4, unlabeled-IPv6, or labeled-IPv4 RIB of the base router. To leak a route from one routing instance to another, the origin and destination RIB types must be the same; for example, it is not possible to leak a route from an unlabeled-IPv4 RIB of a VPRN into the labeled-IPv4 RIB of the base router.

The **leak-import** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine final action to accept or reject the route.

Only one of the 15 objects referenced by the **leak-import** command can be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters while the remaining 14 objects have a maximum length of 64 characters each.

When a **leak-import** policy is not specified, no BGP routes from other routing instances are leaked into the base router BGP RIB.

The **no** form of this command removes the policy association.

Default no leak-import

Parameters *plcy-or-long-expr* — Specifies up to 14 route policy names (up to 64 characters long) or a policy logical expression (up to 255 characters long). Allowed values are any string of characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

plcy-or-expr — The route policy name (up to 64 characters long) or a policy logical expression (up to 64 characters long). Allowed values are any string of characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

16.88 learn-ap-mac

learn-ap-mac

Syntax **learn-ap-mac** [**delay-auth**]
no learn-ap-mac

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw learn-ap-mac)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw learn-ap-mac)

Full Context configure service ies subscriber-interface group-interface wlan-gw learn-ap-mac
configure service vprn subscriber-interface group-interface wlan-gw learn-ap-mac

Description This command enables the sending of ARP or ND packets on the WLAN-GW GRE tunnel for certain events. The target IP address in the ARP/ND packet is the endpoint IP address of the AP. The ARP/ND response from the AP should contain the AP MAC, which subsequently can be reported in a called-station-id message. When enabled, a message will be sent for following events:

- CPM: Mobility to an AP for which the AP-MAC is not yet known
- CPM: RS-triggered authentication on an AP for which the AP-MAC is not yet known
- ISA: Any mobility event
- ISA: Any authentication where the AP-MAC is not yet known (for example, from a RADIUS proxy cache or a DHCP circuit-id). If the optional keyword **delay-auth** is configured, then the authentication will be delayed until the ARP/ND is answered or timed out, after which the AP-MAC can be included in the authentication.

This configuration is ignored for L2-AP and L2TPv3 access.

Parameters **delay-auth** — Specifies that authentication will be delayed until the ARP/ND is answered or timed out, after which the AP-MAC can be included in the authentication.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.89 learn-dynamic

learn-dynamic

Syntax [**no**] **learn-dynamic**

Context **[Tree]** (config>service>ies>if>vpls>evpn>arp learn-dynamic)
[Tree] (config>service>ies>if>vpls>evpn>nd learn-dynamic)
[Tree] (config>service>vprn>if>vpls>evpn>arp learn-dynamic)
[Tree] (config>service>vprn>if>vpls>evpn>nd learn-dynamic)

Full Context configure service ies interface vpls evpn arp learn-dynamic
configure service ies interface vpls evpn nd learn-dynamic
configure service vprn interface vpls evpn arp learn-dynamic
configure service vprn interface vpls evpn nd learn-dynamic

Description This command controls whether the ARP or ND frames received on EVPN binds are used to learn dynamic ARP and ND entries in the ARP/ND table.

The **no** form of the command reverts to the default.

Default learn-dynamic

Platforms All

16.90 learn-l2tp-cookie

learn-l2tp-cookie

Syntax **learn-l2tp-cookie** {**if-match** | **never** | **always**} [**cookie** *hex string*]
no learn-l2tp-cookie

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw learn-l2tp-cookie)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw learn-l2tp-cookie)

Full Context configure service ies subscriber-interface group-interface wlan-gw learn-l2tp-cookie
configure service vprn subscriber-interface group-interface wlan-gw learn-l2tp-cookie

Description This command specifies when this system will learn the cookie from L2TP tunnels terminating on this interface. Learning the cookie means that the value of the octets 3-8 of the cookie is interpreted as an access point's MAC address, and used as such, for example in the Called-Station-Id attribute of RADIUS Interim-Update messages.

Parameters **if-match** — Specifies that the cookie is interpreted only if the value of the first two octets of the cookie is equal to the value of the object tmnxWlanGwSoftGreIfL2tpCookie.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cookie *hex string* — Specifies the value used to compare the first two bytes of the cookie. This parameter is only valid if **if-match** is configured.

Values 0x0000 to 0xFFFF...(4 hex nibbles)

never — Specifies that the cookie value will always be ignored.

always — Always learn the AP-MAC from the cookie, regardless of the value of the first two bytes.

16.91 lease-hold-time

lease-hold-time

Syntax **lease-hold-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-hold-time

Context **[Tree]** (config>router>dhcp>server lease-hold-time)
[Tree] (config>router>dhcp6>server lease-hold-time)
[Tree] (config>service>vprn>dhcp>server lease-hold-time)
[Tree] (config>service>vprn>dhcp6>server lease-hold-time)

Full Context configure router dhcp local-dhcp-server lease-hold-time
configure router dhcp6 local-dhcp-server lease-hold-time
configure service vprn dhcp local-dhcp-server lease-hold-time
configure service vprn dhcp6 local-dhcp-server lease-hold-time

Description This command configures the time to remember this lease and is applicable for unsolicited release conditions such as lease timeout if the **lease-hold-time-for** command is set to the default value **no solicited-release** and is additionally applicable for normal solicited releases from DHCP clients if the **lease-hold-time-for** command is set to **solicited-release**.

The **no** form of this command reverts to the default.

Default lease-hold-time sec 0

Parameters *lease-hold-time* — Specifies the amount of time to remember the lease.

Values

days	0 to 7305
hours	0 to 23
minutes	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.92 lease-hold-time-for

lease-hold-time-for

Syntax [**no**] **lease-hold-time-for**

Context **[Tree]** (config>router>dhcp>server lease-hold-time-for)
[Tree] (config>router>dhcp6>server lease-hold-time-for)
[Tree] (config>service>vprn>dhcp>server lease-hold-time-for)
[Tree] (config>service>vprn>dhcp6>server lease-hold-time-for)

Full Context configure router dhcp local-dhcp-server lease-hold-time-for
configure router dhcp6 local-dhcp-server lease-hold-time-for
configure service vprn dhcp local-dhcp-server lease-hold-time-for
configure service vprn dhcp6 local-dhcp-server lease-hold-time-for

Description Commands in this context configure **lease-hold-time-for** parameters which define additional types of lease or triggers that cause system to hold up leases.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.93 lease-populate

lease-populate

Syntax **lease-populate** [*nbr-of-leases*]
lease-populate [*nbr-of-leases*] **l2-header** [**mac** *ieee-address*]
no lease-populate

Context **[Tree]** (config>service>vpls>sap>dhcp lease-populate)
[Tree] (config>service>ies>if>dhcp lease-populate)
[Tree] (config>service>ies>sub-if>grp-if>dhcp lease-populate)
[Tree] (config>service>vprn>if>dhcp lease-populate)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp lease-populate)
[Tree] (config>service>vprn>sub-if>dhcp lease-populate)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp lease-populate)

Full Context configure service ies interface dhcp lease-populate
configure service ies subscriber-interface group-interface dhcp lease-populate
configure service vpls sap dhcp lease-populate
configure service vprn interface dhcp lease-populate
configure service vprn subscriber-interface dhcp lease-populate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface dhcp lease-populate
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp lease-populate

Description Commands in this context configure IPoE host parameters.

For VPLS, DHCP snooping must be explicitly enabled (using the **snoop** command) at all points where DHCP messages requiring snooping enter the VPLS instance (both from the DHCP server and from the subscribers). Lease state information is extracted from snooped DHCP ACK messages to populate lease state table entries for the SAP.

The optional *nbr-of-leases* parameter defines the number lease state table entries allowed.

- for this SAP in case of a VPLS service
- for this interface in case of an IES or VPRN interface
- for each SAP in case of an IES or VPRN group-interface
- for this interface in case of an IES or VPRN retail subscriber-interface

If the *nbr-of-leases* parameter is omitted, only a single entry is allowed. Once the maximum number of entries has been reached, subsequent lease state entries are not allowed and subsequent DHCP ACK messages are discarded.

The retained lease state information representing dynamic hosts may be used to:

- Populate a SAP based anti-spoof filter table to provide dynamic anti-spoof filtering. If the system is unable to populate the dynamic host information in the anti-spoof filter table on the SAP, the DHCP ACK message must be discarded without adding new lease state entry or updating an existing lease state entry.
- Populate the system's ARP cache based on the arp-populate configuration. Applicable to IES and VPRN interfaces or group-interfaces.
- Populate managed entries into a VPLS forwarding database. VPLS forwarding database population is an implicit feature that automatically places the dynamic host's MAC address into the VPLS FDB. When a dynamic host's MAC address is placed in the lease state table, it will automatically be populated into the VPLS forwarding database associated with the SAP on which the host is learned. The dynamic host MAC address will override any static MAC entries using the same MAC and prevent dynamic learning of the MAC on another interface. Existing static MAC entries with the same MAC address as the dynamic host are marked as inactive but not deleted. If all entries in the lease state table associated with the MAC address are removed, the static MAC may be populated. New static MAC definitions for the VPLS instance may be created while a dynamic host exists associated with the static MAC address.
- Generate dynamic ARP replies if **arp-reply-agent** is enabled. Applicable to VPLS service SAPs

The **no** form of this command reverts to the default.

Parameters *nbr-of-leases* — Specifies the number of DHCPv4 leases allowed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

l2-header — Indicates a mode of operation where anti-spoof entry associated with the given DHCP state is created based on the *src-mac* address from the Layer 2 header of the DHCP request message. The Layer 2 header flag is not set by default. This parameter is only applicable for group interfaces.

mac — Specifies that the provisioned *ieee-address* is used in the anti-spoofing entries for this SAP. The parameter may be changed mid-session. Existing sessions will not be re-programmed unless a **tools>perform>subscriber-mgmt>remap-lease-state** command is issued for the lease. This parameter is only applicable for group interfaces.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface dhcp lease-populate
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp lease-populate
- configure service vprn subscriber-interface dhcp lease-populate
- configure service vprn subscriber-interface group-interface dhcp lease-populate

All

- configure service vprn interface dhcp lease-populate
- configure service ies interface dhcp lease-populate
- configure service vpls sap dhcp lease-populate

lease-populate

Syntax **lease-populate** [*nbr-of-leases*]
lease-populate [*nbr-of-leases*] **route-populate** [**pd**] **na** [**ta**]
lease-populate [*nbr-of-leases*] **route-populate pd** [**na**] [**ta**] [**exclude**]
lease-populate [*nbr-of-leases*] **route-populate** [**pd**] [**na**] **ta**
no lease-populate

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6-relay lease-populate)

Full Context configure service ies interface ipv6 dhcp6-relay lease-populate

Description This command specifies the maximum number of DHCPv6 lease states allocated by the DHCPv6 relay function, allowed on this interface.

Optionally, by specifying **route-populate** parameter, system could:

- Create routes based on the IA_PD/IA_NA/IA_TA prefix option in relay-reply message.
- Create black hole routes based on OPTION_PD_EXCLUDE in IA_PD in relay-reply message.

These routes could be redistributed into IGP/BGP by using route-policy, following protocol types that could be used in “from protocol”:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- dhcpv6-pd
- dhcpv6-na
- dhcpv6-ta
- dhcpv6-pd-excl

Parameters *nbr-of-leases* — Defines the number lease state table entries allowed for this interface. If this parameter is omitted, only a single entry is allowed. Once the maximum number of entries has been reached, subsequent lease state entries are not allowed and subsequent DHCPv6 REPLY messages are discarded.

Values 1 to 8000

route-populate — Specifies the route populate parameter.

Values pd/na/ta — Create route based on specified option.
exclude — Create blackhole route based on OPTION_PD_EXCLUDE.

Platforms All

lease-populate

Syntax **lease-populate** [*nbr-of-leases*]
lease-populate [*nbr-of-leases*] **route-populate** [**pd**] **na** [**ta**]
lease-populate [*nbr-of-leases*] **route-populate pd** [**na**] [**ta**] [**exclude**]
lease-populate [*nbr-of-leases*] **route-populate** [**pd**] [**na**] **ta**
no lease-populate

Context **[Tree]** (config>service>ies>if>ipv6>dhcp-relay lease-populate)

Full Context configure service ies interface ipv6 dhcp-relay lease-populate

Description This command specifies the maximum number of DHCPv6 lease states allocated by the DHCPv6 relay function, allowed on this interface.

Optionally, by specifying “route-populate” parameter, system could:

- Create routes based on the IA_PD/IA_NA/IA_TA prefix option in relay-reply message.
- Create black hole routes based on OPTION_PD_EXCLUDE in IA_PD in relay-reply message.

These routes could be redistributed into IGP/BGP by using route-policy, following protocol types that could be used in “from protocol”:

- dhcpv6-pd
- dhcpv6-na
- dhcpv6-ta
- dhcpv6-pd-excl

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *nbr-of-entries* — Defines the number lease state table entries allowed for this interface. If this parameter is omitted, only a single entry is allowed. Once the maximum number of entries has been reached, subsequent lease state entries are not allowed and subsequent DHCPv6 ACK messages are discarded.

Values 1 to 8000

route-populate — Specifies the route populate parameter.

Values pd/na/ta — Create route based on specified option.
exclude — Create blackhole route based on OPTION_PD_EXCLUDE.

16.94 lease-query

lease-query

Syntax **lease-query** [**max-retry** *Max nbr of retries*]
no lease-query

Context **[Tree]** (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client lease-query)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client lease-query)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client lease-query
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client lease-query

Description This command enables lease-query. If this is specified the dhcp6-client will retrieve any existing addresses when becoming active. The lease-query is performed for all of the configured servers

The **no** form of this command disables lease-query.

Parameters *Max nbr of retries* — Specifies the maximum number of retries before the lease query assumes no existing subnets were allocated.

Values 0 to 10

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.95 lease-rebind-time

lease-rebind-time

Syntax **lease-rebind-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-rebind-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>dhcp>server>pool>options lease-rebind-time)
[Tree] (config>service>vprn>dhcp>server>pool>options lease-rebind-time)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options lease-rebind-time)

Full Context configure router dhcp local-dhcp-server pool options lease-rebind-time
configure service vprn dhcp local-dhcp-server pool options lease-rebind-time
configure subscriber-mgmt local-user-db ipoe host options lease-rebind-time

Description This command configures the time the client transitions to a rebinding state for a DHCP client.

The **no** form of this command removes the time from the configuration.

Parameters *lease-rebind-time* — Specifies the lease rebind time.

Values

days:	0 to 3650
hours:	0 to 23
minutes:	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.96 lease-renew-time

lease-renew-time

Syntax **lease-renew-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-renew-time

Context [Tree] (config>router>dhcp>server>pool>options lease-renew-time)
[Tree] (config>service>vprn>dhcp>server>pool>options lease-renew-time)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options lease-renew-time)

Full Context configure router dhcp local-dhcp-server pool options lease-renew-time
configure service vprn dhcp local-dhcp-server pool options lease-renew-time
configure subscriber-mgmt local-user-db ipoe host options lease-renew-time

Description This command configures the time the client transitions to a renew state for a DHCP client.

The **no** form of this command removes the time from the configuration.

Parameters *lease-renew-time* — Specifies the lease renew time.

Values

days:	0 to 3650
hours:	0 to 23

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

minutes: 0 to 59
seconds 0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.97 lease-time

lease-time

Syntax **lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-time

Context **[Tree]** (config>router>dhcp>server>pool>options lease-time)
[Tree] (config>service>vprn>dhcp>server>pool>options lease-time)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options lease-time)

Full Context configure router dhcp local-dhcp-server pool options lease-time
configure service vprn dhcp local-dhcp-server pool options lease-time
configure subscriber-mgmt local-user-db ipoe host options lease-time

Description This command configures the amount of time that the DHCP server grants to the DHCP client permission to use a specific IP address.

The **no** form of this command removes the lease time parameters from the configuration.

Parameters *days* — Specifies the number of days that the given IP address is valid.

Values 0 to 3650

hours — Specifies the number of hours that the given IP address is valid.

Values 0 to 23

minutes — Specifies the number of minutes that the given IP address is valid.

Values 0 to 59

seconds — Specifies the number of seconds that the given IP address is valid.

Values 0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

lease-time

Syntax **lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**override**]
no lease-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>service>vpls>sap>dhcp>proxy-server lease-time)
[Tree] (config>service>ies>if>dhcp>proxy-server lease-time)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>proxy-server lease-time)
[Tree] (config>service>vprn>if>dhcp>proxy lease-time)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>proxy-server lease-time)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>proxy lease-time)

Full Context
configure service ies interface dhcp proxy-server lease-time
configure service ies subscriber-interface group-interface dhcp proxy-server lease-time
configure service vpls sap dhcp proxy-server lease-time
configure service vprn interface dhcp proxy-server lease-time
configure service vprn subscriber-interface group-interface dhcp proxy-server lease-time
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp proxy-server lease-time

Description
This command defines the length of lease-time that is provided to DHCP clients. By default, the local-proxy-server always makes use of the lease time information provide by either a RADIUS or DHCP server.

The **no** form of this command disables the use of the lease-time command. The local-proxy-server will use the lease-time offered by either a RADIUS or DHCP server.

Default
lease-time days 7

Parameters
override — Specifies that the local-proxy-server will use the configured lease-time information to provide DHCP clients

days — Specifies the number of days that the given IP address is valid.

Values 0 to 3650

hours — Specifies the number of hours that the given IP address is valid.

Values 0 to 23

minutes — Specifies the number of minutes that the given IP address is valid.

Values 0 to 59

seconds — Specifies the number of seconds that the given IP address is valid.

Values 0 to 59

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface dhcp proxy-server lease-time
- configure service vprn subscriber-interface group-interface dhcp proxy-server lease-time
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp proxy-server lease-time

All

- configure service vpls sap dhcp proxy-server lease-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface dhcp proxy-server lease-time
- configure service ies interface dhcp proxy-server lease-time

lease-time

Syntax **lease-time** [*lease-time*]
no lease-time

Context **[Tree]** (config>service>ies>sub-if>grp-if>wpp lease-time)
[Tree] (config>service>vprn>sub-if>grp-if>wpp lease-time)

Full Context configure service ies subscriber-interface group-interface wpp lease-time
configure service vprn subscriber-interface group-interface wpp lease-time

Description This command configures the amount of time that the DHCP server grants to the DHCP client permission to use a particular IP address.

The **no** form of this command removes the lease time parameters from the configuration.

Parameters *lease-time* — Specifies the lease time.

Values

days *days*	0 to 3650
hrs *hours*	0 to 23
min *minutes*	0 to 59
sec *seconds*	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

lease-time

Syntax **lease-time** *seconds*
lease-time [**days** <*days*>] [**hrs** <*hrs*>] [**min** <*min*>] [**sec** <*sec*>]
no lease-time

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool lease-time)

Full Context configure subscriber-mgmt vrgw brg brg-profile dhcp-pool lease-time

Description This command configures the lease time, in seconds, to be used when allocating addresses from the pool. This time value should always be longer than the renew/rebind time.

The **no** form of this command reverts to the default.

Default lease-time hrs 6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the lease time in seconds.

Values 300 to 315446399

days — Specifies the lease time in days.

Values 1 to 3650

hrs — Specifies the lease time in hours.

Values 1 to 23

min — Specifies the lease time in minutes.

Values 1 to 59

sec — Specifies the lease time in seconds.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.98 least-fill

least-fill

Syntax [**no**] **least-fill**

Context **[Tree]** (config>router>mpls>lsp least-fill)
[Tree] (config>router>mpls>lsp-template least-fill)

Full Context configure router mpls lsp least-fill
configure router mpls lsp-template least-fill

Description This command enables the use of the least-fill path selection method for the computation of the path of this LSP.

When MPLS requests the computation of a path for this LSP, CSPF will find all equal cost shortest paths which satisfy the constraints of this path. Then, CSPF identifies the single link in each of these paths which has the least available bandwidth as a percentage of its maximum reservable bandwidth. It then selects the path which has the largest value of this percentage least available bandwidth figure. CSPF identifies the least available bandwidth link in each equal cost path after it has accounted for the bandwidth of the new requested path of this LSP.

CSPF applies the least-fill path selection method to all requests for a path, primary and secondary, of an LSP for which this option is enabled. The bandwidth of the path can be any value, including zero.

CSPF applies the least-fill criterion separately to each preemption priority in the base TE. A higher setup priority path can preemptively lower holding priority paths.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

CSPF also applies the least-fill criterion separately to each Diff-Serv TE class if Diff-Serv TE is enabled on this node. A higher setup priority path can preemptively lower holding priority paths within a Class Type.

MPLS will re-signal and move the LSP to the new path in the following cases:

- Initial LSP path signaling.
- Re-try of an LSP path after failure.
- Make-before-break (MBB) due to pending soft preemption of the LSP path.
- MBB due to LSP path configuration change, that is, a user change to bandwidth parameter of primary or secondary path, or a user enabling of fast-reroute option for the LSP.
- MBB of secondary path due to an update to primary path SRLG.
- MBB due to FRR Global Revertive procedures on the primary path.
- Manual re-signaling of an LSP path or of all LSP paths by the user.

During a manual re-signaling of an LSP path, MPLS will always re-signal the path regardless of whether the new path is exactly the same or different than the current path and regardless of whether the metric of the new path is different or not from that of the current path.

During a timer-based re-signaling of an LSP path which has the least-fill option enabled, MPLS will only re-signal the path if the metric of the new path is different than the one of the current path.

The **no** form of this command deletes a specific node entry in this database.

Default no least-fill. The path of an LSP is randomly chosen among a set of equal cost paths.

Platforms All

16.99 least-fill-min-thd

least-fill-min-thd

Syntax **least-fill-min-thd** *percent*
no least-fill-min-thd

Context **[Tree]** (config>router>mpls least-fill-min-thd)

Full Context configure router mpls least-fill-min-thd

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This parameter is used in the least-fill path selection process. When comparing the percentage of least available link bandwidth across the sorted paths, whenever two percentages differ by less than the value configured as the least-fill-min-thresh, CSPF will consider them equal and will apply a random number generator to select the path among these paths

The **no** form of this command resets this parameter to its default value.

Default least-fill-min-thd 5

Parameters *percentage* — Specifies the least fill minimum threshold value as a percentage.

Values 1 to 100%

Platforms All

16.100 least-fill-reoptim-thd

least-fill-reoptim-thd

Syntax **least-fill-reoptim-thd** *percent*
no least-fill-reoptim-thd

Context **[Tree]** (config>router>mpls least-fill-reoptim-thd)

Full Context configure router mpls least-fill-reoptim-thd

Description This parameter is used in the least-fill path selection method. During a timer-based re-signaling of an LSP path which has the least-fill option enabled, CSPF will first update the least-available bandwidth figure for the current path of this LSP. It then applies the least-fill path selection method to select a new path for this LSP. If the new computed path has the same cost as the current path, it will compare the least-available bandwidth figures of the two paths and if the difference exceeds the user configured optimization threshold, MPLS will generate a trap to indicate that a better least-fill path is available for this LSP. This trap can be used by an external SNMP based device to trigger a manual re-signaling of the LSP path since the timer-based re-signaling will not re-signal the path in this case. MPLS will generate a path update trap at the first MBB event which results in the re-signaling of the LSP path. This should clear the eligibility status of the path at the SNMP device.

The **no** form of this command resets this parameter to its default value.

Default least-fill-reoptim-thd 10

Parameters *percentage* — Specifies the least fill reoptimization threshold value as a percentage.

Values 1 to 100%

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.101 leave-all-sm

leave-all-sm

Syntax [**no**] **leave-all-sm**

Context **[Tree]** (debug>service>id>mrp leave-all-sm)

Full Context debug service id mrp leave-all-sm

Description This command enables debugging of the leave all state machine.

The **no** form of this command disables debugging of the leave all state machine.

Platforms All

16.102 leave-all-time

leave-all-time

Syntax **leave-all-time** *value*
no leave-all-time

Context **[Tree]** (config>service>vpls>sap>mrp leave-all-time)
[Tree] (config>service>vpls>spoke-sdp>mrp leave-all-time)
[Tree] (config>service>vpls>mesh-sdp>mrp leave-all-time)

Full Context configure service vpls mesh-sdp mrp leave-all-time
configure service vpls sap mrp leave-all-time
configure service vpls spoke-sdp mrp leave-all-time

Description This command controls the frequency with which the LeaveAll state machine generates LeaveAll PDUs. The timer is required on a per-Port, per-MRP Participant basis. The Leave All Period Timer is set to a random value, T, in the range LeaveAllTime<T<1.5*leave-all-time when it is started. Refer to IEEE 802.1ak-2007 section 10.7.4.3.

Default leave-all-time 100

Parameters *value* — The frequency with which the LeaveAll state machine generates LeaveAll PDUs, in tenths of a second.

Values 60 to 300

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.103 leave-time

leave-time

Syntax **leave-time** *value*
no leave-time

Context **[Tree]** (config>service>vpls>sap>mrp leave-time)
[Tree] (config>service>vpls>spoke-sdp>mrp leave-time)
[Tree] (config>service>vpls>mesh-sdp>mrp leave-time)

Full Context configure service vpls mesh-sdp mrp leave-time
configure service vpls sap mrp leave-time
configure service vpls spoke-sdp mrp leave-time

Description This command controls the period of time that the Registrar state machine will wait in the leave state before transitioning to the MT (Empty) state when it is removed. An instance of the timer is required for each state machine that is in the leave state. The leave period timer is set to the value specified for **leave-time** when it is started.

A registration is normally in an “in” state where there is an MFIB entry and traffic is being forwarded. When a “leave all” is performed (periodically around every 10-15 seconds per SAP/SDP binding - see leave-all-time-below), a node sends a message to its peer indicating a leave all is occurring and puts all of its registrations in leave state.

The peer refreshes its registrations based on the leave all PDU it receives and sends a PDU back to the originating node with the state of all its declarations.

Refer to IEEE 802.1ak-2007 section 10.7.4.2.

Default leave-time 30

Parameters *value* — The period of time that the Registrar state machine waits in the leave state before transitioning to the MT state, in tenths of a second.

Values 30 to 60

Platforms All

16.104 legacy

legacy

Syntax [**no**] **legacy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis>te>application-link-attributes legacy)

Full Context configure router isis traffic-engineering-options application-link-attributes legacy

Description This command enables legacy mode of advertising TE attributes.

The **no** form of this command disables legacy mode, but enables the per-application TE attribute advertisement for RSVP-TE.

Default legacy

Platforms All

16.105 legacy-dns-nbns

legacy-dns-nbns

Syntax [**no**] **legacy-dns-nbns**

Context [Tree] (config>subscr-mgmt>sys-bhv legacy-dns-nbns)

Full Context configure subscriber-mgmt system-behavior legacy-dns-nbns

Description This command enables legacy DNS NBNS behavior, which restricts the supported default extended authentication origins for DNS and NBNS name servers. The main differences include:

- only support DHCP server as origin for DHCP relay: IPoE DHCPv4/DHCPv6 and PPPoE DHCPv6
- Local Address Assignment (LAA) is highest priority origin: IPoE and PPPoE SLAAC DNSv6 and PPPoE DNSv4
- no default DNS for IPoE DHCPv4 proxy

The **no** form of this command reverts to the recommended default extended DNS and NBNS name server origin priorities.

Default no legacy-dns-nbns

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.106 legacy-ipv4-lsr-interop

legacy-ipv4-lsr-interop

Syntax [**no**] **legacy-ipv4-lsr-interop**

Context **[Tree]** (config>router>ldp legacy-ipv4-lsr-interop)

Full Context configure router ldp legacy-ipv4-lsr-interop

Description This command provides for a global LDP knob to allow interoperability with legacy IPv4 LSR implementations which do not comply with the processing of Hello TLVs with the U-bit set. Specifically, this feature disables the following Hello TLVs:

- The Nokia proprietary Interface Info TLV (0x3E05) in the Hello message sent to the peer. This also results in the non-generation of the Nokia proprietary Hello Adjacency Status TLV (0x3E06) since the Interface Info TLV is not sent.

  This is performed in SR OS releases 12 and higher.
- The RFC 7552 standard dual-stack capability TLV (0x701) and the Nokia proprietary Adjacency capability TLV (0x3E07) in SR OS releases 13 and higher.

Platforms All

16.107 length

length

Syntax **length** {**133** | **266** | **399** | **533** | **655**}

Context **[Tree]** (config>port>tdm length)

Full Context configure port tdm length

Description This command applies only to a DS-1 port configured with a 'short' buildout. The **length** command configures the length of the line (in feet). For line lengths longer than 655 feet, configure the DS-1 port buildout as 'long'.

For 'long' buildout the following values are valid:

NotApplicable — Not applicable

For 'short' buildout the following values are valid:

- 0 to 133 For line length from 0 to 133 feet
- 134 to 266 For line length from 134 to 266 feet

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- 267 to 399 For line length from 267 to 399 feet
- 400 to 533 For line length from 400 to 533 feet
- 534 to 655 For line length from 534 to 655 feet

The default for 'long' buildout is 'NotApplicable' while the default for 'short' buildout is '0 to 133'.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

length

Syntax **length** *lines*

Context **[Tree]** (environment>terminal length)

Full Context environment terminal length

Description This command sets the number of lines on a screen.

Parameters *lines* — Specifies the number of lines for the terminal screen length, expressed as a decimal integer.

Values 1 to 512

Default 24 — terminal dimensions are set to 24 lines long by 80 characters wide

Platforms All

length

Syntax **length** *lines*

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment>console length)

Full Context configure system management-interface cli md-cli environment console length

Description This command configures the set number of lines displayed on screen.

Default length 24

Parameters *lines* — Specifies the number of lines displayed in the console window.

Values 24 to 512

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.108 ler-use-dscp

ler-use-dscp

Syntax [**no**] **ler-use-dscp**

Context **[Tree]** (config>qos>network>ingress ler-use-dscp)

Full Context configure qos network ingress ler-use-dscp

Description This command is used to enable tunnel QoS mapping on all ingress network IP interfaces that the network-qos-policy-id is associated with. The command may be defined at any time after the network QoS policy has been created. Any network IP interfaces currently associated with the policy will immediately start to use the internal IP ToS field of any tunnel terminated IP routed packet received on the interface, ignoring any QoS markings in the tunnel portion of the packet.

This attribute provides the ability to ignore the network ingress QoS mapping of a terminated tunnel containing an IP packet that is to be routed to a base router or VPRN destination. This is advantageous when the mapping for the tunnel QoS marking does not accurately or completely reflect the required QoS handling for the IP routed packet. When the mechanism is enabled on an ingress network IP interface, the IP interface will ignore the tunnel's QoS mapping and derive the internal forwarding class and profile based on the precedence or DiffServ Code Point (DSCP) values within the routed IP header ToS field compared to the Network QoS policy defined on the IP interface.

The default state is not to enforce tunnel termination IP routed QoS override within the network QoS policy.

The **no** form of this command removes tunnel termination IP routed QoS override from the network QoS policy and all ingress network IP interfaces associated with the policy.

Default no ler-use-dscp

Platforms All

16.109 less-specific

less-specific

Syntax **less-specific** [**allow-default**]
no less-specific

Context **[Tree]** (config>vrrp>policy>priority-event>route-unknown less-specific)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure vrrp policy priority-event route-unknown less-specific

Description This command allows a CIDR shortest match hit on a route prefix that contains the IP route prefix associated with the route unknown priority event.

The **less-specific** command modifies the search parameters for the IP route prefix specified in the **route-unknown** priority event. Specifying **less-specific** allows a CIDR shortest match hit on a route prefix that contains the IP route prefix.

The **less-specific** command eases the RTM lookup criteria when searching for the *prefix/mask-length*. When the **route-unknown** priority event sends the prefix to the RTM (as if it was a destination lookup), the result route table prefix (if a result is found) is checked to see if it is an exact match or a less specific match. The **less-specific** command enables a less specific route table prefix to match the configured prefix. When **less-specific** is not specified, a less specific route table prefix fails to match the configured prefix. The **allow-default** optional parameter extends the **less-specific** match to include the default route (0.0.0.0).

The **no** form of the command prevents RTM lookup results that are less specific than the route prefix from matching.

Default no less-specific — The route unknown priority events requires an exact prefix/mask match.

Parameters **allow-default** — When the **allow-default** parameter is specified with the **less-specific** command, an RTM return of 0.0.0.0 matches the IP prefix. If **less-specific** is entered without the **allow-default** parameter, a return of 0.0.0.0 will not match the IP prefix. To disable **allow-default**, but continue to allow **less-specific** match operation, only enter the **less-specific** command (without the **allow-default** parameter).

Platforms All

16.110 level

level

Syntax **level** *level-id* **bw** *bandwidth*
no level *level-id*

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac>mc-constraints level)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac mc-constraints level

Description This command configures levels and their associated bandwidth for multicast CAC policy on an interface.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *level-id* — Specifies has an entry for each multicast CAC policy constraint level configured on a system.

Values 1 to 8

bandwidth — Specifies the bandwidth in kilobits per second (kb/s) for the level.

Values 1 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

level

Syntax **level** *priority-level* **rate** *pir-rate* [**cir** *cir-rate*]
level *priority-level* **percent-rate** *pir-percent* [**percent-cir** *cir-percent*]
no level *priority-level*

Context **[Tree]** (config>port>ethernet>egr-scheduler-override level)
[Tree] (config>port>sonet-sdh>path>egr-scheduler-override level)
[Tree] (config>port>tdm>ds1>channel-group>egr-scheduler-override level)
[Tree] (config>port>tdm>ds3>egr-scheduler-override level)
[Tree] (config>port>tdm>e1>egr-scheduler-override level)
[Tree] (config>port>tdm>e3>egr-scheduler-override level)

Full Context configure port ethernet egress-scheduler-override level
configure port sonet-sdh path egress-scheduler-override level
configure port tdm ds1 channel-group egress-scheduler-override level
configure port tdm ds3 egress-scheduler-override level
configure port tdm e1 egress-scheduler-override level
configure port tdm e3 egress-scheduler-override level

Description This command overrides the maximum and CIR rate parameters for a specific priority level on the port or channel's port scheduler instance. When the **level** command is executed for a priority level, the corresponding priority level command in the port-scheduler-policy associated with the port is ignored.

The override level command supports the keyword **max** for the **rate** and **cir** parameter. When executing the level override command, at least the **rate** or **cir** keywords and associated parameters must be specified for the command to succeed.

The **no** form of this command removes the local port priority level rate overrides. Once removed, the port priority level will use the port scheduler policies level command for that priority level.

Parameters *priority-level* — Identifies which of the eight port priority levels are being overridden.

Values 1 to 8

pir-rate — Overrides the port scheduler policy's maximum level rate and requires either the **max** keyword or a rate defined in kilobits per second to follow.

Values For Ethernet: 1 to 6400000000, **max**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For SONET-SDH and TDM: 1 to 3200000000, **max**

cir-rate — Overrides the port scheduler policy's within-cir level rate and requires either the max keyword or a rate defined in kilobits per second to follow.

Values For Ethernet: 1 to 6400000000, **max**
For SONET-SDH and TDM: 1 to 3200000000, **max**

pir-percent — Specifies the PIR as a percentage.

Values 0.01 to 100.00

cir-percent — Specifies the CIR as a percentage.

Values 0.00 to 100.00

max — removes any existing rate limit imposed by the port scheduler policy for the priority level allowing it to use as much total bandwidth as possible.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path egress-scheduler-override level

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group egress-scheduler-override level
- configure port tdm ds3 egress-scheduler-override level
- configure port tdm e3 egress-scheduler-override level

All

- configure port ethernet egress-scheduler-override level

level

Syntax **level** *level-number*

Context **[Tree]** (config>service>vpls>spb level)

Full Context configure service vpls spb level

Description This command creates the context to configure SPB Level 1 or Level 2 area attributes. This is IS-IS levels. Only Level 1 can be configured.

A Level 1 adjacency can be established only with other Level 1 B-VPLS. A Level 2 adjacency can be established only with other Level 2 B-VPLS. Currently there is no support for level 1 and level 2 in the same instance of SPB.

Default level 1

Parameters *level-number* — The SPB level number.

Values 1, 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

level

Syntax **level** [1 to 1]

Context **[Tree]** (config>service>vpls>spb level)
[Tree] (config>service>vpls>sap>spb level)
[Tree] (config>service>vpls>spoke-sdp>spb level)

Full Context configure service vpls sap spb level
configure service vpls spb level
configure service vpls spoke-sdp spb level

Description Commands in this context configure SPB level information.

Platforms All

level

Syntax **level** *level-id* **bw** *bandwidth*
no level *level-id*

Context **[Tree]** (config>service>vpls>sap>igmp-snooping>mcac>mc-constraints level)
[Tree] (config>service>vpls>sap>mld-snooping>mcac>mc-constraints level)

Full Context configure service vpls sap igmp-snooping mcac mc-constraints level
configure service vpls sap mld-snooping mcac mc-constraints level

Description This command configures levels and their associated bandwidth for multicast CAC policy on this interface.

Parameters *level-id* — Specifies has an entry for each multicast CAC policy constraint level configured on this system

Values 1 to 8

bandwidth — Specifies the bandwidth in kilobits per second (kb/s) for the level.

Values 1 to 2147483647

Platforms All

level

Syntax **level** *level-id* **bw** *bandwidth*
no level *level-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>igmp>if>mcac>mc-constraints level)
[Tree] (config>service>vprn>mld>if>mcac>mc-constraints level)
[Tree] (config>service>vprn>pim>if>mcac>mc-constraints level)

Full Context configure service vprn igmp interface mcac mc-constraints level
configure service vprn mld interface mcac mc-constraints level
configure service vprn pim interface mcac mc-constraints level

Description This command configures interface levels and associated bandwidth for multicast CAC policy.

The **no** form of this command removes the values from the configuration.

Parameters *level-id* — Specifies an entry for the multicast CAC policy constraint level configured on this system.

Values 1 to 8

bandwidth — Specifies the bandwidth in kb/s for the level.

Values 1 to 2147483647

Platforms All

level

Syntax **level** *level-number*

Context [Tree] (config>service>vprn>isis level)
[Tree] (config>service>vprn>isis>if level)
[Tree] (config>service>vprn>isis>link-group level)

Full Context configure service vprn isis interface level
configure service vprn isis level
configure service vprn isis link-group level

Description This command creates the context to configure IS-IS Level 1 or Level 2 area attributes.

A router can be configured as a Level 1, Level 2, or Level 1-2 system. A Level 1 adjacency can be established if there is at least one area address shared by this router and a neighbor. A Level 2 adjacency cannot be established over this interface.

Level 1/2 adjacency is created if the neighbor is also configured as Level 1/2 router and has at least one area address in common. A Level 2 adjacency is established if there are no common area IDs.

A Level 2 adjacency is established if another router is configured as Level 2 or a Level 1/2 router with interfaces configured as Level 1/2 or Level 2. Level 1 adjacencies are not established over this interface.

To reset global and/or interface level parameters to the default, the following commands must be entered independently:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

level> no hello-authentication-key level> no hello-authentication-type level> no hello-interval level> no hello-multiplier level> no metric level> no passive level> no priority

Default level 1 or level 2

Special Cases **Global IS-IS Level —** The **config>router>isis** context configures default global parameters for both Level 1 and Level 2 interfaces.

IS-IS Interface Level — The **config>router>isis>if** context configures IS-IS operational characteristics of the interface at Level 1 and/or Level 2. A logical interface can be configured on one Level 1 and one Level 2. In this case, each level can be configured independently and parameters must be removed independently.

By default an interface operates in both Level 1 and Level 2 modes.

Parameters *level-number* — The IS-IS level number.

Values 1, 2

Platforms All

level

Syntax **level** *syslog-level*

Context **[Tree]** (config>service>vprn>log>syslog level)

Full Context configure service vprn log syslog level

Description This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.

Only a single threshold level can be specified. If multiple levels are entered, the last **level** entered will overwrite the previously entered commands.

Default level info

Parameters *syslog-* — The threshold severity level name.

Values emergency, alert, critical, error, warning, notice, info, debug

Router severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
	0	emergency	system is unusable
3	1	alert	action must be taken immediately
4	2	critical	critical condition
5	3	error	error condition
6	4	warning	warning condition
	5	notice	normal but significant condition

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Router severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
1 cleared 2 indeterminate	6	info	informational messages
	7	debug	debug-level messages

Platforms All

level

Syntax **level** *level* **bw** *bandwidth*
no level *level*

Context **[Tree]** (config>router>igmp>interface>mcac>mc-constraints level)
[Tree] (config>router>mcac>policy>bundle>mc-constraints level)
[Tree] (config>router>mld>interface>mcac>mc-constraints level)
[Tree] (config>router>pim>interface>mcac>mc-constraints level)

Full Context configure router igmp interface mcac mc-constraints level
configure router mcac policy bundle mc-constraints level
configure router mld interface mcac mc-constraints level
configure router pim interface mcac mc-constraints level

Description This command configures the amount of bandwidth available within a given bundle for MC traffic for a specified level. The amount of allowable BW for the specified level is expressed in kb/s and this can be defined for up to eight different levels.

If no bandwidth is defined for a given level then no limit is applied.

The **no** form of this command removes the level from the configuration.

Parameters *level* — Specifies the bandwidth for a given level. Level 1 has the highest priority. Level 8 has the lowest priority.

Values 1 to 8

bw *bandwidth* — Specifies the bandwidth, in kb/s, for the level.

Values 1 to 2147483647 kb/s

Default 1

Platforms All

level

Syntax **level** *priority-level* **rate** *pir-rate* [**cir** *cir-rate*] **group** *name* [**weight** *weight*] [**monitor-threshold** *percent*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

level *priority-level* **percent-rate** *pir-percent* [**percent-cir** *cir-percent*] **group** *name* [**weight** *weight*] [**monitor-threshold** *percent*]
level *priority-level* **rate** *pir-rate* [**cir** *cir-rate*] [**monitor-threshold** *percent*]
level *priority-level* **percent-rate** *pir-percent* [**percent-cir** *cir-percent*] [**monitor-threshold** *percent*]
no level *priority-level*

Context **[Tree]** (config>qos>port-scheduler-policy level)

Full Context configure qos port-scheduler-policy level

Description This command configures an explicit within-CIR bandwidth limit and a total bandwidth limit for each port scheduler's priority level. To understand how to set the level rate and CIR parameters, a basic understanding of the port-level scheduler bandwidth allocation mechanism is required. The port scheduler takes all available bandwidth for the port or channel (after the max-rate and any port egress-rate limits have been accounted for) and offers it to each of the eight priority levels twice.

The first pass is called the within-CIR pass and consists of providing the available port bandwidth to each of the 8 priority levels, starting with level 8 and moving down to level 1. Each level takes the offered load and distributes it to all child members that have a port-parent cir-level equal to the current priority level. (Any child with a cir-weight equal to 0 is skipped in this pass.) Each child may consume bandwidth up to the child's frame-based within-CIR offered load. The remaining available port bandwidth is then offered to the next lower priority level until level 1 is reached.

The second pass is called the above-CIR pass and consists of providing the remaining available port bandwidth to each of the eight priority levels a second time. Again, each level takes the offered load and distributes it to all child members that have a port-parent level equal to the current priority level. Each child may consume bandwidth up to the remainder of the child's frame-based offered load (some of the offered load may have been serviced during the within-CIR pass). The remaining available port bandwidth is then offered to the next priority level until level 1 is again reached.

If the port scheduling policy is using the default orphan behavior (orphan-override has not been configured on the policy), the system then takes any remaining port bandwidth and allocates it to the orphan queues and scheduler on priority level 1. In a non-override orphan state, all orphans are attached to priority level 1 using a weight of 0. The zero weight value causes the system to allocate bandwidth equally to all orphans based on each orphan queue or scheduler's ability to use the bandwidth. If the policy has an orphan-override configured, the orphans are handled based on the override commands parameters in a similar fashion to properly parented queues and schedulers.

The port scheduler priority level command rate keyword is used to optionally limit the total amount of bandwidth that is allocated to a priority level (total for the within-CIR and above-CIR passes). The cir keyword optionally limits the first pass bandwidth allocated to the priority level during the within-CIR pass.

When executing the level command, at least one of the optional keywords, **rate** or **cir,** must be specified. If neither keyword is included, the command will fail.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a previous explicit value for rate or cir exists when the level command is executed, and either rate or cir is omitted, the previous value for the parameter is overwritten by the default value and the previous value is lost.

The configured priority level rate limits may be overridden at the egress port or channel using the egress-scheduler-override level priority-level command. When a scheduler instance has an override defined for a priority level, both the rate and cir values are overridden even when one of them is not explicitly expressed in the override command. For instance, if the cir kilobits per second portion of the override is not expressed, the scheduler instance defaults to not having a CIR rate limit for the priority level even when the port scheduler policy has an explicit CIR limit defined.

The **no** form of this command returns the level to its default value.

Default no level priority-level

Parameters *priority-level* — Specifies to which priority level the level command pertains. Each of the eight levels is represented by an integer value of 1 to 8, with 8 being the highest priority level.

Values 1 to 8 (8 is the highest priority)

pir-rate — Specifies the total bandwidth limits allocated to priority-level, in kilobits per second.

Values 1 to 6400000000, **max**

pir-percent — Specifies the percent bandwidth limits allocated to priority-level.

Values 0.01 to 100.00

cir-rate — The cir specified limits the total bandwidth allocated in the within-CIR distribution pass to priority-level. When cir is not specified, all the available port or channel bandwidth may be allocated to the specified priority level during the within-CIR pass.

Values 0 to 6400000000, **max**

The value given for kilobits per second is expressed in kilobits per second on a base 10 scale as is usual for line rate calculations. If a value of 1 is given, the result is 1000 bits per second (as opposed to a base 2 interpretation that would be 1024 bits per second).

cir-percent — Specifies the percent bandwidth limits allocated to priority-level.

Values 0.00 to 100.00

group *name* — specifies the existing group that the weighted scheduler group this level maps to, up to 32 characters.

weight — Specifies the weight of the level within this weighted scheduler group.

Values 1 to 100

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

monitor-threshold *percent* — Specifies the percent of the configured rate. If the offered rate exceeds the configured threshold, a counter monitoring the threshold will be increased.

Values 0 to 100

Platforms All

level

Syntax **level** *syslog-level*
no level

Context **[Tree]** (config>log>syslog level)

Full Context configure log syslog level

Description This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.

Only a single threshold level can be specified. If multiple levels are entered, the last **level** entered will overwrite the previously entered commands.

The **no** form of this command reverts to the default value.

Default level info

Parameters *value* — Specifies the threshold severity level name.

Values emergency, alert, critical, error, warning, notice, info, debug

Table 73 **Level Parameter Value Descriptions**

Router severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
	0	emergency	system is unusable
3	1	alert	action must be taken immediately
4	2	critical	critical condition
5	3	error	error condition
6	4	warning	warning condition
	5	notice	normal but significant condition
1 cleared 2 indeterminate	6	info	informational messages

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 73 **Level Parameter Value Descriptions**

Router severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
	7	debug	debug-level messages

Platforms All

level

Syntax **level** {**1** | **2**}

Context **[Tree]** (config>router>isis level)
[Tree] (config>router>isis>interface level)

Full Context configure router isis interface level
configure router isis level

Description This command creates the context to configure IS-IS Level 1 or Level 2 area attributes.

A router can be configured as a Level 1, Level 2, or Level 1-2 system. A Level 1 adjacency can be established if there is at least one area address shared by this router and a neighbor. A Level 2 adjacency cannot be established over this interface.

Level 1/2 adjacency is created if the neighbor is also configured as Level 1/2 router and has at least one area address in common. A Level 2 adjacency is established if there are no common area IDs.

A Level 2 adjacency is established if another router is configured as Level 2 or a Level 1/2 router with interfaces configured as Level 1/2 or Level 2. Level 1 adjacencies will not be established over this interface.

To reset global and/or interface level parameters to the default, the following commands must be entered independently:

CLI Syntax:
```
level>no hello-authentication-key
level>no hello-authentication-type
level>no hello-interval
level>no hello-multiplier
level>no metric
level>no passive
level>no priority
```

Default level 1 or level 2

Special Cases **Global IS-IS Level —** The **config>router>isis** context configures default global parameters for both Level 1 and Level 2 interfaces.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IS-IS Interface Level — The **config>router>isis>interface** context configures IS-IS operational characteristics of the interface at Level 1 and/or Level 2. A logical interface can be configured on one Level 1 and one Level 2. In this case, each level can be configured independently and parameters must be removed independently.

By default, an interface operates in both Level 1 and Level 2 modes.

Parameters 1 — Specifies the IS-IS operational characteristics of the interface at level 1.

2 — Specifies the IS-IS operational characteristics of the interface at level 2.

Platforms All

level

Syntax **level** *level-number*

Context **[Tree]** (config>router>isis>srv6>locator level)

Full Context configure router isis segment-routing-v6 locator level

Description Commands in this context configure the ISIS level attributes of the SRv6 locator.

Parameters *level-number* — Specifies the IS-IS level number.

Values 1, 2

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

level

Syntax **level** {**1** | **2**}
no level

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from level)
[Tree] (config>router>policy-options>policy-statement>entry>to level)

Full Context configure router policy-options policy-statement entry from level
configure router policy-options policy-statement entry to level

Description This command specifies the ISIS route level as a match criterion for the entry.

Default no level

Parameters **1 | 2** — Matches the IS-IS route learned from level 1 or level 2.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.111 level-capability

level-capability

Syntax **level-capability** {**level-1** | **level-2** | **level-1/2**}
no level-capability

Context **[Tree]** (config>service>vprn>isis level-capability)
[Tree] (config>service>vprn>isis>if level-capability)

Full Context configure service vprn isis interface level-capability
configure service vprn isis level-capability

Description This command configures the routing level for an instance of the IS-IS routing process.

An IS-IS router and an IS-IS interface can operate at Level 1, Level 2 or both Level 1 *and* 2.

Table 74 displays configuration combinations and the potential adjacencies that can be formed.

Table 74 **Potential Adjacency Capabilities**

Global Level	Interface Level	Potential Adjacency
L 1/2	L 1/2	Level 1 and/or Level 2
L 1/2	L 1	Level 1 only
L 1/2	L 2	Level 2 only
L 2	L 1/2	Level 2 only
L 2	L 2	Level 2 only
L 2	L 1	none
L 1	L 1/2	Level 1 only
L 1	L 2	none
L 1	L 1	Level 1 only

The **no** form of this command removes the level capability from the configuration.

Default level-capability level-1/2

Special Cases **IS-IS Router —** In the **config>router>isis** context, changing the **level-capability** performs a restart on the IS-IS protocol instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IS-IS Interface — In the **config>router>isis>if** context, changing the **level-capability** performs a restart of IS-IS on the interface.

Parameters **level-1** — Specifies the router/interface can operate at Level 1 only.

level-2 — Specifies the router/interface can operate at Level 2 only.

level-1/2 — Specifies the router/interface can operate at both Level 1 and Level 2.

Platforms All

level-capability

Syntax **level-capability** {**level-1** | **level-2** | **level-1/2**}
no level-capability

Context **[Tree]** (config>router>isis level-capability)
[Tree] (config>router>isis>interface level-capability)

Full Context configure router isis interface level-capability
configure router isis level-capability

Description This command configures the routing level for an instance of the IS-IS routing process.

An IS-IS router and an IS-IS interface can operate at Level 1, Level 2 or both Level 1 and 2.

Table 75 displays configuration combinations and the potential adjacencies that can be formed.

Table 75 **Potential Adjacency**

Global Level	Interface Level	Potential Adjacency
L 1/2	L 1/2	Level 1 and/or Level 2
L 1/2	L 1	Level 1 only
L 1/2	L 2	Level 2 only
L 2	L 1/2	Level 2 only
L 2	L 2	Level 2 only
L 2	L 1	—
L 1	L 1/2	Level 1 only
L 1	L 2	—
L 1	L 1	Level 1 only

The **no** form of this command removes the level capability from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default level-capability level-1/2

Special Cases **IS-IS Router —** In the **config>router>isis** context, changing the **level-capability** performs a restart on the IS-IS protocol instance.

IS-IS Interface — In the **config>router>isis>interface** context, changing the **level-capability** performs a restart of IS-IS on the interface.

Parameters **level-1** — Specifies the router/interface can operate at Level 1only.

level-2 — Specifies the router/interface can operate at Level 2 only.

level-1/2 — Specifies the router/interface can operate at both Level 1 and Level 2.

Platforms All

level-capability

Syntax **level-capability** {**level-1** | **level-2** | **level-1/2**}
no level-capability

Context **[Tree]** (config>router>isis>srv6>locator level-capability)

Full Context configure router isis segment-routing-v6 locator level-capability

Description This command configures the ISIS routing level scope of a SRv6 locator. An SRv6 locator can be advertised at level 1 only, level 2 only, or both level 1 and level 2.

The **no** form of this command reverts to the default value.

Default level-capability level-1/2

Parameters **level-1** — Specifies the SRv6 locator is advertised at level 1 only.

level-2 — Specifies the SRv6 locator is advertised at level 2 only.

level-1/2 — Specifies the SRv6 locator is advertised at both level 1 and level 2.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

16.112 lfa-policy-map

lfa-policy-map

Syntax **lfa-policy-map route-nh-template** *template-name*
no lfa-policy-map

Context **[Tree]** (config>service>vprn>isis>if lfa-policy-map)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn isis interface lfa-policy-map

Description This command applies a route next-hop policy template to the IS-IS interface for the VPRN instance.

When a route next-hop policy template is applied to an interface in IS-IS, it is applied in both level 1 and level 2. When a route next-hop policy template is applied to an interface in OSPF, it is applied in all areas. However, the command in an OSPF interface context can only be executed under the area in which the specified interface is primary and then applied in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command fails.

If the user excluded the interface from LFA using the command **loopfree-alternate-exclude**, the LFA policy, if applied to the interface, has no effect.

Finally, if the user applied a route next-hop policy template to a loopback interface or to the system interface, the command will not be rejected, but it will result in no action being taken.

The **no** form deletes the mapping of a route next-hop policy template to an OSPF or IS-IS interface.

Parameters *template-name* — Specifies the name of the template, up to 32 characters.

Platforms All

lfa-policy-map

Syntax **lfa-policy-map route-nh-template** *template-name*
no lfa-policy-map

Context **[Tree]** (config>router>ospf>area>if lfa-policy-map)
[Tree] (config>router>ospf3>area>if lfa-policy-map)
[Tree] (config>router>isis>if lfa-policy-map)
[Tree] (config>service>vprn>ospf>area>if lfa-policy-map)
[Tree] (config>service>vprn>ospf3>area>if lfa-policy-map)

Full Context configure router isis interface lfa-policy-map
configure router ospf area interface lfa-policy-map
configure router ospf3 area interface lfa-policy-map
configure service vprn ospf area interface lfa-policy-map
configure service vprn ospf3 area interface lfa-policy-map

Description This command applies a route next-hop policy template to an OSPF or IS-IS interface.

When a route next-hop policy template is applied to an interface in IS-IS, it is applied in both level 1 and level 2. When a route next-hop policy template is applied to an interface in OSPF, it is applied in all areas. However, the command in an OSPF interface context can only be executed under the area in which the specified interface is primary and then applied in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command fails.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the user excluded the interface from LFA using the command **loopfree-alternate-exclude**, the LFA policy, if applied to the interface, has no effect.

Finally, if the user applied a route next-hop policy template to a loopback interface or to the system interface, the command will not be rejected, but it results in no action being taken.

The **no** form deletes the mapping of a route next-hop policy template to an OSPF or IS-IS interface.

Default no lfa-policy-map

Parameters *template-name* — Specifies the name of the template, up to 32 characters.

Platforms All

16.113 li

li

Syntax **li**

Context **[Tree]** (config li)

Full Context configure li

Description Commands in this context configure lawful intercept (LI) parameters.

Platforms All

li

Syntax [**no**] **li**

Context **[Tree]** (config>system>security>profile li)

Full Context configure system security profile li

Description This command enables the Lawful Intercept (LI) profile identifier.

The **no** form of this command disables the LI profile identifier.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.114 li-filter

li-filter

Syntax **li-filter**

Context **[Tree]** (config>li li-filter)

Full Context configure li li-filter

Description Commands in this context configure the li-filter branch to create LI filter lists and entries.

Platforms All

16.115 li-filter-associations

li-filter-associations

Syntax **li-filter-associations**

Context **[Tree]** (config>li li-filter-associations)

Full Context configure li li-filter-associations

Description Commands in this context configure the LI filter associations entries that are inserted into normal filters.

Platforms All

16.116 li-filter-block-reservation

li-filter-block-reservation

Syntax **li-filter-block-reservation**

Context **[Tree]** (config>li li-filter-block-reservation)

Full Context configure li li-filter-block-reservation

Description This command enable the LI filter block reservation branch to configure lawful intercept filter reservations.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

16.117 li-filter-lock-state

li-filter-lock-state

Syntax **li-filter-lock-state** {**locked** | **unlocked-for-li-users** | **unlocked-for-all-users**}
no li-filter-lock-state

Context **[Tree]** (config>li li-filter-lock-state)

Full Context configure li li-filter-lock-state

Description This command configures the lock state of the filters used by LI. With the configurable filter lock for LI feature an LI user can control the behavior of filters when they are used for LI.

Prior to Release 12.0.R1, when a filter entry was used as a Lawful Intercept (LI) mirror source criteria, all subsequent attempts to modify the filter were then blocked to avoid having the LI session impacted by a non-LI user.

The **no** form of this command reverts to the default.

Default li-filter-lock-state locked

Parameters **locked** — When an li-source criteria is configured that references any entry of filter Y, then filter Y can no longer be changed (until there are no longer any li-source references to entries of filter Y).

unlocked-for-li-users — Filters can continue to be edited by LI users only even when an li-source references an entry in that filter.

unlocked-for-all-users — Filters can continue to be edited by all users even when an li-source references an entry in that filter.

Platforms All

16.118 li-group

li-group

Syntax **li-group** *isa-group-id*
no li-group

Context **[Tree]** (config>li>x-interfaces>x3 li-group)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure li x-interfaces x3 li-group

Description This command configures the ISA group used for the X3 interface.

The **no** form of this command reverts to the default.

Parameters *isa-group-id* — Specifies the ISA group ID.

Values 1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.119 li-ip-filter

li-ip-filter

Syntax **li-ip-filter** *li-filter-name* [**create**]
no li-ip-filter *li-filter-name*

Context **[Tree]** (config>li>li-filter li-ip-filter)

Full Context configure li li-filter li-ip-filter

Description This command creates a Lawful Interception (LI) IPv4 filter list, or enters the CLI context for a LI IPv4 filter list. LI IPv4 filters are used as a manner to create confidential IPv4 filter based li-source entries. The LI IPv4 filter entries are inserted/merged into normal IPv4 filters as configured with the **li-filter-associations** and **li-filter-block-reservation** commands, but the LI IPv4 filter entries are not visible to users without LI permissions.

The **no** form of this command removes the LI IPv4 filter name from the configuration.

Parameters *li-filter-name* — Specifies the name of the IPv4 address filter. Filter names cannot start with an underscore character (for example, “_my-filter”) and cannot use the name “default”.

Platforms All

li-ip-filter

Syntax [**no**] **li-ip-filter** *li-filter-name*

Context **[Tree]** (config>li>li-filter-assoc li-ip-filter)

Full Context configure li li-filter-associations li-ip-filter

Description Specifies the **li-ip-filter** that will have its entries inserted into a list of normal IP filters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the LI filter name from the configuration.

Parameters *li-filter-name* — Specifies an existing li-ip-filter, up to 32 characters.

Platforms All

li-ip-filter

Syntax **li-ip-filter** *li-filter-name* **entry** *li-entry-id* [*li-entry-id*] [**intercept-id** *intercept-id* [*intercept-id*]] [**session-id** *session-id* [*session-id*]]
no li-ip-filter *li-filter-name* [**entry** *li-entry-id* [*li-entry-id*]]

Context **[Tree]** (config>li>li-source li-ip-filter)

Full Context configure li li-source li-ip-filter

Description This command enables lawful interception (LI) of packets that match specific entries in an existing LI IP filter that has been associated with a normal IP filter. The specification of an li-ip-filter entry as an li-source means that packets matching the li-ip-filter entry will be intercepted on all interfaces/saps/and so on where the associated normal ip-filter(s) are applied.

Parameters *li-filter-name* — Specifies the name of the **li-ip-filter**, up to 32 characters.

li-entry-id — Specifies the entry ID in the **li-ip-filter** that is to be used as an li-source criteria.

Values 1 to 65535

intercept-id — Specifies the intercept-id that is inserted into the packet header for all mirrored packets of the associated li-source entry. This intercept ID can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, an *intercept-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *intercept-id* configured for an **li-source** entry, then the default value will be inserted. When the mirror service is configured with **ip-gre** routable encap, no intercept ID is inserted and none should be specified against the **li-source** entries.

session-id — Specifies the session-id that is inserted into the packet header for all mirrored packets of the associated li-source entry. This *session-id* can be used (for example by a downstream LI Gateway) to identify the particular LI session to which the packet belongs. The session-id is only valid and used for mirror services that are configured with ip-udp-shim routable encap (**config>mirror>mirror-dest>encap>ip-udp-shim**). For all types of li-source entries (filter, nat, sap, or subscriber), when the mirror service is configured with

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-udp-shim routable encap, a session-id field (as part of the routable encap) is always present in the mirrored packets. If there is no *session-id* configured for an li-source entry, then the default value will be inserted. When a mirror service is configured with ip-gre routable encap, no session-id is inserted and none should be specified against the li-source entries.

Platforms All

16.120 li-ipv6-filter

li-ipv6-filter

Syntax **li-ipv6-filter** *li-filter-name* [**create**]
no li-ipv6-filter *li-filter-name*

Context **[Tree]** (config>li>li-filter li-ipv6-filter)

Full Context configure li li-filter li-ipv6-filter

Description This command creates a Lawful Interception (LI) IPv6 filter list, or enters the CLI context for a LI IPv6 filter list. LI IPv6 filters are used as a manner to create confidential IPv6 filter based li-source entries. The LI IPv6 filter entries are inserted or merged into normal IPv6 filters as configured with the **li-filter-associations** and **li-filter-block-reservation** commands, but the LI IPv6 filter entries are not visible to users without LI permissions.

The **no** form of this command removes the LI IPv6 filter name from the configuration.

Parameters *li-filter-name* — Specifies the name of the IPv6 address filter. Filter names cannot start with an underscore character (for example, “_my-filter”) and cannot use the name “default”.

create — creates a LI IPv6 filter.

Platforms All

li-ipv6-filter

Syntax [**no**] **li-ipv6-filter** *li-filter-name*

Context **[Tree]** (config>li>li-filter-assoc li-ipv6-filter)

Full Context configure li li-filter-associations li-ipv6-filter

Description This command specifies the **li-ipv6-filter** that will have its entries inserted into a list of normal IPv6 filters.

The **no** form of this command removes the filter name from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *li-filter-name* — Specifies an existing li-ipv6-filter up to 32 characters.

Platforms All

li-ipv6-filter

Syntax **li-ipv6-filter** *li-filter-name* **entry** *li-entry-id* [*li-entry-id*] [**intercept-id** *intercept-id* [*intercept-id*]] [**session-id** *session-id* [*session-id*]]
no li-ipv6-filter *li-filter-name* [**entry** *li-entry-id* [*li-entry-id*]]

Context **[Tree]** (config>li>li-source li-ipv6-filter)

Full Context configure li li-source li-ipv6-filter

Description This command enables lawful interception (LI) of packets that match specific entries in an existing LI IPv6 filter that has been associated with a normal IPv6 filter. The specification of an li-ipv6-filter entry as an li-source means that packets matching the **li-ipv6-filter** entry will be intercepted on all interfaces/saps/and so on, where the associated normal ip-filter(s) are applied.

Parameters *li-filter-name* — Specifies the name of the **li-ipv6-filter** up to 32 characters.

li-entry-id — Specifies the entry ID in the **li-ipv6-filter** that is to be used as an LI source criteria.

Values 1 to 65535

intercept-id — Specifies the intercept ID that is inserted into the packet header for all mirrored packets of the associated li-source entry. This *intercept-id* can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. For all types of li-source entries (filter, nat, sap, or subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, an intercept-id field (as part of the routable encapsulation) is always present in the mirrored packets. If there is no *intercept-id* configured for an **li-source** entry, then the default value will be inserted. When the mirror service is configured with IP GRE routable encap, no intercept ID is inserted and none should be specified against the LI source entries.

session-id — Specifies the session ID that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This *session-id* can be used (for example, by a downstream LI gateway) to identify the particular LI session to which the packet belongs. The *session-id* is only valid and used for mirror services that are configured with **ip-udp-shim** routable encap (**config>mirror>mirror-dest>encap>ip-udp-shim**). For all types of li-source entries (filter, nat, sap, subscriber), when the mirror service is configured with ip-udp-shim routable encap, a session-id field (as part of the routable encap) is always present in the mirrored packets. If there is no session ID configured for an **li-source** entry, then the default value is inserted. When a mirror service is configured with IP GRE routable encap, no session ID is inserted and none should be specified against the li-source entries.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

16.121 li-local-save

li-local-save

Syntax [**no**] **li-local-save**

Context **[Tree]** (bof li-local-save)

Full Context bof li-local-save

Description This command specifies whether or not lawful intercept (LI) configuration is allowed to be saved to a local file. Modifying this command will not take effect until the system is rebooted.

Default li-local-save

Platforms All

16.122 li-mac-filter

li-mac-filter

Syntax **li-mac-filter** *li-filter-name* [**create**]
no li-mac-filter *li-filter-name*

Context **[Tree]** (config>li>li-filter li-mac-filter)

Full Context configure li li-filter li-mac-filter

Description This command creates a Lawful Interception (LI) MAC filter list, or enters the CLI context for a LI MAC filter list. LI MAC filters are used as a manner to create confidential MAC filter based li-source entries. The LI MAC filter entries are inserted/merged into normal MAC filters as configured via the li-filter-associations and li-filter-block-reservation commands, but the LI MAC filter entries are not visible to users without LI permissions.

The **no** form of this command removes the MAC LI filter name from the configuration.

Parameters *li-filter-name* — Specifies the name of the MAC filter. Filter names cannot start with an underscore character (for example, “_my-filter”) and cannot use the name “default”.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

li-mac-filter

Syntax [**no**] **li-mac-filter** *li-filter-name*

Context **[Tree]** (config>li>li-filter-assoc li-mac-filter)

Full Context configure li li-filter-associations li-mac-filter

Description Specifies the li-mac-filter that will have its entries inserted into a list of normal mac filters.

Parameters *li-filter-name* — Specifies the name of the LI MAC filter, up to 32 characters. Filter names cannot start with an underscore character (for example, "_my-filter") and cannot use the name "default".

Platforms All

li-mac-filter

Syntax **li-mac-filter** *li-filter-name* **entry** *li-entry-id* [*li-entry-id*] [**intercept-id** *intercept-id* [*intercept-id*]] [**session-id** *session-id* [*session-id*]]
no li-mac-filter *li-filter-name* [**entry** *li-entry-id* [*li-entry-id*]]

Context **[Tree]** (config>li>li-source li-mac-filter)

Full Context configure li li-source li-mac-filter

Description This command enables lawful interception (LI) of packets that match specific entries in an existing LI MAC filter that has been associated with a normal MAC filter. The specification of an **li-mac-filter** entry as an li-source means that packets matching the **li-mac-filter** entry will be intercepted on all interfaces, saps and so on where the associated normal mac-filter(s) are applied.

Parameters *li-filter-name* — Specifies the name of the **li-mac-filter**, up to 32 characters.

li-entry-id — Specifies the entry id in the **li-mac-filter** that is to be used as an li-source criteria.

Values 1 to 65535

intercept-id — Specifies the intercept ID that is inserted into the packet header for all mirrored packets of the associated li-source entry. This intercept ID can be used (for example, by a downstream LI gateway) to identify the particular LI session to which the packet belongs. For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, an *intercept-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *intercept-id* configured for an **li-source** entry, then the default value will be inserted. When the mirror service is configured with **ip-gre** routable encap, no *intercept-id* is inserted and none should be specified against the **li-source** entries.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

session-id — Specifies the *session-id* that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This *session-id* can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. The *session-id* is only valid and used for mirror services that are configured with **ip-udp-shim** routable encap (**config>mirror>mirror-dest>encap>ip-udp-shim**). For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, a *session-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *session-id* configured for an **li-source** entry, then the default value will be inserted. When a mirror service is configured with **ip-gre** routable encap, no *session-id* is inserted and none should be specified against the **li-source** entries.

Platforms All

16.123 li-reserved-block

li-reserved-block

Syntax **li-reserved-block** *block-name* [**create**]
no li-reserved-block *block-name*

Context **[Tree]** (config>li>li-filter-block-reservation li-reserved-block)

Full Context configure li li-filter-block-reservation li-reserved-block

Description This command creates or edits an LI reserved block. An LI reserved block allows an operator to define where entries from an LI filter should be inserted into a normal filter. The block reserves a configurable number of entries in the normal filter that can only be used for entries inserted from associated LI filters. The LI filter entries that get inserted into the reserved block in each normal filter are not visible to non-LI operators. The block also defines to which normal filters the reservation is applied.

The **no** form of this command removes the block name from the configuration.

Parameters *block-name* — Specifies the name of the MAC filter. Block names cannot start with an underscore character (for example, “_my-filter”) and cannot use the name “default”.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.124 li-separate

li-separate

Syntax [**no**] **li-separate**

Context **[Tree]** (bof li-separate)

Full Context bof li-separate

Description This command specifies whether or not a non-LI user has access to lawful intercept (LI) information. When this command is enabled, a user who does not have LI access will not be allowed to access CLI or SNMP objects in the li context. Modifying this command will not take effect until the system is rebooted.

When the **no li-separate** command is set (the default mode), those who are allowed access to the **config>system>security>profile** context and user command nodes are allowed to modify the configuration of the LI parameters. In this mode, a user that has a profile allowing access to the **config>li** and/or **show>li** command contexts can enter and use the commands under those nodes.

When the **li-separate** command is configured, only users that have the LI access capabilities set in the **config>system>security>user>access li** context are allowed to access the **config>li** and/or **show>li** command contexts. A user who does not have LI access is not allowed to enter the **config>li** and **show>li** contexts even though they have a profile that allows access to these nodes. When in the **li-separate** mode, only users with **config>system>security>user>access li** set in their user account have the ability modify the setting LI parameters in either their own or other profiles and user configurations.

Default no li-separate

Platforms All

16.125 li-source

li-source

Syntax [**no**] **li-source** *mirror-service-id* [**name** *mirror-service-name*]

Context **[Tree]** (config>li li-source)

Full Context configure li li-source

Description This command configures a lawful intercept (LI) mirror source.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mirror-service-id* — Specifies the service ID in the service domain. This ID is unique to this service and cannot be used by any other service, regardless of service type. The same service ID must be configured on every router that this particular service is defined on.

Values *service-id*:1 to 2147483647
svc-name: up to 64 characters

Platforms All

16.126 lic

lic

Syntax **lic** *lic-name* [**create**]
no lic *lic-name*

Context **[Tree]** (config>li>x-interfaces>lics lic)

Full Context configure li x-interfaces lics lic

Description This command configures the parameters to communicate with a specific LIC.

The **no** form of this command removes the LIC name.

Parameters *lic-name* — Specifies the LIC name to be used as a reference, up to 32 characters.

create — Mandatory keyword to create this entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.127 lic-identifier

lic-identifier

Syntax **lic-identifier** *identifier*
no lic-identifier

Context **[Tree]** (config>li>x-interfaces>lics>lic lic-identifier)

Full Context configure li x-interfaces lics lic lic-identifier

Description This command configures the string that identifies this LIC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *identifier* — Specifies the LIC identifying string, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.128 license

license

Syntax **license**

Context **[Tree]** (admin>system license)

Full Context admin system license

Description Enters a context for administrative commands related to licensing.

Platforms All

16.129 license-file

license-file

Syntax **license-file** *file-url*
no license-file

Context **[Tree]** (bof license-file)

Full Context bof license-file

Description This command configures the license location and file name.

The **no** form of this command removes the file URL from the configuration.

Parameters *file-url* — Specifies the *file-url*.

Values

file-url	{*local-url* | *remote-url*} (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

16.130 lics

lics

Syntax **lics**

Context **[Tree]** (config>li>x-interfaces lics)

Full Context configure li x-interfaces lics

Description Commands in this context configure the Network Element to communicate with LI Centers (LICs).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.131 lifetime

lifetime

Syntax **lifetime minimum** *minimum* **maximum** *maximum*
no lifetime

Context **[Tree]** (config>service>nat>pcp-server-policy lifetime)

Full Context configure service nat pcp-server-policy lifetime

Description This command configures the lifetime of explicit mappings made by the PCP servers.

Default lifetime minimum 120 maximum 86400

Parameters *minimum* — Specifies the minimum lifetime of explicit mappings made by the PCP servers using this PCP policy, in seconds.

Values 60 to 86399

maximum — Specifies the maximum lifetime of explicit mappings made by the PCP servers using this PCP policy, in seconds.

Values 61 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lifetime

Syntax **lifetime** {*seconds* | **forever**}

Context **[Tree]** (config>system>script-control>script-policy lifetime)

Full Context configure system script-control script-policy lifetime

Description This command is used to configure the maximum amount of time that a script may run.

Default lifetime 3600

Parameters *seconds* — Specifies the maximum amount of time that a script may run, in seconds.

Values 0 to 21474836

Default 3600 (1 hour)

forever — Specifies to allow a script to run indefinitely.

Platforms All

16.132 limit

limit

Syntax **limit** {**all-packet-matches** | **first-session-match**}

Context **[Tree]** (debug>app-assure>group>traffic-capture>record limit)

Full Context debug application-assurance group traffic-capture record limit

Description This command records limit conditions.

Parameters **all-packet-matches** — Records all the packets matching the condition.

first-session-match — Records only the first session matching the condition.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.133 limit-init-exchange

limit-init-exchange

Syntax **limit-init-exchange** [**reduced-max-exchange-timeout** *seconds*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no limit-init-exchange

Context [Tree] (config>ipsec>ike-policy limit-init-exchange)

Full Context configure ipsec ike-policy limit-init-exchange

Description This command limits the number of ongoing IKEv2 initial exchanges per tunnel to 1. When the system receives a new IKEv2 IKE_SA_INIT request when there is an ongoing IKEv2 initial exchange from same peer, then system reduces the timeout value of the existing exchange to the specified **reduced-max-exchange-timeout**. If the **reduced-max-exchange-timeout** is **disabled**, then the system does not reduce the timeout value.

The **no** form of this command reverts to the default value.

Default limit-init-exchange reduced-max-exchange-timeout 2

Parameters *seconds* — Specifies the maximum timeout for the in-progress initial IKE exchange.

Values 2 to 60, disabled

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.134 limit-mac-move

limit-mac-move

Syntax **limit-mac-move** [**blockable** | **non-blockable**]
no limit-mac-move

Context [Tree] (config>service>vpls>sap limit-mac-move)
[Tree] (config>service>vpls>spoke-sdp limit-mac-move)

Full Context configure service vpls sap limit-mac-move
configure service vpls spoke-sdp limit-mac-move

Description This command indicates whether or not the mac-move agent, when enabled using **config>service>vpls>mac-move** or **config>service>epipe>mac-move**, limits the MAC re-learn (move) rate on this SAP.

Default limit-mac-move blockable

Parameters **blockable** — Specifies that the agent monitors the MAC re-learn rate on the SAP, and it blocks it when the re-learn rate is exceeded.

non-blockable — Specifies that this SAP is not blocked, and another blockable SAP is blocked instead.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

limit-mac-move

Syntax **limit-mac-move** [**blockable** | **non-blockable**]
no limit-mac-move

Context **[Tree]** (config>service>pw-template limit-mac-move)

Full Context configure service pw-template limit-mac-move

Description This command indicates whether or not the mac-move agent will limit the MAC re-learn (move) rate.

Default limit-mac-move blockable

Parameters **blockable** — The agent will monitor the MAC re-learn rate, and it will block it when the re-learn rate is exceeded.

non-blockable — When specified, a SAP will not be blocked, and another blockable SAP will be blocked instead.

Platforms All

16.135 limit-pir-zero-drain

limit-pir-zero-drain

Syntax [**no**] **limit-pir-zero-drain**

Context **[Tree]** (config>qos>adv-config-policy>child-control>bandwidth-distribution limit-pir-zero-drain)

Full Context configure qos adv-config-policy child-control bandwidth-distribution limit-pir-zero-drain

Description This command is used to configure the system to use the minimum configurable PIR instead of an H-QoS derived zero operational PIR. The default behavior is to allow the operational PIR of the queue to remain the last configured value while setting the queue MBS to zero (preventing queuing of newly arriving packets). Retaining the previous PIR value may cause a momentary burst above an aggregate rate associated with the queue as it drains. Using the **limit-pir-zero-drain** command causes the queue to drain at the lowest rate possible (typically 1 kb/s) that limits overrun situations.

The **no** form of this command reverts to default behavior.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.136 limit-unused-bandwidth

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>agg-rate limit-unused-bandwidth)
[Tree] (config>port>ethernet>access>egress>vport limit-unused-bandwidth)
[Tree] (config>port>ethernet>network>egr>qgrp>agg-rate limit-unused-bandwidth)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress limit-unused-bandwidth)
[Tree] (config>port>sonet-sdh>path>access>egress>vport limit-unused-bandwidth)

Full Context configure port ethernet access egress queue-group agg-rate limit-unused-bandwidth
configure port ethernet access egress vport limit-unused-bandwidth
configure port ethernet network egress queue-group agg-rate limit-unused-bandwidth
configure port sonet-sdh path access egress vport limit-unused-bandwidth
configure service vprn subscriber-interface group-interface sap egress limit-unused-bandwidth

Description This command specifies to limit the unused bandwidth and allow a tighter control in allocation of bandwidth by HQoS. When enabled, HQoS algorithm distributes any unused aggregate bandwidth between queues operating below their fair share rates. This allows a simplified aggregate rate protection while allocating bandwidth by HQoS.

The **no** form of this command reverts to the default.

Platforms All

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>ies>if>sap>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress>agg-rate limit-unused-bandwidth)

Full Context configure service ies interface sap egress agg-rate limit-unused-bandwidth
configure service ies subscriber-interface group-interface sap egress agg-rate limit-unused-bandwidth
configure service vprn subscriber-interface group-interface sap egress agg-rate limit-unused-bandwidth

Description This command enables aggregate rate overrun protection.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn subscriber-interface group-interface sap egress agg-rate limit-unused-bandwidth
- configure service ies subscriber-interface group-interface sap egress agg-rate limit-unused-bandwidth

All

- configure service ies interface sap egress agg-rate limit-unused-bandwidth

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context **[Tree]** (config>service>apipe>sap>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>cpipe>sap>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>epipe>sap>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>fpipe>sap>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>ipipe>sap>egress>agg-rate limit-unused-bandwidth)

Full Context configure service apipe sap egress agg-rate limit-unused-bandwidth
configure service cpipe sap egress agg-rate limit-unused-bandwidth
configure service epipe sap egress agg-rate limit-unused-bandwidth
configure service fpipe sap egress agg-rate limit-unused-bandwidth
configure service ipipe sap egress agg-rate limit-unused-bandwidth

Description This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress agg-rate limit-unused-bandwidth
- configure service cpipe sap egress agg-rate limit-unused-bandwidth

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress agg-rate limit-unused-bandwidth

All

- configure service ipipe sap egress agg-rate limit-unused-bandwidth
- configure service epipe sap egress agg-rate limit-unused-bandwidth

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context **[Tree]** (config>service>vpls>sap>egress>agg-rate limit-unused-bandwidth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>template>vpls-sap-template>egress>agg-rate limit-unused-bandwidth)
[Tree] (config>service>vpls>sap>egress>encap-defined-qos>encap-group>agg-rate limit-unused-bandwidth)

Full Context configure service template vpls-sap-template egress agg-rate limit-unused-bandwidth
configure service vpls sap egress agg-rate limit-unused-bandwidth
configure service vpls sap egress encap-defined-qos encap-group agg-rate limit-unused-bandwidth

Description This command is used to enable aggregate rate overrun protection on the agg-rate context.

The **no** form of this command disables the overrun protection.

Platforms All

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context [Tree] (config>service>vprn>if>sap>egress>agg-rate limit-unused-bandwidth)

Full Context configure service vprn interface sap egress agg-rate limit-unused-bandwidth

Description This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

Platforms All

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context [Tree] (config>qos>scheduler-policy>tier>scheduler limit-unused-bandwidth)

Full Context configure qos scheduler-policy tier scheduler limit-unused-bandwidth

Description This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

Platforms All

limit-unused-bandwidth

Syntax [**no**] **limit-unused-bandwidth**

Context [Tree] (config>service>cust>multi-service-site>egress>agg-rate limit-unused-bandwidth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service customer multi-service-site egress agg-rate limit-unused-bandwidth

Description This command is used to enable aggregate rate overrun protection.

The **no** form of the command disables aggregate rate overrun protection.

Default no limit-unused-bandwidth

Platforms All

16.137 line-length

line-length

Syntax **line-length** {**110** | **220** | **330** | **440** | **550** | **660**}

Context **[Tree]** (config>system>sync-if-timing>bits>output line-length)

Full Context configure system sync-if-timing bits output line-length

Description This command configures the **line-length** parameter of the BITS output, This is the distance in feet between the network element and the office clock (BITS/SSU). There are two possible BITS-out interfaces, one for each CPM. They are configured together, but they are displayed separately in the show command. This command is only applicable when the interface-type is DS1.

Default line-length 110

Parameters **110** — Specifies that the distance is from 0 to 110 feet.

220 — Specifies that the distance is from 110 to 220 feet.

330 — Specifies that the distance is from 220 to 330 feet.

440 — Specifies that the distance is from 330 to 440 feet.

550 — Specifies that the distance is from 440 to 550 feet.

660 — Specifies that the distance is from 550 to 660 feet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.138 link

link

Syntax **link** *port-id* {**primary** | **secondary**}
no link *port-id*

Context **[Tree]** (config>lag>link-map-profile link)

Full Context configure lag link-map-profile link

Description This command designates one of the configured ports of the LAG to be used on egress as either a primary or secondary link (based on the option selected) by all SAPs and network interfaces that use this LAG link map profile.

Links are part of a profile When a link is added or deleted, all SAPs and network interfaces that use this link-map-profile may be re-hashed if required.

The **no** form of this command deletes the link from this LAG link mapping profile. A port must be deleted from all LAG link profiles if it is to be deleted from the LAG.

Parameters *port-id* — Specifies a physical port ID that is an existing member of this LAG.

port-id	*slot*/*mda*/*port*[.*channel*]	
eth-sat-id	esat-*id*/*slot*/*port*	
	esat	keyword
	id	1 to 20
pxc-id	pxc-*id*.*sub-port*	
	pxc	keyword
	id	1 to 64
	sub-port	a, b

primary — Designates one of the configured ports of the LAG to be used on egress as a primary link by SAPs/network interfaces that use this LAG link map profile.

secondary — Designates one of the configured ports of the LAG to be used on egress as a secondary link by SAPs/network interfaces that use this LAG link map profile.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.139 link-addr

link-addr

Syntax **link-addr** *ipv6-address*
no link-addr

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client>slaac link-addr)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client>slaac link-addr)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client>ia-na link-addr)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client>ia-na link-addr)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client>dhcpv4-nat link-addr)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client>dhcpv4-nat link-addr)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client dhcpv4-nat link-addr
configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client ia-na link-addr
configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client slaac link-addr
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client dhcpv4-nat link-addr
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client ia-na link-addr
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client slaac link-addr

Description This command specifies the ipv6-address that should be included in the link-address field of the relay header. This can be used for pool selection by the DHCPv6 server.

The **no** form of this command falls back to the default.

Parameters *ipv6-address* — Specifies the IPv6 address up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.140 link-address

link-address

Syntax **link-address** *ipv6-address*
no link-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host link-address)
[Tree] (config>service>ies>if>ipv6>dhcp6-relay link-address)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>relay link-address)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay link-address)
[Tree] (config>service>vprn>if>ipv6>dhcp6-relay link-address)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay link-address)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay link-address)

Full Context
configure service ies interface ipv6 dhcp6-relay link-address
configure service ies subscriber-interface group-interface ipv6 dhcp6 relay link-address
configure service ies subscriber-interface ipv6 dhcp6 relay link-address
configure service vprn interface ipv6 dhcp6-relay link-address
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay link-address
configure service vprn subscriber-interface ipv6 dhcp6 relay link-address
configure subscriber-mgmt local-user-db ipoe host link-address

Description
This command configures the link address used for prefix selection at the DHCP server.

The link-address is a field in DHCP6 Relay-Forward message that is used in DHCP6 server to select the IPv6 address (IA-NA) or IPv6 prefix (IA-PD) from a pool with configured prefix range covering the link-address. The selection scope is the pool or a prefix range within the pool.

The **no** form of this command reverts to the default.

Default
no link-address

Parameters
ipv6-address — Specifies the link-address.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface ipv6 dhcp6 relay link-address
- configure subscriber-mgmt local-user-db ipoe host link-address
- configure service vprn subscriber-interface ipv6 dhcp6 relay link-address
- configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay link-address
- configure service ies subscriber-interface ipv6 dhcp6 relay link-address

All

- configure service vprn interface ipv6 dhcp6-relay link-address
- configure service ies interface ipv6 dhcp6-relay link-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

link-address

Syntax **link-address** *ipv6-address*
no link-address

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>dhcp6 link-address)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp6 link-address)

Full Context configure service ies interface sap ipsec-gw dhcp6 link-address
configure service vprn interface sap ipsec-gw dhcp6 link-address

Description This command specifies the link address of the relayed DHCPv6 packets sent by the system.

Default no link-address

Parameters *ipv6-address* — Specifies a global unicast IPv6 address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.141 link-bandwidth

link-bandwidth

Syntax **link-bandwidth**

Context **[Tree]** (config>service>vprn>bgp>group link-bandwidth)
[Tree] (config>service>vprn>bgp>group>neighbor link-bandwidth)

Full Context configure service vprn bgp group link-bandwidth
configure service vprn bgp group neighbor link-bandwidth

Description This command enables the configuration context for handling the link-bandwidth extended community attached to specific BGP routes.

When all used multipaths of an IP prefix correspond to BGP routes with a link-bandwidth extended community, the datapath is programmed to do weighted ECMP across the BGP next-hops in proportion to the bandwidth values.

Platforms All

link-bandwidth

Syntax **link-bandwidth**

Context **[Tree]** (config>router>bgp>group link-bandwidth)
[Tree] (config>router>bgp>group>neighbor link-bandwidth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bgp group link-bandwidth
configure router bgp group neighbor link-bandwidth

Description This command enables the configuration context for handling the link-bandwidth extended community attached to specific BGP routes.

When all used multipaths of an IP prefix correspond to BGP routes with a link-bandwidth extended community, the datapath is programmed to do weighted ECMP across the BGP next-hops in proportion to the bandwidth values.

Platforms All

16.142 link-delay

link-delay

Syntax **link-delay** {**activate** | **deactivate**} *milli-seconds*
no link-delay {**activate** | **deactivate**}

Context **[Tree]** (config>port>ml-bundle>ima link-delay)

Full Context configure port multilink-bundle ima link-delay

Description This command specifies the time to delay between detection of a link activation/deactivation condition and acting upon it (going in/out of the RX failure state on a link).

Parameters **activate** *milli-seconds* — Specifies the time, in milli-seconds, used to clear an existing LIF or LODS alarm. The time specified determines how long is needed for member links to stabilize before being activated.

Values 1 to 30000

Default 10000

deactivate *milli-seconds* — Specifies the time, in milli-seconds, used to raise an LIF or LODS alarm. The time specified determines how long before a member link is declared in error and is deactivated.

Values 1 to 30000

Default 2000

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.143 link-fault

link-fault

Syntax **link-fault local-port-action** {**log-only** | **out-of-service**}

Context **[Tree]** (config>port>ethernet>efm-oam>peer-rdi-rx link-fault)

Full Context configure port ethernet efm-oam peer-rdi-rx link-fault

Description This command defines how to react to the reception of a link fault flag set in the informational PDU from a peer.

Default link-fault local-port-action out-of-service

Parameters **local-port-action** — Defines whether or not the local port will be affected when a link fault is received from a peer.

log-only — Keyword that prevents the port from being affected when the local peer receives a link fault. The dying gasp will be logged but the port will remain operational.

out-of-service — Keyword that causes the port to enter a non-operation down state with a port state of link up. The error will be logged upon reception of link fault event. The port will not be available to service data but will continue to carry Link OAM traffic to ensure the link is monitored.

Platforms All

16.144 link-group

link-group

Syntax [**no**] **link-group** *link-group-name*

Context **[Tree]** (config>service>vprn>isis link-group)

Full Context configure service vprn isis link-group

Description This command configures a link-group for the router or VPRN instance.

The **no** form of this command removes the specified link-group.

Parameters *link-group-name* — Name of the link-group to be added or removed from the router or VPRN service.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

link-group

Syntax **link-group** *link-group-name*
no link-group

Context **[Tree]** (config>router>isis link-group)

Full Context configure router isis link-group

Description This command specifies the IS-IS link group associated with this particular level of the interface.

Parameters *link-group-name* — Specifies an IS-IS link group on the system up to 32 characters in length.

Platforms All

16.145 link-local-address

link-local-address

Syntax **link-local-address** *ipv6-address* [**dad-disable**]
no link-local-address

Context **[Tree]** (config>router>if>ipv6 link-local-address)
[Tree] (config>service>ies>if>ipv6 link-local-address)
[Tree] (config>service>ies>sub-if>ipv6 link-local-address)
[Tree] (config>service>vprn>if>ipv6 link-local-address)
[Tree] (config>service>vprn>sub-if>ipv6 link-local-address)

Full Context configure router interface ipv6 link-local-address
configure service ies interface ipv6 link-local-address
configure service ies subscriber-interface ipv6 link-local-address
configure service vprn interface ipv6 link-local-address
configure service vprn subscriber-interface ipv6 link-local-address

Description This command configures the IPv6 Link Local address that is used as a virtual SRRP IPv6 address by the Master SRRP node. This address is sent in the Router Advertisements initiated by the Master SRRP node. Clients use this address as IPv6 default-gateway. Both SRRP nodes, Master and Backup, must be configured with the same Link Local address.

Only one link-local-address is allowed per interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Caution: Removing a manually configured link local address may impact routing protocols or static routes that have a dependency on that address. It is not recommended to remove a link local address when there are active IPv6 subscriber hosts on an IES or VPRN interface.

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the IPv6 address in the form:

Values

ipv6-address:	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

dad-disable — Disables Duplicate Address Detection (DAD) and sets the address to preferred, even if there is a duplicated address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface ipv6 link-local-address
- configure service ies subscriber-interface ipv6 link-local-address

All

- configure service ies interface ipv6 link-local-address
- configure service vprn interface ipv6 link-local-address
- configure router interface ipv6 link-local-address

16.146 link-local-modifier

link-local-modifier

Syntax **link-local-modifier** *modifier*
no link-local-modifier

Context **[Tree]** (config>service>ies>if>ipv6>secure-nd link-local-modifier)

Full Context configure service ies interface ipv6 secure-nd link-local-modifier

Description This command configures the Cryptographically Generated Address (CGA) modifier for link-local addresses.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters modifier — Specifies the modifier in 32 hexadecimal nibbles.

Values 0x0 to 0xFFFFFFFF

Platforms All

link-local-modifier

Syntax **link-local-modifier** *modifier*
[**no**] **link-local-modifier**

Context **[Tree]** (config>service>vprn>if>secure-nd link-local-modifier)

Full Context configure service vprn interface secure-nd link-local-modifier

Description This command configures the Cryptographically Generated Address (CGA) modifier for link-local addresses.

Parameters *modifier* — Specifies the modifier in 32 hexadecimal nibbles.

Values 0x0–0xFFFFFFFF

link-local-modifier

Syntax **link-local-modifier** *modifier*
no link-local-modifier

Context **[Tree]** (config>router>if>ipv6>secure-nd link-local-modifier)

Full Context configure router interface ipv6 secure-nd link-local-modifier

Description This command configures the Cryptographically Generated Address (CGA) modifier for link-local addresses.

Parameters *modifier* — Specifies the modifier in 32 hexadecimal nibbles.

Values 0x0 to 0xFFFFFFFF

Platforms All

16.147 link-map-profile

link-map-profile

Syntax **link-map-profile** *link-map-profile-id* [**create**]
no link-map-profile *link-map-profile-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>lag link-map-profile)

Full Context configure lag link-map-profile

Description This command creates the link map profile that can to control which LAG ports are to be used on egress or enables the configuration context for previously created link map profile. link map profiles are not created by default.

The **no** form of this command, deletes the specified link map profile.

Parameters *link-map-profile-id* — An integer from 1 to 64 that defines a unique LAG link map profile on this LAG.

Platforms All

16.148 link-measurement

link-measurement

Syntax **link-measurement**

Context [Tree] (config>test-oam link-measurement)

Full Context configure test-oam link-measurement

Description Commands in this context configure various link measurement template attributes that are inherited on associated IP interfaces for delay reporting to the routing engine.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.149 link-monitoring

link-monitoring

Syntax [**no**] **link-monitoring**

Context [Tree] (config>port>ethernet>efm-oam>discovery>advertise-capabilities link-monitoring)

Full Context configure port ethernet efm-oam discovery advertise-capabilities link-monitoring

Description When the link monitoring function is in a no shutdown state, the Link Monitoring capability (EV) is advertised to the peer through the EFM OAM protocol. This may not be desired if the remote peer does not support the Link Monitoring functionality.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** version of this command suppresses the advertisement of capabilities.

Default link-monitoring

Platforms All

link-monitoring

Syntax **link-monitoring**

Context **[Tree]** (config>port>ethernet>efm-oam link-monitoring)

Full Context configure port ethernet efm-oam link-monitoring

Description This context contains link monitoring specific options defining the various local thresholds, port interaction and peer notification methods. In order to activate Link monitoring function, this context must be configured with the no shutdown option. Shutting down link monitoring will clear all historical link monitoring counters. If the port was removed from service and placed in a non-operational down state and a port state of link up because a signal failure threshold was crossed and link monitoring is shutdown, the port will be returned to service assuming no underlying conditions prevent this return to service.

When the link monitoring function is in a **no shutdown** state, the Link Monitoring capability (EV) is advertised to the peer through the EFM OAM protocol. This may not be desired if the remote peer does not support the Link Monitoring functionality.

Platforms All

16.150 link-name

link-name

Syntax **link-name** *te-link-name*
no link-name

Context **[Tree]** (config>router>lmp>te-link link-name)

Full Context configure router lmp te-link link-name

Description This command configures text names for the TE Link.

Parameters *te-link-name* — Specifies the text name for the TE Link.

Values 32 characters maximum text string

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.151 link-specific-rate

link-specific-rate

Syntax **link-specific-rate** *packet-rate-limit*
no link-specific-rate

Context **[Tree]** (config>sys>security>cpu-protection link-specific-rate)

Full Context configure system security cpu-protection link-specific-rate

Description This command configures a link-specific rate for CPU protection. This limit is applied to all ports within the system. The CPU will receive no more than the configured packet rate for all link level protocols such as LACP from any one port. The measurement is cleared each second and is based on the ingress port.

Default link-specific-rate 15000

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit, in packets per second, for link level protocols.

Values 1 to 65535, **max** (no limit)

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

16.152 link-state-export-enable

link-state-export-enable

Syntax [**no**] **link-state-export-enable**

Context **[Tree]** (config>router>bgp link-state-export-enable)

Full Context configure router bgp link-state-export-enable

Description This command enables the export of link-state information from the BGP-LS address family into the local Traffic Engineering Database (TED).

The **no** form of this command disables the export of link state information into the TED.

Default no link-state-export-enable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.153 link-state-import-enable

link-state-import-enable

Syntax [**no**] **link-state-import-enable**

Context **[Tree]** (config>router>bgp link-state-import-enable)

Full Context configure router bgp link-state-import-enable

Description This command enables the import of link-state information into the BGP-LS address family for advertisement to other BGP neighbors.

The **no** form of this command disables the import of link state information into the BGP-LS address family.

Default no link-state-import-enable

Platforms All

16.154 link-type

link-type

Syntax **link-type** {**pt-pt** | **shared**}
no link-type [**pt-pt** | **shared**]

Context **[Tree]** (config>service>vpls>sap>stp link-type)
[Tree] (config>service>template>vpls-sap-template>stp link-type)
[Tree] (config>service>vpls>spoke-sdp>stp link-type)

Full Context configure service template vpls-sap-template stp link-type
configure service vpls sap stp link-type
configure service vpls spoke-sdp stp link-type

Description This command instructs STP on the maximum number of bridges behind this SAP or spoke-SDP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected via a shared media, their SAP or spoke-SDPs should all be configured as shared, and timer-based transitions are used.

The **no** form of this command returns the link type to the default value.

Default link-type pt-pt

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

link-type

Syntax **link-type** {**pt-pt** | **shared**}
no link-type

Context **[Tree]** (config>service>pw-template>stp link-type)

Full Context configure service pw-template stp link-type

Description This command instructs STP on the maximum number of bridges behind this SAP or spoke SDP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected via a shared media, their SAP or spoke SDPs should all be configured as shared, and timer-based transitions are used.

The **no** form of this command returns the link type to the default value.

Default link-type pt-pt

Platforms All

16.155 linktrace

linktrace

Syntax **linktrace** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**ttl** *ttl-value*]

Context **[Tree]** (oam>eth-cfm linktrace)

Full Context oam eth-cfm linktrace

Description The command initiates a linktrace test.

Parameters *mac-address* — Specifies a unicast MAC address destination.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID of the peer within the association. The domain and association information are derived from the **source mep** for the session. The Layer 2 IEEE MAC address is resolved from previously-learned remote MAC addressing, derived from the reception and processing of the ETH-CC PDU. The local MEP must be administratively enabled.

Values 1 to 8191

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

ttl-value — Specifies the TTL for a returned linktrace.

Values 0 to 255

Default 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.156 live-output

live-output

Syntax **live-output** {*ip-address* | *fqdn*} [**port** *port*] [**router** {*router-instance* | **service-name** *service-name*}]
no live-output

Context **[Tree]** (config>call-trace>trace-profile live-output)

Full Context configure call-trace trace-profile live-output

Description This command specifies a live output destination for this trace. When configured, captures will not be stored locally but sent (over UDP) to the server in the specified routing context. The destination can be specified as either an IP address or a DNS FQDN. The **live-output** and **debug-output** commands are mutually exclusive.

The **no** form of this command disables live output streaming.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the server to stream to.

fqdn — Specifies the FQDN that represents the server in DNS, up to 255 characters.

port — Specifies the UDP port on which the server is listening.

Values 1 to 65535

Default 29770

router-instance — Specifies the router instance in which the live output is forwarded.

service-name — Specifies the name of the Layer 3 service in which the live output is forwarded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.157 lldp

lldp

Syntax **lldp**

Context **[Tree]** (config>port>ethernet lldp)

Full Context configure port ethernet lldp

Description Commands in this context configure Link Layer Discovery Protocol (LLDP) parameters on the specified port.

Platforms All

lldp

Syntax **lldp**

Context **[Tree]** (config>port>ethernet lldp)

Full Context configure port ethernet lldp

Description Commands in this context configure Link Layer Discovery Protocol (LLDP) parameters on the specified port.

Platforms All

lldp

Syntax **lldp**

Context **[Tree]** (config>system lldp)

Full Context configure system lldp

Description Commands in this context configure system-wide Link Layer Discovery Protocol parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.158 llf

llf

Syntax [**no**] **llf**

Context **[Tree]** (config>service>apipe>sap>atm llf)
[Tree] (config>service>epipe>sap>ethernet llf)

Full Context configure service apipe sap atm llf
configure service epipe sap ethernet llf

Description This command enables Link Loss Forwarding (LLF) on an Ethernet port or an ATM port. This feature provides an end-to-end OAM fault notification for Ethernet VLL service and for ATM VLL service of vc-type atm-cell. It brings down the Ethernet port (Ethernet LLF) or sends a SONET/SDH Path AIS (ATM LLF) toward the attached CE when there is a local fault on the Pseudowire or service, or a remote fault on the SAP or pseudowire, signaled with label withdrawal or T-LDP status bits. It ceases when the fault disappears.

The Ethernet port must be configured for null encapsulation.

For the 7750 SR, the ATM port must be configured as a SAP on an Apipe service of vc-type atm-cell. The ATM port must also be configured on the following MDAs:

- 1-port OC12/STM4 ASAP MDA. At OC3/STM1 port level
- 4-port ATM MDA at OC12/STM4 or OC3/STM1 port level

The ATM port must be configured as a SAP on an Apipe service of vc-type atm-cell. The ATM port must also be configured on the following MDAs:

- 1-port OC12/STM4 ASAP MDA. At OC3/STM1 port level
- 4-port ATM MDA at OC12/STM4 or OC3/STM1 port level

This feature is also supported in Epipes with BGP-EVPN enabled. In this case, upon removal of the EVPN destination, the port is brought oper-down with flag LinkLossFwd, however the AD per-EVI route for the SAP is still advertised (the SAP is kept oper-up).

The **no** form of this command disables LLF on an Ethernet port or an ATM port.

Default no llf

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap atm llf

All

- configure service epipe sap ethernet llf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.159 lmi

lmi

Syntax **lmi** [*port-id*]
no lmi

Context **[Tree]** (debug>frame-relay lmi)

Full Context debug frame-relay lmi

Description This debug command enables tracing of all the LMI messages in both receive and transmit directions for one or all of the Frame Relay interfaces. All types of Frame Relay interfaces are supported. If the port ID is not specified, debug is enabled on all Frame Relay interfaces.

The **no** form of this command turns off LMI and Frame-Relay debugging, **debug>frame-relay>no lmi** and **debug>no frame-relay**.

Parameters *port-id* — Specifies the ILMI-supporting port ID.

Values

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

Output The following output is an example of frame relay LMI information.

Sample Output

```
2959 2007/04/11 23:01:34.63 MINOR: DEBUG #2001 - FR
"FR: TX STATUS Msg on dce Port: 1/1/1 LMI: itu
FR Hdr: 00 01 03 08 00 7D
Rpt IE: 51 01 01 LINK_INT_VERIFY
KA IE: 53 02 31 45 TxSeqNo=49 RxSeqNo=69"

2960 2007/04/11 23:01:44.63 MINOR: DEBUG #2001 - FR
"FR: RX STATUS ENQ Msg on dce Port: 1/1/1 LMI: itu
FR Hdr: 00 01 03 08 00 75
Rpt IE: 51 01 01 LINK_INT_VERIFY
KA IE: 53 02 46 31 TxSeqNo=70 RxSeqNo=49"
```

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.160 lmi-type

lmi-type

Syntax **lmi-type** {**ansi** | **itu** | **none** | **rev1**}
no lmi-type

Context **[Tree]** (config>port>ml-bundle>mlfr>frame-relay lmi-type)
[Tree] (config>port>sonet-sdh>path>frame-relay lmi-type)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay lmi-type)
[Tree] (config>port>tdm>ds3>frame-relay lmi-type)
[Tree] (config>port>tdm>e1>channel-group>frame-relay lmi-type)
[Tree] (config>port>tdm>e3>frame-relay lmi-type)

Full Context configure port multilink-bundle mlfr frame-relay lmi-type
configure port sonet-sdh path frame-relay lmi-type
configure port tdm ds1 channel-group frame-relay lmi-type
configure port tdm ds3 frame-relay lmi-type
configure port tdm e1 channel-group frame-relay lmi-type
configure port tdm e3 frame-relay lmi-type

Description This command configures the Local Management Interface (LMI) type for Frame Relay interfaces. LMIs are sets of enhancements to the basic Frame Relay specification.

The **no** form of this command changes the LMI type back to the default value.

Default itu

Parameters **ansi** — Specifies to use ANSI T1.617 Annex D.

itu — Specifies to use ITU-T Q933 Annex A.

none — Specifies to disable Frame Relay LMI on the given port/channel.

rev1 — Specifies to use the Rev 1 version of ANSI T1.617 Annex D.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay lmi-type

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlfr frame-relay lmi-type

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group frame-relay lmi-type
- configure port tdm ds1 channel-group frame-relay lmi-type
- configure port tdm e3 frame-relay lmi-type
- configure port tdm ds3 frame-relay lmi-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.161 lmm

lmm

Syntax **lmm** [**test-id** *test-id*] [**create**]
no lmm

Context **[Tree]** (config>oam-pm>session>ethernet lmm)

Full Context configure oam-pm session ethernet lmm

Description This command configures the LMM test ID to be assigned to the Tx and Rx counter-based loss test and creates the individual test. LMM does not carry this test ID in the PDU; the value is of local significance.

The **no** form of this command removes the LMM test function from the PM Session.

Parameters *test-id* — Specifies the value to be placed in the 4-byte test ID field of an ETH-DMM PDU.

Values 0 to 2147483647

create — Creates the test.

Platforms All

16.162 lmp

lmp

Syntax [**no**] **lmp**

Context **[Tree]** (config>router lmp)

Full Context configure router lmp

Description This command creates a context for the configuration of the Link Management Protocol (LMP) on the system.

Default no lmp

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.163 lns-group

lns-group

Syntax **lns-group** *lns-group-id*
no lns-group

Context **[Tree]** (config>router>l2tp>group lns-group)
[Tree] (config>router>l2tp>group>tunnel lns-group)
[Tree] (config>service>vprn>l2tp>group lns-group)
[Tree] (config>service>vprn>l2tp>group>tunnel lns-group)

Full Context configure router l2tp group lns-group
configure router l2tp group tunnel lns-group
configure service vprn l2tp group lns-group
configure service vprn l2tp group tunnel lns-group

Description This command configures the ISA LNS group for the L2TP group.

The **no** form of this command removes the LNS group ID from the configuration.

Default no lns-group

Parameters *lns-group-id* — Specifies the LNS group ID.

Values 1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

lns-group

Syntax **lns-group** *lns-group-id* [**create**]
no lns-group *lns-group-id*

Context **[Tree]** (config>isa lns-group)

Full Context configure isa lns-group

Description This command configures an LNS group.

The **no** form of the command removes the LNS group ID from the configuration.

Default none

Parameters *lns-group-id* — Specifies the LNS group identifier.

Values 1 to 4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.164 load

load

Syntax **load** *file-url* [**overwrite** | **insert** | **append**]

Context **[Tree]** (candidate load)

Full Context candidate load

Description This command loads a previously saved candidate configuration into the current candidate. The edit point will be set to the end of the loaded configuration lines. The candidate configuration cannot be modified while a load is in progress.

Default If the candidate is empty then a load without any of the optional parameters (such as overwrite, and so on) will load the file-url into the candidate. If the candidate is not empty then one of the options, such as overwrite, insert, and so on, must be specified.

Parameters *file-url* — Specifies the directory and filename to load.

overwrite — Discards the contents of the current candidate and replace it with the contents of the file.

insert — Inserts the contents of the file at the current edit point.

append — Inserts the contents of the file at the end of the current candidate.

16.165 load-balance-key

load-balance-key

Syntax **load-balance-key** [**vendor** *vendor-id* [*vendor-id*]] **attribute-type** *attribute-type* [*attribute-type*]
load-balance-key source-ip-udp
no load-balance-key

Context **[Tree]** (config>router>radius-proxy>server load-balance-key)
[Tree] (config>service>vprn>radius-proxy>server load-balance-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router radius-proxy server load-balance-key
configure service vprn radius-proxy server load-balance-key

Description This command specifies the key used in calculating a hash to select an external RADIUS server from the pool of configured servers.

The key can be the source IP and source UDP port tuple, or the specified RADIUS attribute in RADIUS packets.

The **no** form of this command removes the parameters from the configuration.

Parameters *vendor-id* — Specifies the vendor-id of vendor-specific attribute.

Values 0 to 16777215

attribute-type — Specifies that the key is constructed with the attributes in the RADIUS message.

Values 1 to 255

source-ip-udp — Specifies that the key consists of the source IP address and source UDP port of the RADIUS message.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.166 load-balance-method

load-balance-method

Syntax **load-balance-method** {**per-session** | **per-tunnel**}
no load-balance-method

Context **[Tree]** (config>router>l2tp>group load-balance-method)
[Tree] (config>router>l2tp>group>tunnel load-balance-method)
[Tree] (config>service>vprn>l2tp>group load-balance-method)
[Tree] (config>service>vprn>l2tp>group>tunnel load-balance-method)

Full Context configure router l2tp group load-balance-method
configure router l2tp group tunnel load-balance-method
configure service vprn l2tp group load-balance-method
configure service vprn l2tp group tunnel load-balance-method

Description This command is applicable only to LNS. By default traffic load balancing between the BB-ISAs is based on sessions. Each session is individually assigned to an BB-ISA during session establishment phase.

By introducing MLPPPoX, all sessions of a bundle must be terminated on the same LNS BB-ISA. This is necessary for two reasons:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- QoS in the carrier IOM has a uniform view of the subscriber
- a single BB-ISA is responsible for MLPPPoX encapsulation/fragmentation for a given bundle.

Therefore, if fragmentation is enabled, load-balancing per tunnel must be configured. In the per tunnel load-balancing mode, all sessions within the same tunnel are terminated on the same LNS BB-ISA.

In the case that we have MLPPPoX sessions with a single member link, both load-balancing methods are valid.

The **no** form of this command reverts to the default.

Default load-balance-method per-session

Parameters **per-session** — Specifies that the traffic load balancing between the LNS BB-ISAs is based on individual PPPoE sessions.

per-tunnel — Specifies that the traffic load balancing between the LNS BB-ISAs is based on tunnels.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.167 load-balancing

load-balancing

Syntax load-balancing

Context **[Tree]** (config>service>epipe load-balancing)

Full Context configure service epipe load-balancing

Description This command enables the load-balancing context to configure interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ECMP on system-egress. This is a per interface setting. For load-balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.

Default not applicable

Platforms All

load-balancing

Syntax **load-balancing**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>service>vpls>config>service>template>vpls-template load-balancing)

Full Context configure service vpls config service template vpls-template load-balancing

Description This command enables the load-balancing context to configure interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ ECMP on system-egress. This is a per interface setting. For load-balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.

load-balancing

Syntax **load-balancing**

Context **[Tree]** (config>service>ies>if load-balancing)

Full Context configure service ies interface load-balancing

Description This command enables the load-balancing context to configure interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ ECMP on system-egress. This is a per interface setting. For load balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.

Platforms All

load-balancing

Syntax **load-balancing**

Context **[Tree]** (config>service>vprn>nw-if load-balancing)

Full Context configure service vprn network-interface load-balancing

Description This command enables the load-balancing context to configure interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ ECMP on system-egress. This is a per interface setting. For load-balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.

Platforms All

load-balancing

Syntax **load-balancing**

Context **[Tree]** (config>router>if load-balancing)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface load-balancing

Description This command enables the load-balancing context to configure interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ ECMP on system-egress. This is a per interface setting. For load-balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.

Platforms All

load-balancing

Syntax **load-balancing**

Context **[Tree]** (config>system load-balancing)

Full Context configure system load-balancing

Description This command enables the load-balancing context to configure the interface per-flow load balancing options that will apply to traffic entering this interface and egressing over a LAG/ ECMP on system-egress. This is a per interface setting. For load-balancing options that can also be enabled on the system level, the options enabled on the interface level overwrite system level configurations.

Platforms All

16.168 load-balancing-algorithm

load-balancing-algorithm

Syntax **load-balancing-algorithm** *option*
no load-balancing-algorithm

Context **[Tree]** (config>port>ethernet load-balancing-algorithm)
[Tree] (config>port>sonet-sdh>path load-balancing-algorithm)
[Tree] (config>port>tdm>ds1>channel-group load-balancing-algorithm)
[Tree] (config>port>tdm>ds3 load-balancing-algorithm)
[Tree] (config>port>tdm>e1>channel-group load-balancing-algorithm)
[Tree] (config>port>tdm>e3 load-balancing-algorithm)

Full Context configure port ethernet load-balancing-algorithm
configure port sonet-sdh path load-balancing-algorithm
configure port tdm ds1 channel-group load-balancing-algorithm
configure port tdm ds3 load-balancing-algorithm
configure port tdm e1 channel-group load-balancing-algorithm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port tdm e3 load-balancing-algorithm

Description This command specifies the load balancing algorithm to be used on this port.

In the default mode, **no load-balancing-algorithm**, the port inherits the global settings. The value is not applicable for ports that do not pass any traffic.

The configuration of load-balancing-algorithm at logical port level has three possible values:

- **include-l4** — Enables inherits system-wide settings including Layer 4 source and destination port value in hashing algorithm.
- **exclude-l4** — Layer 4 source and destination port value will not be included in hashing.
- **no load-balancing-algorithm** — Inherits system-wide settings.

The hashing algorithm addresses finer spraying granularity where many hosts are connected to the network. To address more efficient traffic distribution between network links (forming a LAG group), a hashing algorithm extension takes into account Layer 4 information (src/dst L4-protocol port). The hashing index can be calculated according to the following algorithm:

If [(TCP or UDP traffic) & enabled]

hash (<TCP/UDP ports>, <IP addresses>)

else if (IP traffic)

hash (<IP addresses>)

else

hash (<MAC addresses>)

endif

This algorithm will be used in all cases where IP information in per-packet hashing is included (refer to “Traffic Load Balancing Options” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide*). However the Layer 4 information (TCP/UDP ports) will not be used in the following cases:

- fragmented packets

Default no load-balancing-algorithm

Parameters *option* — Specifies the load balancing algorithm to be used on this port.

Values **include-l4** — Specifies that the source and destination ports are used in the hashing algorithm.**exclude-l4** — Specifies that the source and destination ports are not used in the hashing algorithm.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path load-balancing-algorithm

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port tdm ds3 load-balancing-algorithm
- configure port tdm e1 channel-group load-balancing-algorithm
- configure port tdm ds1 channel-group load-balancing-algorithm
- configure port tdm e3 load-balancing-algorithm

All

- configure port ethernet load-balancing-algorithm

16.169 load-balancing-weight

load-balancing-weight

Syntax **load-balancing-weight** *value*
no load-balancing-weight [*value*]

Context **[Tree]** (config>service>vprn>static-route-entry>next-hop load-balancing-weight)

Full Context configure service vprn static-route-entry next-hop load-balancing-weight

Description This command configures a weighted ECMP load-balancing weight for a static route next-hop.

If all of the ECMP next-hops of a static route have a configured load-balancing-weight then packets matching the route are sprayed according to the relative weights. In other words, the next-hop interface with the largest load-balancing weight should receive the most forwarded traffic if weighted ECMP is applicable.

The **no** form of this command disables weighted ECMP for the interface and effectively disables weighted ECMP for the entire static route.

Parameters *value* — Specifies the cost metric value.

Values 0 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** [*weight*]
no load-balancing-weight

Context **[Tree]** (config>service>vprn>ospf>area>if load-balancing-weight)
[Tree] (config>service>vprn>ospf3>area>if load-balancing-weight)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ospf area interface load-balancing-weight
configure service vprn ospf3 area interface load-balancing-weight

Description This command configures the weighted ECMP load-balancing weight for an IS-IS, OSPF, and OSPF3 interface. If the interface becomes an ECMP next hop for an IPv4 or IPv6 route, and all the other ECMP next hops are interfaces with configured (non-zero) load-balancing weights, then the traffic distribution over the ECMP interfaces is proportional to the weights. This means that the interface with the largest load-balancing weight receives the most forwarded traffic if weighted ECMP is applicable.

The **no** form of this command disables weighted ECMP for the interface which effectively disables weighted ECMP for any IP prefix that has this interface as a next hop.

Default no load-balancing-weight

Parameters *weight* — Specifies the load balancing weight.

Values 1 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** *weight*
no load-balancing-weight

Context **[Tree]** (config>service>vprn>isis>if load-balancing-weight)

Full Context configure service vprn isis interface load-balancing-weight

Description This command configures the weighted ECMP load-balancing weight for an IS-IS interface of the VPRN. If the interface becomes an ECMP next-hop for IPv4 or IPv6 route and all the other ECMP next-hops are interfaces with configured (non-zero) load-balancing weights, then the traffic distribution over the ECMP interfaces is proportional to the weights. In other words, the interface with the largest **load-balancing-weight** should receive the most forwarded traffic if weighted ECMP is applicable.

The **no** form of this command disables weighted ECMP for the interface and, therefore, effectively disables weighted ECMP for any IP prefix that has this interface as a next-hop.

Default no load-balancing-weight

Parameters *weight* — Specifies the load balancing weight.

Values 0 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

load-balancing-weight

Syntax **load-balancing-weight** *weight*
no load-balancing-weight

Context **[Tree]** (config>router>ldp>if-params>if load-balancing-weight)

Full Context configure router ldp interface-parameters interface load-balancing-weight

Description This command configures the load balancing weight for the LDP interface. The load balancing weight, normalized to 64, is used for weighted ECMP of LDP labeled packets over direct network IP interfaces.

If the interface becomes an ECMP next hop for an LDP FEC, and all the other ECMP next hops are interfaces with configured (non-zero) load-balancing weights, then the traffic distribution over the ECMP interfaces is proportional to the normalized weight with a granularity of 64.

If one or more of the LDP interfaces in the ECMP set does not have a configured load-balancing weight, then the system falls back to ECMP.

The **no** form of this command removes the load balancing weight for the LDP interface.

Parameters *weight* — Specifies the load balancing weight value.

Values 0 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** *weight*
no load-balancing-weight

Context **[Tree]** (config>router>mpls>lsp load-balancing-weight)

Full Context configure router mpls lsp load-balancing-weight

Description This command assigns a weight to an MPLS LSP for use in the weighted load-balancing, or weighted ECMP, over MPLS feature.

Parameters *weight* — Specifies a 32-bit integer representing the weight of the LSP.

Values 0 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** *weight*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no load-balancing-weight

Context [Tree] (config>router>mpls>fwd-policies>fwd-policy>nh-grp load-balancing-weight)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group load-balancing-weight

Description This command configures the load balancing weight of an NHG entry in a forwarding policy.

A weight for each NHG of a policy must be assigned to the weighted ECMP forwarding to operate over the set of NHGs of the policy.

The **no** form of this command removes the load balancing weight from an NHG entry in a forwarding policy.

Parameters *weight* — Specifies the load balancing weight value.

Values 1 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** *value*
no load-balancing-weight [*value*]

Context [Tree] (config>router>static-route-entry>next-hop load-balancing-weight)

Full Context configure router static-route-entry next-hop load-balancing-weight

Description This command configures a weighted ECMP load-balancing weight for a static route next-hop.

If all of the ECMP next-hops of a static route have a configured load-balancing-weight then packets matching the route are sprayed according to the relative weights. In other words, the next-hop interface with the largest load-balancing weight should receive the most forwarded traffic if weighted ECMP is applicable.

The **no** form of this command disables weighted ECMP for the interface and effectively disables weighted ECMP for the entire static route.

Parameters *value* — Specifies the load balancing weight value.

Values 0 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** [*value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no load-balancing-weight

Context [Tree] (config>router>isis>interface load-balancing-weight)

Full Context configure router isis interface load-balancing-weight

Description This command configures the weighted ECMP load-balancing weight for an IS-IS interface. If the interface becomes an ECMP next hop for an IPv4 or IPv6 route, and all the other ECMP next hops are interfaces with configured (non-zero) load-balancing weights, then the traffic distribution over the ECMP interfaces is proportional to the weights. In other words, the interface with the largest load-balancing weight should receive the most forwarded traffic if weighted ECMP is applicable.

The **no** form of this command disables weighted ECMP for the interface and therefore effectively disables weighted ECMP for any IP prefix that has this interface as a next hop.

Default no load-balancing-weight

Parameters *value* — 0 to 4294967295

Platforms All

load-balancing-weight

Syntax **load-balancing-weight** [*weight*]
no load-balancing-weight

Context [Tree] (config>router>ospf>area>if load-balancing-weight)
[Tree] (config>router>ospf3>area>if load-balancing-weight)

Full Context configure router ospf area interface load-balancing-weight
configure router ospf3 area interface load-balancing-weight

Description This command configures the weighted ECMP load-balancing weight for an OSPF or OSPF3 interface. If the interface becomes an ECMP next hop for an IPv4 or IPv6 route, and all the other ECMP next hops are interfaces with configured (non-zero) load-balancing weights, then the traffic distribution over the ECMP interfaces is proportional to the weights. This means that the interface with the largest load-balancing weight receives the most forwarded traffic if weighted ECMP is applicable.

The **no** form of this command disables weighted ECMP for the interface which effectively disables weighted ECMP for any IP prefix that has this interface as a next hop.

Default no load-balancing-weight

Parameters *weight* — Specifies the load balancing weight.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.170 local

local

Syntax [**no**] **local**

Context **[Tree]** (config>subscr-mgmt>sla-profile>control local)

Full Context configure subscriber-mgmt sla-profile control local

Description This command enables a session that is set up with local control plane handling to use this SLA profile. This command cannot be disabled.

Default local

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local

Syntax [**no**] **local**

Context **[Tree]** (config>subscr-mgmt>sub-profile>control local)

Full Context configure subscriber-mgmt sub-profile control local

Description This command enables a session that is set up with local control plane handling to use this subscriber profile. This command cannot be disabled.

Default local

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local

Syntax **local** [**inherit** | **all** | **vc-only** | **none**]

Context **[Tree]** (config>service>vprn>ttl-propagate local)

Full Context configure service vprn ttl-propagate local

Description This command overrides the global configuration of the TTL propagation for locally generated packets which are forwarded over a MPLS LSPs in a given VPRN service context.

The global configuration is performed under config>router>ttl-propagate>vprn-local.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default behavior for a given VPRN instance is to inherit the global configuration for the same command. The user can explicitly set the default behavior by configuring the inherit value

Default local inherit

Parameters **inherit** — Specifies the TTL propagation behavior is inherited from the global configuration under config>router>ttl-propagate>vprn-local.

none — Specifies the TTL of the IP packet is not propagated into the VC label or labels in the transport label stack.

vc-only — Specifies the TTL of the IP packet is propagated into the VC label and not into the labels in the transport label stack.

all — Specifies the TTL of the IP packet is propagated into the VC label and all labels in the transport label stack.

Platforms All

local

Syntax **local**

Context **[Tree]** (config>ipsec>ts-list local)

Full Context configure ipsec ts-list local

Description Commands in this context configure local TS-list parameters. The TS-list is the traffic selector of the local system, such as TSr, when the system acts as an IKEv2 responder.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.171 local-address

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>router>l2tp local-address)
[Tree] (config>router>l2tp>group local-address)
[Tree] (config>router>l2tp>group>tunnel local-address)
[Tree] (config>service>vprn>l2tp local-address)
[Tree] (config>service>vprn>l2tp>group local-address)
[Tree] (config>service>vprn>l2tp>group>tunnel local-address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router l2tp group local-address
configure router l2tp group tunnel local-address
configure router l2tp local-address
configure service vprn l2tp group local-address
configure service vprn l2tp group tunnel local-address
configure service vprn l2tp local-address

Description This command configures the local address.

The **no** form of this command removes the local IP address from the configuration.

Default no local-address

Parameters *ip-address* — Specifies the IP address used during L2TP authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy local-address)

Full Context configure subscriber-mgmt bgp-peering-policy local-address

Description This command configures the local IP address used by the group or neighbor when communicating with BGP peers.

Outgoing connections use the **local-address** as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the 7750 SR OS uses the system IP address when communicating with IBGP peers and uses the interface address for directly connected EBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of this command removes the configured local-address for BGP.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the local address.

For IPv4, the local address is expressed in dotted decimal notation. Allowed values are a valid routable IP address on the router, either an interface or system IP address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For IPv6, the local address is expressed in semi-colon hexadecimal notation. Allowed values is an interface or a system IP address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0 to FFFF]H d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>service>vpls>gsmp>group>neighbor local-address)
[Tree] (config>service>vprn>gsmp>group>neighbor local-address)

Full Context configure service vpls gsmp group neighbor local-address
configure service vprn gsmp group neighbor local-address

Description This command configures the source ip-address used in the connection towards the neighbor. The local address is optional. If specified the node will accept connections only for that address in the service running ANCP. The address may be created after the reference but connections will not be accepted until it is created. If the local address is not used, the system accepts connections on any interface within the routing context.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the source IP address to be used in the connection toward the neighbor.

Values *ip-address*: a.b.c.d. (unicast address only)

Platforms All

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query local-address)

Full Context configure subscriber-mgmt wlan-gw tunnel-query local-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables matching on tunnels that are terminated by the specified IP address on the WLAN-GW.

The **no** form of this command disables matching on the local IP address.

Default no local-address

Parameters *ip-address* — Specifies the IPv4 or IPv6 address.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>service>vprn>bgp>group local-address)
[Tree] (config>service>vprn>bgp>group>neighbor local-address)

Full Context configure service vprn bgp group local-address
configure service vprn bgp group neighbor local-address

Description Configures the local IP address used by the group or neighbor when communicating with BGP peers.

Outgoing connections use the **local-address** as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the OS uses the system IP address when communicating with IBGP peers and uses the interface address for directly connected EBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of this command removes the configured local-address for BGP.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Parameters **no local-address** — The router ID is used when communicating with IBGP peers and the interface address is used for directly connected EBGP peers.

ip-address — The local address expressed in dotted decimal notation. Allowed values are a valid routable IP address on the router, either an interface or system IP address.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>service>vprn>msdp local-address)
[Tree] (config>service>vprn>msdp>group local-address)
[Tree] (config>service>vprn>msdp>group>peer local-address)
[Tree] (config>service>vprn>msdp>peer local-address)

Full Context configure service vprn msdp group local-address
configure service vprn msdp group peer local-address
configure service vprn msdp local-address
configure service vprn msdp peer local-address

Description This command configures the local end of a Multicast Source Discovery Protocol (MSDP) session. For MSDP to function, at least one peer must be configured. When configuring a peer, you must include this **local-address** command to configure the local end of the MSDP session. This address must be present on the node and is used to validate incoming connections to the peer and to establish connections to the remote peer.

If the user enters this command, then the address provided is validated and will be used as the local address for MSDP peers from that point. If a subsequent **local-address** command is entered, it will replace the existing configuration and existing sessions will be terminated.

Similarly, when the **no** form of this command is entered, the existing local address will be removed from the configuration and the existing sessions will be terminated.

Whenever a session is terminated, all information pertaining to and learned from that peer will be removed.

Whenever a new peering session is created or a peering session is lost, an event message should be generated.

The **no** form of this command removes the local address from the configuration.

Default no local-address

Parameters *ip-address* — Specifies an existing address on the node.

Platforms All

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>router>pcep>pcc local-address)
[Tree] (config>router>pcep>pce local-address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router pcep pcc local-address
configure router pcep pce local-address

Description This command configures the local address of the PCEP speaker.

The PCEP protocol operates over TCP using destination TCP port 4189. The PCE client (PCC) always initiates the connection. Once the user configures the PCEP local address and the peer address on the PCC, the latter initiates a TCP connection to the PCE. When the connection is established, the PCC and PCE exchange OPEN messages, which initializes the PCEP session and exchanges the session parameters to be negotiated.

The PCC always checks first if the remote PCE address is reachable out-of-band via the management port. If not, it will check if the remote PCE address is reachable in-band. When the session comes up out-of-band, the system IP address is always used. The local address configured by the user is only used for in-band sessions, and is otherwise ignored.

The **no** form of the command removes the configured local address of the PCEP speaker.

Parameters *ip-address* — the IP address of the PCEP speaker to be used for in-band sessions

Platforms All

local-address

Syntax **local-address control** *ip-address* **data** *ip-address*
no local-address

Context **[Tree]** (config>service>ies>video-interface>adi>scte30 local-address)
[Tree] (config>service>vprn>video-interface>adi>scte30 local-address)

Full Context configure service ies video-interface adi scte30 local-address
configure service vprn video-interface adi scte30 local-address

Description SCTE 30 requires a TCP session per zone-channel between the ad server and splicer for control communication and it requires UDP sessions on which the video ad stream is sent. This command specifies the splicer's control IP address to which the ad-servers should setup TCP connections and the data IP address to which the video ad streams should be sent.

The **no** form of the command removes the address information from the local address configuration.

Parameters **control** *ip-address* — Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad control streams. This address should be in the same subnet as the ip address assigned to the video interface.

The values of **control** *ip-address* and the **data** *ip-address* specify the local IP address to which ad servers send SCTE 30 ad data streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

data *ip-address* — Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad data streams. This address should be in the same subnet as the IP address assigned to the video interface.

The values of the **control** *ip-address* and the **data** *ip-address* specify the local IP address to which ad servers send SCTE 30 ad control streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

local-address

Syntax **local-address** *address*
no local-address

Context **[Tree]** (config>router>msdp local-address)
[Tree] (config>router>msdp>peer local-address)
[Tree] (config>router>msdp>group local-address)
[Tree] (config>router>msdp>group>peer local-address)

Full Context configure router msdp group local-address
configure router msdp group peer local-address
configure router msdp local-address
configure router msdp peer local-address

Description This command configures the local end of a Multicast Source Discovery Protocol (MSDP) session. For MSDP to function, at least one peer must be configured. When configuring a peer, you must include this local-address command to configure the local end of the MSDP session. This address must be present on the node and is used to validate incoming connections to the peer and to establish connections to the remote peer.

If the user enters this command, then the address provided is validated and will be used as the local address for MSDP peers from that point. If a subsequent **local-address** command is entered, it will replace the existing configuration and existing sessions will be terminated.

Similarly, when the **no** form of this command is entered, the existing local-address will be removed from the configuration and the existing sessions will be terminated.

Whenever a session is terminated, all information pertaining to and learned from that peer will be removed.

Whenever a new peering session is created or a peering session is lost, an event message should be generated.

The **no** form of this command removes the `local-address` from the configuration.

Default no local-address

Parameters *address* — Specifies an existing address on the node.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

local-address

Syntax **local-address** *ip-address*
no local-address

Context **[Tree]** (config>router>origin-validation>rpki-session local-address)

Full Context configure router origin-validation rpki-session local-address

Description This command configures the local address to use for setting up the TCP connection used by an RPKI-Router session. The default local-address is the outgoing interface IPv4 or IPv6 address. The local-address cannot be changed without first shutting down the session.

Default no local-address

Parameters *ip-address* — Specifies an IPv4 address or an IPv6 address.

Platforms All

local-address

Syntax **local-address** [*ip-int-name* | *ip-address* | *ipv6-address*]
no local-address

Context **[Tree]** (config>router>bgp>group local-address)
[Tree] (config>router>bgp>group>neighbor local-address)

Full Context configure router bgp group local-address
configure router bgp group neighbor local-address

Description This command configures the local IP address used by the group or neighbor when communicating with BGP peers.

Outgoing connections use the **local-address** as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the router uses the system IP address when communicating with IBGP peers and uses the interface address for directly connected EBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

When set to a router interface, the **local-address** inherits the primary IPv4 or IPv6 address of the router interface depending on whether BGP is configured for IPv4 or IPv6. If the corresponding IPv4 or IPv6 address is not configured on the router interface, the BGP sessions that have this interface set as the **local-address** are kept down until an interface address is configured on the router interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the configured local-address for BGP.

The **no** form of this command used at the group level returns the configuration to the value defined at the global level.

The **no** form of this command used at the neighbor level returns the configuration to the value defined at the group level.

Default no local-address

Parameters *ip-address* — Specifies the local address expressed in dotted decimal notation. Allowed value is a valid routable IP address on the router, either an interface or system IP address.

Values ipv4-address:

- a.b.c.d (host bits must be 0)

ipv6-address — Specifies the local address expressed in dotted decimal notation. Allowed value is a valid routable IPv6 address on the router, either an interface or system IPv6 address.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

ip-int-name — Specifies the IP interface name whose address the local address will inherit. The interface can be any network interface configured on the system.

Platforms All

local-address

Syntax **local-address** *ip-address* | *ipv6-address*
no local-address

Context **[Tree]** (config>bmp>station>connection local-address)

Full Context configure bmp station connection local-address

Description This command configures the local IP address used by the local router when communicating with the BMP monitoring station. This configuration is optional.

Outgoing connections use the local-address as the source of the TCP connection when initiating connections with a monitoring station.

The BMP session may flap when this parameter is changed. Shut down the BMP session before changing the values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the configured local-address for the BMP session. The default is to use the system IP address.

Default local-address ip-address (system IP address)

Parameters *ip-address* — Specifies the local address expressed in dotted decimal notation. Allowed value is a valid routable IP address on the router, either an interface or system IP address.

Values ipv4-address:

- a.b.c.d (host bits must be 0)

ipv6-address — Specifies the local address expressed in dotted decimal notation. Allowed value is a valid routable IPv6 address on the router, either an interface or system IPv6 address.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

16.172 local-address-assignment

local-address-assignment

Syntax **local-address-assignment**

Context **[Tree]** (config>service>ies>sub-if local-address-assignment)
[Tree] (config>service>vprn>sub-if local-address-assignment)
[Tree] (config>service>ies>sub-if>grp-if local-address-assignment)
[Tree] (config>service>vprn>sub-if>grp-if local-address-assignment)

Full Context configure service ies subscriber-interface group-interface local-address-assignment
configure service ies subscriber-interface local-address-assignment
configure service vprn subscriber-interface group-interface local-address-assignment
configure service vprn subscriber-interface local-address-assignment

Description Commands in this context configure local address assignment parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-address-assignment

Syntax **local-address-assignment** [**terminate-only**]
no local-address-assignment

Context **[Tree]** (debug>service>id>ppp>event local-address-assignment)

Full Context debug service id ppp event local-address-assignment

Description This command enables debugging for **local-address-assignment** events.

The **no** form of this command disables debugging.

Parameters **terminate-only** — Enables debugging for local address assignment.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-address-assignment

Syntax [**no**] **local-address-assignment**

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw local-address-assignment)
[Tree] (config>service>vprn>if>sap>ipsec-gw local-address-assignment)

Full Context configure service ies interface sap ipsec-gw local-address-assignment
configure service vprn interface sap ipsec-gw local-address-assignment

Description Commands in this context configure local address assignments for the IPsec gateway.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.173 local-age

local-age

Syntax **local-age** *aging-timer*
no local-age [*aging-timer*]

Context **[Tree]** (config>service>vpls local-age)
[Tree] (config>service>template>vpls-template local-age)

Full Context configure service template vpls-template local-age
configure service vpls local-age

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Specifies the aging time for locally learned MAC addresses in the forwarding database (FDB) for the Virtual Private LAN Service (VPLS) instance. In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the FDB. The **local-age** timer specifies the aging time for local learned MAC addresses.

The **no** form of this command returns the local aging timer to the default value.

Default local age 300 — Local MACs aged after 300 seconds.

Parameters *aging-timer* — Specifies the aging time for local MACs expressed in seconds

Values 60 to 86400

Platforms All

16.174 local-as

local-as

Syntax **local-as** *as-number* [**private**]
no local-as

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy local-as)

Full Context configure subscriber-mgmt bgp-peering-policy local-as

Description This command configures a BGP virtual autonomous system (AS) number.

In addition to the AS number configured for BGP in the config>router>autonomous-system context, a virtual (local) AS number is configured. The virtual AS number is added to the as-path message before the router's AS number makes the virtual AS the second AS in the as-path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). Thus, by specifying this at each neighbor level, it is possible to have a separate as-number per EBGP session.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The **private** attribute can be added or removed dynamically by reissuing the command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to re-establish the peer relationship with the new local AS number.

This is an optional command and can be used in the following circumstance:

Provider router P is moved from AS1 to AS2. The customer router that is connected to P, however, is configured to belong to AS1. To avoid reconfiguring the customer router, the **local-as** value on router P can be set to AS1. Thus, router P adds AS1 to the as-path message for routes it advertises to the customer router.

The **no** form of this command used at the global level will remove any virtual AS number configured.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Parameters *as-number* — Specifies the virtual autonomous system number, expressed as a decimal integer.

Values 1 to 4294967295

private — Specifies that the local-as number is hidden in paths learned from the peering.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-as

Syntax **local-as** *as-number* [**private**] [**no-prepend-global-as**]
no local-as

Context **[Tree]** (config>service>vprn>bgp local-as)
[Tree] (config>service>vprn>bgp>group local-as)
[Tree] (config>service>vprn>bgp>group>neighbor local-as)

Full Context configure service vprn bgp group local-as
configure service vprn bgp group neighbor local-as
configure service vprn bgp local-as

Description This command configures a BGP virtual autonomous system (AS) number.

In addition to the global AS number configured for BGP in the config>router>autonomous-system context, a virtual (local) AS number can be configured to support various AS number migration scenarios. The local AS number is added to the to the beginning the as-path attribute ahead of the router's AS number.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This configuration parameter can be set at three levels: global level (applies to all EBGP peers), group level (applies to all EBGP peers in peer-group) or neighbor level (only applies to EBGP specified peer). Thus, by specifying this at each neighbor level, it is possible to have a separate local-as per EBGP session. The local-as command is not supported for IBGP sessions. When the optional **private** keyword is specified in the command the local-as number is not added to inbound routes from the EBGP peer that has **local-as** in effect.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The **private** attribute can be added or removed dynamically by reissuing the command.

Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to re-establish the peer relationship with the new local AS number.

This is an optional command and can be used in the following circumstance:

Provider router P is moved from AS1 to AS2. The customer router that is connected to P, however, is configured to belong to AS1. To avoid reconfiguring the customer router, the **local-as** value on router P can be set to AS1. Thus, router P adds AS1 to the as-path message for routes it advertises to the customer router.

The **no** form of this command used at the global level removes any virtual AS number configured.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no local-as

Parameters *as-number* — The virtual autonomous system number, expressed as a decimal integer.

Values 1 to 65535

private — Specifies the local-as is hidden in paths learned from the peering.

no-prepend-global-as — Specifies that the global-as is hidden in paths announced to the EBGP peer.

Platforms All

local-as

Syntax **local-as** *as-number* [**private**] [no-prepend-global-as]
no local-as

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp local-as)
[Tree] (config>router>bgp>group local-as)
[Tree] (config>router>bgp>group>neighbor local-as)

Full Context configure router bgp group local-as
configure router bgp group neighbor local-as
configure router bgp local-as

Description This command configures a BGP local autonomous system (AS) number. In addition to the global AS number configured for BGP using the autonomous-system command, a local AS number can be configured to support various AS number migration scenarios.

When the **local-as** command is applied to a BGP neighbor and the local-as is different from the peer-as, the session comes up as EBGP and by default the global-AS number and then (in that order) the local-as number are prepended to the AS_PATH attribute in outbound routes sent to the peer. In received routes from the EBGP peer, the local AS is prepended to the AS path by default, but this can be disabled with the **private** option.

When the **local-as** command is applied to a BGP neighbor and the local-as is the same as the peer-as, the session comes up as IBGP, and by default, the global-AS number is prepended to the AS_PATH attribute in outbound routes sent to the peer.

This configuration parameter can be set at three levels: global level (applies to all BGP peers), group level (applies to all BGP peers in group) or neighbor level (only applies to one specific BGP neighbor). By specifying this at the neighbor level, it is possible to have a separate **local-as** for each BGP session.

When the optional **no-prepend-global-as** command is configured, the global-as number is not added in outbound routes sent to an IBGP or EBGP peer.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The private option can be added or removed dynamically by reissuing the command. Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to re-establish the peer relationship with the new local AS number.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no local-as

Parameters *as-number* — Specifies the virtual autonomous system number expressed as a decimal integer.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

private — Specifies the local-as is hidden in paths learned from the peering.

no-prepend-global-as — Specifies that the global-as is hidden in paths announced to the BGP peer.

Platforms All

16.175 local-attachment-circuit

local-attachment-circuit

Syntax **local-attachment-circuit** *ac-name* [**endpoint** *endpoint-name*] [**create**]
no local-attachment-circuit *ac-name*

Context **[Tree]** (config>service>epipe>bgp-evpn local-attachment-circuit)

Full Context configure service epipe bgp-evpn local-attachment-circuit

Description This command configures a local attachment circuit (AC) in which the local Ethernet tag can be configured.

The **no** form of this command disables the context.

Default no local-attachment-circuit

Parameters *ac-name* — Specifies the name of the local attachment circuit, up to 32 characters.

endpoint-name — Specifies the name of the endpoint, up to 32 characters.

create — Keyword used to create the local AC.

Platforms All

16.176 local-auth-db

local-auth-db

Syntax **local-auth-db** *name*
no local-auth-db

Context **[Tree]** (config>service>dynsvc>policy>auth local-auth-db)

Full Context configure service dynamic-services dynamic-services-policy authentication local-auth-db

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the local authentication database to be used for local authentication of data-triggered dynamic services.

Local authentication and RADIUS authentication are mutually exclusive.

The **no** form of this command removes the local authentication database from the configuration and disables local authentication.

Parameters *name* — local authentication database name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-auth-db

Syntax **local-auth-db** *name* [**create**]
no local-auth-db *name*

Context **[Tree]** (config>service>dynsvc local-auth-db)

Full Context configure service dynamic-services local-auth-db

Description This command creates a local authentication database that can be used for local authentication of data-triggered dynamic services.

The **no** form of this command removes the local authentication database from the configuration.

Parameters *name* — Specifies a local authentication database name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.177 local-dhcp-server

local-dhcp-server

Syntax **local-dhcp-server** *server-name* [**create**]
no local-dhcp-server *server-name*

Context **[Tree]** (config>router>dhcp local-dhcp-server)
[Tree] (config>service>vprn>dhcp local-dhcp-server)

Full Context configure router dhcp local-dhcp-server
configure service vprn dhcp local-dhcp-server

Description This command instantiates a local DHCP server. A local DHCP server can serve multiple interfaces but is limited to the routing context it was which it was created.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *server-name* — Specifies the name of local DHCP server, up to 32 characters.

create — Keyword used to create the local DHCP server. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-dhcp-server

Syntax **local-dhcp-server** *server-name* [**create**] [**auto-provisioned**]
no local-dhcp-server *server-name*

Context **[Tree]** (config>router>dhcp6 local-dhcp-server)

Full Context configure router dhcp6 local-dhcp-server

Description This command instantiates a DHCP6 server. A local DHCP6 server can serve multiple interfaces but is limited to the routing context it was which it was created.

The **no** form of this command reverts to the default.

Parameters *server-name* — Specifies the name of local DHCP6 server, up to 32 characters.

create — Keyword used to create the local DHCP or DHCP6 server. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

auto-provisioned — Specifies the auto provisioning mode. This parameter only applies to DHCP6 creation to configure DHCP6 default values.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-dhcp-server

Syntax [**no**] **local-dhcp-server** *server-name* [**lease-address** *ip-prefix*[*prefix-length*]]
[**no**] **local-dhcp-server** *server-name* [**mac** *ieee-address*]
[**no**] **local-dhcp-server** *server-name* [**link-local-address** *ipv6z-address*]

Context **[Tree]** (debug>router local-dhcp-server)

Full Context debug router local-dhcp-server

Description This command enables, disables or configures debugging for a local DHCP server.

Parameters *server-name* — Specifies an existing local DHCP server name.

ip-prefix[/prefix-length] — Specifies the IP prefix and prefix length of the subnet.

Values ip-prefix — a.b.c.d (host bits must be 0)
length — 0 to 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ieee-address — Specifies that the provisioned MAC address for the local DHCP server.

ipv6z-address — Specifies the IPv6z address.

ipv6-address:	x:x:x:x:x:x:x:x [-interface]
	x:x:x:x:x:x:d.d.d.d [-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
interface	up to 32 characters, mandatory for link local addresses

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-dhcp-server

Syntax [**no**] **local-dhcp-server**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync local-dhcp-server)

Full Context configure redundancy multi-chassis peer sync local-dhcp-server

Description This command synchronizes DHCP server information.

Default no local-dhcp-server

Platforms All

local-dhcp-server

Syntax **local-dhcp-server** *local-server-name*
no local-dhcp-server

Context **[Tree]** (config>service>ies>if local-dhcp-server)
[Tree] (config>service>vprn>if>ipv6 local-dhcp-server)

Full Context configure service ies interface local-dhcp-server
configure service vprn interface ipv6 local-dhcp-server

Description This command assigns a DHCP server to the interface.

Parameters *local-server-name* — Specifies an existing local server name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-dhcp-server

Syntax **local-dhcp-server** *local-server-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no local-dhcp-server

Context [Tree] (config>router>if local-dhcp-server)
[Tree] (config>router>if>ipv6 local-dhcp-server)

Full Context configure router interface ipv6 local-dhcp-server
configure router interface local-dhcp-server

Description This command instantiates a local DHCP server. A local DHCP server can serve multiple interfaces but is limited to the routing context in which it was created.

The **no** form of this command reverts to the default value.

Default no local-dhcp-server

Parameters *local-server-name* — Specifies the name of local DHCP server, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.178 local-ecid

local-ecid

Syntax **local-ecid** *emulated circuit identifier*
no local-ecid

Context [Tree] (config>service>epipe>sap>cem local-ecid)

Full Context configure service epipe sap cem local-ecid

Description This command defines the Emulated Circuit Identifiers (ECID) to be used for the local (source) end of the circuit emulation service.

The **no** form of this command removes the ECID from the configuration.

Default local-ecid 65535

Parameters *emulated circuit identifier* — Specifies the value to be used as the local (source) ECID for the circuit emulation service. On CES packet reception, the ECID in the packet will be compared to the configured local-ecid value. These must match for the packet payload to be used for the TDM circuit. The remote-ecid value is inserted into the MEF-8 CES packet to be transmitted.

Values 0 to 1048575

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.179 local-end

local-end

Syntax **local-end** {*ip-address* | *ipv6-address*}
no local-end

Context **[Tree]** (config>service>sdp local-end)

Full Context configure service sdp local-end

Description This command configures the local-end address of the following SDP encapsulation types:

- IPv6 address of the termination point of a SDP of encapsulation **l2tpv3** (L2TP v3 tunnel).
- IPv4/IPv6 source address of a SDP of encapsulation **eth-gre-bridged** (L2oGRE SDP).
- IPv4 source address of a SDP of encapsulation **gre** (GRE SDP).

A change to the value of the local-end parameter requires that the SDP be shut down.

When used as the source address of a SDP of encapsulation **gre** (GRE SDP), the primary IPv4 address of any local network IP interface, loopback or otherwise, may be used.

The address of the following interfaces are not supported:

- unnumbered network IP interface
- IES interface
- VPRN interface
- CSC VPRN interface

The **local-end** parameter value adheres to the following rules:

- A maximum of 15 distinct address values can be configured for all GRE SDPs under the **config**>**service**>**sdp**>**local-end** context, and all L2oGRE SDPs under the **config**>**service**>**system**>**gre-eth-bridged**>**tunnel-termination** context.
- The same source address cannot be used in both contexts since an address configured for a L2oGRE SDP matches an internally created interface that is not available to other applications.
- The **local-end** address of a GRE SDP, when different from system, need not match the primary address of an interface that has the MPLS-over-GRE termination subnet configured, unless a GRE SDP or tunnel from the far-end router terminates on this address.

The **no** form of the command removes the address from the local-end configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* | *ipv6-address* — Specifies a IPv4 or IPv6 address for local-end of an SDP in dotted decimal notation.

Values

ip-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

Platforms All

16.180 local-fcc-port

local-fcc-port

Syntax **local-fcc-port** *port*
no local-fcc-port

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video local-fcc-port)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video local-fcc-port)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video local-fcc-port)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video local-fcc-port
configure mcast-management multicast-info-policy bundle channel video local-fcc-port
configure mcast-management multicast-info-policy bundle video local-fcc-port

Description This command configures the local port on which Fast Channel Change (FCC) requests are received. The value of this object can only be set for the default bundle and will be used by all bundles and channels.

The **local-fcc-port** *port* value is the only configuration parameter in the bundle “default” context.

The **no** form of the command removes the port from the video configuration.

Parameters *port* — Specifies a local port for FCC requests.

Values 1024 to 5999, 6251 to 65535

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.181 local-filtering

local-filtering

Syntax **local-filtering**

Context **[Tree]** (config>app-assure>group>url-filter local-filtering)

Full Context configure application-assurance group url-filter local-filtering

Description This command configures a URL filter policy for local filtering in order to filter traffic based on a list of URLs located on a file stored in the router compact flash.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.182 local-forward

local-forward

Syntax **local-forward** *local-forward-id* [**create**]
no local-forward *local-forward-id*

Context **[Tree]** (config>system>satellite local-forward)

Full Context configure system satellite local-forward

Description This command creates a local-forward instance.

A local-forward instance creates a traffic bypass within the Ethernet satellite, which allows traffic to be forwarded between satellite client ports.

The **no** form of this command deletes the specified local-forward instance.

Parameters **local-forward-id** — Specifies the ID number for the local-forward instance.

Values 1 to 10240

create — Creates a new local-forward instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.183 local-gateway-address

local-gateway-address

Syntax **local-gateway-address** [*ip-address* | *ipv6-address*]
no local-gateway-address

Context **[Tree]** (config>router>if>ipsec>ipsec-tunnel local-gateway-address)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel local-gateway-address)

Full Context configure router interface ipsec ipsec-tunnel local-gateway-address
configure service ies interface ipsec ipsec-tunnel local-gateway-address

Description This command configures local gateway address of the IPsec gateway.

Parameters *ip-address* — Specifies a unicast IPv4 address, up to 64 characters.

ipv6-address — Specifies a unicast global unicast IPv6 address, up to 64 characters.

Platforms VSR

local-gateway-address

Syntax **local-gateway-address** *ip-address*
no local-gateway-address

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw local-gateway-address)
[Tree] (config>service>vprn>if>sap>ipsec-gw local-gateway-address)

Full Context configure service ies interface sap ipsec-gw local-gateway-address
configure service vprn interface sap ipsec-gw local-gateway-address

Description This command configures local gateway address of the IPsec gateway.

Parameters *ip-address* — Specifies a unicast IPv4 address or a global unicast IPv6 address. This address must be within the subnet of the public interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

local-gateway-address

Syntax **local-gateway-address** *ip-address* **peer** *ip-address* **delivery-service** *service-id*
no local-gateway-address

Context **[Tree]** (config>service>vprn>if>sap>ipsec-tunnel local-gateway-address)

Full Context configure service vprn interface sap ipsec-tunnel local-gateway-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the local gateway address used for the tunnel and the address of the remote security gateway at the other end of the tunnel remote peer IP address to use.

Default no local-gateway-address

Parameters *ip-address* — IP address of the local end of the tunnel.

delivery-service *service-id* — The ID of the IES or VPRN (front-door) delivery service of this tunnel. Use this service-id to find the VPRN used for delivery.

Values *service-id*: 1 to 2147483648

svc-name: Specifies an existing service name up to 64 characters in length.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.184 local-id

local-id

Syntax **local-id** *type* [**value** *value*]
no local-id

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>dyn local-id)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn local-id)
[Tree] (config>service>ies>if>sap>ipsec-gw local-id)
[Tree] (config>service>vprn>if>sap>ipsec-gw local-id)
[Tree] (config>service>vprn>if>sap>ipsec-tun>dyn local-id)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn local-id)
[Tree] (config>ipsec>trans-mode-prof>dyn local-id)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying local-id
configure router interface ipsec ipsec-tunnel dynamic-keying local-id
configure service ies interface ipsec ipsec-tunnel dynamic-keying local-id
configure service ies interface sap ipsec-gw local-id
configure service vprn interface ipsec ipsec-tunnel dynamic-keying local-id
configure service vprn interface sap ipsec-gw local-id
configure service vprn interface sap ipsec-tunnel dynamic-keying local-id

Description This command specifies the local ID used for IDi or IDr for IKEv2 negotiation.

The default behavior depends on the local-auth-method as follows:

- Psk: local tunnel IP address
- Cert-auth: subject of the local certificate

The **no** form of this command removes the parameters from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no local-id

Parameters *type* — Specifies the type of local ID payload, which could be IPv4 or IPv6 address or FQDN domain name or distinguish the name of the subject in the X.509 certificate.

Values ipv4 — Specifies to use IPv4 as the local ID type; the default value is the local tunnel end-point address.

ipv6 — Specifies to use IPv6 as the local ID type; the default value is the local tunnel end-point address.

fq1dn — Specifies to use FQDN as the local ID type. The value must be configured.

value — Specifies the data type as an enumerated integer that describes the local identifier type used for IDi or IDr for IKEv2, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel dynamic-keying local-id
- configure service vprn interface sap ipsec-gw local-id
- configure ipsec ipsec-transport-mode-profile dynamic-keying local-id
- configure service ies interface sap ipsec-gw local-id

VSR

- configure service vprn interface ipsec ipsec-tunnel dynamic-keying local-id
- configure router interface ipsec ipsec-tunnel dynamic-keying local-id
- configure service ies interface ipsec ipsec-tunnel dynamic-keying local-id

16.185 local-ip

local-ip

Syntax **local-ip** {*ip-prefix/prefix-length* | *ip-prefix netmask* | **any**}

Context **[Tree]** (config>router>ipsec>sec-plcy>entry local-ip)
[Tree] (config>service>vprn>ipsec>sec-plcy>entry local-ip)

Full Context configure router ipsec security-policy entry local-ip
configure service vprn ipsec security-policy entry local-ip

Description This command configures the local (from the VPN) IP prefix/mask for the policy parameter entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Only one entry is necessary to describe a potential flow. The **local-ip** and **remote-ip** commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

Parameters *ip-prefix* — The destination address of the aggregate route in dotted decimal notation

Values a.b.c.d (host bits must be 0)
prefix-length 1 to 32

netmask — The subnet mask in dotted decimal notation

any — keyword to specify that it can be any address

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec security-policy entry local-ip

VSR

- configure router ipsec security-policy entry local-ip

16.186 local-ip-address

local-ip-address

Syntax **local-ip-address** *ip-address*
no local-ip-address

Context **[Tree]** (config>lag>bfd>family local-ip-address)

Full Context configure lag bfd family local-ip-address

Description This command is used to specify the IPv4 or IPv6 address of the BFD source.

The **no** form of this command removes this address from the configuration.

Default no local-ip-address

Parameters *ip-address* — Specifies the IP address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x:-[0 to FFFF]H
	d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

16.187 local-ip-range-start

local-ip-range-start

Syntax **local-ip-range-start** *ip-address*
no local-ip-range-start

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy local-ip-range-start)

Full Context configure isa nat-group inter-chassis-redundancy local-ip-range-start

Description This command configures the first IP address that is assigned to a first member ISA in the nat-group. The remaining member ISAs in the **nat-group** are automatically assigned the consecutive IP addresses, starting from the first IP address. These IP addresses are used to communicate between the ISAs on redundant nodes for the purpose of flow synchronization. Traffic from the first local IP address (member ISA), is sent to the first IP address from the remote IP range.

The **no** form of this command reverts to the default.

Default no local-ip-range-start

Parameters *ip-address* — Specifies the first IP address from the range assigned to the first member ISA in the form of a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.188 local-lsr-id

local-lsr-id

Syntax **local-lsr-id** {**system** | **interface**} [**32bit-format**]
local-lsr-id *interface-name* [**32bit-format**]
no local-lsr-id

Context **[Tree]** (config>router>ldp>if-params>if>ipv4 local-lsr-id)
[Tree] (config>router>ldp>if-params>if>ipv6 local-lsr-id)

Full Context configure router ldp interface-parameters interface ipv4 local-lsr-id
configure router ldp interface-parameters interface ipv6 local-lsr-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the use of the address of the local LDP interface, or any other network interface configured on the system, as the LSR-ID to establish link LDP Hello adjacency and LDP session with directly connected LDP peers. The network interface can be a loopback or not.

Link LDP sessions to all peers discovered over a given LDP interface share the same local LSR-ID. However, LDP sessions on different LDP interfaces can use different network interface addresses as their local LSR-ID.

By default, the LDP session to a peer uses the system interface address as the LSR-ID unless explicitly configured using this command. The system interface must always be configured on the router, or the LDP protocol will not come up on the node. There is no requirement to include the system interface in any routing protocol.

At initial configuration, the LDP session to a peer will remain down while the network interface used as LSR-ID is down. LDP will not try to bring it up using the system interface.

If the network IP interface used as LSR-ID goes down, the LDP sessions to all discovered peers using this LSR-ID go down.

When an interface other than the system is used as the LSR-ID, the transport connection (TCP) for the link LDP session will also use the address of that interface as the transport address. If the system or interface value is configured in the **config**>**router**>**ldp**>**if-params**>**if**>**ipv4** or **config**>**router**>**ldp**>**if-params**>**if**>**ipv6**>**transport-address** context, it will be overridden with the address of the LSR-ID interface.

When the **local-lsr-id** command is enabled with the **32bit-format** option, an SR OS LSR will be able to establish an LDP IPv6 Hello adjacency and an LDP IPv6 session with an RFC 7552 compliant peer LSR. The LSR uses a 32-bit LSR-ID set to the value of the IPv4 address of the specified local LSR-ID interface and a 128-bit transport address set to the value of the IPv6 address of the specified local LSR-ID interface.

Note: The system interface cannot be used as a local LSR-ID with the **32bit-format** option enabled because the system interface is the default LSR-ID and transport address for all LDP sessions to peers on this LSR. This configuration is blocked in the CLI.

If the user enables the **32bit-format** option in the IPv6 context of a running LDP interface, the already established LDP IPv6 Hello adjacency and LDP IPv6 session will be brought down and re-established with the new 32-bit LSR-ID value.

If the user changes the LSR-ID value between **system**, **interface**, and *interface-name*, or enables the **32bit-format** option while the LDP session is up, LDP will immediately tear down all sessions using this LSR-ID and will attempt to re-establish them using the new LSR-ID.

The **no** form of this command returns to the default behavior, in which case the system interface address is used as the LSR-ID.

Default no local-lsr-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **system** — Specifies the use of the address of the system interface as the value of the LSR-ID of this LDP LSR.

interface — Specifies the use of the address of the local LDP interface as the value of the LSR-ID of this LDP LSR.

interface-name *interface-name* — Specifies the name, up to 32 character, of the network IP interface (which address is used as the LSR-ID of this LDP LSP). An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

32bit-format — Specifies the use of the IPv4 address of the local LSR-ID interface as the LSR-ID of this LDP LSR.

Platforms All

local-lsr-id

Syntax **local-lsr-id** *interface-name* [**32bit-format**]
no local-lsr-id

Context **[Tree]** (config>router>ldp>targ-session>peer local-lsr-id)
[Tree] (config>router>ldp>targ-session>peer-template local-lsr-id)

Full Context configure router ldp targeted-session peer local-lsr-id
configure router ldp targeted-session peer-template local-lsr-id

Description This command enables the use of the address of any network interface configured on the system, as the LSR-ID to establish a targeted LDP Hello adjacency and a targeted LDP session with an LDP peer. The network interface can be a loopback or not.

By default, the targeted LDP session to a peer uses the system interface address as the LSR-ID and as the transport address, unless explicitly configured using this command. The system interface must always be configured on the router, or the LDP protocol will not come up on the node. There is no requirement to include the system interface in any routing protocol.

When the **local-lsr-id** command is enabled with the **32bit-format** option, an SR OS LSR will be able to establish a targeted LDP IPv6 Hello adjacency and a targeted LDP IPv6 session with an RFC 7552 compliant peer LSR. The LSR uses a 32-bit LSR-ID set to the value of the IPv4 address of the specified local LSR-ID interface and a 128-bit transport address set to the value of the IPv6 address of the specified local LSR-ID interface.

Note: The system interface cannot be used as a local LSR-ID with the 3**2bit-format** option enabled because the system interface is the default LSR-ID and transport address for all targeted LDP sessions to peers on this LSR. This configuration is blocked in the CLI.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the user enables the **32bit-format** option in the IPv6 context of a running targeted LDP peer, the already established targeted LDP IPv6 Hello adjacency and targeted LDP IPv6 session will be brought down and re-established with the new 32-bit LSR-ID value.

If the user changes the local LSR-ID value or enables/disables the **32bit-format** option, while the targeted LDP session is up, LDP will immediately tear down the targeted session using this LSR-ID and will attempt to re-establish it using the new LSR-ID.

The **no** form of this command returns to the default behavior, in which case the system interface address is used as the LSR-ID.

Default no local-lsr-id

Parameters *interface-name* — Specifies the name, up to 32 characters, of the network IP interface (which address is used as the LSR-ID of this LDP LSP). An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

32bit-format — Specifies the use of the IPv4 address of the local LSR-ID interface as the LSR-ID of this LDP LSR.

Platforms All

16.189 local-max-checkpoints

local-max-checkpoints

Syntax **local-max-checkpoints** [*number-of-files*]
no local-max-checkpoints

Context **[Tree]** (config>system>rollback local-max-checkpoints)

Full Context configure system rollback local-max-checkpoints

Description This command configures the maximum number of rollback checkpoint files when the rollback-location is on local compact flash.

Default no local-max-checkpoints

Parameters *number of files* — Specifies the maximum rollback files on a compact flash.

Values 1 to 50

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.190 local-monitoring-policer

local-monitoring-policer

Syntax [**no**] **local-monitoring-policer** *policer-name* [**create**]

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy local-monitoring-policer)

Full Context configure system security dist-cpu-protection policy local-monitoring-policer

Description This command configures a monitoring policer that is used to monitor the aggregate rate of several protocols arriving on an object (for example, SAP). When the **local-monitoring-policer** is determined to be in a nonconforming state (at the end of a minimum monitoring time of 60 seconds) then the system will attempt to allocate dynamic policers for the particular object for any protocols associated with the local monitor (for example, using the **protocol** *name* **enforcement dynamic** *policer-name* CLI command).

If the system cannot allocate all the dynamic policers within 150 seconds, it will stop attempting to allocate dynamic policers, raise a LocMonExcdAllDynAlloc log event, and go back to using the local monitor. The local monitor may then detect exceeded packets again and make another attempt at allocating dynamic policers.

Once this *policer-name* is referenced by a protocol then this policer will be instantiated for each “object” that is created and references this DDoS policy. If there is no policer free then the object will be blocked from being created.

Parameters *policy-name* — Specifies name of the policy, up to 32 characters.

Platforms All

16.191 local-name

local-name

Syntax **local-name** *host-name*
no local-name

Context **[Tree]** (config>router>l2tp local-name)
[Tree] (config>router>l2tp>group local-name)
[Tree] (config>router>l2tp>group>tunnel local-name)
[Tree] (config>service>vprn>l2tp local-name)
[Tree] (config>service>vprn>l2tp>group local-name)
[Tree] (config>service>vprn>l2tp>group>tunnel local-name)

Full Context configure router l2tp group local-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router l2tp group tunnel local-name
configure router l2tp local-name
configure service vprn l2tp group local-name
configure service vprn l2tp group tunnel local-name
configure service vprn l2tp local-name

Description This command creates the local host name used by this system for the tunnels in this L2TP group during the authentication phase of tunnel establishment. It can be used to distinguish tunnels.

The **no** form of this command removes the host name from the configuration.

Default no local-name

Parameters *host-name* — Specifies the host name, up to 64 characters in length, that the router will use to identify itself during L2TP authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.192 local-port-action

local-port-action

Syntax **local-port-action** {**log-only** | **out-of-service**}

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>local-sf-action local-port-action)

Full Context configure port ethernet efm-oam link-monitoring local-sf-action local-port-action

Description This command configures the parameters that define if and how the local port will be affected when the local signal failure threshold (**sf-threshold**) has been reached within the configured window.

Interactions: The signal failure threshold will trigger these actions.

Default local-port-action out-of-service

Parameters **log-only** — Keyword that prevents the port from being affected when the configured signal failure threshold is reach within the window. The event will be logged but the port will remain operational.

out-of-service — Keyword that causes the port to enter a non-operation down state with a port state of link up. The error will be logged when the configured signal failure threshold (**sf-threshold**) is reached within the window. The port will not be available to service data but will continue to carry Link OAM traffic to ensure the link is monitored.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.193 local-preference

local-preference

Syntax **local-preference** *local-preference*
no local-preference

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy local-preference)

Full Context configure subscriber-mgmt bgp-peering-policy local-preference

Description This command enables setting the BGP local-preference attribute in incoming routes if not specified and configures the default value for the attribute. This value is used if the BGP route arrives from a BGP peer without the **local-preference** integer set.

The specified value can be overridden by any value set via a route policy.

The **no** form of this command at the global level specifies that incoming routes with local-preference set are not overridden and routes arriving without local-preference set are interpreted as if the route had local-preference value of 100.

Parameters *local-preference* — The local preference value to be used as the override value, expressed as a decimal integer.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

local-preference

Syntax **local-preference** *local-preference*
no local-preference

Context **[Tree]** (config>service>vprn>bgp local-preference)
[Tree] (config>service>vprn>bgp>group local-preference)
[Tree] (config>service>vprn>bgp>group>neighbor local-preference)

Full Context configure service vprn bgp group local-preference
configure service vprn bgp group neighbor local-preference
configure service vprn bgp local-preference

Description This command enables setting the BGP local-preference attribute in incoming routes if not specified and configures the default value for the attribute. This value is used if the BGP route arrives from a BGP peer without the **local-preference** integer set.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The specified value can be overridden by any value set via a route policy. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command at the global level specifies that incoming routes with local-preference set are not overridden and routes arriving without local-preference set are interpreted as if the route had local-preference value of 100.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no local-preference - Does not override the local-preference value set in arriving routes and analyze routes without local preference with value of 100.

Parameters *local-preference* — The local preference value to be used as the override value, expressed as a decimal integer.

Values 0 to 4294967295

Platforms All

local-preference

Syntax **local-preference** *local-preference*
no local-preference

Context **[Tree]** (config>router>bgp local-preference)
[Tree] (config>router>bgp>group local-preference)
[Tree] (config>router>bgp>group>neighbor local-preference)

Full Context configure router bgp group local-preference
configure router bgp group neighbor local-preference
configure router bgp local-preference

Description This command enables setting the BGP local-preference attribute in incoming routes if not specified and configures the default value for the attribute.

This value is used if the BGP route arrives from a BGP peer without the **local-preference** integer set.

The specified value can be overridden by any value set via a route policy. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to the specified peer). The most specific value is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command at the global level specifies that incoming routes with local-preference set are not overridden and routes arriving without local-preference set are interpreted as if the route had local-preference value of 100.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no local-preference

Parameters *local-preference* — Specifies the local preference value to be used as the override value expressed as a decimal integer.

Values 0 to 4294967295

Platforms All

local-preference

Syntax **local-preference** *preference* [**equal** | **or-higher** | **or-lower**]
no local-preference

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from local-preference)

Full Context configure router policy-options policy-statement entry from local-preference

Description This command matches BGP routes based on local preference (the value in the LOCAL_PREF attribute).

If no comparison qualifiers are present (**equal**, **or-higher**, **or-lower**), then **equal** is the implied default.

A non-BGP route does not match a policy entry if it contains the **local-preference** command.

Default no local-preference

Parameters *preference* — Specifies the local preference value.

Values 0 to 4294967295, or a parameter name delimited by starting and ending at-sign (@) characters

equal — Specifies that matched routes should have the same local preference as the value specified.

or-higher — Specifies that matched routes should have the same or a greater local preference as the value specified.

or-lower — Specifies that matched routes should have the same or a lower local preference as the value specified.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-preference

Syntax **local-preference** *preference*
no local-preference

Context **[Tree]** (config>router>policy-options>policy-statement>default-action local-preference)
[Tree] (config>router>policy-options>policy-statement>entry local-preference)

Full Context configure router policy-options policy-statement default-action local-preference
configure router policy-options policy-statement entry local-preference

Description This command assigns a BGP local preference to routes matching a route policy statement entry.

If no local preference is specified, the BGP configured local preference is used.

The **no** form of this command disables assigning a local preference in the route policy entry.

Default no local-preference

Parameters *preference* — Specifies the local preference expressed as a decimal integer.

Values 0 to 4294967295 name — Specifies the local preference parameter variable name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

16.194 local-prefix

local-prefix

Syntax **local-prefix** *local-prefix* [**create**]
no local-prefix *local-prefix*

Context **[Tree]** (config>service>pw-routing local-prefix)

Full Context configure service pw-routing local-prefix

Description This command configures one or more node prefix values to be used for MS-PW routing. At least one prefix must be configured on each node that is an S-PE or a T-PE.

The **no** form of this command removes a previously configured prefix, and will cause the corresponding route to be withdrawn if it has been advertised in BGP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no local-prefix

Parameters *local-prefix* — Specifies a 32 bit prefix for the AII. One or more prefix values, up to a maximum of 16, may be assigned to the 7450 ESS, 7750 SR, or 7950 XRS node. The global ID can contain the 2-octet or 4-octet value of the provider's Autonomous System Number (ASN). The presence of a global ID based on the provider's ASN ensures that the AII for spoke-SDPs configured on the node will be globally unique.

Values <global-id>:<ip-addr>| <raw-prefix>

ip-addr	a.b.c.d
raw-prefix	1 to 4294967295
global-id	1 to 4294967295

Platforms All

16.195 local-priority

local-priority

Syntax **local-priority** *local-priority*

Context **[Tree]** (config>service>vprn>ptp>peer local-priority)

Full Context configure service vprn ptp peer local-priority

Description This command configures the local priority used to choose between PTP masters in the best master clock algorithm (BMCA). This setting is relevant when the profile is set to either g8265dot1-2010 or g8275dot1-2014. The parameter is ignored when any other profile is selected.

The value 1 is the highest priority and 255 is the lowest priority. The priority of a peer cannot be configured if the PTP profile is ieee1588-2008.

For g8265dot1-2010, this parameter configures the priority used to choose between master clocks with the same quality (see G.8265.1 for more information).

For g8275dot1-2014, this parameter sets the value of the **localPriority** associated with the Announce messages received from external clocks (**ptp>peer** or **ptp>port**), or the local clock (**ptp**). See G.8275.1 for more information.

Default local-priority 128

Parameters *local-priority* — Specifies the value of the local priority.

Values 1 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

local-priority

Syntax **local-priority** *priority*

Context **[Tree]** (config>system>ptp local-priority)
[Tree] (config>system>ptp>peer local-priority)
[Tree] (config>system>ptp>port local-priority)

Full Context configure system ptp local-priority
configure system ptp peer local-priority
configure system ptp port local-priority

Description This command configures the local priority used to choose between PTP masters in the best master clock algorithm (BMCA). This setting is relevant when the profile is set to either g8265dot1-2010 or g8275dot1-2014. The parameter is ignored when any other profile is selected.

The value 1 is the highest priority and 255 is the lowest priority. The priority of a peer cannot be configured if the PTP profile is ieee1588-2008.

For g8265dot1-2010, this parameter configures the priority used to choose between master clocks with the same quality (refer to G.8265.1 for more details).

For g8275dot1-2014, this parameter sets the value of the **localPriority** associated with the Announce messages received from the external clocks (**ptp>peer** or **ptp>port**), or the local clock (**PTP**). Refer to G.8275.1 for detailed information.

Default local-priority 128

Parameters *priority* — Specifies the value of the local priority.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.196 local-proxy-arp

local-proxy-arp

Syntax [**no**] **local-proxy-arp**

Context **[Tree]** (config>service>ies>if local-proxy-arp)
[Tree] (config>service>ies>sub-if>grp-if local-proxy-arp)
[Tree] (config>service>vprn>if local-proxy-arp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if local-proxy-arp)

Full Context configure service ies interface local-proxy-arp
configure service ies subscriber-interface group-interface local-proxy-arp
configure service vprn interface local-proxy-arp
configure service vprn subscriber-interface group-interface local-proxy-arp

Description This command enables local proxy ARP. When local proxy ARP is enabled on an IP interface, the system responds to all ARP requests for IP addresses belonging to the subnet with its own MAC address, and thus becomes the forwarding point for all traffic between hosts in that subnet.

When **local-proxy-arp** is enabled, ICMP redirects on the ports associated with the service are automatically blocked.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface local-proxy-arp
- configure service ies subscriber-interface group-interface local-proxy-arp

All

- configure service vprn interface local-proxy-arp
- configure service ies interface local-proxy-arp

local-proxy-arp

Syntax [**no**] **local-proxy-arp**

Context **[Tree]** (config>router>if local-proxy-arp)

Full Context configure router interface local-proxy-arp

Description This command enables local proxy ARP on the interface.

Default no local-proxy-arp

Platforms All

16.197 local-proxy-nd

local-proxy-nd

Syntax [**no**] **local-proxy-nd**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>ipv6 local-proxy-nd)
[Tree] (config>service>vprn>if>ipv6 local-proxy-nd)

Full Context configure service ies interface ipv6 local-proxy-nd
configure service vprn interface ipv6 local-proxy-nd

Description This command enables local proxy neighbor discovery on the interface.

When this command is enabled, the interface replies to neighbor solicitation requests when both the hosts are on the same subnet. In this case, ICMP redirects are disabled. When this command is disabled, the interface does not reply to neighbor solicitation requests if both the hosts are on the same subnet.

The **no** form of this command reverts to the default.

Platforms All

local-proxy-nd

Syntax [**no**] **local-proxy-nd**

Context [Tree] (config>router>if>ipv6 local-proxy-nd)

Full Context configure router interface ipv6 local-proxy-nd

Description This command enables local proxy neighbor discovery on the interface.

The **no** form of this command disables local proxy neighbor discovery.

Platforms All

16.198 local-routes-domain-id

local-routes-domain-id

Syntax **local-routes-domain-id** [*global-field*:*local-field*]
no local-routes-domain-id

Context [Tree] (config>service>vprn local-routes-domain-id)

Full Context configure service vprn local-routes-domain-id

Description This command specifies the domain ID that is used in the D-PATH attribute for local routes before those routes are exported to a BGP neighbor using BGP-IPVPN, EVPN-IFF, EVPN-IFL or PE-CE BGP. A local route is a non-BGP route installed in the VPRN route table and learned using static route or an IGP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The domain IDs are used in the D-PATH attribute, in accordance with *draft-ietf-bess-evpn-ipvpn-interworking*. The D-PATH attribute is modified by gateway routers, where a gateway is defined as a PE where a VPRN is instantiated, and that VPRN advertises or receives routes from multiple BGP owners (for example, EVPN-IFL and BGP-IPVPN).

The D-PATH attribute is used on gateways to detect loops (for received routes where the D-PATH contains a local domain ID) and to make BGP best path selection decisions based on the D-PATH length (shorter D-PATH is preferred).

The **no** form of this command removes the domain ID for local routes.

Default no local-routes-domain-id

Parameters *global-field:local-field* — Specifies the domain ID for local routes.

Values
4byte-GlobalAdminValue:2byte-LocalAdminValue

4byte-GlobalAdminValue:	0 to 4294967295
2byte-LocalAdminValue	0 to 65535

Platforms All

16.199 local-rt-port

local-rt-port

Syntax **local-rt-port** *port*
no local-rt-port

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video local-rt-port)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video local-rt-port)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video local-rt-port)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video local-rt-port
configure mcast-management multicast-info-policy bundle channel video local-rt-port
configure mcast-management multicast-info-policy bundle video local-rt-port

Description This command configures the local port on which retransmission (RET) requests are received. The value of this object can only be set for the default bundle and will be used by all channels.

The **local-rt-port** *port* value is the only configuration parameter in the bundle “default” context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the port from the video configuration.

Parameters *port* — Specifies a local port for RT requests.

Values 1024 to 5999, 6251 to 65535

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

16.200 local-rt-server

local-rt-server

Syntax [**no**] **local-rt-server**

Context **[Tree]** (config>isa>video-group local-rt-server)

Full Context configure isa video-group local-rt-server

Description This command enables the local RET server for the group. A local RET server cannot be enabled if an FCC server or ad insertion is enabled.

The **no** form of the command disables the server.

Default no local-rt-server

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

local-rt-server

Syntax [**no**] **local-rt-server**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd local-rt-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip local-rt-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd local-rt-server)

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd local-rt-server
configure mcast-management multicast-info-policy video-policy video-interface pip local-rt-server
configure mcast-management multicast-info-policy video-policy video-interface sd local-rt-server

Description This command enables the local retransmission server function for requests directed to the IP address.

The **no** form of the command disables the retransmission server.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no local-rt-server

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

local-rt-server

Syntax **local-rt-server** [**disable**]
no local-rt-server

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video local-rt-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video local-rt-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video local-rt-server)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video local-rt-server
configure mcast-management multicast-info-policy bundle channel video local-rt-server
configure mcast-management multicast-info-policy bundle video local-rt-server

Description This command enables the local retransmission server capability on the ISA video group.

RET server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the RET server is disabled or if the video group is administratively disabled (shutdown).

The **no** form of the command returns the parameter to the default value where the RET server is disabled on the video group.

Default no local-rt-server

Parameters **disable** — Specifies to disable the RET server.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

16.201 local-sf-action

local-sf-action

Syntax **local-sf-action**

Context **[Tree]** (config>port>ethernet>efm-oam>link-monitoring local-sf-action)

Full Context configure port ethernet efm-oam link-monitoring local-sf-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines how crossing the local signal failure threshold (sf-threshold) will be handled. This includes local actions and if and how to notify the peer that the threshold has been crossed.

Platforms All

16.202 local-source-address

local-source-address

Syntax **local-source-address** {*ip-int-name* | *ip-address*}
no local-source-address

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription>local-ip-address local-source-address)

Full Context configure system telemetry persistent-subscriptions subscription local-ip-address local-source-address

Description This command is used to assign a source IP address in the respective persistent subscription context for use when packets are sent out.

The **no** form of this command removes this address from the configuration.

Parameters *ip-int-name* — Specifies the source IP address name, up to 64 characters.

ip-address — Specifies the source IP address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x:-[0 to FFFF]H
	d: [0 to 255]D

local-source-address

Syntax **local-source-address** {*ip-int-name* | *ip-address*}
no local-source-address

Context **[Tree]** (config>system>grpc-tunnel>destination-group>destination local-source-address)

Full Context configure system grpc-tunnel destination-group destination local-source-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a local source IP address in the destination group context for use when packets are sent out.

The **no** form of this command removes this address from the configuration.

Default no local-source-address

Parameters *ip-int-name* — Specifies the source IP address name, up to 64 characters.

ip-address — Specifies the source IPv4 address (in dotted decimal notation) or IPv6 address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x:-[0 to FFFF]H
	d: [0 to 255]D

Platforms All

16.203 local-sr-protection

local-sr-protection

Syntax **local-sr-protection** *local-sr-protection*
no local-sr-protection

Context **[Tree]** (config>router>mpls>lsp local-sr-protection)
[Tree] (config>router>mpls>lsp-template local-sr-protection)

Full Context configure router mpls lsp local-sr-protection
configure router mpls lsp-template local-sr-protection

Description This command configures the SR LFA protection needed for the adjacencies used in the path computation of an SR-TE LSP by the local CSPF.

The default value of the command is **preferred**. The local CSPF will prefer a protected adjacency over an unprotected adjacency whenever both exist for a TE link. However, the entire computed path can combine both types of adjacencies.

When the user enables the **mandatory** value, CSPF uses it as an additional path constraint and selects protected adjacencies exclusively in computing the path of the SR-TE LSP. CSPF will return no path if all candidate paths that otherwise satisfy all other LSP path constraints do not have an unprotected SID for each of their TE links.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Similarly, if the user enables the value **none**, CSPF uses it as an additional path constraint and selects unprotected adjacencies exclusively in computing the path of the SR-TE LSP. CSPF will return no path if all candidate paths that otherwise satisfy all other LSP path constraints do not have a protected SID for each of their TE links.

The **no** form of this command returns the command to its default value.

Default no local-sr-protection

Parameters *local-sr-protection* — Specifies the local-sr-protection for LSPs.

Values none — Selects unprotected adjacencies only in the SR-TE LSP path computation.

preferred — Prefers protected adjacencies in the SR-TE LSP path computation.

mandatory — Selects protected adjacencies only in the SR-TE LSP path computation.

Platforms All

16.204 local-state

local-state

Syntax **local-state** {**admin-down** | **up**}
no local-state

Context **[Tree]** (config>bfd>seamless-bfd>reflector local-state)

Full Context configure bfd seamless-bfd reflector local-state

Description This command specifies the setting of the local state field in reflected seamless BFD control packets.

The **no** form of this command means that the field is not explicitly set by the reflector.

Default local-state up

Parameters **admin-down** — Specifies that the local state of the reflected seamless BFD control packets is administratively down.

up — Specifies that the local state of the reflected seamless BFD control packets is up.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.205 local-switching-service-state

local-switching-service-state

Syntax **local-switching-service-state** {**pbb-tunnel** | **sap**}

Context **[Tree]** (config>service>epipe>pbb local-switching-service-state)

Full Context configure service epipe pbb local-switching-service-state

Description In a PBB Epipe with two SAPs and a PBB tunnel, this command controls whether the operational status of the PBB-Epipe service depends on the status of the PBB tunnel only.

Default local-switching-service-state sap

Parameters **pbb-tunnel** — Specifies that the operational state of the PBB-Epipe service is up if the PBB tunnel is operationally up, irrespective of the operational state of the two SAPs.

sap — Specifies that the operational state of the PBB-Epipe service is up, if two of the three endpoints (PBB tunnel and two SAPs) are up. This option implies that at least one of the SAPs must be up for the PBB-Epipe service to be operationally up.

Platforms All

16.206 local-user-db

local-user-db

Syntax **local-user-db** *local-user-db-name* [**create**]
no local-user-db *local-user-db-name*

Context **[Tree]** (config>subscr-mgmt local-user-db)

Full Context configure subscriber-mgmt local-user-db

Description Commands in this context configure a local user database.

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the name of a local user database, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.207 local-v6-ip

local-v6-ip

Syntax **local-v6-ip** *ipv6-prefix/prefix-length*
local-v6-ip any
no local-v6-ip

Context **[Tree]** (config>router>ipsec>sec-plcy>entry local-v6-ip)
[Tree] (config>service>vprn>ipsec>sec-plcy>entry local-v6-ip)

Full Context configure router ipsec security-policy entry local-v6-ip
configure service vprn ipsec security-policy entry local-v6-ip

Description This command specifies the local v6 prefix for the security-policy entry.

Parameters *ipv6-prefix/prefix-length* — Specifies the local v6 prefix and length

Values

ipv6-address/prefix: ipv6-address	x:x:x:x:x:x:x:x	(eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d	
	x [0 to FFFF]H	
	d [0 to 255]D	
	host bits must be 0	
	:: not allowed	
	prefix-length [1 to 128]	

any — keyword to specify that it can be any address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec security-policy entry local-v6-ip

VSR

- configure router ipsec security-policy entry local-v6-ip

16.208 location

location

Syntax **location** *cflash-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no location

Context [Tree] (config>system>persistence>ancp location)
[Tree] (config>system>persistence>dhcp-server location)
[Tree] (config>system>persistence>nat-fwd location)
[Tree] (config>system>persistence>python location)
[Tree] (config>system>persistence>subscriber-mgmt location)

Full Context configure system persistence ancp location
configure system persistence dhcp-server location
configure system persistence nat-port-forwarding location
configure system persistence python-policy-cache location
configure system persistence subscriber-mgmt location

Description This command instructs the system where to write the persistency files for the corresponding application. Each application creates two files on the flash card, one with suffix .i<version>, referencing an index file, and the other with suffix .0<version>, where <version> is a 2-digit number reflecting the file version. These versions are not related to the SR OS release running on the node. The <version> can remain the same over two major releases, for example, when no format change is made to the persistency file. On boot, the system scans the file systems looking for the corresponding persistency files, and the load begins.

For example, in the subscriber management context, the location specifies the flash device on a CPM card where the data for handling subscriber management persistency is stored.

The **no** form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.

Default no location

Parameters *cflash-id* — Specifies the compact flash device name.

Values cf1:, cf2:, cf3:

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure system persistence dhcp-server location
- configure system persistence subscriber-mgmt location

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure system persistence nat-port-forwarding location

All

- configure system persistence ancp location
- configure system persistence python-policy-cache location

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

location

Syntax **location** {**cf1** | **cf2**}

Context **[Tree]** (config>call-trace location)

Full Context configure call-trace location

Description This command specifies the compact flash (CF) configuration to store call trace files.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

location

Syntax **location** *cflash-id*
no location

Context **[Tree]** (config>system>persistence>application-assurance location)

Full Context configure system persistence application-assurance location

Description This command instructs the system where to write the file. The name of the file is: appassure.db. On boot the system scans the file systems looking for appassure.db, if it finds it, it starts to load it.

The **no** form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.

Default no location

Parameters *cflash-id* — Specifies the compact flash type.

Values cf1:, cf2:, cf3:

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

location

Syntax **location** *remote-url*
no location

Context **[Tree]** (config>service>nat>deterministic-script location)

Full Context configure service nat deterministic-script location

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the remote location where the Python script will be exported. The Python script is then used off-line to perform reverse query. If this command is configured, the Python script generation is triggered by any modification of the deterministic NAT configuration. The new script reflects the change in mappings caused by configuration change. However, the script must be manually exported to the outside location with the **admin nat save-deterministic-nat** command. The script cannot be stored locally on the system.

The script allows two forms of queries:

- Forward – input is NAT inside parameters, output is NAT outside parameters.
- Backward – input is NAT outside parameters, output is NAT inside parameters.

Forward Query:

```
user@external-server:/home/ftp/pub/det-nat-script$ ./
det-nat.py -f -s 10 -a 10.0.5.10
```

output:

```
subscriber has public ip address 198.51.100.1 from service 0 and is using ports [132
4 - 1353]
```

Reverse Query:

```
user@external-server:/home/ftp/pub/det-nat-script$./
det-nat.py -b -s 0 -a 198.51.100.1 -p 3020
```

output:

```
subscriber has private ip address 10.0.5.66 from service 10
```

Default no location

Parameters *remote-url* — A remote location where the script is stored: [{ftp:// | tftp:// }<login>:<pswd>@ <remote-locn>/][<file-path>] Maximum length is 180 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

location

Syntax **location** *location*
no location

Context **[Tree]** (config>system location)

Full Context configure system location

Description This command creates a text string that identifies the system location for the device.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Only one location can be configured. If multiple locations are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Parameters *location* — Specifies the location as a character string. The string may be up to 80 characters. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

location

Syntax **location** *file-url*
no location

Context **[Tree]** (config>system>script-control>script location)

Full Context configure system script-control script location

Description This command is used to identify the location of a script to be scheduled.

The **no** form of the command removes the location.

Default no location

Parameters *file-url* — Specifies the location to search for scripts.

Values *local-url* | *remote-url*

local-url — [*cflash-id/*] [*file-path*] 200 chars max, including *cflash-id*directory length 99 characters max each

remote url — [{ftp:// | tftp://}*login*:*password*@*remote-location*/][*file-path*] 255 characters max directory length 99 characters max each

remote-location — [*hostname* | *ipv4-address* | *ipv6-address*]

ipv4-address — *a.b.c.d*

ipv6-address — x:x:x:x:x:x:x:x[-*interface*]
x:x:x:x:x:x:d.d.d.d[-*interface*] x — [0 to FFFF]H d — [0 to 255]D
interface — 32 characters max, for link local addresses

cflash-id — cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

location

Syntax **location** *cflash-id* [*backup-cflash-id*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no location

Context [Tree] (config>log>file>file-id location)

Full Context configure log file file-id location

Description This command specifies the primary and optional backup location where the log or billing file will be created.

The **location** command is optional. If the location command not explicitly configured, log files will be created on cf1: and accounting files will be created on cf2: without overflow onto other devices. Generally, cf3: is reserved for system files (configurations, images, and so on).

When multiple location commands are entered in a single file ID context, the last command overwrites the previous command.

When the location of a file ID that is associated with an active log ID is changed, the log events are not immediately written to the new location. The new location does not take effect until the log is rolled over either because the rollover period has expired or a **clear log log-id** command is entered to manually rollover the log file.

When creating files, the primary location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

A medium severity trap is issued to indicate that a compact flash is either not available or that no space is available on the specified flash and that the backup location is being used.

A high priority alarm condition is raised if none of the configured compact flash devices for this file ID are present or if there is insufficient space available. If space does becomes available, then the alarm condition will be cleared.

Log files are created on cf1: and accounting files are created on cf2.

Use the **no** form of this command to revert to default settings.

Default no location

Parameters *cflash-id* — Specify the primary location.

Values cflash-id:cf1:, cf2:, cf3:

backup-cflash-id — Specify the secondary location.

Values cflash-id: cf1:, cf2:, cf3:

location

Syntax **location** *location-id* [**primary-ip-address** *ipv4-address*] [**secondary-ip-address**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-address] [**tertiary-ip-address** *ipv4-address*]

Context **[Tree]** (config>router>bgp>optimal-route-reflection location)

Full Context configure router bgp optimal-route-reflection location

Description This command configures the location ID for the for the route reflector. A BGP neighbor can be associated with a location if it is a route-reflector client.

Parameters *location-id* — Specifies an optimal-route-reflection location.

Values 1 to 255

ipv4-address — Specifies the primary, secondary, or tertiary IP address.

Values primary ipv4-address, secondary ipv4-address, tertiary ipv4-address

Platforms All

16.209 locator

locator

Syntax [**no**] **locator** *locator-name*

Context **[Tree]** (config>router>segment-routing>srv6 locator)

Full Context configure router segment-routing segment-routing-v6 locator

Description This command configures the name of an SRv6 locator to be used by the routing protocols and services. This also creates the context to configure the locator block, locator node, function and argument lengths.

A limit of 16 locators per system is enforced.

The **no** form of this command removes the specified locator name.

Parameters *locator-name* — Specifies a locator name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

locator

Syntax [**no**] **locator** *locator-name*

Context **[Tree]** (config>router>segment-routing>srv6>inst locator)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command refers to a locator name defined under the **config**>**router**>**segment-routing**>**srv6** context. This command assigns a locator to BGP for use with base router routes.

The **no** form of this command removes the reference to a locator name locator.

Parameters *locator-name* — Specifies a locator name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

locator

Syntax [**no**] **locator** *locator-name*

Context **[Tree]** (config>router>isis>srv6 locator)

Full Context configure router isis segment-routing-v6 locator

Description This command refers to a locator name defined under the **config**>**router**>**segment-routing**>**srv6** context.

This command assigns a locator to each algorithm in an IS-IS instance. The same locator of a specific algorithm number can be shared with other IGP instances and BGP instances in IP-VPN or EVPN.

The locator block, locator node, function and argument lengths are defined under the **config**>**router**>**segment-routing**>**srv6** context.

The **no** form of this command removes the reference to a locator name.

Parameters *locator-name* — Specifies a locator name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

locator

Syntax [**no**] **locator** *locator-name*

Context **[Tree]** (config>service>vprn>srv6 locator)
[Tree] (config>service>epipe>srv6 locator)

Full Context configure service epipe segment-routing-v6 locator
configure service vprn segment-routing-v6 locator

Description This command refers to a locator name defined under the **config**>**router**>**segment-routing**>**srv6** context.

This command assigns a locator to the SRv6 instance in the service. The same locator can be referenced in multiple BGP instances used by IPVPN or EVPN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The locator block, locator node, function and argument lengths are defined under the **config**>**router**>**segment-routing**>**srv6** context.

The **no** form of this command removes the reference to a locator name.

Parameters *locator-name* — Specifies a locator name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

16.210 lock

lock

Syntax [**no**] **lock**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization lock)

Full Context configure system security profile netconf base-op-authorization lock

Description This command authorizes a user associated with the profile to send a NETCONF <lock> operation. This lock operation allows a NETCONF client to lock a configuration datastore.

The **no** form of the command denies the user from requesting a lock.

Default no lock

Platforms All

16.211 lock-override

lock-override

Syntax [**no**] **lock-override**

Context **[Tree]** (config>system>script-control>script-policy lock-override)

Full Context configure system script-control script-policy lock-override

Description This command allows a triggered EHS/CRON script to execute while there is a datastore lock, started by an MD interface, in place.

A triggered EHS/CRON script queues until an **ongoing commit** (or **confirmed-commit**) is done. When an EHS/CRON script is triggered while the **lock-override** CLI knob is on, SR OS behaves as follows.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an exclusive session is in place:

- Keep if it is an MD-CLI session. Disconnect if it is a NETCONF session
- Lose the exclusive lock
- Lose any uncommitted configuration changes

When a global session is in place:

- Keep the MD-CLI or NETCONF session
- Keep the uncommitted configuration changes
- An update may be required after committing the EHS/CRON script configuration changes

The **no** form of this command does not allow the script to execute while there is a datastore lock in place.

Default lock-override

Platforms All

16.212 lockout

lockout

Syntax **lockout failed-attempts** *count* **duration** *duration-minutes* **block** *block-minutes* [**max-port-per-ip** *number-of-ports*]
no lockout

Context **[Tree]** (config>ipsec>ike-policy lockout)

Full Context configure ipsec ike-policy lockout

Description This command enables the lockout mechanism for the IPsec tunnel. The system will lock out an IPsec client for the configured time interval if the number of failed authentications exceeds the configured value within the specified duration. This command only applies when the system acts as a tunnel responder.

A client is defined as the tunnel IP address plus the port.

Optionally, the **max-port-per-ip** parameter can be configured as the maximum number of ports allowed behind the same IP address. If this threshold is exceeded, then all ports behind the IP address are blocked.

The **no** form of this command disables the lockout mechanism.

Default no lockout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the maximum number of failed authentications allowed during the *duration-minutes* interval.

Values 1 to 64

Default 3

duration-minutes — Specifies the interval of time, in minutes, during which the configured failed authentication count must be exceeded in order to trigger a lockout.

Values 1 to 60

Default 5

block-minutes — Specifies the number of minutes that the client is blocked if the configured failed authentication count is exceeded.

Values 1 to 1440, infinite

Default 10

number-of-ports — Specifies the maximum number of ports allowed behind the same IP address.

Values 1 to 32000

Default 16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

lockout

Syntax **clear lockout** {**user** *user-name* | **all**}

Context **[Tree]** (admin>clear lockout)

Full Context admin clear lockout

Description This command is used to clear any lockouts for a specific user, or for all users.

Parameters *user-name* — Clears the locked username.

all — Clears all locked usernames.

Platforms All

16.213 lockout-reset-time

lockout-reset-time

Syntax **lockout-reset-time** *seconds*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no lockout-reset-time

Context [Tree] (config>subscr-mgmt>host-lockout-plcy lockout-reset-time)

Full Context configure subscriber-mgmt host-lockout-policy lockout-reset-time

Description This command configures the time that needs to elapse from the point a client enters lockout to when the client's lockout time can be reset to the configured minimum value. The range is 1 second.

The **no** form of this command reverts to the default value.

Default lockout-reset-time 60

Parameters *seconds* — Specifies the lockout reset time, in seconds.

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.214 lockout-time

lockout-time

Syntax **lockout-time** [**min** *seconds*] [**max** *seconds*]
no lockout-time

Context [Tree] (config>subscr-mgmt>host-lockout-plcy lockout-time)

Full Context configure subscriber-mgmt host-lockout-policy lockout-time

Description This command configures the time for which a client stays in the lockout state during which authentication and ESM host creation is suppressed.

The **no** form of this command reverts to the default value.

Default lockout-time min 10 max 3600

Parameters **min** *seconds* — Specifies the minimum lockout-time for this host lockout policy.

Values 1 to 86400

Default 10 seconds

max *seconds* — Specifies the maximum lockout-time for this host lockout policy.

Values 1 to 86400

Default 3600 seconds

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.215 log

log

Syntax **log**

Context **[Tree]** (config log)

Full Context configure log

Description Commands in this context are used to configure both event logs and accounting logs. Event logs control the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. Event logging configuration includes syslog, snmp notifications (traps), NETCONF notifications and other types of event log outputs.Accounting logs collect comprehensive accounting statistics and write them to XML files on the compact flash in order to support a variety of billing models.

Platforms All

log

Syntax [**no**] **log**

Context **[Tree]** (config>service>vprn>static-route-entry>indirect>cpe-check log)
[Tree] (config>service>vprn>static-route-entry>next-hop>cpe-check log)

Full Context configure service vprn static-route-entry indirect cpe-check log
configure service vprn static-route-entry next-hop cpe-check log

Description This optional parameter enables the ability to log transitions between active and in-active based on the CPE connectivity check. Events will be sent to the system log, syslog and SNMP traps.

Default no log

Platforms All

log

Syntax **log**

Context **[Tree]** (config>service>vprn log)
[Tree] (config>service>vprn>log-id log)

Full Context configure service vprn log
configure service vprn log-id log

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure event logging within a specific VPRN.

By default, the log events in a VPRN log are a subset of the complete set of possible log events in SR OS. See the **config**>**log**>**services-all-events** command for more details.

Platforms All

log

Syntax **log**

Context **[Tree]** (config>li log)

Full Context configure li log

Description Commands in this context configure an event log for LI.

Platforms All

log

Syntax **log** *log-id*
no log

Context **[Tree]** (config>filter>ip-filter>entry log)
[Tree] (config>filter>ipv6-filter>entry log)
[Tree] (config>filter>mac-filter>entry log)

Full Context configure filter ip-filter entry log
configure filter ipv6-filter entry log
configure filter mac-filter entry log

Description This command associates a filter log to the current filter policy entry and therefore enables logging for that filter entry.

The filter log must exist before a filter entry can be enabled to use the filter log.

The **no** form of the command disables logging for the filter entry.

Default no log

Parameters *log-id* — Specifies the filter log ID expressed as a decimal integer.

Values 101 to 199

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

log

Syntax **log** *log-id* [**create**]
no log *log-id*

Context **[Tree]** (config>filter log)

Full Context configure filter log

Description This command, creates a configuration context for the specified filter log if it does not exist, and enables the context to configure the specified filter log.

The **no** form of the command deletes the filter log. The log cannot be deleted if there are filter entries configured to write to the log. All filter entry logging associations need to be removed before the log can be deleted.

Default log 101

Special Cases **Filter log 101 —** Filter log 101 is the default log and is automatically created by the system. Filter log 101 is always a memory filter log and cannot be changed to a Syslog filter log. The log size defaults to 1000 entries, the filter log description is set to "Default filter log". The number of entries and **wrap-around** behavior can be modified.

Parameters *log-id* — Specifies the filter log ID expressed as a decimal integer.

Values 101 to 199

create — This keyword is required to create the configuration context. After it is created, the context can be enabled with or without the **create** keyword.

Platforms All

log

Syntax [**no**] **log**

Context **[Tree]** (config>router>static-route-entry>indirect>cpe-check log)
[Tree] (config>router>static-route-entry>next-hop>cpe-check log)

Full Context configure router static-route-entry indirect cpe-check log
configure router static-route-entry next-hop cpe-check log

Description This optional parameter enables the ability to log transitions between active and in-active based on the CPE connectivity check. Events will be sent to the system log, syslog and SNMP traps.

Default no log

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

log

Syntax [**no**] log

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry log)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry log)
[Tree] (config>system>security>mgmt-access-filter>mac-filter>entry log)

Full Context configure system security management-access-filter ip-filter entry log
configure system security management-access-filter ipv6-filter entry log
configure system security management-access-filter mac-filter entry log

Description This command enables match logging. When enabled, matches on this entry will cause the Security event mafEntryMatch to be raised.

Default no log

Platforms All

log

Syntax **log** *log-id*

Context **[Tree]** (config>sys>security>cpm-filter>ip-filter>entry log)
[Tree] (config>sys>security>cpm-filter>ipv6-filter>entry log)
[Tree] (config>sys>security>cpm-filter>mac-filter>entry log)

Full Context configure system security cpm-filter ip-filter entry log
configure system security cpm-filter ipv6-filter entry log
configure system security cpm-filter mac-filter entry log

Description This command specifies the log in which packets matching this entry should be entered. The value zero indicates that logging is disabled.

The **no** form of this command deletes the log ID.

Parameters *log-id* — Specifies the log ID where packets matching this entry should be entered.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.216 log-anno-interval

log-anno-interval

Syntax **log-anno-interval** *log-interval*
no log-anno-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>ptp log-anno-interval)

Full Context configure system ptp log-anno-interval

Description This command configures the announce message interval used for both unicast and multicast messages.

For unicast messages, it defines the announce message interval that is requested during unicast negotiation to any peer. This controls the announce message rate sent from remote peers to the local node. It does not affect the announce message rate that may be sent from the local node to remote peers. Remote peers may request an announce message rate anywhere within the acceptable grant range.

For multicast messages, used on PTP Ethernet ports, this configures the message interval used for Announce messages transmitted by the local node.

This value also defines the interval between executions of the BMCA within the node.

The announce-interval cannot be changed unless the PTP is shut down.

Note: In order to minimize BMCA driven reconfigurations, the IEEE recommends that the announce-interval should be consistent across the entire 1588 network.

Default log-anno-interval 1 (1 packet every 2 seconds) for ieee1588-2008

log-anno-interval 1 (1 packet every 2 seconds) for g8265dot1-2010

log-anno-interval -3 (8 packets per second) for g8275dot1-2014

Parameters *log-interval* — Specifies the announce packet interval, in log form.

Values -3 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.217 log-delay-interval

log-delay-interval

Syntax **log-delay-interval** *log-interval*
no log-delay-interval

Context [Tree] (config>system>ptp>port log-delay-interval)

Full Context configure system ptp port log-delay-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the minimum interval used for multicast Delay_Req messages. This parameter is applied on a per-port basis. For ports in a slave state, it shall be the interval used, unless the parent port indicates a longer interval. For a port in master state, it shall be the interval advertised to external slave ports as the minimum acceptable interval for Delay_Req messages from those slave ports.

It is a requirement of the 1588 standard that a port in Slave state shall check the logMessageInterval field of received multicast Delay_Resp messages. If the value of the logMessageInterval field of those messages is greater than the value programmed locally for the generation of Delay_Req messages, then the Slave must change to use the greater value (i.e. longer interval) for the generation of Delay_Req messages. This requirement is supported in the router.

The parameter is only applicable to ports and not to peers.

Default log-delay-interval -6 for ieee1588-2008

log-delay-interval -6 for g8265dot1-2010

log-delay-interval -4 for g8275dot1-2014

Parameters *log-interval* — Specifies the Delay_Req message interval, in log form.

Values -6 to 0

Default -6

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.218 log-events

log-events

Syntax **log-events** [**verbose**]
no log-events

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>local-monitoring-policer log-events)

Full Context configure system security dist-cpu-protection policy local-monitoring-policer log-events

Description This command controls the creation of log events related to **local-monitoring-policer** status and activity.

Default log-events

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **verbose** — Sends the same events as just “log-events” plus DcpLocMonExcd, DcpLocMonExcdAllDynAlloc, and DcpLocMonExcdAllDynFreed. The optional “verbose” includes some events that are more likely used during debug/tuning/ investigations

Platforms All

log-events

Syntax [**no**] **log-events** [**verbose**]
no log-events

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>protocol>dyn-para log-events)

Full Context configure system security dist-cpu-protection policy protocol dynamic-parameters log-events

Description This command controls the creation of log events related to dynamic enforcement policer status and activity.

Default log-events

Parameters **verbose** — This parameter sends the same events as just “log-events” plus Hold Down Start, Hold Down End, DcpDynamicEnforceAlloc and DcpDynamicEnforceFreed events. This includes the allocation/de-allocation events (typically used for debug/ tuning only – could be very noisy even when there is nothing much of concern).

Platforms All

log-events

Syntax **log-events** [**verbose**]
no log-events

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>static-policer log-events)

Full Context configure system security dist-cpu-protection policy static-policer log-events

Description This command controls the creation of log events related to static-policer status and activity.

Default log-events

Parameters **verbose** — Sends the same events as just “log-events” plus Hold Down Start and Down End events. The optional “verbose” includes some events that are more likely used during debug/tuning/investigations.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.219 log-filter

log-filter

Syntax **log-filter** *filter-id*
no log-filter

Context **[Tree]** (config>log>event-trigger>event>trigger-entry log-filter)

Full Context configure log event-trigger event trigger-entry log-filter

Description This command configures the log filter to be used for this trigger entry. The log filter defines the matching criteria that must be met in order for the log event to trigger the handler execution. The log filter is applied to the log event and, if the filtering decision results in a forward action, then the handler is triggered.

It is typically unnecessary to configure match criteria for the application or number in the log filter used for EHS since the particular filter is only applied for a specific log event application and number, as configured under the **config**>**log**>**event-trigger** context.

The **no** form of this command removes the log filter configuration.

Parameters *filter-id* — Specifies the identifier of the filter.

Values 1 to 1500

Platforms All

16.220 log-id

log-id

Syntax **log-id** *log-id* [**name** *log-name*]
no log-id *log-id*

Context **[Tree]** (config>service>vprn>log log-id)

Full Context configure service vprn log log-id

Description This command creates a context to configure destinations for event streams.

The **log-id** context is used to direct events, alarms or traps, and debug information to respective destinations.

A maximum of 30 logs can be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Before an event can be associated with this log-id, the **from** command identifying the source of the event must be configured.

Only one destination can be specified for a *log-id*. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, Syslog, or file.

Use the **event-control** command to suppress the generation of events, alarms, and traps for all log destinations.

An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.

By default, the log events in a VPRN log are a subset of the complete set of possible log events in SR OS. See the **config**>**log**>**services-all-events** command for more details.

The **no** form of this command deletes the log destination ID from the configuration.

Default No log destinations are defined.

Parameters *log-id* — Specifies the log ID number, expressed as a decimal integer.

Values 1 to 100

name *log-name* — Configures an optional log name, up to 64 characters, that can be used to refer to the log destination after it is created.

Platforms All

log-id

Syntax **log-id** *log-id* [**name** *li-log-name*]
no log-id *log-id*

Context **[Tree]** (config>li>log log-id)

Full Context configure li log log-id

Description This command configures an LI event log destination. The *log-id* is used to direct events, alarms or traps, and debug information for specific destinations.

Parameters *log-id* — Specifies the log ID, expressed as a decimal number.

Values 1 to 100

name *li-log-name* — Configures an optional log name, up to 64 characters, that can be used to refer to the log destination after it is created.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

log-id

Syntax **log-id** *log-id* [**name** *log-name*]
no log-id *log-id*

Context **[Tree]** (config>log log-id)

Full Context configure log log-id

Description This command creates a context to configure destinations for event streams.

The **log-id** context is used to direct events, alarms or traps, and debug information for specific destinations.

A maximum of 30 logs can be configured.

Before an event can be associated with this log ID, the **from** command identifying the source of the event must be configured.

Only one destination can be specified for a *log-id*. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.

Use the **event-control** command to suppress the generation of events, alarms, and traps for all log destinations.

An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.

Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages. Log-ID 100 captures log messages with a severity level of major and above.

Note: Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.

The **no** form of this command deletes the log destination ID from the configuration.

Parameters *log-id* — Specifies the log ID, expressed as a decimal integer.

Values 1 to 101

name *log-name* — Configures an optional log name, up to 64 characters, that can be used to refer to the log destination after it is created.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.221 log-prefix

log-prefix

Syntax **log-prefix** *log-prefix-string*
no log-prefix

Context **[Tree]** (config>service>vprn>log>syslog log-prefix)

Full Context configure service vprn log syslog log-prefix

Description This command adds the string prepended to every syslog message sent to the syslog host.

RFC3164, *The BSD syslog Protocol,* allows an alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.

Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.

The **no** form of this command removes the log prefix string.

Default log-prefix "TMNX".

Parameters *log-prefix-string* — Specifies the alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

Platforms All

log-prefix

Syntax **log-prefix** *prefix-text*

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy log-prefix)

Full Context configure service nat syslog syslog-export-policy log-prefix

Description This command configures the syslog log prefix. For more information, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. The **config>log>syslog>level** hierarchy also applies to this context.

Default log-prefix “TMNX”

Parameters *prefix-text* — Specifies an alphanumeric string, up to 32 characters. Spaces and colons (:) cannot be used in the string.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

log-prefix

Syntax **log-prefix** *log-prefix-string*
no log-prefix

Context **[Tree]** (config>log>syslog log-prefix)

Full Context configure log syslog log-prefix

Description This command adds the string prepended to every syslog message sent to the syslog host.

RFC 3164, allows an alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.

Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0 to 9) characters.

The **no** form of this command removes the log prefix string.

Default no log-prefix

Parameters *log-prefix-string* — Specifies an alphanumeric string up to 32 characters in length. Spaces and colons (:) cannot be used in the string.

Platforms All

16.222 log-sync-interval

log-sync-interval

Syntax **log-sync-interval** *log-interval*
no log-sync-interval

Context **[Tree]** (config>service>vprn>ptp>peer log-sync-interval)

Full Context configure service vprn ptp peer log-sync-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the message interval used for unicast event messages. It defines the message interval for both Sync and Delay_Resp messages that are requested during unicast negotiation to the specific peer. This controls the Sync and Delay_Resp message rate sent from remote peers to the local node. It does not affect the Sync or Delay_Resp packet rate that may be sent from the local node to remote peers. Remote peers may request a Sync or Delay_Resp packet rate anywhere within the acceptable grant range.

The **log-sync-interval** cannot be changed unless the peer is shutdown.

This command only applies to the 7450 ESS and 7750 SR.

Default -6 (64 packets per second) for 1588-2008 or

-6 (64 packets per second) for g8265dot1-2010 or

-4 (16 packets per second) for g8275dot1-2014

Parameters *log-interval* — Specifies the sync message interval, in log form.

Values -6 to 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

log-sync-interval

Syntax **log-sync-interval** *log-interval*
no log-sync-interval

Context **[Tree]** (config>system>ptp>peer log-sync-interval)

Full Context configure system ptp peer log-sync-interval

Description This command configures the message interval used for unicast event messages. It defines the message interval for both Sync and Delay_Resp messages that are requested during unicast negotiation to the specific peer. This controls the Sync and Delay_Resp message rate sent from remote peers to the local node. It does not affect the Sync or Delay_Resp packet rate that may be sent from the local node to remote peers. Remote peers may request a Sync or Delay_Resp packet rate anywhere within the acceptable grant range.

The **log-sync-interval** cannot be changed unless the peer is shutdown.

Default log-sync-interval -6 (64 packets per second) for 1588-2008

log-sync-interval -6 (64 packets per second) for g8265dot1-2010

log-sync-interval -4 (16 packets per second) for g8275dot1-2014

Parameters *log-interval* — Specifies the sync message interval, in log form.

Values -6 to 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

log-sync-interval

Syntax **log-sync-interval** *log-interval*
no log-sync-interval

Context **[Tree]** (config>system>ptp>port log-sync-interval)

Full Context configure system ptp port log-sync-interval

Description This command configures the message interval used for transmission of multicast Sync messages.

For multicast messages used on PTP Ethernet ports, this configures the message interval used for Sync messages transmitted by the local node when the port is in Master state.

Default log-sync-interval -6 (64 packets per second) for ieee1588-2008 or

log-sync-interval -6 (64 packets per second) for g8265dot1-2010 or

log-sync-interval -4 (16 packets per second) for g8275dot1-2014

Parameters *log-interval* — Specifies the message interval, in log form.

Values -6 to 0 (This corresponds to a maximum rate of 64 packets per second, and a minimum rate of 1 packet per second.)

Default -6

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.223 logger-event-bundling

logger-event-bundling

Syntax [**no**] **logger-event-bundling**

Context **[Tree]** (config>router>mpls logger-event-bundling)

Full Context configure router mpls logger-event-bundling

Description This feature merges two of the most commonly generated MPLS traps, vRtrMplsXCCreate and vRtrMplsXCDelete, which can be generated at both LER and LSR into a new specific trap vRtrMplsSessionsModified. In addition, this feature perform bundling of traps of multiple RSVP sessions, that is LSPs, into this new specific trap.

The intent is to provide a tool for the user to minimize trap generation in an MPLS network. Note that the MPLS trap throttling will not be applied to this new trap.

The **no** version of this command disables the merging and bundling of the above MPLS traps.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

16.224 logical-access-id

logical-access-id

Syntax [**no**] **logical-access-id**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp logical-access-id)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp logical-access-id

Description This command includes the logical-access-id.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

16.225 logical-port-status

logical-port-status

Syntax **logical-port-status** {**rsvp-te** | **mpls-tp** | **sr-te**}
no logical-port-status [{**rsvp-te** | **mpls-tp** | **sr-te**}]

Context **[Tree]** (config>open-flow>of-switch logical-port-status)

Full Context configure open-flow of-switch logical-port-status

Description This command enables status change reporting to the OpenFlow controller for the specified logical port type. To report on multiple logical port types, the command needs to be executed multiple times with different logical port specified as required.

The **no** form of this command disables status reporting for specified or all (no argument) logical ports.

Default no logical-port-status

Parameters **rsvp-te** — Enables reporting on RSVP-TE LSP logical ports.

mpls-te — Enables reporting on MPLS-TE logical ports.

sr-te — Enables reporting on SR-TE logical ports.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.226 login-banner

login-banner

Syntax [**no**] **login-banner**

Context **[Tree]** (config>system>login-control login-banner)

Full Context configure system login-control login-banner

Description This command enables or disables the display of a login banner. The login banner contains the SR OS copyright and build date information for a console login attempt.

The **no** form of this command causes only the configured pre-login-message and a generic login prompt to display.

Platforms All

16.227 login-control

login-control

Syntax **login-control**

Context **[Tree]** (config>system login-control)

Full Context configure system login-control

Description This command creates the context to configure the session control for console, Telnet, SSH, and FTP sessions.

Platforms All

16.228 login-exec

login-exec

Syntax **login-exec** *url-prefix*: *source-url*
no login-exec

Context **[Tree]** (config>system>security>user>console login-exec)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>system>security>user-template>console login-exec)

Full Context configure system security user console login-exec
configure system security user-template console login-exec

Description This command configures a user's login exec file which executes whenever the user successfully logs in to a console session.

Only one exec file can be configured. If multiple **login-exec** commands are entered for the same user, each subsequent entry overwrites the previous entry.

The **no** form of this command disables the login exec file for the user.

Default no login-exec

Parameters *url-prefix: source-url* — Specifies either a local or remote URL, up to 200 characters, that identifies the exec file that is executed after the user successfully logs in.

Platforms All

16.229 login-scripts

login-scripts

Syntax **login-scripts**

Context **[Tree]** (config>system>login-control login-scripts)

Full Context configure system login-control login-scripts

Description Commands in this context configure CLI scripts that execute when a user (authenticated via any method including local user database, TACACS+, or RADIUS) first logs into a CLI session.

Platforms All

16.230 logout

logout

Syntax **logout**

Context **[Tree]** (global logout)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context global logout

Description This command logs out of the router session.

When the **logout** command is issued from the console, the login prompt is displayed, and any log IDs directed to the console are discarded. When the console session resumes (regardless of the user), the log output to the console resumes.

When a Telnet session is terminated from a **logout** command, all log IDs directed to the session are removed. When a user logs back in, the log IDs must be re-created.

16.231 long-duration-flow-count

long-duration-flow-count

Syntax [**no**] **long-duration-flow-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-cntr long-duration-flow-count)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-counters long-duration-flow-count

Description This command includes the long duration flow count. This command only applies to the 7750 SR.

The **no** form of this command excludes the long duration flow count in the AA subscriber's custom record.

Default no long-duration-flow-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.232 long-lived

long-lived

Syntax [**no**] **long-lived**

Context **[Tree]** (config>service>vprn>bgp>graceful-restart long-lived)
[Tree] (config>service>vprn>bgp>group>graceful-restart long-lived)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart long-lived)

Full Context configure service vprn bgp graceful-restart long-lived

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp group graceful-restart long-lived
configure service vprn bgp group neighbor graceful-restart long-lived

Description Commands in this context configure BGP Long-Lived Graceful-Restart (LLGR) procedures.

LLGR, known informally as BGP persistence, is an extension of BGP graceful restart that allows a session to stay down for a longer period of time. During this time, learned routes are marked and re-advertised as stale but they can continue to be used as routes of last resort.

The LLGR handling of a session failure can be invoked immediately or it can be delayed until the end of the traditional GR restart window.

Default no long-lived

Platforms All

long-lived

Syntax [**no**] **long-lived**

Context **[Tree]** (config>router>bgp>graceful-restart long-lived)
[Tree] (config>router>bgp>group>graceful-restart long-lived)
[Tree] (config>router>bgp>group>neighbor>graceful-restart long-lived)

Full Context configure router bgp graceful-restart long-lived
configure router bgp group graceful-restart long-lived
configure router bgp group neighbor graceful-restart long-lived

Description Commands in this context enter commands related to BGP Long-Lived Graceful-Restart (LLGR) procedures.

LLGR, known informally as BGP persistence, is an extension of BGP GR that allows a session to stay down for a longer period of time. During this time, learned routes are marked and re-advertised as stale but they can continue to be used as routes of last resort.

The LLGR handling of a session failure can be invoked immediately or it can be delayed until the end of the traditional GR restart window.

Default no long-lived

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.233 loop-detect

loop-detect

Syntax **loop-detect** {**drop-peer** | **discard-route** | **ignore-loop** | **off**}
no loop-detect

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy loop-detect)

Full Context configure subscriber-mgmt bgp-peering-policy loop-detect

Description This command configures how the BGP peer session handles loop detection in the AS path.

Note: Dynamic configuration changes of **loop-detect** are not recognized.

The **no** form of this command used at the global level reverts to default, which is **loop-detect ignore-loop**.

Parameters **drop-peer** — Sends a notification to the remote peer and drops the session.

discard-route — Discards routes received with loops in the AS path.

ignore-loop — Ignores routes with loops in the AS path but maintains peering.

off — Disables loop detection.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

loop-detect

Syntax **loop-detect** {**drop-peer** | **discard-route** | **ignore-loop** | **off**}
no loop-detect

Context **[Tree]** (config>service>vprn>bgp loop-detect)
[Tree] (config>service>vprn>bgp>group loop-detect)
[Tree] (config>service>vprn>bgp>group>neighbor loop-detect)

Full Context configure service vprn bgp group loop-detect
configure service vprn bgp group neighbor loop-detect
configure service vprn bgp loop-detect

Description This command configures how the BGP peer session handles loop detection in the AS path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Dynamic configuration changes of **loop-detect** are not recognized.

The **no** form of this command used at the global level reverts to default, which is **loop-detect ignore-loop**.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default loop-detect ignore-loop

Parameters **drop-peer** — Sends a notification to the remote peer and drops the session.

discard-route — Discards routes received with loops in the AS path.

ignore-loop — ignores routes with loops in the AS path but maintains peering.

off — Disables loop detection.

Platforms All

loop-detect

Syntax **loop-detect** {**drop-peer** | **discard-route** | **ignore-loop** | **off**}
no loop-detect

Context **[Tree]** (config>router>bgp loop-detect)
[Tree] (config>router>bgp>group loop-detect)
[Tree] (config>router>bgp>group>neighbor loop-detect)

Full Context configure router bgp group loop-detect
configure router bgp group neighbor loop-detect
configure router bgp loop-detect

Description This command configures how the BGP peer session handles loop detection in the AS path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

Note: Dynamic configuration changes of **loop-detect** are not recognized.

The **no** form of this command used at the global level reverts to default, which is **loop-detect ignore-loop**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default loop-detect ignore-loop

Parameters **drop-peer** — Sends a notification to the remote peer and drops the session.

discard-route — Discards routes received from a peer with the same AS number as the router itself. This option prevents routes looped back to the router from being added to the routing information base and consuming memory. When this option is changed, the change will not be active for an established peer until the connection is re-established for the peer.

ignore-loop — Ignores routes with loops in the AS path but maintains peering.

off — Disables loop detection.

Platforms All

16.234 loop-detect-threshold

loop-detect-threshold

Syntax **loop-detect-threshold** *loop-detect-threshold*
no loop-detect-threshold

Context **[Tree]** (config>service>vprn>bgp loop-detect-threshold)
[Tree] (config>service>vprn>bgp>group loop-detect-threshold)
[Tree] (config>service>vprn>bgp>group>neighbor loop-detect-threshold)

Full Context configure service vprn bgp group loop-detect-threshold
configure service vprn bgp group neighbor loop-detect-threshold
configure service vprn bgp loop-detect-threshold

Description This command provides additional control over the behavior enabled by the **loop-detect** command. If this command specifies a threshold value of *n,* then a route received by the local BGP speaker with an AS path that contains up to *n* occurrences of the local speaker's AS number is considered valid and not treated as an AS path loop. An AS loop is considered to occur only when the received AS path has more than *n* occurrences of the local speaker's AS number.

The **no** form of this command removes the configuration and sets the value to 0. One or more occurrence of the local speaker's AS number in the received AS path triggers the **loop-detect** behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no loop-detect-threshold

Parameters *loop-detect-threshold* — The maximum number of occurrences of the local speaker's AS number in the received AS path before the AS path is considered to be a loop.

Values 0 to 15

Default 0

Platforms All

loop-detect-threshold

Syntax **loop-detect-threshold** *loop-detect-threshold*
no loop-detect-threshold

Context **[Tree]** (config>router>bgp loop-detect-threshold)
[Tree] (config>router>bgp>group loop-detect-threshold)
[Tree] (config>router>bgp>group>neighbor loop-detect-threshold)

Full Context configure router bgp group loop-detect-threshold
configure router bgp group neighbor loop-detect-threshold
configure router bgp loop-detect-threshold

Description This command provides additional control over the behavior enabled by the **loop-detect** command. If this command specifies a threshold value of *n*, then a route received by the local BGP speaker with an AS path that contains up to *n* occurrences of the local speaker's AS number is considered valid and not treated as an AS path loop. An AS loop is considered to occur only when the received AS path has more than *n* occurrences of the local speaker's AS number.

The **no** form of this command removes the configuration and sets the value to 0. One or more occurrence of the local speaker's AS number in the received AS path triggers the **loop-detect** behavior.

Default no loop-detect-threshold

Parameters *loop-detect-threshold* — The maximum number of occurrences of the local speaker's AS number in the received AS path before the AS path is considered to be a loop.

Values 0 to 15

Default 0

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.235 loopback

loopback

Syntax [**no**] **loopback**

Context **[Tree]** (config>service>ies>if loopback)
[Tree] (config>service>vprn>if loopback)

Full Context configure service ies interface loopback
configure service vprn interface loopback

Description This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated IES/VPRN interface cannot be bound to a SAP.

Note: Configure an IES interface as a loopback interface by issuing the **loopback** command instead of the **sap** *sap-id* command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

The **no** form of this command reverts to the default.

Platforms All

loopback

Syntax [**no**] **loopback**

Context **[Tree]** (config>service>vprn>nw-if loopback)

Full Context configure service vprn network-interface loopback

Description This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated interface cannot be bound to a SAP.

When using mtrace/mstat in a Layer 3 VPN context then the configuration for the VPRN should have a loopback address configured which has the same address as the core instance's system address (BGP next-hop).

Default no loopback

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

loopback

Syntax **loopback** {**line** | **internal**}
no loopback

Context **[Tree]** (config>port>sonet-sdh loopback)

Full Context configure port sonet-sdh loopback

Description This command activates a loopback on the SONET/SDH port.

The SONET port must be in a shut down state to activate any type of loopback. The loopback setting is never saved to the generated/saved configuration file.

Note that loopback mode changes on a SONET/SDH port can affect traffic on the remaining ports.

This command is supported by TDM satellite.

Default no loopback

Parameters **line** — Set the port into line loopback state.

internal — Set the port into internal loopback state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

loopback

Syntax **loopback** {**line** | **internal** | **fdl-ansi** | **fdl-bellcore** | **payload-ansi** | **inband-ansi** | **inband-bellcore**}
no loopback

Context **[Tree]** (config>port>tdm>ds1 loopback)

Full Context configure port tdm ds1 loopback

Description This command puts the specified port or channel into a loopback mode.

The corresponding port or channel must be in a shutdown state in order for the loopback mode to be enabled. The upper level port or channel or parallel channels should not be affected by the loopback mode.

Note that this command is not saved in the router configuration between boots.

The **no** form of this command disables the specified type of loopback.

Default no loopback

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **line** — Places the associated port or channel into a line loopback mode. A line loopback loops frames received on the corresponding port or channels back to the remote router.

internal — Places the associated port or channel into an internal loopback mode. An internal loopback loops the frames from the local router back at the framer.

fdl-ansi — Requests FDL line loopback according to ANSI T1.403.

fdl-bellcore — Requests FDL line loopback according to Bellcore TR-TSY-000312.

payload-ansi — Requests payload loopback using ANSI signaling.

inband-ansi — Requests inband line loopback according to ANSI T1.403.

inband-bellcore — Requests inband line loopback according to Bellcore signaling.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

loopback

Syntax **loopback** {**line** | **internal** | **remote**}
no loopback

Context **[Tree]** (config>port>tdm>ds3 loopback)

Full Context configure port tdm ds3 loopback

Description This command puts the specified port or channel into a loopback mode.

The corresponding port or channel must be in a shutdown state in order for the loopback mode to be enabled. The upper level port or channel or parallel channels should not be affected by the loopback mode.

Note that this command is not saved in the router configuration between boots.

The **no** form of this command disables the specified type of loopback.

Default no loopback

Parameters **line** — Places the associated port or channel into a line loopback mode. A line loopback loops frames received on the corresponding port or channels back to the remote router.

internal — Places the associated port or channel into an internal loopback mode. A internal loopback loops the frames from the local router back at the framer.

remote — Sends a signal to the remote device to provide a line loopback.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

loopback

Syntax **loopback** {**line** | **internal**}
no loopback

Context **[Tree]** (config>port>tdm>e1 loopback)
[Tree] (config>port>tdm>e3 loopback)

Full Context configure port tdm e1 loopback
configure port tdm e3 loopback

Description This command puts the specified port or channel into a loopback mode.

The corresponding port or channel must be in a shutdown state in order for the loopback mode to be enabled. The upper level port or channel or parallel channels should not be affected by the loopback mode

Note that this command is not saved in the router configuration between boots.

The **no** form of this command disables the specified type of loopback.

Default no loopback

Parameters **line** — Places the associated port or channel into a line loopback mode. A line loopback loops frames received on the corresponding port or channels back to the remote router.

internal — Places the associated port or channel into an internal loopback mode. An internal loopback loops the frames from the local router back at the framer.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

loopback

Syntax **loopback** {*mac-address* | **multicast** | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**send-count** *send-count*] [**size** *data-size*] [**priority** *priority*] [**lbm-padding** *padding-size*] [**timeout** *timeout-time*] [**interval** *interval-time*]

Context **[Tree]** (oam>eth-cfm loopback)

Full Context oam eth-cfm loopback

Description The command initiates a loopback test.

Parameters *mac-address* — Specifies a unicast MAC address or multicast MAC address. The last nibble of the multicast address must match the level of the local MEP, or the command fails and the test is not instantiated.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx or multicast

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multicast — Builds the class one destination multicast address based on the level of the local MEP. The last nibble of the multicast address must match the level of the local MEP or the command fails and the test is not instantiated.

remote-mepid *mep-id* — Specifies the remote MEP ID of the peer within the association. The domain and association information are derived from the **source mep** for the session. The Layer 2 IEEE MAC address is resolved from previously-learned remote MAC addressing, derived from the reception and processing of the ETH-CC PDU. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

send-count — Specifies the number of messages to send, expressed as a decimal integer. Loopback messages are sent back-to-back, with no delay between the transmissions.

Values 1 to 1024

Default 1

data-size — Specifies the size of the variable data pattern only of the data TLV. This value does not include the 1 Byte Type, 2 Byte Length. This means that the total size of the data TLV is the configured value plus the 3 addition bytes to accommodate the type and length fields. If 0 is specified, no data TLV is added to the packet. This parameter and **lbm-padding** are mutually exclusive.

Values 0 to 1500

Default 0

priority — Specifies a 3-bit value to be used in the VLAN tag, if present, in the transmitted frame.

Values 0 to 7

Default The CCM and LTM priority of the MEP

padding-size — Specifies the complete size of the data TLV, which includes the 1 Byte Type, 2 Byte Length, and the variable data pad. If 0 is specified, no data TLV is added to the packet. MSDU is not processed when **lbm-padding** is in use. This parameter and **size** are mutually exclusive.

Values 0, 3 to 9000

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout-time — Specifies the time, in seconds, used to override the default *timeout-time* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded.

Values 1 to 10

Default 5

interval-time — Specifies the time, in deciseconds (100 ms), to configure the spacing between probes within the test run. A value of 0 means probes are sent with no enforced delay. This value is only applicable to tests where the **send-count** is 5 or less.

Values 0 to 600

Default 0 or 10 depending on the **send-count**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

loopback

Syntax [**no**] **loopback**

Context **[Tree]** (config>router>if loopback)

Full Context configure router interface loopback

Description This command configures the interface as a loopback interface. The **vas-if-type** and **loopback** commands are mutually exclusive.

Default Not enabled

Platforms All

loopback

Syntax **loopback** *loopback-id* [**create**]
no loopback *loopback-id*

Context **[Tree]** (config>card>mda>xconnect>mac loopback)
[Tree] (config>card>xiom>mda>xcon>mac loopback)

Full Context configure card mda xconnect mac loopback
configure card xiom mda xconnect mac loopback

Description This command configures a MAC loopback on a MAC chip. The system and services can start using the loopback only when a port is associated with it (for example, port 1/1/m1/1, where m1 represents the MAC ID).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the loopback ID from the configuration.

Parameters *loopback-id* — Specifies the loopback ID for the MDA cross-connect.

Values 1, 2

create — Keyword used to create a new loopback. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

- configure card mda xconnect mac loopback

7750 SR-s

- configure card xiom mda xconnect mac loopback

16.236 loopback-period

loopback-period

Syntax **loopback-period** *period*
no loopback-period

Context **[Tree]** (config>system>atm>oam loopback-period)

Full Context configure system atm oam loopback-period

Description This command specifies the number of seconds between periodic loopback attempts on an ATM endpoint that has periodic loopback enabled.

Default no loopback-period

Parameters *period* — Specifies the time, in seconds, between periodic loopback attempts.

Values 1 to 40

Default 10

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.237 loopfree-alternate-exclude

loopfree-alternate-exclude

Syntax [**no**] **loopfree-alternate-exclude**

Context **[Tree]** (config>router>isis>level loopfree-alternate-exclude)
[Tree] (config>router>isis>interface loopfree-alternate-exclude)
[Tree] (config>service>vprn>isis>level loopfree-alternate-exclude)
[Tree] (config>service>vprn>isis>interface loopfree-alternate-exclude)

Full Context configure router isis interface loopfree-alternate-exclude
configure router isis level loopfree-alternate-exclude
configure service vprn isis interface loopfree-alternate-exclude
configure service vprn isis level loopfree-alternate-exclude

Description This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

The **no** form of this command re-instates the default value for this command.

Default no loopfree-alternate-exclude

Platforms All

loopfree-alternate-exclude

Syntax [**no**] **loopfree-alternate-exclude**

Context **[Tree]** (config>service>vprn>ospf>area loopfree-alternate-exclude)
[Tree] (config>service>vprn>ospf3>area loopfree-alternate-exclude)
[Tree] (config>service>vprn>ospf>area>if loopfree-alternate-exclude)
[Tree] (config>service>vprn>ospf3>area>if loopfree-alternate-exclude)

Full Context configure service vprn ospf area interface loopfree-alternate-exclude
configure service vprn ospf area loopfree-alternate-exclude
configure service vprn ospf3 area interface loopfree-alternate-exclude
configure service vprn ospf3 area loopfree-alternate-exclude

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command fails.

The **no** form of this command re-instates the default value for this command.

Default no loopfree-alternate-exclude

Platforms All

loopfree-alternate-exclude

Syntax **loopfree-alternate-exclude prefix-policy** *prefix-policy* [*prefix-policy*)]
no loopfree-alternate-exclude

Context **[Tree]** (config>router>ospf loopfree-alternate-exclude)
[Tree] (config>router>ospf3 loopfree-alternate-exclude)

Full Context configure router ospf loopfree-alternate-exclude
configure router ospf3 loopfree-alternate-exclude

Description This command excludes from the LFA SPF calculation those prefixes that match a prefix entry or a tag entry in a prefix policy. If a prefix is excluded from LFA, it is not included in LFA calculations regardless of its priority. The prefix tag will, however, be used in the main SPF.

The implementation also allows the user to exclude a specific interface in IS-IS or OSPF, a or all interfaces in an OSPF area or IS-IS level from the LFA SPF.

Note: Prefix tags are defined for the IS-IS protocol but not for the OSPF protocol.

The default action of the **loopfree-alternate-exclude** command, when not explicitly specified by the user in the prefix policy, is “reject”. Therefore, regardless of whether the user explicitly added the statement “default-action reject” to the prefix policy, a prefix that does not match any entry in the policy will be accepted into LFA SPF.

The **no** form of this command deletes the exclude prefix policy.

Default no loopfree-alternate-exclude

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *prefix-policy* — Specifies up to five policy prefix names. The specified policy name must already be defined. Prefix policies are created with the command **config>router>policy-options>prefix-list**; for information on prefix lists, refer to "Route Policies" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*.

loopfree-alternate-exclude

Syntax [**no**] **loopfree-alternate-exclude**

Context **[Tree]** (config>router>ospf>area loopfree-alternate-exclude)
[Tree] (config>router>ospf>area>interface loopfree-alternate-exclude)
[Tree] (config>router>ospf3>area loopfree-alternate-exclude)
[Tree] (config>router>ospf3>area>interface loopfree-alternate-exclude)

Full Context configure router ospf area interface loopfree-alternate-exclude
configure router ospf area loopfree-alternate-exclude
configure router ospf3 area interface loopfree-alternate-exclude
configure router ospf3 area loopfree-alternate-exclude

Description This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

The **no** form of this command re-instates the default value for this command.

Default no loopfree-alternate-exclude

Platforms All

16.238 loopfree-alternates

loopfree-alternates

Syntax [**no**] **loopfree-alternates**

Context **[Tree]** (config>service>vprn>isis loopfree-alternates)

Full Context configure service vprn isis loopfree-alternates

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level or under the OSPF routing protocol instance level.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The **no** form of this command disables the LFA computation by IGP SPF.

Default no loopfree-alternates

Platforms All

loopfree-alternates

Syntax [**no**] **loopfree-alternates**

Context **[Tree]** (config>service>vprn>ospf loopfree-alternates)
[Tree] (config>service>vprn>ospf3 loopfree-alternates)

Full Context configure service vprn ospf loopfree-alternates
configure service vprn ospf3 loopfree-alternates

Description This command enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level, or under the OSPF routing protocol instance level.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. IS-IS computes the primary SPF first and then computes the LFA SPF. The LFA backup next-hop is only available after the LFA SPF is completed. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The **no** form of this command disables the LFA computation by IGP SPF.

Default no loopfree-alternates

Platforms All

loopfree-alternates

Syntax [**no**] **loopfree-alternates**

Context **[Tree]** (config>router>isis>flex-algos>flex-algo loopfree-alternates)
[Tree] (config>router>ospf>flex-algos>flex-algo loopfree-alternates)

Full Context configure router isis flexible-algorithms flex-algo loopfree-alternates
configure router ospf flexible-algorithms flex-algo loopfree-alternates

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the advertisement of flexible-algorithm aware loop free alternates (LFAs).

The flexible algorithm LFA configuration (for example, LFA, remote-LFA or TI-LFA) inherits the LFA configuration for base SPF algorithm 0.

LFAs are administratively disabled for flexible algorithms in which IS-IS is participating. LFAs must be explicitly enabled using the **loopfree-alternates** command.

The **no** form of this command disables LFAs for the specific flexible algorithm in which the router is participating.

Default no loopfree-alternates

Platforms All

loopfree-alternates

Syntax [**no**] **loopfree-alternates**

Context **[Tree]** (config>router>isis loopfree-alternates)

Full Context configure router isis loopfree-alternates

Description This command enables Loop-Free Alternate (LFA) computation by SPF for the IS-IS routing protocol.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary nexthop and an LFA next-hop for every learned prefix. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The user enables the remote LFA next-hop calculation by the IGP LFA SPF by appending the remote-lfa option. When this option is enabled in an IGP instance, SPF performs the remote LFA additional computation following the regular LFA next-hop calculation when the latter resulted in no protection for one or more prefixes which are resolved to a given interface.

Remote LFA extends the protection coverage of LFA-FRR to any topology by automatically computing and establishing/tearing-down shortcut tunnels, also referred to as repair tunnels, to a remote LFA node which puts the packets back into the shortest without looping them back to the node which forwarded them over the repair tunnel. The remote LFA node is referred to as PQ node. A repair tunnel can in theory be an RSVP LSP, a LDP-in-LDP tunnel, or a SR tunnel. In this feature, it is restricted to use SR repair tunnel to the remote LFA node.

The remote LFA algorithm is a per-link LFA SPF calculation and not a per-prefix like the regular LFA one. So, it provides protection for all destination prefixes which share the protected link by using the neighbor on the other side of the protected link as a proxy for all these destinations.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The Topology-Independent LFA (TI-LFA) further improves the protection coverage of a network topology by computing and automatically instantiating a repair tunnel to a Q node which is not in shortest path from the computing node. The repair tunnel uses shortest path to the P node and a source routed path from the P node to the Q node.

In addition, the TI-LFA algorithm selects the backup path which matches the post-convergence path. This helps the capacity planning in the network since traffic will always flow on the same path when transitioning to the FRR next-hop and then onto the new primary next-hop.

At a high level, the TI-LFA protection algorithm is searching for a candidate P-Q set separated with a number of hops such that the label stack size does not exceed the value of **ti-lfa max-sr-frr-labels**, on each of the post-convergence paths to each destination node or prefix D.

When the **ti-lfa** option is enabled in IS-IS, it provides TI-LFA node-protect or link-protect backup path in IS-IS MT=0 for an SR-ISIS IPV4/IPv6 tunnel (node SID and adjacency SID), for an IPv4 SR-TE LSP, and for LDP IPv4 FEC when the LDP **fast-reroute backup-sr-tunnel** option is enabled.

The **max-sr-frr-labels** parameter is used to limit the search for the TI-LFA backup next-hop:

a. 0 — The IGP LFA SPF restricts the search to TI-LFA backup next-hop which does not require a repair tunnel, meaning that P node and Q node are the same and match a neighbor. This is also the case when both P and Q node match the advertising router for a prefix.
b. 1 to 3 — The IGP LFA SPF will widen the search to include a repair tunnel to a P node which itself is connected to the Q nodes with a 0-to-2 hops for a total of maximum of three labels: one node SID to P node and two adjacency SIDs from P node to the Q node. If the P node is a neighbor of the computing node, its node SID is compressed and meaning that up to three adjacency SIDs can separate the P and Q nodes.
c. 2 (default) — Corresponds to a repair tunnel to a non-adjacent P which is adjacent to the Q node. If the P node is a neighbor of the computing node, then the node SID of the P node is compressed and the default value of two labels corresponds to two adjacency SIDs between the P and Q nodes.

When the **node-protect** command is enabled, the router will prefer a node-protect over a link-protect repair tunnel for a given prefix if both are found in the Remote LFA or TI-LFA SPF computations. The SPF computations may only find a link-protect repair tunnel for prefixes owned by the protected node. This node-protect backup protects against the failure of a downstream node in the path of the prefix of a node SID except for the node owner of the node SID.

The parameter **max-pq-nodes** in Remote LFA controls the maximum number of PQ nodes found in the LFA SPFs for which the node protection check is performed. The node-protect condition means the router must run the original Remote LFA algorithm plus one extra forward SPF on behalf of each PQ node found, potentially after applying the **max-pq-cost** parameter, to check if the path from the PQ node to the destination does not traverse the protected node. Setting this parameter to a lower value means the LFA SPFs will use less computation time and resources but may result in not finding a node-protect repair tunnel.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the LFA computation by IGP SPF.

Default no loopfree-alternates

Platforms All

loopfree-alternates

Syntax [**no**] **loopfree-alternates**

Context **[Tree]** (config>router>ospf loopfree-alternates)
[Tree] (config>router>ospf3 loopfree-alternates)

Full Context configure router ospf loopfree-alternates
configure router ospf3 loopfree-alternates

Description This command enables Loop-Free Alternate (LFA) computation by SPF under the OSPF or OSPFv3 routing protocol instance.

When this command is enabled, it instructs the IGP SPF to attempt to precalculate both a primary next hop and an LFA next hop for every learned prefix. When found, the LFA next hop is populated into the routing table along with the primary next hop for the prefix.

The user enables the remote LFA next hop calculation by the IGP LFA SPF by appending the **remote-lfa** option. When this option is enabled in an IGP instance, SPF performs the remote LFA additional computation following the regular LFA next hop calculation when the latter resulted in no protection for one or more prefixes which are resolved to a particular interface.

Remote LFA extends the protection coverage of LFA-FRR to any topology by automatically computing and establishing or tearing down shortcut tunnels, also referred to as repair tunnels, to a remote LFA node that puts the packets back into the shortest path without looping them back to the node that forwarded them over the repair tunnel. The remote LFA node is referred to as a PQ node. A repair tunnel can, in theory, be an RSVP-TE LSP, an LDP-in-LDP tunnel, or a segment routing (SR) tunnel. In this command, **remote-lfa** is restricted to using an SR repair tunnel to the remote LFA node.

The remote LFA algorithm is a per-link LFA SPF calculation and not a per-prefix calculation like the regular LFA algorithm. The remote LFA algorithm provides protection for all destination prefixes that share the protected link by using the neighbor on the other side of the protected link as a proxy for all the destinations.

The Topology-Independent LFA (TI-LFA) further improves the protection coverage of a network topology by computing and automatically instantiating a repair tunnel to a Q node which is not in shortest path from the computing node. The repair tunnel uses shortest path to the P node and a source routed path from the P node to the Q node.

In addition, the TI-LFA algorithm selects the backup path which matches the post-convergence path. This helps the capacity planning in the network since traffic will always flow on the same path when transitioning to the FRR next hop and then onto the new primary next hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

At a high level, the TI-LFA protection algorithm is searching for a candidate P-Q set separated with a number of hops such that the label stack size does not exceed the value of **ti-lfa max-sr-frr-labels**, on each of the post-convergence paths to each destination node or prefix D.

When the **ti-lfa** option is enabled in OSPF, it provides TI-LFA node-protect or link-protect backup path for a SR-OSPF IPV4 tunnel (node SID and adjacency SID), and for a IPv4 SR-TE LSP.

The **max-sr-frr-labels** parameter is used to limit the search for the TI-LFA backup next hop:

a. 0 — The IGP LFA SPF restricts the search to TI-LFA backup next hop which does not require a repair tunnel, meaning that P node and Q node are the same and match a neighbor. This is also the case when both P and Q node match the advertising router for a prefix.
b. 1 to 3 — The IGP LFA SPF will widen the search to include a repair tunnel to a P node which itself is connected to the Q nodes with a 0-to-2 hops for a total of maximum of three labels: one node SID to P node and two adjacency SIDs from P node to the Q node. If the P node is a neighbor of the computing node, its node SID is compressed and meaning that up to three adjacency SIDs can separate the P and Q nodes.
c. 2 (default) — Corresponds to a repair tunnel to a non-adjacent P which is adjacent to the Q node. If the P node is a neighbor of the computing node, then the node SID of the P node is compressed and the default value of two labels corresponds to two adjacency SIDs between the P and Q nodes.

The TI-LFA repair tunnel can have a maximum of three labels pushed in addition to the label of the destination node or prefix. The user can set a lower maximum value for the additional FRR labels by configuring the CLI option **max-sr-frr-labels** *labels*. The default value is 2.

When the **node-protect** command is enabled, the router will prefer a node-protect over a link-protect repair tunnel for a given prefix if both are found in the Remote LFA or TI-LFA SPF computations. The SPF computations may only find a link-protect repair tunnel for prefixes owned by the protected node. This node-protect backup protects against the failure of a downstream node in the path of the prefix of a node SID except for the node owner of the node SID.

The parameter **max-pq-nodes** in Remote LFA controls the maximum number of PQ nodes found in the LFA SPFs for which the node protection check is performed. The node-protect condition means the router must run the original Remote LFA algorithm plus one extra forward SPF on behalf of each PQ node found, potentially after applying the **max-pq-cost** parameter, to check if the path from the PQ node to the destination does not traverse the protected node. Setting this parameter to a lower value means the LFA SPFs will use less computation time and resources but may result in not finding a node-protect repair tunnel.

The **no** form of this command disables the LFA computation by the IGP SPF.

Default no loopfree-alternates

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.239 loss

loss

Syntax **loss**

Context **[Tree]** (config>oam-pm>session>ip>twamp-light loss)

Full Context configure oam-pm session ip twamp-light loss

Description Commands in this context configure loss parameters for the TWAMP-Light test.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.240 loss-event

loss-event

Syntax **loss-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
no loss-event

Context **[Tree]** (config>saa>test loss-event)

Full Context configure saa test loss-event

Description Specifies that at the termination of an SAA test run, the calculated loss event value is evaluated against the configured rising and falling loss event thresholds. SAA threshold events are generated as required.

The configuration of loss event thresholds is optional.

The **no** form of this command disables the loss-event test run.

Parameters **rising-threshold** *threshold* — Specifies a rising threshold loss event value, in packets. When the test run is completed, the calculated loss event value is compared to the configured loss event rising threshold. If the test run loss event value is greater than the configured rising threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Values 0 to 2147483647

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

falling-threshold *threshold* — Specifies a falling threshold loss event value, in packets. When the test run is completed, the calculated loss event value is compared to the configured loss event falling threshold. If the test run loss event value is greater than the configured falling threshold value then an SAA threshold event is generated. The SAA threshold event is tmnxOamSaaThreshold, logger application OAM, event #2101.

Values 0 to 2147483647

Default 0

direction — Specifies the direction for OAM ping responses received for an OAM ping test run.

Values **inbound** — Monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run.

outbound — Monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run.

roundtrip — Monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run.

Default roundtrip

Platforms All

16.241 loss-events

loss-events

Syntax [**no**] **loss-events**

Context **[Tree]** (config>oam-pm>session>measurement-interval>event-mon loss-events)

Full Context configure oam-pm session measurement-interval event-mon loss-events

Description This enables the monitoring of all configured loss events. Adding this functionality starts the monitoring of the configured loss events at the start of the next measurement interval. If the function is removed using the **no** command, all monitoring of configured loss events, logging, and recording of new events for that session are suspended. Any existing events at the time of the shut down are maintained until the active measurement window in which the removal was performed has completed. The state of this monitoring function can be changed without having to shut down all the tests in the session.

The **no** form of this command disables the monitoring of all configured loss events.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

loss-events

Syntax **loss-events**

Context **[Tree]** (config>oam-pm>session>ethernet>slm loss-events)
[Tree] (config>oam-pm>session>ethernet>lmm loss-events)
[Tree] (config>oam-pm>session>ip>twamp-light loss-events)

Full Context configure oam-pm session ethernet lmm loss-events
configure oam-pm session ethernet slm loss-events
configure oam-pm session ip twamp-light loss-events

Description This context allows the operator to define the loss events and thresholds that are to be tracked.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events

All

- configure oam-pm session ethernet lmm loss-events
- configure oam-pm session ethernet slm loss-events

16.242 low

low

Syntax **low**

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2>prim-path>queue>drop-tail low)
[Tree] (config>mcast-mgmt>bw-plcy>t2>sec-path>queue>drop-tail low)

Full Context configure mcast-management bandwidth-policy t2-paths primary-path queue-parameters drop-tail low
configure mcast-management bandwidth-policy t2-paths secondary-path queue-parameters drop-tail low

Description Commands in this context configure the queue low drop-tail parameters. The low drop-tail defines the queue depth beyond which out-of-profile packets are not accepted into the queue and are discarded.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

low

Syntax **low**

Context [Tree] (config>service>ies>if>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue>drop-tail low)
[Tree] (config>service>vpls>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue>drop-tail low)

Full Context configure service ies interface sap egress queue-override queue drop-tail low
configure service ies interface sap ingress queue-override queue drop-tail low
configure service vpls sap egress queue-override queue drop-tail low
configure service vpls sap ingress queue-override queue drop-tail low

Description Commands in this context configure the queue **low drop-tail** parameters. The low drop tail defines the queue depth beyond which out-of-profile packets are not accepted into the queue and are discarded.

Platforms All

low

Syntax **low**

Context [Tree] (config>port>eth>access>ing>qgrp>qover>q>drop-tail low)
[Tree] (config>port>eth>access>egr>qgrp>qover>q>drop-tail low)
[Tree] (config>port>ethernet>network>egr>qgrp>qover>q>drop-tail low)

Full Context configure port ethernet access egress queue-group queue-overrides queue drop-tail low
configure port ethernet access ingress queue-group queue-overrides queue drop-tail low
configure port ethernet network egress queue-group queue-overrides queue drop-tail low

Description Commands in this context configure the queue low drop tail parameters. The low drop tail defines the queue depth beyond which out-of-profile packets will not be accepted into the queue and will be discarded.

Platforms All

low

Syntax **low**

Context [Tree] (config>service>apipe>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue>drop-tail low)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue>drop-tail low)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue>drop-tail low)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ipipe>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue>drop-tail low)
[Tree] (config>service>epipe>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue>drop-tail low)

Full Context configure service apipe sap egress queue-override queue drop-tail low
configure service apipe sap ingress queue-override queue drop-tail low
configure service cpipe sap egress queue-override queue drop-tail low
configure service cpipe sap ingress queue-override queue drop-tail low
configure service epipe sap egress queue-override queue drop-tail low
configure service epipe sap ingress queue-override queue drop-tail low
configure service fpipe sap egress queue-override queue drop-tail low
configure service fpipe sap ingress queue-override queue drop-tail low
configure service ipipe sap egress queue-override queue drop-tail low
configure service ipipe sap ingress queue-override queue drop-tail low

Description Commands in this context configure the queue low drop-tail parameters. The low drop tail defines the queue depth beyond which out-of-profile packets are not accepted into the queue and will be discarded.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress queue-override queue drop-tail low
- configure service fpipe sap egress queue-override queue drop-tail low
- configure service fpipe sap ingress queue-override queue drop-tail low
- configure service cpipe sap egress queue-override queue drop-tail low

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue drop-tail low
- configure service apipe sap ingress queue-override queue drop-tail low

All

- configure service ipipe sap ingress queue-override queue drop-tail low
- configure service epipe sap ingress queue-override queue drop-tail low
- configure service epipe sap egress queue-override queue drop-tail low
- configure service ipipe sap egress queue-override queue drop-tail low

low

Syntax **low**

Context [Tree] (config>service>vprn>if>sap>egress>queue-override>queue>drop-tail low)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue>drop-tail low)

Full Context configure service vprn interface sap egress queue-override queue drop-tail low
configure service vprn interface sap ingress queue-override queue drop-tail low

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the queue low drop tail parameters. The low drop tail defines the queue depth beyond which out-of-profile packets are not accepted into the queue and will be discarded.

Platforms All

low

Syntax **low**

Context **[Tree]** (config>qos>sap-egress>queue>drop-tail low)
[Tree] (config>qos>sap-ingress>queue>drop-tail low)

Full Context configure qos sap-egress queue drop-tail low
configure qos sap-ingress queue drop-tail low

Description Commands in this context configure the queue low drop-tail parameters. The low drop tail defines the queue depth beyond which out-of-profile packets will not be accepted into the queue and will be discarded.

Platforms All

low

Syntax **low**

Context **[Tree]** (config>qos>network-queue>queue>drop-tail low)

Full Context configure qos network-queue queue drop-tail low

Description Commands in this context configure the queue low drop tail parameters. The low drop tail defines the queue depth beyond which out-of-profile packets will not be accepted into the queue and will be discarded.

Platforms All

low

Syntax **low**

Context **[Tree]** (config>qos>qgrps>ing>qgrp>queue>drop-tail low)
[Tree] (config>qos>qgrps>egr>qgrp>queue>drop-tail low)

Full Context configure qos queue-group-templates egress queue-group queue drop-tail low
configure qos queue-group-templates ingress queue-group queue drop-tail low

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the queue low drop-tail parameters. The low drop tail defines the queue depth beyond which out-of-profile packets will not be accepted into the queue and will be discarded.

Platforms All

low

Syntax **low**

Context **[Tree]** (config>qos>shared-queue>queue>drop-tail low)

Full Context configure qos shared-queue queue drop-tail low

Description Commands in this context configure the queue low drop-tail parameters. The low drop-tail defines the queue depth beyond which out-of-profile packets will not be accepted into the queue and will be discarded.

Platforms All

16.243 low-burst-max-class

low-burst-max-class

Syntax **low-burst-max-class** *class*
no low-burst-max-class

Context **[Tree]** (config>port>ethernet>egress>hs-sec-shaper>agg low-burst-max-class)

Full Context configure port ethernet egress hs-secondary-shaper aggregate low-burst-max-class

Description This command specifies which scheduling classes map to the low burst-limit threshold of an egress HS secondary shaper. Egress SAPs can be configured to use an HS secondary shaper that manages their maximum burst limit over a specified aggregate shaping rate. Each HS secondary shaper supports two thresholds, a low burst limit threshold and a high burst limit threshold.

By default, all scheduling classes are mapped to the low burst limit threshold. It is important to note that when mapping scheduling classes to the high burst limit threshold an adequate value for the **card>fp>egress>hs-fixed-high-thresh-delta** must be specified. This is due to the fact that the queues associated with the lower classes may burst over the lower threshold in normal operation due to the scheduler forwarding whole packets. The **hs-fixed-high-thresh-delta** value should be set to at least two times the maximum frame size to prevent lower threshold class forwarding from also affecting the higher threshold classes when forwarding larger packet sizes. An insufficient high threshold delta defeats the intended purpose of mapping classes to the higher threshold.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The system utilizes the lowest value attainable for each low threshold aggregate burst limit without causing shaper underrun conditions. The high burst limit threshold is determined by adding the **hs-fixed-high-thresh-delta** value configured in the **config>card>fp>egress** context to the aggregate's low burst limit threshold value.

The low-burst-max-class value can be changed at any time for an HS secondary shaper.

The **no** form of this command restores the HS secondary shaper's aggregate low burst limit threshold maximum scheduling class mapping to the default value. This causes all sets of queues associated with the hs-secondary-shaper secondary-shaper-name to have all scheduling classes mapped to the low burst limit threshold.

Default low-burst-max-class 6

Parameters *class* — Specifies the low burst maximum class. This parameter is required when executing the **low-burst-max-class** command. The parameter reflects the highest scheduling class that will be associated with the low burst limit threshold associated with the HS secondary aggregate shaper. Scheduling classes higher than scheduling class ID will be associated with the high burst limit threshold.

Values 1 to 6

Platforms 7750 SR-7/12/12e

low-burst-max-class

Syntax **low-burst-max-class** *class*
no low-burst-max-class

Context **[Tree]** (config>qos>hs-attachment-policy low-burst-max-class)

Full Context configure qos hs-attachment-policy low-burst-max-class

Description This command specifies which scheduling classes map to the low burst-limit threshold of the queue-level aggregate shaper. Each egress SAP or subscriber SLA profile instance (SPI), per port set of network interface queues and egress queue group template instance has an aggregate shaper that manages the maximum burst limit over a specified shaping rate. Each aggregate shaper supports two thresholds. As the scheduling rate for the set of queues increases, eventually the aggregate rate exceeds the rate limit and the aggregate burst limit starts to be consumed. If this continues, the low burst limit threshold is exceeded and the queues mapped to the scheduling classes associated with low threshold are removed from the scheduler. If the remaining aggregate rate (from the higher scheduling classes) continues to exceed the shaping rate, then the burst limit continues to be consumed and eventually the high burst limit threshold is exceeded. This causes the queues for all scheduling classes to be removed from the scheduler.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The second (high) threshold exists to allow the higher priority classes to continue to forward, thereby mitigating the effects of low priority bursts beyond the aggregate shaping rate. Typically, the higher scheduling class queues are either individually rate-limited so their aggregate allowed throughput is less than the aggregate rate or the expected aggregate unshaped traffic from the individual higher scheduling classes does not exceed the aggregate shaping rate. Determining the value of **low-burst-max-class** class involves anticipating the proper dividing line between the low and high scheduling classes by evaluating the forwarding behavior and SLA enforcement of each class.

By default, all scheduling classes are mapped to the low burst limit threshold. When mapping scheduling classes to the high burst limit threshold, an adequate value for the **card>fp>egress>hs-fixed-high-thresh-delta** must be specified. This is due to the fact that the queues associated with the lower classes may burst over the lower threshold in normal operation due to the scheduler forwarding whole packets. Set the **hs-fixed-highthresh-delta** value to at least two times the maximum frame size to prevent lower threshold class forwarding from also affecting the higher threshold classes when forwarding larger packet sizes. An insufficient high threshold delta defeats the intended purpose of mapping classes to the higher threshold.

The system utilizes the lowest value attainable for each low threshold aggregate burst limit without causing shaper underrun conditions. The high burst limit threshold is determined by adding the **hs-fixed-high-thresh-delta** value configured in the **config>card>fp>egress** CLI context to the aggregate's low burst limit threshold value.

The **low-burst-max-class** value can be changed at any time in the HS attachment policy. Modifying the setting causes all queue aggregate shapers to reconfigure the scheduling class mappings to the low and high burst limit thresholds to reflect the new value for scheduling class ID.

Scheduling Classes — As described in the **queue** and **wrr-group** attachment commands, each queue is either directly or indirectly (through a WRR group) mapped to a scheduling class. Each scheduling class has an inherent priority at the port scheduler. The inherent descending priority is as follows:

- Scheduling Class 6 (Highest)
- Scheduling Class 5
- Scheduling Class 4
- Scheduling Class 3
- Scheduling Class 2
- Scheduling Class 1 (lowest)

Placing scheduling classes into the port level WRR group causes those classes to compete for scheduling opportunities based on their associated weights instead of inherent priority. If higher weights are given to higher scheduling class IDs, then the relative proportional scheduling priority may continue to exhibit the priority level indicated by the class ID.

Setting Low and High Burst Limit Threshold Association — Table 76 demonstrates the effect of the **low-burst-max-class** command parameters on scheduling class mappings to the low and high burst limit thresholds.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 76 **Low and High Burst Limit Threshold Association**

low-burst-max-class *sched-class*	**Scheduling Classes on Low Threshold**	**Scheduling Classes on High Threshold**
1	1	2, 3, 4, 5, and 6
2	1 and 2	3, 4, 5, and 6
3	1, 2, and 3	4, 5, and 6
4	1, 2, 3, and 4	5 and 6
5	1, 2, 3, 4, and 5	6
6	1, 2, 3, 4, 5, and 6	—

The **no** form of the command restores the queue aggregate low burst limit threshold maximum scheduling class mapping to the default value. This causes all sets of queues associated with the specified **hs-attachment-policy** *policy-name* to have all scheduling classes mapped to the low burst limit threshold.

Default low-burst-max-class 6

Parameters *class* — Specifies the low burst maximum class. This parameter is required when executing the **low-burst max-class** command. The parameter reflects the highest scheduling class that is associated with the low burst limit threshold associated with the queue aggregate shaper. Scheduling classes higher than the scheduling class ID are associated with the high burst limit threshold.

Values 1 to 6

Platforms 7750 SR-7/12/12e

16.244 low-octets-discarded-count

low-octets-discarded-count

Syntax [**no**] **low-octets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters low-octets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters low-octets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters low-octets-discarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters low-octets-discarded-count

Description This command includes the low octets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv6 octets discarded count instead.

The **no** form of this command excludes the low octets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

low-octets-discarded-count

Syntax [**no**] **low-octets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters low-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters low-octets-discarded-count)

Full Context configure log accounting-policy custom-record queue i-counters low-octets-discarded-count
configure log accounting-policy custom-record ref-queue i-counters low-octets-discarded-count

Description This command includes the low octets discarded count.

The **no** form of this command excludes the low octets discarded count.

Default no low-octets-discarded-count

Platforms All

16.245 low-octets-offered-count

low-octets-offered-count

Syntax [**no**] **low-octets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-count low-octets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-count low-octets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters low-octets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters low-octets-offered-count

Description This command includes the low octets discarded count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command excludes the low octets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

low-octets-offered-count

Syntax [**no**] **low-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters low-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters low-octets-offered-count)

Full Context configure log accounting-policy custom-record queue i-counters low-octets-offered-count
configure log accounting-policy custom-record ref-queue i-counters low-octets-offered-count

Description This command includes the low octets discarded count.

The **no** form of this command excludes the low octets discarded count.

Default no low-octets-offered-count

Platforms All

16.246 low-packets-discarded-count

low-packets-discarded-count

Syntax [**no**] **low-packets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters low-packets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters
low-packets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters
low-packets-discarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters
low-packets-discarded-count

Description This command includes the low packets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv6 packets discarded count instead.

The **no** form of this command excludes the low packets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

low-packets-discarded-count

Syntax [**no**] **low-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters low-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters low-packets-discarded-count)

Full Context configure log accounting-policy custom-record queue i-counters low-packets-discarded-count
configure log accounting-policy custom-record ref-queue i-counters low-packets-discarded-count

Description This command includes the low packets discarded count.

The **no** form of this command excludes the low packets discarded count.

Default no low-packets-discarded-count

Platforms All

16.247 low-packets-offered-count

low-packets-offered-count

Syntax [**no**] **low-packets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-count low-packets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-count low-packets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters low-packets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters low-packets-offered-count

Description This command includes the low packets discarded count.

The **no** form of this command excludes the low packets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

low-packets-offered-count

Syntax [**no**] **low-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>queue>i-counters low-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters low-packets-offered-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log accounting-policy custom-record queue i-counters low-packets-offered-count
configure log accounting-policy custom-record ref-queue i-counters low-packets-offered-count

Description This command includes the low packets discarded count.

The **no** form of this command excludes the low packets discarded count.

Default no low-packets-offered-count

Platforms All

16.248 low-priority-defect

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep low-priority-defect)
[Tree] (config>eth-tunnel>path>eth-cfm>mep low-priority-defect)

Full Context configure eth-ring path eth-cfm mep low-priority-defect
configure eth-tunnel path eth-cfm mep low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default low-priority-defect remErrXcon

Parameters **low-priority-defect** — Specifies the lowest priority defect using the following:

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon**}

Context **[Tree]** (config>lag>eth-cfm>mep>ais low-priority-defect)

Full Context configure lag eth-cfm mep ais-enable low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default low-priority-defect remErrXcon

Parameters **allDef** | **macRemErrXcon** — Specifies the lowest priority defect.

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context **[Tree]** (config>lag>eth-cfm>mep>eth-test low-priority-defect)
[Tree] (config>port>ethernet>eth-cfm>mep>eth-test low-priority-defect)

Full Context configure lag eth-cfm mep eth-test low-priority-defect
configure port ethernet eth-cfm mep eth-test low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm. This setting is also used to determine the fault state of the MEP which, when enabled to do so, causes a network reaction.

Default low-priority-defect macRemErrXcon

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon** — Specifies the lowest priority defect.

Values allDefDefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM macRemErrXconOnly DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM remErrXcon Only DefRemoteCCM, DefErrorCCM, and DefXconCCM errXcon Only DefErrorCCM and DefXconCCM xconOnly DefXconCCM; or noXconNo defects DefXcon or lower are to be reported

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon**}

Context **[Tree]** (config>port>ethernet>eth-cfm>mep>ais low-priority-defect)
[Tree] (config>service>epipe>sap>eth-cfm>mep>ais low-priority-defect)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>ais low-priority-defect)
[Tree] (cfg>service>vpls>mesh-sdp>eth-cfm>mep>ais low-priority-defect)

Full Context configure service vpls mesh-sdp eth-cfm mep ais-enable low-priority-defect
configure port ethernet eth-cfm mep ais-enable low-priority-defect
configure service epipe sap eth-cfm mep ais-enable low-priority-defect
configure service epipe spoke-sdp eth-cfm mep ais-enable low-priority-defect

Description This command allows the operator to include all CCM Defect conditions or exclude the Remote Defect Indication CCM (DefRDICCM) as a trigger for generating AIS. AIS generation can only occur when the client-meg-level configuration option has been included. Changing this parameter will evaluate the MEP for AIS triggers based on the new criteria.

Parameters **allDef** — Keyword that includes any CCM defect condition to trigger AIS generation.

macRemErrXcon — Keyword that excludes RDI CCM Defect condition to trigger AIS generation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context **[Tree]** (config>service>epipe>spoke-sdp>eth-cfm>mep low-priority-defect)
[Tree] (config>service>epipe>sap>eth-cfm>mep low-priority-defect)
[Tree] (config>service>ipipe>sap>eth-cfm>mep low-priority-defect)

Full Context configure service epipe sap eth-cfm mep low-priority-defect
configure service epipe spoke-sdp eth-cfm mep low-priority-defect
configure service ipipe sap eth-cfm mep low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default low-priority-defect macRemErrXcon

Parameters **low-priority-defect** — The low priority defect values are defined as follows:

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM
noXcon	No defects DefXcon or lower are to be reported

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon**}

Context **[Tree]** (config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable low-priority-defect)

Full Context configure service vpls spoke-sdp eth-cfm mep ais-enable low-priority-defect

Description This command allows the operator to include all CCM Defect conditions or exclude the Remote Defect Indication CCM (DefRDICCM) as a trigger for generating AIS. AIS generation can only occur when the client-meg-level configuration option has been included. Changing this parameter will evaluate the MEP for AIS triggers based on the new criteria.

Parameters **allDef** — Keyword that includes any CCM defect condition to trigger AIS generation.

macRemErrXcon — Keyword that excludes RDI CCM Defect condition to trigger AIS generation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm>mep low-priority-defect)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep low-priority-defect)

Full Context configure service vpls mesh-sdp eth-cfm mep low-priority-defect
configure service vpls spoke-sdp eth-cfm mep low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default low-priority-defect macRemErrXcon

Parameters **low-priority-defect** — The low priority defect values are defined below.

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep low-priority-defect)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep low-priority-defect)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep low-priority-defect)

Full Context configure service ies interface sap eth-cfm mep low-priority-defect
configure service ies interface spoke-sdp eth-cfm mep low-priority-defect
configure service ies subscriber-interface group-interface sap eth-cfm mep low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default low-priority-defect macRemErrXcon

Parameters **low-priority-defect** — The following values are used to specify the lowest priority defect that is allowed to generate a fault alarm.

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, efErrorCCM, and DefXconCCM
macRemErrXcon	only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	only DefErrorCCM and DefXconCCM
xcon	only DefXconCCM; or
noXcon	no defects DefXcon or lower are to be reported

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep low-priority-defect

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep low-priority-defect
- configure service ies interface sap eth-cfm mep low-priority-defect

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep low-priority-defect)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep low-priority-defect)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm low-priority-defect)

Full Context configure service vprn interface sap eth-cfm mep low-priority-defect
configure service vprn interface spoke-sdp eth-cfm mep low-priority-defect
configure service vprn subscriber-interface group-interface sap eth-cfm low-priority-defect

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default low-priority-defect macRemErrXcon

Parameters *parameters* — Specifies the lowest priority defect.

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

low-priority-defect

Syntax **low-priority-defect** *low-priority-defect*

Context **[Tree]** (config>router>if>eth-cfm>mep low-priority-defect)

Full Context configure router interface eth-cfm mep low-priority-defect

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the lowest priority defect that generates a fault alarm. This setting is also used to determine the fault state of the MEP which, when enabled to do so, causes a network reaction.

Default low-priority-defect macRemErrXcon

Parameters *low-priority-defect* — Specifies the lowest priority defect.

Values allDef, macRemErrXcon, remErrXcon, errXcon, xcon, noXcon

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.249 low-slope

low-slope

Syntax [**no**] **low-slope**

Context **[Tree]** (config>qos>slope-policy low-slope)

Full Context configure qos slope-policy low-slope

Description The **low-slope** context contains the commands and parameters for defining the low Random Early Detection (RED) slope graph. Each buffer pool supports a low RED slope for managing access to the shared portion of the buffer pool for low out-of-profile packets.

The **low-slope** parameters can be changed at any time and the affected buffer pool low RED slopes must be adjusted appropriately.

The **no** form of this command restores the low slope configuration commands to the default values. If the leaf commands within **low-slope** are set to the default parameters, the **low-slope** node will not appear in save config and show config output unless the detail parameter is present.

Platforms All

16.250 low-wmark

low-wmark

Syntax **low-wmark** *percent*

Context **[Tree]** (config>app-assure>group>dns-ip-cache>ip-cache low-wmark)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group dns-ip-cache ip-cache low-wmark

Description This command configures the low watermark value for the dns-ip-cache. If the dns-ip-cache has previously crossed the high-watermark value, the system will clear the trap in case the number of IP addresses stored in the cache crosses below the low watermark value.

Default low-wmark 80

Parameters *percent* — Specifies the low watermark value, in percent.

Values 0 to 100

Default 80

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.251 lower-bound

lower-bound

Syntax **lower-bound** *microseconds*
no lower-bound

Context **[Tree]** (config>oam-pm>bin-group>bin-type>bin lower-bound)

Full Context configure oam-pm bin-group bin-type bin lower-bound

Description This command allows the operator specify the individual floors thresholds for the bins. The operator does not have to specific a lower threshold for every bin that was previously defined by the bin-count for the specific type. By default, each bin is the bin-number times 5000 microseconds. Lower thresholds in the previous adjacent bin must be lower than the threshold of the next higher bin threshold. A separate line per bin is required to configure an operator-specific threshold. An error prevents the bin from entering the active state if this is not maintained, at the time the **no shutdown** is issued. Bin 0 is the result of the difference between 0 and the configured lower-threshold of bin 1. The highest bin in the bin-count captures every result above the threshold. Any negative delay metric result is treated as zero and placed in bin 0.

The **no** form of this command removes the user configured threshold value and applies the default for the bin.

Parameters *microseconds* — Specifies the threshold that defines the floor of the bin. The bin range is the difference between its configured threshold and the threshold of the next higher bin in microsecond threshold value.

Values 1 to 4294967295

Default bin-number * 5000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

16.252 lsa-accumulate

lsa-accumulate

Syntax **lsa-accumulate** *lsa-accumulate*
no lsa-accumulate

Context **[Tree]** (config>router>ospf>timers lsa-accumulate)
[Tree] (config>router>ospf3>timers lsa-accumulate)

Full Context configure router ospf timers lsa-accumulate
configure router ospf3 timers lsa-accumulate

Description This command sets the internal OSPF delay to allow for the accumulation of multiple LSA so OSPF messages can be sent as efficiently as possible. The **lsa-accumulate** timer applies to all LSAs except Type 1 and Type 2 LSAs, which are sent immediately. LSAs are accumulated and then sent when:

- its size reaches the MTU size of the interface
- a new LSA is received on the interface
- the **lsa-accumulate** timer expires

Shorting this delay can speed up the advertisement of LSAs to OSPF neighbors but may increase the number of OSPF messages sent.

The **no** form of this command reverts to the default value.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is greater than or equal to 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default lsa-accumulate 1000

Parameters *lsa-accumulate* — Specifies the LSA accumulation delay in milliseconds.

Values 0 to 1000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.253 lsa-arrival

lsa-arrival

Syntax **lsa-arrival** *lsa-arrival-time*
no lsa-arrival

Context **[Tree]** (config>service>vprn>ospf>timers lsa-arrival)
[Tree] (config>service>vprn>ospf3>timers lsa-arrival)

Full Context configure service vprn ospf timers lsa-arrival
configure service vprn ospf3 timers lsa-arrival

Description This parameter defines the minimum delay that must pass between receipt of the same Link State Advertisements (LSAs) arriving from neighbors.

It is recommended that the neighbor's configured **lsa-generate** *lsa-second-wait* interval is equal to or greater than the **lsa-arrival** timer configured here.

Use the **no** form of this command to return to the default.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is ≥ 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default lsa-arrival 1000

Parameters *lsa-arrival-time* — Specifies the timer in milliseconds.

Values 0 to 600000

Platforms All

lsa-arrival

Syntax **lsa-arrival** *lsa-arrival-time*
no lsa-arrival

Context **[Tree]** (config>router>ospf>timers lsa-arrival)
[Tree] (config>router>ospf3>timers lsa-arrival)

Full Context configure router ospf timers lsa-arrival
configure router ospf3 timers lsa-arrival

Description This parameter defines the minimum delay that must pass between receipt of the same Link State Advertisements (LSAs) arriving from neighbors.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

It is recommended that the neighbors configured **lsa-generate** *lsa-second-wait* interval is equal or greater than the **lsa-arrival** timer configured here.

The **no** form of this command reverts to the default.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is greater than or equal to 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default lsa-arrival 1000

Parameters *lsa-arrival-time* — Specifies the timer, in milliseconds.

Values 0 to 600000

Platforms All

16.254 lsa-filter-out

lsa-filter-out

Syntax **lsa-filter-out** [**all** | **except-own-rtrlsa** | **except-own-rtrlsa-and-defaults**]
no lsa-filter-out

Context **[Tree]** (config>router>ospf>area>if lsa-filter-out)
[Tree] (config>router>ospf3>area>if lsa-filter-out)
[Tree] (config>service>vprn>ospf>area>if lsa-filter-out)
[Tree] (config>service>vprn>ospf3>area>if lsa-filter-out)

Full Context configure router ospf area interface lsa-filter-out
configure router ospf3 area interface lsa-filter-out
configure service vprn ospf area interface lsa-filter-out
configure service vprn ospf3 area interface lsa-filter-out

Description This command enables filtering of outgoing OSPF LSAs on the selected OSPFv2 or OSPFv3 interface. Three filtering options are provided:

- Do not flood any LSAs out the interface. This option is suitable if the neighbor is simply-connected and has a statically configured default route with the address of this interface as next-hop.
- Flood the router's own router-LSA out the interface and suppress all other flooded LSAs. This option is suitable if the neighbor is simply-connected and has a statically configured default route with a loopback or system interface address (contained in the router-LSA) as next-hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Flood the router's own router-LSA and all self-generated type-3, type-5 and type-7 LSAs advertising a default route (0/0) out the interface; suppress all other flooded LSAs. This option is suitable if the neighbor is simply-connected and does not have a statically configured default route.

The **no** form of this command disables OSPF LSA filtering (normal operation).

Default no lsa-filter-out

Platforms All

16.255 lsa-generate

lsa-generate

Syntax **lsa-generate** *max-lsa-wait* [lsa-initial-wait *lsa-initial-wait* [*lsa-second-wait lsa-second-wait*]]
no lsa-generate-interval

Context **[Tree]** (config>service>vprn>ospf>timers lsa-generate)
[Tree] (config>service>vprn>ospf3>timers lsa-generate)

Full Context configure service vprn ospf timers lsa-generate
configure service vprn ospf3 timers lsa-generate

Description This parameter customizes the throttling of OSPF LSA-generation. Timers that determine when to generate the first, second, and subsequent LSAs can be controlled with this command. Subsequent LSAs are generated at increasing intervals of the *lsa-second-wait* timer until a maximum value is reached.

Configuring the **lsa-arrival** interval to equal or less than the *lsa-second-wait* interval configured in the **lsa-generate** command is recommended.

The **no** form of this command reverts to the default.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is ≥ 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Parameters *max-lsa-wait* — Specifies the maximum interval, in milliseconds, between two consecutive occurrences of an LSA being generated.

Values 10 to 600000

Default 5000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsa-initial-wait — Specifies the first waiting period between link-state advertisements (LSA) originate(s), in milliseconds. When the LSA exceeds the **lsa-initial-wait** timer value and the topology changes, there is no wait period and the LSA is immediately generated.

When an LSA is generated, the initial wait period commences. If, within the specified **lsa-initial-wait** period and another topology change occurs, then the **lsa-initial-wait** timer applies.

Values 10 to 600000

Default 5000

lsa-second-wait — Specifies the hold time in milliseconds between the first and second LSA generation. The next topology change is subject to this second wait period. With each subsequent topology change, the wait time doubles (this is 2x the previous wait time). This assumes that each failure occurs within the relevant wait period.

Values 10 to 600000

Default 5000

Platforms All

lsa-generate

Syntax **lsa-generate** *max-lsa-wait* [**lsa-initial-wait** *lsa-initial-wait* [**lsa-second-wait** *lsa-second-wait*]]
no lsa-generate

Context **[Tree]** (config>router>ospf>timers lsa-generate)
[Tree] (config>router>ospf3>timers lsa-generate)

Full Context configure router ospf timers lsa-generate
configure router ospf3 timers lsa-generate

Description This parameter customizes the throttling of OSPF LSA-generation. Timers that determine when to generate the first, second, and subsequent LSAs can be controlled with this command. Subsequent LSAs are generated at increasing intervals of the *lsa-second-wait* timer until a maximum value is reached.

Configuring the **lsa-arrival** interval to equal or less than the *lsa-second-wait* interval configured in the **lsa-generate** command is recommended.

The **no** form of this command reverts to the default.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is greater than or equal to 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default lsa-generate 5000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *max-lsa-wait* — Specifies the maximum interval in milliseconds between two consecutive occurrences of an LSA being generated.

Values 10 to 600000

Default 5000

lsa-initial-wait — Specifies the first waiting period between link-state advertisements (LSA) originate(s), in milliseconds. When the LSA exceeds the **lsa-initial-wait** timer value and the topology changes, there is no wait period and the LSA is immediately generated.

When an LSA is generated, the initial wait period commences. If, within the specified **lsa-initial-wait** period and another topology change occurs, then the **lsa-initial-wait** timer applies.

Values 10 to 600000

Default 5000

lsa-second-wait — Specifies the hold time in milliseconds between the first and second LSA generation. The next topology change is subject to this second wait period. With each subsequent topology change, the wait time doubles (this is 2x the previous wait time). This assumes that each failure occurs within the relevant wait period.

Values 10 to 600000

Default 5000

Platforms All

16.256 lsdb

lsdb

Syntax [**no**] **lsdb** [*level-number*] [*system-id* | *lsp-id*]

Context **[Tree]** (debug>router>isis lsdb)

Full Context debug router isis lsdb

Description This command enables debugging for Link State DataBase (LSDB).

The **no** form of the command disables debugging.

Parameters *system-id* — When specified, only the specified system-id is debugged. Host name up to 38 characters.

lsp-id — When specified, only the specified lsp-id is debugged. Hostname up to 38 characters.

level-number — Specifies the interface level (1, 2, or 1 and 2).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

lsdb

Syntax **lsdb** [*type*] [*ls-id*] [*adv-rtr-id*] [**area** *area-id*]
no lsdb

Context **[Tree]** (debug>router>ospf lsdb)
[Tree] (debug>router>ospf3 lsdb)

Full Context debug router ospf lsdb
debug router ospf3 lsdb

Description This command enables debugging for an OSPF link-state database (LSDB).

Parameters *type* — Specifies the OSPF link-state database (LSDB) type.

Values in the **ospf** context — router, network, summary, asbr, extern, nssa, area-opaque, as-opaque, link-opaque
in the **ospf3** context — router, network, inter-area-pfx, inter-area-rtr, external, nssa, intra-area-pfx, rtr-info-link, rtr-info-area, rtr-info-as

ls-id — Specifies an LSA type specific field containing either a router ID or an IP address. It identifies the piece of the routing domain being described by the advertisement.

adv-rtr-id — Specifies the router identifier of the router advertising the LSA.

area *area-id* — Specifies a 32-bit integer uniquely identifying an area.

Values ip-address — a.b.c.d
area — 0 to 4294967295

Platforms All

16.257 lsn

lsn

Syntax [**no**] **lsn**

Context **[Tree]** (config>isa>wlan-gw-group>nat lsn)

Full Context configure isa wlan-gw-group nat lsn

Description This command enables Large Scale NAT (LSN).

The **no** form of this command disables LSN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

lsn

Syntax **lsn router** *router-instance* [**b4** *ipv6-address*] [**aftr** *ipv6-address*] **ip** *ip-address* **protocol** {**tcp** | **udp**} [**port** *port*] [**outside-ip** *ipv4-address*] [**outside-port** *port*] [**nat-policy** *nat-policy-name*]

no lsn router *router-instance* [**b4** *ipv6-address*] **ip** *ip-address* **protocol** {**tcp** | **udp**} **port** *port* [**nat-policy** *nat-policy-name*]

Context **[Tree]** (config>service>nat>fwd lsn)

Full Context configure service nat port-forwarding lsn

Description This command creates NAT static port forwards for LSN44, Ds-Lite and NAT64. Static port forwards (SPF) are static mappings created so that certain applications on the inside (private side) can be reached from host that are on the outside of the NAT. SPF statically map the subscriber (inside IP address in LSN44, CPE IPv6 address/prefix in DS-Lite and IPv6 prefix in NAT64), inside port and protocol to an outside IPv4 address, port and the same protocol.

If only the inside router, the inside IPv4/v6 address/prefix and the protocol are configured as parameters in the SPF request, the remaining fields in the mapping (outside port and outside IPv4 address) will be selected automatically by the node and reported in CLI once the command execution is completed.

Specifying the outside IPv4 address in the SPF request, mandates that all other, otherwise optional, parameters be also specified in the request (inside port and outside port). This creates a fully specified SPF request. Fully specified SPF request can be used in multi-chassis NAT redundancy deployments where the SPF is manually replicated between the SR OS nodes. In single chassis NAT deployments, fully specified SPF request is guaranteed to work only in the system with a single MS-ISA in it. Otherwise (multiple MS-ISAs in the system) a conflict may arise where two distinct inside IP addresses that may reside on separate MS-ISAs are requested to be mapped to the same outside IPv4 address. This will not be possible since the outside IPv4 address cannot be split across the MS-ISAs (each IP address, inside or outside, is tied to a single MS-ISA).

In non-fully specified SPF requests (missing the inside port and/or outside port and the outside IPv4 address within the SPF request), the outside IPv4 address selection will depend on the configuration of the outside port in the SPF request:

- If the outside port is not specified or is specified from the configured **port-forwarding-range** [1024..port-forwarding-range], then the outside IPv4 address will be the same as the outside IPv4 address in an existing dynamic mapping for the same subscriber. If the subscriber does not exist (no dynamic mappings exist at the time of SPF creation request), then the subscriber will be automatically created and an outside IPv4 address will be assigned. In case that the outside ports are not available from the outside IPv4 address of the corresponding dynamic mapping, then the SPF request will fail. In other words, the dynamic and static mappings (created in this manner) for the same subscriber must use the same outside IPv4 address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If the outside port from the well-known port range [0 to 1023] is requested, then the outside IPv4 address does not have to match the outside IPv4 address of an existing dynamic mapping for the same subscriber, but can instead be any outside IPv4 address.

If multiple NAT policies per inside routing context are used, then the NAT policy must be specified in the SPF creation request. This is needed so the SPF be created in the correct pool.

SPFs are disabled by default and they must be explicitly enabled by the **port-limits forwarding** command within the NAT policy.

Configured SPFs, unlike SPFs created with the **tools** commands, are preserved across reboots without having to configure persistency (**config>system>persistence>nat-port-forwarding**) since they are part of the configuration. When the pool is shutdown the SPFs are deactivated. When the pool is enabled (no shutdown), the SPFs (as created by the **tools** command or by configuration) are activated.

To avoid possible persistency related conflicts, SPFs can only be created using one method on a given node: either as configuration (the CLI **configure** branch) or using the **tools** command. For example: if a first SPF entry is created via CLI **tools** commands, the node prevents SPF creation via configuration (the CLI **configure** branch) and vice versa.

The **no** form of the command deletes NAT static port forwards for LSN44, Ds-Lite and NAT64.

Default none

Parameters **router** *router-instance* — This mandatory parameter specifies the inside routing instance; router name or service-id.

Values router-name, service-id

b4 *ipv6-address* — This optional parameter specifies the IPv6 address of the B4 element in DS-Lite.

Values <ipv6-address> : ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D

aftr *ipv6-address* — This optional parameter specifies IPv6 address of the AFTR element in DS-Lite.

Values <ip-address> : ipv4-address - a.b.c.d
ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

protocol {**tcp** | **udp**} — This mandatory parameter specifies the protocol to use, either TCP or UDP.

port *port* — This optional parameter specifies a source port.

Values 1 to 65535

outside-ip *ipv4-address* — This mandatory parameter specifies the outside IPv4 address. If the outside IPv4 address is specified, then all other optional parameters become mandatory.

outside-port *port* — This optional parameter specifies the outside port.

nat-policy *policy-name* — If multiple NAT policies are used inside the routing context, then the NAT policy should be specified in the SPF request so the SPF is created in the correct NAT pool. Otherwise, the default NAT policy from the inside routing context will be used.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

16.258 lsp

lsp

Syntax [**no**] **lsp** *lsp-name*

Context **[Tree]** (config>router>gmpls lsp)

Full Context configure router gmpls lsp

Description This command creates a GMPLS LSP that is signaled dynamically by the router.

When the LSP is created, the egress router must be specified using the **to** command and a **working-path** must be specified.

GMPLS LSPs are created in the administratively down (**shutdown**) state.

The **no** form of this command deletes the GMPLS LSP. All configuration information associated with this GMPLS LSP is lost. The GMPLS LSP must be administratively shut down before it can be deleted.

Parameters *lsp-name* — Specifies the identifier for the GMPLS LSP, up to 32 characters.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

lsp

Syntax [**no**] **lsp** *lsp-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ldp>targ-session>peer>tunneling lsp)

Full Context configure router ldp targeted-session peer tunneling lsp

Description This command configures a specific LSP destined to this peer and to be used for tunneling of LDP FEC over RSVP. A maximum of 4 RSVP LSPs can be explicitly used for tunneling LDP FECs to the T-LDP peer.

It is not necessary to specify any RSVP LSP in this context unless there is a need to restrict the tunneling to selected LSPs. All RSVP LSPs with a to address matching that of the T-LDP peer are eligible by default. The user can also exclude specific LSP names by using the ldp-over-rsvp exclude command in the **configure->router->mpls->lsp** *lsp-name* context.

Platforms All

lsp

Syntax [**no**] **lsp** *lsp-name*

Context [Tree] (config>router>ldp>targ-session>peer>mcast-tunneling lsp)

Full Context configure router ldp targeted-session peer mcast-tunneling lsp

Description This command configures a specific LSP destined to this peer and to be used for tunneling of multicast LDP FEC over RSVP.

Parameters *lsp-name* — Specifies the LSP name, up to 64 characters in length.

Platforms All

lsp

Syntax [**no**] **lsp** *lsp-name* **sender** *sender-address*

Context [Tree] (config>router>mpls>ingress-statistics lsp)

Full Context configure router mpls ingress-statistics lsp

Description This command configures statistics in the ingress data path of a terminating RSVP LSP at an egress LER. The LSP name must correspond to the name configured by the operator at the ingress LER. It must not contain the special character ":" which is used as a field separator by the ingress LER for encoding the LSP and path names into the RSVP session name field in the session_attribute object. The operator must execute the **no shutdown** for this command to effectively enable statistics.

The same set of counters is updated for packets received over any path of this LSP and over the lifetime of the LSP. In steady-state, the counters are updated for packets received over the active path of the LSP. The active path can be the primary path, one of the secondary paths, the FRR detour path, or the FRR bypass path when the tail-end node is also the MP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a hierarchy of LSPs is in use, statistics collection on the outermost label corresponding to the tunneling LSP and on the inner labels, corresponding to the tunneled LSPs are mutually exclusive. A consequence of this is that when the operator enables statistics collection on an RSVP LSP which is also used for tunneling LDP FECs with the LDP over RSVP feature, then statistics will be collected on the RSVP LSP only. There will be no statistics collected for an LDP FEC tunneled over this RSVP LSP and also egressing on the same node regardless if the operator enabled statistics collection on this FEC. When, the operator disables statistics collection on the RSVP LSP, then statistics collection, if enabled, will be performed on a tunneled LDP FEC.

The operator can enable statistics collection on a manual bypass terminating on the egress LER. However all LSPs which primary path is protected by the manual bypass will not collect statistics when they activate forwarding over the manual bypass. When, the operator disables statistics collection on the manual bypass LSP, then statistics collection on the protected LSP, if enabled, will continue when the bypass LSP is activated.

The **no** form of this command disables statistics for this RSVP LSP in the ingress data path and removes the accounting policy association from the LSP.

Parameters **sender-address** *ip-address* — Specifies a string of 15 characters representing the IP address of the ingress LER for the LSP.

lsp-name — Specifies the LSP name, up to 64 characters in length, as configured at the ingress LER.

Platforms All

lsp

Syntax [**no**] **lsp** *lsp-name* [**bypass-only** | **p2mp-lsp** | **mpls-tp** *src-tunnel-num* | **sr-te**]

Context **[Tree]** (config>router>mpls lsp)

Full Context configure router mpls lsp

Description This command creates an LSP that is either signaled dynamically by the router, or a statically provisioned MPLS-TP LSP.

When the LSP is created, the egress router must be specified using the **to** command and at least one **primary** or **secondary** path must be specified for signaled LSPs, or at least one working path for MPLS-TP LSPs. All other statements under the LSP hierarchy are optional.

LSPs are created in the administratively down (**shutdown**) state.

The **no** form of this command deletes the LSP. All configuration information associated with this LSP is lost. The LSP must be administratively shutdown before it can be deleted. The LSP must also be unbound from all SDPs before it can be deleted.

Parameters *lsp-name* — Specifies the name that identifies the LSP. The LSP name can be up to 64 characters long and must be unique.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bypass-only — Defines an LSP as a manual bypass LSP exclusively. When a path message for a new LSP requests bypass protection, the PLR first checks if a manual bypass tunnel satisfying the path constraints exists. If one if found, the router selects it. If no manual bypass tunnel is found, the router dynamically signals a bypass LSP in the default behavior. The CLI for this feature includes a knob that provides the user with the option to disable dynamic bypass creation on a per node basis.

p2mp-lsp — Defines an LSP as a point-to-multipoint LSP. The following parameters can be used with a P2MP LSP: adaptive, adspec, cspf, exclude, fast-reroute, from, hop-limit, include, metric, retry-limit, retry-timer, resignal-timer. The following parameters cannot be used with a P2MP LSP: primary, secondary, to, dest-global-id, dest-tunnel-number, working-tp-path, protect-tp-path.

This option is not supported on the 7450 ESS.

mpls-tp *src-tunnel-num* — Defines an LSP as an MPLS-TP LSP. The *src-tunnel-num* is a mandatory create time parameter for mpls-tp LSPs, and has to be assigned by the user based on the configured range of tunnel IDs. The following parameters can only be used with an MPLS-TP LSP: to, dest-global-id, dest-tunnel-number, working-tp-path, protect-tp-path. Other parameters defined for the above LSP types cannot be used.

sr-te — Defines an LSP of type Segment Routing Traffic Engineering (SR-TE) LSP. The user can associate an empty path or a path with strict or loose explicit hops with the primary path of the SR-TE LSP. A hop which corresponds to an adjacency SID must be identified with its far-end host IP address (next-hop) on the subnet. If the local end host IP address is provided, this hop is ignored since this router can have multiple adjacencies (next-hops) on the same subnet. A hop which corresponds to a node SID is identified by the prefix address. The user is only allowed to configure a primary path for the SR-TE LSP.

Platforms All

lsp

Syntax [**no**] **lsp**

Context **[Tree]** (config>oam-pm>session>mpls lsp)

Full Context configure oam-pm session mpls lsp

Description Commands in this context define the type of label switched path and the identification of the LSP for which packets traverse. Only a single LSP can be configured per session. Once an LSP has been configured, other LSP types under this context is blocked.

The **no** form of this command deletes the configured LSP under the context, when there are no active tests are executing under this session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsp

Syntax **lsp** *lsp-name*
no lsp

Context **[Tree]** (config>oam-pm>session>mpls>lsp>mpls-tp lsp)
[Tree] (config>oam-pm>session>mpls>lsp>rsvp lsp)

Full Context configure oam-pm session mpls lsp mpls-tp-static lsp
configure oam-pm session mpls lsp rsvp lsp

Description This command specifies the MPLS LSP to be tested.

Parameters *lsp-name* — Specifies the LSP name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

lsp

Syntax [**no**] **lsp** *lsp-name*

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter>rsvp-te lsp)
[Tree] (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter>sr-te lsp)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter rsvp-te lsp
configure router static-route-entry indirect tunnel-next-hop resolution-filter sr-te lsp

Description This command restricts the search for a resolving LSP to a specific set of named LSPs. Only those LSPs named in the associated name list will be searched for a match to resolve the associated static route.

Parameters *lsp-name* — Specifies the name of the LSP to be searched for a valid resolving tunnel for the static route's next-hop.

Platforms All

lsp

Syntax [**no**] **lsp** *lsp-name*

Context **[Tree]** (config>service>sdp lsp)

Full Context configure service sdp lsp

Description This command creates associations between one or more label switched paths (LSPs) and an Multi-Protocol Label Switching (MPLS) Service Distribution Point (SDP). This command is implemented *only* on MPLS-type encapsulated SDPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In MPLS SDP configurations *either* one or more LSP names can be specified *or* LDP can be enabled. The SDP **ldp** and **lsp** commands are mutually exclusive except if the mixed-lsp-mode option is also enabled. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the **no lsp lsp-name** command.

Alternatively, if LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. To specify an LSP on the SDP, the LDP must be disabled or the mixed-lsp-mode option is also enabled. The LSP must have already been created in the **config>router>mpls** context. with a valid far-end IP address. RSVP must be enabled.

If no LSP is associated with an MPLS SDP, the SDP cannot enter the operationally up state. The SDP can be administratively enabled (**no shutdown)** with no LSP associations. The *lsp-name* may be shutdown, causing the association with the SDP to be operationally down (the LSP will not be used by the SDP).

Up to 16 LSP names can be entered on a single command line.

The **no** form of this command deletes one or more LSP associations from an SDP. If the *lsp-name* does not exist as an association or as a configured LSP, no error is returned. An *lsp-name* must be removed from all SDP associations before the *lsp-name* can be deleted from the system. The SDP must be administratively disabled (**shutdown)** before the last *lsp-name* association with the SDP is deleted.

Parameters *lsp-name* — Specifies the name of the LSP to associate with the SDP. An LSP name is case sensitive and is limited to 32 ASCII 7-bit printable characters with no spaces. If an exact match of *lsp-name* does not already exist as a defined LSP, an error message is generated. If the *lsp-name* does exist and the LSP **to** IP address matches the SDP **far-end** IP address, the association is created.

Platforms All

16.259 lsp-bfd

lsp-bfd

Syntax **lsp-bfd** *prefix-list-name*
no lsp-bfd *prefix-list-name*

Context **[Tree]** (config>router>ldp lsp-bfd)

Full Context configure router ldp lsp-bfd

Description Commands in this context configure LSP BFD for a set of LDP LSPs with FECs matching those defined in the specified prefix list.

Up to 16 LSP BFD instances can be configured for LDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a prefix corresponding to an LDP FEC appears in more than one prefix list, then the system will apply the LSP BFD configuration to the LSP only once. A prefix list may contain a longest match corresponding to one or more LDP FECs, in which case the BFD configuration is applied to all of those LDP LSPs.

The **no** form of the command removes LSP BFD. Specifying a prefix list name will remove LSP BFD for all LDP FECs that match the specified prefix list, except those LDP FECs that also match another LSP BFD prefix list.

Default no lsp-bfd

Parameters *prefix-list-name* — Specifies the name of the prefix list configured using the **config**>**router**>**policy-options**>**prefix-list** *name* command, up to 32 characters maximum. The prefix list name can be specified by the **lsp-bfd** command prior to the prefix list being defined in the **config**>**router**>**policy-options** context.

Platforms All

lsp-bfd

Syntax **lsp-bfd**

Context **[Tree]** (config>router lsp-bfd)

Full Context configure router lsp-bfd

Description This command creates a context for the configuration of LSP BFD parameters.

Platforms All

16.260 lsp-exp

lsp-exp

Syntax **lsp-exp** *lsp-exp-value* [**fc** *fc-name*] [**priority** {**low** | **high**}]
no lsp-exp *lsp-exp-value*

Context **[Tree]** (config>qos>sap-ingress lsp-exp)

Full Context configure qos sap-ingress lsp-exp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command explicitly sets the forwarding class or subclass enqueuing priority when a packet is marked with a MPLS EXP bits specified. Adding a lsp-exp rule on the policy forces packets that match the MPLS LSP EXP specified to override the forwarding class and enqueuing priority based on the parameters included in the lsp-exp rule. When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueuing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueuing priority derived from earlier matches in the classification hierarchy.

The *lsp-exp-value* is derived from the MPLS LSP EXP bits of the top label.

Multiple commands can be entered to define the association of some or all eight LSP EX bit values to the forwarding class.

The **no** form of this command removes the explicit lsp-exp classification rule from the SAP ingress policy. Removing the rule on the policy immediately removes the rule on all ingress SAPs using the policy.

This command applies to Ethernet Layer 2 SAPs only.

Parameters *lsp-exp-value* — This value is a required parameter that specifies the unique MPLS LSP EXP value that will match the lsp-exp rule. If the command is executed multiple times with the same *lsp-exp-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight lsp-exp rules are allowed on a single policy.

Values 0 to 7

fc *fc-name* — The value given for the *fc-name* parameter must be one of the predefined forwarding classes in the system. Specifying the *fc-name* is optional. When a packet matches the rule, the forwarding class is only overridden when the *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

The *subclass-name* parameter is optional and used with the *fc-name* parameter to define a pre-existing subclass. The *fc-name* and *subclass-name* parameters must be separated by a period (dot). If *subclass-name* does not exist in the context of *fc -name*, an error will occur.

Values *class*[.*subclass*]

class: be, l2, af, l1, h2, ef, h1, nc

subclass: 29 characters max

priority — The **priority** parameter is used to override the default enqueuing priority for all packets received on an ingress SAP using this policy that match this rule. Specifying the priority is optional. When a packet matches the rule, the enqueuing priority is only overridden when the **priority** parameter is defined on the rule. If the packet matches and priority is not explicitly defined in the rule, the enqueuing priority is inherited based on previous rule matches.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

high — The **high** parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **high** for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

low — The **low** parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **low** for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Default no override

Platforms All

lsp-exp

Syntax **lsp-exp** *lsp-exp-value* **fc** *fc-name* **profile** {**in** | **out**}
no lsp-exp

Context **[Tree]** (config>qos>network>ingress lsp-exp)

Full Context configure qos network ingress lsp-exp

Description This command creates a mapping between the LSP EXP bits of the network ingress traffic and the forwarding class.

Ingress traffic that matches the specified LSP EXP bits will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all eight LSP EXP bit values to the forwarding class. For undefined values, packets are assigned to the forwarding class specified under the **default-action** command.

The **no** form of this command removes the association of the LSP EXP bit value to the forwarding class. The **default-action** then applies to that LSP EXP bit pattern.

Default no lsp-exp

Parameters *lsp-exp-value* — Specify the LSP EXP values to be associated with the forwarding class.

Values 0 to 8 (Decimal representation of three EXP bit field)

fc *fc-name* — Enter this required parameter to specify the fc-name that the EXP bit pattern will be associated with.

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out} — Enter this required parameter to indicate whether the LSP EXP value is the in-profile or out-of-profile value.

Values in, out

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.261 lsp-exp-in-profile

lsp-exp-in-profile

Syntax **lsp-exp-in-profile** *lsp-exp-value*
no lsp-exp-in-profile

Context **[Tree]** (config>qos>network>egress>fc lsp-exp-in-profile)

Full Context configure qos network egress fc lsp-exp-in-profile

Description This command specifies the in-profile LSP EXP value for the forwarding class. The EXP value will be used for all LSP labeled packets requiring marking that require marking at egress on this forwarding class queue, and that are in-profile. The inplus-profile traffic is marked with the same value as in-profile traffic.

When multiple EXP values are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command resets the configuration to the factory default in-profile EXP setting.

Default

Policy-id 1:	Factory setting
Policy-id 2 to 65535:	Policy-id setting

Parameters *lsp-exp-value* — The 3-bit LSP EXP bit value, expressed as a decimal integer.

Values 0 to 7

Platforms All

16.262 lsp-exp-out-profile

lsp-exp-out-profile

Syntax **lsp-exp-out-profile** *lsp-exp-value*
no lsp-exp-out-profile

Context **[Tree]** (config>qos>network>egress>fc lsp-exp-out-profile)

Full Context configure qos network egress fc lsp-exp-out-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the out-of-profile LSP EXP value for the forwarding class. The EXP value will be used for all LSP labeled packets that require marking at egress on this forwarding class queue, and that are out-of-profile. The exceed-profile traffic is marked with the same value as out-of-profile traffic.

When multiple EXP values are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command resets the configuration to the factory default out-of-profile EXP setting.

Default

Policy-id 1:	Factory setting
Policy-id 2 to 65535:	Policy-id setting

Parameters *mpls-exp-value* — The 3-bit MPLS EXP bit value, expressed as a decimal integer.

Values 0 to 7

Platforms All

16.263 lsp-hold-timer

lsp-hold-timer

Syntax [**no**] **lsp-hold-timer** *hold-time*

Context **[Tree]** (config>router>gmpls>peer lsp-hold-timer)

Full Context configure router gmpls peer lsp-hold-timer

Description This command specifies the amount of time that the ingress node holds before programming its data plane and declaring a GMPLS LSP up. This occurs anytime the ingress UNI-C node brings up a GMPLS LSP path or reroutes a GMPLS LSP. The *hold-time* value should be configured to reflect the data path programming time for the optical technology used between the ingress and egress UNI-N nodes.

The **no** form of the command resets the configuration to the default value.

Default lsp-hold-timer 60

Parameters *hold-timer* — Specifies the ingress node hold time, in seconds.

Values 5 to 300

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.264 lsp-init-retry-timeout

lsp-init-retry-timeout

Syntax **lsp-init-retry-timeout** *seconds*
no lsp-init-retry-timeout

Context **[Tree]** (config>router>gmpls lsp-init-retry-timeout)

Full Context configure router gmpls lsp-init-retry-timeout

Description This command configures the initial GMPLS LSP path retry timer.

The new GMPLS LSP path initial retry timer is used instead of the retry-timer to abort the retry cycle when no RESV is received. The retry-timer exclusively governs the time between two retry cycles and to handle retrying of a GMPLS LSP path in a failure case with PATH errors or RESVTear.

The **no** form of this command returns the timer to the default value.

Default lsp-init-retry-timeout 30

Parameters *seconds* — Specifies the time (in seconds), between retry cycles.

Values 10 to 600

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

lsp-init-retry-timeout

Syntax **lsp-init-retry-timeout** *seconds*
no lsp-init-retry-timeout

Context **[Tree]** (config>router>mpls lsp-init-retry-timeout)

Full Context configure router mpls lsp-init-retry-timeout

Description This command configures the initial LSP path retry-timer.

The new LSP path initial retry-timer is used instead of the retry-timer to abort the retry cycle when no RESV is received. The retry-timer exclusively governs the time between two retry cycles and to handle retrying of an LSP path in a failure case with PATH errors or RESVTear.

The intent is that the user can now control how many refreshes of the pending PATH state can be performed before starting a new retry-cycle with a new LSP ID. This is all done without affecting the ability to react faster to failures of the LSP path, which will continue to be governed by the retry-timer.

The **no** form of this command returns the timer to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default lsp-init-retry-timeout 30

Parameters *seconds* — Specifies the value (in s), used as the fast retry timer for a secondary path.

Values 10 to 600

Default 30

Platforms All

16.265 lsp-lifetime

lsp-lifetime

Syntax **lsp-lifetime** *seconds*
no lsp-lifetime

Context **[Tree]** (config>service>vpls>spb lsp-lifetime)

Full Context configure service vpls spb lsp-lifetime

Description This command sets the time, in seconds, SPB wants the LSPs it originates to be considered valid by other routers in the domain. This is a control B-VPLS command.

Each LSP received is maintained in an LSP database until the lsp-lifetime expires unless the originating router refreshes the LSP. By default, each router refreshes its LSPs every 20 minutes (1200 seconds) so other routers will not age out the LSP.

The LSP refresh timer is derived from this formula: lsp-lifetime/2.

The **no** form of this command reverts to the default value.

Default lsp-lifetime 1200 — LSPs originated by SPB should be valid for 1200 seconds (20 minutes).

Parameters *seconds* — The time, in seconds, that SPB wants the LSPs it originates to be considered valid by other routers in the domain.

Values 350 to 65535

Platforms All

lsp-lifetime

Syntax **lsp-lifetime** *seconds*
no lsp-lifetime

Context **[Tree]** (config>service>vprn>isis lsp-lifetime)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn isis lsp-lifetime

Description This command sets the time, in seconds, the router wants the LSPs it originates to be considered valid by other routers in the domain.

Each LSP received is maintained in an LSP database until the **lsp-lifetime** expires unless the originating router refreshes the LSP. By default, each router refreshes its LSPs every 20 minutes (1200 seconds) so other routers will not age out the LSP.

The LSP refresh timer is derived from this formula: lsp-lifetime/2

The **no** form of this command reverts to the default value.

Default lsp-lifetime 1200 — LSPs originated by the router should be valid for 1200 seconds (20 minutes).

Parameters *seconds* — Specifies the time, in seconds, that the router wants the LSPs it originates to be considered valid by other routers in the domain.

Values 350 to 65535

Platforms All

lsp-lifetime

Syntax **lsp-lifetime** *seconds*
no lsp-lifetime

Context **[Tree]** (config>router>isis lsp-lifetime)

Full Context configure router isis lsp-lifetime

Description This command sets the time, in seconds, the router wants the LSPs it originates to be considered valid by other routers in the domain.

Each LSP received is maintained in an LSP database until the **lsp-lifetime** expires unless the originating router refreshes the LSP. By default, each router refreshes its LSPs every 20 minutes (1200 seconds) so other routers will not age out the LSP.

The LSP refresh timer is derived from this formula: lsp-lifetime/2

The **no** form of this command reverts to the default value.

Default lsp-lifetime 1200

Parameters *seconds* — Specifies the time, in seconds, that the router wants the LSPs it originates to be considered valid by other routers in the domain.

Values 350 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.266 lsp-minimum-remaining-lifetime

lsp-minimum-remaining-lifetime

Syntax **lsp-minimum-remaining-lifetime** *seconds*
no lsp-minimum-remaining-lifetime

Context **[Tree]** (config>service>vprn>isis lsp-minimum-remaining-lifetime)

Full Context configure service vprn isis lsp-minimum-remaining-lifetime

Description This command configures the minimum value to which the remaining lifetime of the LSP is set. The value is a counter that decrements, in seconds, starting from the value in the received LSP (if not self-originated) or from **lsp-lifetime** *seconds* (if self-originated). When the remaining lifetime becomes zero, the contents of the LSP is purged. The remaining lifetime of an LSP is not changed when there is no **lsp-minimum-remaining-lifetime** value configured.

The configured value must be greater than or equal to the **lsp-lifetime** value.

The **no** form of this command removes the *seconds* value from the configuration.

Default no lsp-minimum-remaining-lifetime

Parameters *seconds* — Specifies the decrementing counter, in seconds. The configured value must be greater than or equal to the locally configured value of lsp-lifetime (MaxAge).

Values 350 to 65535

Platforms All

lsp-minimum-remaining-lifetime

Syntax **lsp-minimum-remaining-lifetime** *seconds*
no lsp-minimum-remaining-lifetime

Context **[Tree]** (config>router>isis lsp-minimum-remaining-lifetime)

Full Context configure router isis lsp-minimum-remaining-lifetime

Description This command configures the minimum value to which the remaining lifetime of the LSP is set. The value is a counter that decrements, in seconds, starting from the value in the received LSP (if not self-originated) or from **lsp-lifetime** *seconds* (if self-originated). When the remaining lifetime becomes zero, the contents of the LSP is purged. The remaining lifetime of an LSP is not changed when there is no **lsp-minimum-remaining-lifetime** value configured.

The configured value must be greater than or equal to the **lsp-lifetime** value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the *seconds* value from the configuration.

Parameters *seconds* — Specifies the decrementing counter, in seconds. The configured value must be greater than or equal to the locally configured value of lsp-lifetime (MaxAge).

Values 350 to 65535

Platforms All

16.267 lsp-mtu-size

lsp-mtu-size

Syntax **lsp-mtu-size** *size*
no lsp-mtu-size

Context **[Tree]** (config>service>vprn>isis lsp-mtu-size)
[Tree] (config>service>vprn>isis>level lsp-mtu-size)

Full Context configure service vprn isis level lsp-mtu-size
configure service vprn isis lsp-mtu-size

Description This command configures the LSP MTU size. If the *size* value is changed from the default using CLI or SNMP, then ISIS must be restarted for the change to take effect. This can be done by performing a **shutdown** command and then a **no shutdown** command in the **config>router>isis** context.

Note: Using the **exec** command to execute a configuration file to change the LSP MTU size from its default value will automatically restart IS-IS for the change to take effect.

The **no** form of this command reverts to the default value.

Default lsp-mtu-size 1492

Parameters *size* — Specifies the LSP MTU size.

Values 490 to 9778

Platforms All

lsp-mtu-size

Syntax **lsp-mtu-size** *size*
no lsp-mtu-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis lsp-mtu-size)
[Tree] (config>router>isis>level lsp-mtu-size)

Full Context configure router isis level lsp-mtu-size
configure router isis lsp-mtu-size

Description This command configures the LSP MTU size. If the *size* value is changed from the default using CLI or SNMP, then IS-IS must be restarted in order for the change to take effect. This can be done by performing a **shutdown** command and then a **no shutdown** command in the **config>router>isis** context.

Note: Using the **exec** command to execute a configuration file to change the LSP MTU-size from its default value automatically restarts IS-IS for the change to take effect.

The **no** form of this command reverts to the default value.

Default lsp-mtu-size 1492

Parameters *size* — Specifies the LSP MTU size.

Values 490 to 9778

Platforms All

16.268 lsp-num

lsp-num

Syntax **lsp-num** *lsp-num*
no lsp-num

Context [Tree] (config>router>mpls>lsp>working-tp-path lsp-num)
[Tree] (config>router>mpls>lsp>protect-tp-path lsp-num)

Full Context configure router mpls lsp protect-tp-path lsp-num
configure router mpls lsp working-tp-path lsp-num

Description This command configures the MPLS-TP LSP Number for the working TP path or the Protect TP Path.

Default lsp-num 1 (for a working path), lsp-num 2 (for a protect path)

Parameters *lsp-num* — Specifies the LSP number.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.269 lsp-pacing-interval

lsp-pacing-interval

Syntax **lsp-pacing-interval** *milli-seconds*
no lsp-pacing-interval

Context **[Tree]** (config>service>vpls>sap>spb lsp-pacing-interval)
[Tree] (config>service>vpls>spoke-sdp>spb lsp-pacing-interval)

Full Context configure service vpls sap spb lsp-pacing-interval
configure service vpls spoke-sdp spb lsp-pacing-interval

Description This command configures the interval during which LSPs are sent from the interface.

To avoid overwhelming neighbors that have less CPU processing power with LSPs, the pacing interval can be configured to limit how many LSPs are sent during an interval. LSPs may be sent in bursts during the interval up to the configured limit. If a value of 0 is configured, no LSPs are sent from the interface.

The **no** form of this command reverts to the default value.

Note: The IS-IS timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default lsp-pacing-interval 100 — LSPs are sent in 100 millisecond intervals.

Parameters *milli-seconds* — The interval in milliseconds during which IS-IS LSPs are sent from the interface, expressed as a decimal integer.
0 to 65535

Platforms All

lsp-pacing-interval

Syntax **lsp-pacing-interval** *milliseconds*
no lsp-pacing-interval

Context **[Tree]** (config>service>vprn>isis>if lsp-pacing-interval)

Full Context configure service vprn isis interface lsp-pacing-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the interval at which LSPs are sent from the interface.

To avoid overwhelming neighbors that have less CPU processing power with LSPs, the pacing interval can be configured to limit how many LSPs are sent at the interval. LSPs are sent in bursts at the interval up to the configured limit. If a value of 0 is configured, no LSPs are sent from the interface.

The **no** form of this command reverts to the default value.

Note: The IS-IS LSP pacing interval is 100 milliseconds for values < 100 milliseconds, and 1 second for values ≥ 100 milliseconds. For example, a pacing interval of 2 milliseconds means that a maximum of 50 LSPs are sent in a burst at 100 millisecond intervals. The default pacing interval of 100 milliseconds means that a maximum of 10 LSPs are sent in a burst at 1 second intervals.

Default lsp-pacing-interval 100 — the pacing interval is 100 milliseconds.

Parameters *milliseconds* — Specifies the pacing interval in milliseconds at which IS-IS LSPs are sent from the interface at each interval expressed as a decimal integer.

Values 0 to 65535

Platforms All

lsp-pacing-interval

Syntax **lsp-pacing-interval** *milliseconds*
no lsp-pacing-interval

Context **[Tree]** (config>router>isis>interface lsp-pacing-interval)

Full Context configure router isis interface lsp-pacing-interval

Description This command configures the interval at which LSPs are sent from the interface.

To avoid overwhelming neighbors that have less CPU processing power with LSPs, the pacing interval can be configured to limit how many LSPs are sent at the interval. LSPs are sent in bursts at the interval up to the configured limit. If a value of 0 is configured, no LSPs are sent from the interface. The interval applies to all LSPs: LSPs generated by the router, and LSPs received from other routers.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The IS-IS LSP pacing interval is 100 milliseconds for values < 100 milliseconds, and 1 second for values ≥ 100 milliseconds. For example, a pacing interval of 2 milliseconds means that a maximum of 50 LSPs are sent in a burst at 100 millisecond intervals. The default pacing interval of 100 milliseconds means that a maximum of 10 LSPs are sent in a burst at 1 second intervals.

Default lsp-pacing-interval 100 — LSPs are sent in 100 millisecond intervals.

Parameters *milli-seconds* — Specifies the interval in milliseconds during which IS-IS LSPs are sent from the interface expressed as a decimal integer.

Values 0 to 65535

Platforms All

16.270 lsp-ping

lsp-ping

Syntax **lsp-ping** *lsp-name* [**path** *path-name*]

lsp-ping bgp-label prefix *ip-prefix/prefix-length* [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping ldp prefix *ip-prefix/prefix-length* [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping prefix *ip-prefix/prefix-length* [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping rsvp-te *lsp-name* [**path** *path-name*]

lsp-ping sr-isis prefix *ip-prefixIprefix-length* [**igp-instance** *igp-instance*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping sr-ospf prefix *ip-prefixIprefix-length* [**igp-instance** *igp-instance*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping sr-ospf3 prefix *ip-prefixIprefix-length* [**igp-instance** *igp-instance*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping sr-policy color *color-id* **endpoint** *ip-address* [**segment-list** *segment-list-id*] [**detail**] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping sr-te *lsp-name* [**path** *path-name*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]

lsp-ping static *lsp-name* [**assoc-channel** {**ipv4** | **non-ip** | **none**}] [**dest-global-id** *global-id* **dest-node-id** *node-id*] [**force**] [**path-type** {**active** | **working** | **protect**}]

NOTE: Options common to all **lsp-ping** cases: [**detail**] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**interval** *interval*] [**send-count** *send-count*] [**size** *octets*] [**src-ip-address** *ip-address*] [**timeout** *timeout*] [**ttl** *label-ttl*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (oam lsp-ping)
[Tree] (config>saa>test>type lsp-ping)

Full Context configure saa test type lsp-ping
oam lsp-ping

Description This command performs in-band LSP connectivity tests.

This command performs an LSP ping using the protocol and data structures defined in the RFC 8029, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

The LSP ping operation is modeled after the IP ping utility which uses ICMP echo request and reply packets to determine IP connectivity.

In an LSP ping, the originating device creates an MPLS echo request packet for the LSP and path to be tested. The MPLS echo request packet is sent through the data plane and awaits an MPLS echo reply packet from the device terminating the LSP. The status of the LSP is displayed when the MPLS echo reply packet is received.

This command, when used with the **static** option, performs in-band on-demand LSP connectivity verification tests for static MPLS-TP LSPs. For other LSP types, the **static** option should be excluded and these are described elsewhere in this user guide.

The **lsp-ping static** command performs an LSP ping using the protocol and data structures defined in the RFC 8029, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*, as extended by RFC 6426, *MPLS On-Demand Connectivity Verification and Route Tracing*.

In MPLS-TP, the echo request and echo reply messages are always sent in-band over the LSP, either in a G-ACh channel or encapsulated as an IP packet below the LSP label.

The timestamp format to be sent, and to be expected when received in a PDU, is as configured by the **config>test-oam>mpls-time-stamp-format** command. If RFC 4379 (obsoleted by RFC 8029) is selected, then the timestamp is in seconds and microseconds since 1900, otherwise it is in seconds and microseconds since 1970.

Default The active LSP path

Values: Any path name associated with the LSP

Parameters *lsp-name* — Specifies the name of the target RSVP-TE LSP, up to 64 characters.

rsvp-te *lsp-name* — Specifies the name of the target RSVP-TE LSP, up to 64 characters.

Note: The **rsvp-te** explicit target FEC type is not supported under the SAA context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

path-name — Specifies the LSP path name, up to 32 characters, to which to send the LSP ping request.

Values Any path name associated with the LSP.

Default The active LSP path.

bgp-label prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target BGP IPv4 /32 label route or the target BGP IPv6 /128 label route.

Values

<ipv4-prefix>/32 | <ipv6-prefix>/128

ipv4-prefix a.b.c.d

ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

path-destination *ip-address* — Specifies the IP address of the path destination from the range 127/8. When the LDP FEC prefix is IPv6, the user must enter a 127/8 IPv4 mapped IPv6 address, that is, in the range ::ffff:127/104.

ipv4-address: a.b.c.d

ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

interface *if-name* — Specifies the name of an IP interface, up to 32 characters, to send the MPLS echo request message to. The name must already exist in the **config>router>interface** context.

next-hop *ip-address* — Specifies the next-hop address to send the MPLS echo request message to.

Values

ipv4-address: a.b.c.d

ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target LDP FEC.

Values

<ipv4-prefix>/32 | <ipv6-prefix>/128

ipv4-prefix a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

ldp prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target LDP FEC.

Values
<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix a.b.c.d
ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

sr-isis prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target node SID of the SR-IS-IS tunnel.

Values
<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix a.b.c.d
ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

igp-instance — Specifies the IGP instance of the node SID prefix.

Values isis-inst: 0 to 127
ospf3-inst: 0 to 31, 64 to 95
ospf-inst: 0 to 31

sr-ospf prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target node SID of the SR-OSPF tunnel.

Values
<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix - a.b.c.d
ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sr-ospf3 prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target node SID of the SR-OSPF3 tunnel. Note that only IPv6 prefixes in OSPFv3 instance ID 0-31 are supported.

Values

ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

sr-policy color *color-id* **endpoint** *ip-address* **segment-list** *segment-list-id* — Specifies the name of the target IPv4 or IPv6 SR policy.

Note: The **sr-policy** target FEC type is supported under the OAM context and under **type-multi-line node** in the SAA context.

color *color-id* — Specifies the color ID.

Values 0 to 4294967295

endpoint *ip-address* — Specifies the endpoint address.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

segment-list *segment-list-id* — Specifies the segment list ID.

Values 1 to 32

detail — Displays detailed information.

sr-te *lsp-name* — Specifies the name of the target SR-TE LSP, up to 64 characters.

static — Specifies the target FEC stack sub-type “Static LSP”.

assoc-channel {ipv4 | non-ip | none} — Specifies the launched echo request’s usage of the Associated Channel (ACH) mechanism, when testing an MPLS-TP LSP.

Values **ipv4** — Use an Associated Channel with IP encapsulation, as described in RFC 6426, Section 3.2.

non-ip — Do not use an Associated Channel, as described in RFC 6426, Section 3.1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

none — Use the Associated Channel mechanism described in RFC 6426, Section 3.3.

Default non-ip

global-id — Specifies the MPLS-TP global ID for the far end node of the LSP under test. If this is not entered, then the dest-global-id is taken from the LSP context.

Values 0 to 4294967295

Default 0

node-id — Specifies the MPLS-TP global ID for the far end node of the LSP under test. If this is not entered, then the dest-global-id is taken from the LSP context.

Values a.b.c.d, 1 to 4294967295

Default 0

force — Allows LSP ping to test a path that is operationally down, including cases where MPLS-TP BFD CC/V is enabled and has taken a path down. This parameter is only allowed in the OAM context; it is not allowed for a test configured as a part of an SAA.

Default disabled

path-type {active | working | protect} — The LSP path to test.

Values **active** — The currently active path. If MPLS-TP linear protection is configured on the LSP, then this is the path that is selected by the MPLS-TP PSC protocol for sending user plane traffic. If MPLS-TP linear protection is not configured, then this is the working path.

working — The working path of the MPLS-TP LSP.

protect — The protect path of the MPLS-TP LSP.

Default active

fc-name — Specifies the FC and profile parameters that are used to indicate the forwarding class and profile of the MPLS echo request packet.

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified fc and profile parameter values. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface.

When the MPLS echo request packet is received on the responding node, The FC and profile parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the FC and profile parameter values determined by the classification of the echo request packet, which is being replied to, at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. The ToS byte is not modified. Table 77 summarizes this behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 77 **lsp-ping Request Packet and Behavior**

CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • packet queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet{tos=1, fc2, profile2}
Outgoing interface (responder node)	Echo reply packet: • packet queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

The LSP-EXP mappings on the receive network interface controls the mapping of the message reply at the originating router**.**

Values be, l2, af, l1, h2, ef, h1, nc

Default be

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

profile {in | out} — Specifies the profile state of the MPLS echo request packet.

Default out

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

Values 1 to 10

Default 1

send-count — Specifies the number of messages to send, expressed as a decimal integer. The **send-count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must be expired before the next message request is sent.

Values 1 to 100

Default 1

octets — Specifies the MPLS echo request packet size in octets, expressed as a decimal integer. The request payload is padded with zeros to the specified size.

Values 1 to 9786

Default 1

src-ip-address *ip-address* — Specifies the source IP address. This option is used when an OAM packet must be generated from a different address than the node's system interface address. An example is when the OAM packet is sent over an LDP LSP and the LDP LSR-ID of the corresponding LDP session to the next-hop is set to an address other than the system interface address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

timeout — Specifies number, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of the time out, the test is marked complete and no more packets are processed for any of those request probes.

Values 1 to 10

Default 5

label-ttl — Specifies the TTL value for the MPLS label, expressed as a decimal integer.

Values 1 to 255

Default 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Output

Sample Output

This sample output is for a LDP IPv4 and IPv6 prefix FECs.

```
A:Dut-C# oam lsp-ping prefix 4.4.4.4/32 detail
LSP-PING 4.4.4.4/32: 80 bytes MPLS payload
Seq=1, send from intf dut1_to_dut3, reply from 4.4.4.4
       udp-data-len=32 ttl=255 rtt=5.23ms rc=3 (EgressRtr)

---- LSP 4.4.4.4/32 PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 5.23ms, avg = 5.23ms, max = 5.23ms, stddev = 0.000ms

===============================================================================
LDP LSR ID: 1.1.1.1
===============================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
        WP - Label Withdraw Pending, BU - Alternate For Fast Re-Route
===============================================================================


LDP Prefix Bindings
===============================================================================
Prefix              IngLbl       EgrLbl     EgrIntf/         EgrNextHop
   Peer                                     LspId
-------------------------------------------------------------------------------
4.4.4.4/32          131069N      131067     1/1/1            1.3.1.2
   3.3.3.3
4.4.4.4/32          131069U      131064       --               --
   6.6.6.6
-------------------------------------------------------------------------------
No. of Prefix Bindings: 2
===============================================================================
A:Dut-C#

*A:Dut-A# oam lsp-ping prefix fc00::a14:106/128

LSP-PING fc00::a14:106/128: 116 bytes MPLS payload

Seq=1, send from intf A_to_B, reply from fc00::a14:106

udp-data-len=32 ttl=255 rtt=7.16ms rc=3 (EgressRtr)


---- LSP fc00::a14:106/128 PING Statistics ----

1 packets sent, 1 packets received, 0.00% packet loss

round-trip min = 7.16ms, avg = 7.16ms, max = 7.16ms, stddev = 0.000ms

*A:Dut-A#
```

lsp-ping over SR-ISIS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
*A:Dut-A# oam lsp-ping sr-isis prefix 10.20.1.6/32 igp-instance 0 detail
LSP-PING 10.20.1.6/32: 80 bytes MPLS payload
Seq=1, send from intf int_to_B, reply from 10.20.1.6
       udp-data-len=32 ttl=255 rtt=1220324ms rc=3 (EgressRtr)
---- LSP 10.20.1.6/32 PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1220324ms, avg = 1220324ms, max = 1220324ms, stddev = 0.000ms
```

lsp-ping with SR-TE

```
*A:Dut-A# oam lsp-ping sr-te "srteABCEDF" detail
LSP-PING srteABCEDF: 96 bytes MPLS payload
Seq=1, send from intf int_to_B, reply from 10.20.1.6
       udp-data-len=32 ttl=255 rtt=1220325ms rc=3 (EgressRtr)
---- LSP srteABCEDF PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1220325ms, avg = 1220325ms, max = 1220325ms, stddev = 0.000ms

*A:Dut-A# oam lsp-ping sr-te "srteABCE_loose" detail
LSP-PING srteABCE_loose: 80 bytes MPLS payload
Seq=1, send from intf int_to_B, reply from 10.20.1.5
       udp-data-len=32 ttl=255 rtt=1220324ms rc=3 (EgressRtr)
---- LSP srteABCE_loose PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1220324ms, avg = 1220324ms, max = 1220324ms, stddev = 0.000ms

*A:Dut-F# oam lsp-ping sr-te "srteFECBA_eth" detail
LSP-PING srteFECBA_eth: 116 bytes MPLS payload
Seq=1, send from intf int_to_E, reply from fc00::a14:101
       udp-data-len=32 ttl=255 rtt=1220326ms rc=3 (EgressRtr)
---- LSP srteFECBA_eth PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1220326ms, avg = 1220326ms, max = 1220326ms, stddev = 0.000ms
```

lsp-ping with SR-Policy

```
*A:Dut-A#
# ipv4 sr-policy lsp-ping
*A:Dut-A# oam lsp-ping sr-policy color 200 endpoint 10.20.1.6 LSP-PING color 200 end
point 10.20.1.6: 76 bytes MPLS payload Seq=1, send from intf int_to_C, reply from 10
.20.1.6
       udp-data-len=32 ttl=255 rtt=1220325ms rc=3 (EgressRtr)
---- LSP color 200 endpoint 10.20.1.6 PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss round-trip min = 1220325ms, av
g = 1220325ms, max = 1220325ms, stddev = 0.000ms

# ipv6 sr-policy lsp-ping
*A:Dut-A# oam lsp-ping sr-policy color 200 endpoint fc00::a14:106 LSP-PING color 200
 endpoint fc00::a14:106: 76 bytes MPLS payload Seq=1, send from intf int_to_C, reply
 from 10.20.1.6
       udp-data-len=32 ttl=255 rtt=1220324ms rc=3 (EgressRtr)
---- LSP color 200 endpoint fc00::a14:106 PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss round-trip min = 1220324ms, av
g = 1220324ms, max = 1220324ms, stddev = 0.000ms
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsp-ping with sr-ospf3

```
# sr-ospf3 lsp-ping
*A:Dut-A# oam lsp-ping sr-ospf3 prefix fc00::a14:106/128 LSP-PING fc00::a14:106/
128: 116 bytes MPLS payload Seq=1, send from intf int_to_B, reply from fc00::a14:106
       udp-data-len=32 ttl=255 rtt=3.17ms rc=3 (EgressRtr)
---- LSP fc00::a14:106/128 PING Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss round-trip min = 3.17ms, avg =
 3.17ms, max = 3.17ms, stddev = 0.000ms *A:Dut-A#
```

Platforms All

lsp-ping

Syntax **lsp-ping**

Context **[Tree]** (config>saa>test>type-multi-line lsp-ping)

Full Context configure saa test type-multi-line lsp-ping

Description Commands in this context configure the lsp-ping OAM probe type.

Platforms All

16.271 lsp-ping-interval

lsp-ping-interval

Syntax **lsp-ping-interval** *seconds*
no lsp-ping-interval

Context **[Tree]** (config>router>ldp>lsp-bfd lsp-ping-interval)

Full Context configure router ldp lsp-bfd lsp-ping-interval

Description This command configures the interval between periodic LSP ping messages for LSPs on which **bfd-enable** is configured. The LSP ping messages are used to bootstrap and maintain the LSP BFD session.

Configuring an interval of 0 seconds disables periodic LSP ping. An LSP ping message containing a bootstrap TLV will only be sent when the BFD session is first initialized.

In scaled environments, LSP BFD sessions should use longer intervals to reduce congestion and common resource loading. Unless required, the interval should not be set lower than 300 s.

The **no** form of this command restores the default interval.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default lsp-ping-interval 60

Parameters *seconds* — Specifies the interval between periodic LSP ping messages, in seconds.

Values 0, 60 to 300

Platforms All

lsp-ping-interval

Syntax **lsp-ping-interval** *seconds*
no lsp-ping-interval

Context **[Tree]** (config>router>mpls>lsp>bfd lsp-ping-interval)
[Tree] (config>router>mpls>lsp>primary>bfd lsp-ping-interval)
[Tree] (config>router>mpls>lsp>secondary>bfd lsp-ping-interval)
[Tree] (config>router>mpls>lsp-template>bfd lsp-ping-interval)

Full Context configure router mpls lsp bfd lsp-ping-interval
configure router mpls lsp primary bfd lsp-ping-interval
configure router mpls lsp secondary bfd lsp-ping-interval
configure router mpls lsp-template bfd lsp-ping-interval

Description This command configures the interval for the periodic LSP ping for RSVP LSPs on which **bfd-enable** has been configured. This interval is used to bootstrap and maintain the LSP BFD session. A value of 0 disables periodic LSP Ping, such that an LSP Ping containing a bootstrap TLV is only sent when the BFD session is first initialized.

In scaled environments, LSP BFD sessions should use longer timers to reduce the chance of congestion and loading of common resources. Unless required, the **lsp-ping-interva**l should not be set lower than 300 seconds.

The **no** form of this command reverts to the default value.

Default no lsp-ping-interval

Parameters *seconds* — Sets the periodic LSP Ping interval in seconds.

Values 0, 60 to 300

Default 60

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

16.272 lsp-ping-trace

lsp-ping-trace

Syntax **lsp-ping-trace** [{**tx** | **rx** | **both**}] [{**raw** | **detail**}]
no lsp-ping-trace

Context **[Tree]** (debug>oam lsp-ping-trace)

Full Context debug oam lsp-ping-trace

Description This command enables debugging for lsp-ping.

Parameters **tx | rx | both** — Specifies to enable LSP ping debugging for TX, RX, or both RX and TX for the for debug direction.

raw | detail — Displays output for the for debug mode.

Platforms All

16.273 lsp-refresh-interval

lsp-refresh-interval

Syntax **lsp-refresh-interval** [*seconds*] [**half-lifetime** [**enable** | **disable**]
no lsp-refresh-interval

Context **[Tree]** (config>service>vpls>spb lsp-refresh-interval)

Full Context configure service vpls spb lsp-refresh-interval

Description This command configures the LSP refresh timer interval. When configuring the LSP refresh interval, the value that is specified for **lsp-lifetime** must also be considered. The LSP refresh interval cannot be greater than 90% of the LSP lifetime.

The no form of this command reverts to the default (600 seconds), unless this value is greater than 90% of the LSP lifetime. For example, if the LSP lifetime is 400, then the **no lsp-refresh-interval** command will be rejected.

Default lsp-refresh-interval 600 half-lifetime enable

Parameters *seconds* — Specifies the refresh interval.

Values 150 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

half-lifetime — Sets the refresh interval to always be half the **lsp-lifetime** value. When this parameter is set to **enable**, the configured refresh interval is ignored.

Values enable, disable

Platforms All

lsp-refresh-interval

Syntax **lsp-refresh-interval** [*seconds*] [**half-lifetime** {**enable** | **disable**}]
no lsp-refresh-interval

Context **[Tree]** (config>service>vprn>isis lsp-refresh-interval)

Full Context configure service vprn isis lsp-refresh-interval

Description This command configures the IS-IS LSP refresh timer interval for the VPRN instance. When configuring the LSP refresh interval, the value that is specified for **lsp-lifetime** must also be considered. The LSP refresh interval cannot be greater than 90% of the LSP lifetime.

The **no** form of this command reverts to the default (600 seconds), unless this value is greater than 90% of the LSP lifetime. For example, if the LSP lifetime is 400, then the no lsp-refresh-interval command will be rejected.

Default lsp-refresh-interval 600 half-lifetime enable

Parameters *seconds* — Specifies the refresh interval.

Values 150 to 65535

half-lifetime — Sets the refresh interval to always be half the **lsp-lifetime** value. When this parameter is set to **enable**, the configured refresh interval is ignored.

Values enable, disable

Platforms All

lsp-refresh-interval

Syntax **lsp-refresh-interval** [*seconds*] [**half-lifetime** {**enable** | **disable**}
no lsp-refresh-interval

Context **[Tree]** (config>router>isis lsp-refresh-interval)

Full Context configure router isis lsp-refresh-interval

Description This command configures the IS-IS LSP refresh timer interval. When configuring the LSP refresh interval, the value that is specified for **lsp-lifetime** must also be considered. The LSP refresh interval cannot be greater than 90% of the LSP lifetime.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default (600 seconds), unless this value is greater than 90% of the LSP lifetime. For example, if the LSP lifetime is 400, then the no lsp-refresh-interval command will be rejected.

Default lsp-refresh-interval 600 half-lifetime enable

Parameters *seconds* — Specifies the refresh interval.

Values 150 to 65535

half-lifetime — Sets the refresh interval to always be half the **lsp-lifetime** value. When this parameter is set to **enable**, the configured refresh interval is ignored.

Values enable, disable

Platforms All

16.274 lsp-self-ping

lsp-self-ping

Syntax [**no**] **lsp-self-ping**

Context **[Tree]** (config>router>mpls lsp-self-ping)

Full Context configure router mpls lsp-self-ping

Description Commands in this context configure LSP self-ping parameters.

LSP Self-ping checks that the datapath of an RSVP LSP has been programmed by all LSRs along its path before switching the traffic to it. If enabled, LSP Self-ping packets are sent periodically at a configurable interval following the receipt of the RESV message for an RSVP LSP path following an MBB or other event where the active path changes while the previous active path stayed up. The router will not switch traffic to the new path until an LSP Self-ping reply is received from the far-end LER.

When configured under the MPLS context, LSP Self-ping is enabled for all RSVP LSPs, unless it is explicitly disabled for a given LSP.

The **no** form of this command disables the system check for LSP Self-ping.

Default no lsp-self-ping

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsp-self-ping

Syntax **lsp-self-ping** {**enable** | **disable** | **inherit**}
no lsp-self-ping

Context **[Tree]** (config>router>mpls>lsp lsp-self-ping)
[Tree] (config>router>mpls>lsp-template lsp-self-ping)

Full Context configure router mpls lsp lsp-self-ping
configure router mpls lsp-template lsp-self-ping

Description This command enables LSP Self-ping on a given RSVP-TE LSP or LSP template. If set to **disable**, then LSP Self-ping is disabled irrespective of the setting of **lsp-self-ping**>**rsvp-te** under the **mpls** context. By default, each LSP and LSP template inherits this value.

The **no** form of this command reverts to the default.

Default lsp-self-ping inherit

Parameters **enable** — Enables LSP Self-ping on this RSVP LSP or RSVP LSPs (one-hop-p2p or mesh-p2p) using this LSP template.

disable — Disables LSP Self-ping on this RSVP LSP or RSVP LSPs using this LSP template.

inherit — Inherits the value configured under **config**>**router**>**mpls**>**lsp-self-ping**>**rsvp-te**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router mpls lsp lsp-self-ping

All

- configure router mpls lsp-template lsp-self-ping

16.275 lsp-setup

lsp-setup

Syntax [**no**] **lsp-setup**

Context **[Tree]** (debug>router>gmpls>event lsp-setup)

Full Context debug router gmpls event lsp-setup

Description This command enables and disables debugging for GMPLS LSP Setup events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsp-setup

Syntax **lsp-setup** [**detail**]
no lsp-setup

Context **[Tree]** (debug>router>mpls>event lsp-setup)

Full Context debug router mpls event lsp-setup

Description This command debugs LSP setup events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about LSP setup events.

Platforms All

16.276 lsp-template

lsp-template

Syntax **lsp-template** *p2mp-lsp-template-name*
no lsp-template

Context **[Tree]** (config>service>vpls>provider-tunnel>inclusive>rsvp lsp-template)

Full Context configure service vpls provider-tunnel inclusive rsvp lsp-template

Description This command specifies the template name of the RSVP P2MP LSP instance to be used by the leaf node or the root-and-leaf node that participates in BGP-AD VPLS. The P2MP LSP is referred to as the Inclusive Provider Multicast Service Interface (I-PMSI).

After the user performs a **no shutdown** under the context of the inclusive node and the delay timer expires, BUM packets will be forwarded over an automatically signaled instance of the RSVP P2MP LSP specified in the LSP template.

The **no** version of this command removes the P2MP LSP template from the I-PMSI configuration.

Parameters *p2mp-lsp-template-name* — Specifies the name of the P2MP LSP template up to 32 characters in length.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lsp-template

Syntax **lsp-template**
no lsp-template

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>rsvp lsp-template)

Full Context configure service vprn mvpn provider-tunnel inclusive rsvp lsp-template

Description This command specifies the use of automatically created P2MP LSP as the provider tunnel. The P2MP LSP will be signaled using the parameters specified in the template, such as bandwidth constraints, and so on.

Default no lsp-template

Platforms All

lsp-template

Syntax **lsp-template** *name*
no lsp-template

Context **[Tree]** (config>service>vprn>mvpn>pt>selective>multistream-spmsi lsp-template)

Full Context configure service vprn mvpn provider-tunnel selective multistream-spmsi lsp-template

Description This command creates a RSVP-TE LSP template for S-PMSI. Multi-stream S-PMSIs can share a single template or can each use their own template.

Parameters *name* — Specifies the LSP template name, up to 32 characters.

Platforms All

lsp-template

Syntax **lsp-template** *lsp-template*
no lsp-template

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive lsp-template)
[Tree] (config>service>vprn>mvpn>pt>selective>rsvp lsp-template)

Full Context configure service vprn mvpn pt inclusive lsp-template
configure service vprn mvpn provider-tunnel selective rsvp lsp-template

Description This command specifies the use of automatically created P2MP LSP as the inclusive or selective provider tunnel. The P2MP LSP will be signaled using the parameters specified in the template, such as bandwidth constraints, and so on

Default no lsp-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *lsp-template* — Specifies the LSP template name, up to 32 characters.

Platforms All

lsp-template

Syntax **lsp-template** *template-name* [**mesh-p2p** | **mesh-p2p-srte** | **one-hop-p2p** | **on-demand-p2p-srte** | **one-hop-p2p-srte** | **p2mp** | **pce-init-p2p-srte template-id** {**default** | *template-id*}]
no lsp-template *template-name*

Context **[Tree]** (config>router>mpls lsp-template)

Full Context configure router mpls lsp-template

Description This command creates a template that can be referenced by a client application where dynamic LSP creation is required. The LSP template type (**p2mp**, **one-hop-p2p**, **mesh-p2p**, **one-hop-p2p-srte**, **mesh-p2p-srte**, **pce-init-p2p-srte**, or **on-demand-p2p-srte**) is mandatory.

The **no** form of this command deletes the LSP template. An LSP template cannot be deleted if a client application is using it.

Parameters *template-name* — Specifies the name of the LSP template, up to 32 characters. An LSP template name and LSP name must not be the same.

mesh-p2p | **mesh-p2p-srte** | **one-hop-p2p** | **one-hop-p2p-srte** | **p2mp** | **pce-init-p2p-srte** | **on-demand-p2p-srte** — Identifies the type of LSP this template will signal.

The **p2mp** option is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

default — Sets the template to be the default LSP template for PCE-initiated SR-TE LSPs.

template-id — Specifies the value that is signaled in the PCE to identify the LSP template.

Platforms All

lsp-template

Syntax **lsp-template** *lsp-template*
no lsp-template

Context **[Tree]** (config>router>gtm>provider-tunnel>inclusive>rsvp lsp-template)
[Tree] (config>router>gtm>provider-tunnel>selective>rsvp lsp-template)

Full Context configure router gtm provider-tunnel inclusive rsvp lsp-template
configure router gtm provider-tunnel selective rsvp lsp-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the use of automatically created P2MP LSP as the provider tunnel. The P2MP LSP will be signaled using the parameters specified in the template, such as bandwidth constraints.

The **no** form of this command removes the lsp-template name from this configuration.

Default no lsp-template

Parameters *lsp-template* — Specifies the name of the LSP template, up to 32 characters.

Platforms All

lsp-template

Syntax **lsp-template** *template-name*
no lsp-template

Context **[Tree]** (config>oam-pm>session>mpls>lsp>rsvp-auto lsp-template)

Full Context configure oam-pm session mpls lsp rsvp-auto lsp-template

Description This command specifies the LSP template used to identify the LSP for testing.

One of three mandatory configuration statements that are required to identify automatically created RSVP LSPs, created using **config>router>mpls>lsp-template**. The **config>router>mpls>auto-lsp>lsp-template** links three distinct functions.

The **lsp-template** *template-name* must match the name of **config>router>mpls>lsp-template** used to dynamically create the RSVP LSP. This is a lose reference and does not impede the manipulation of the **config>router>mpls>lsp-template**. The required identifiers are **from**, **lsp-template** and **to**, all under this node.

The **no** form of this command deletes the *template-name* reference from the configuration.

Parameters *template-name* — Specifies the name of the LSP template, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

16.277 lsp-trace

lsp-trace

Syntax **lsp-trace** *lsp-name* [**path** *path-name*]
lsp-trace bgp-label prefix *ip-prefix/prefix-length* [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace ldp prefix *ip-prefix/length* [**path-destination** *ip-address* [{**interface** *if-name* |

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

next-hop *ip-address*}]]
lsp-trace prefix *ip-prefix/length* [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace rsvp-te *lsp-name* [**path** *path-name*]
lsp-trace sr-isis prefix *ip-prefix*|*prefix-length* [**igp-instance** *igp-instance*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace sr-ospf prefix *ip-prefix*|*prefix-length* [**igp-instance** *igp-instance*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace sr-ospf3 prefix *ip-prefix*|*prefix-length* [**igp-instance** *igp-instance*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace sr-policy color *color-id* **endpoint** *ip-address* [**segment-list** *segment-list-id*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace sr-te *lsp-name* [**path** *path-name*] [**path-destination** *ip-address* [{**interface** *if-name* | **next-hop** *ip-address*}]]
lsp-trace static *lsp-name* [**assoc-channel** {**ipv4** | **non-ip** | **none**}] [**path-type** {**active** | **working** | **protect**}]

NOTE: Options common to all **lsp-trace** cases: [**detail**] [**downstream-map-tlv** *downstream-map-tlv*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**interval** *interval*] [**max-fail** *no-response-count*] [**max-ttl** *max-label-ttl*] [**min-ttl** *min-label-ttl*] [**probe-count** *probes-per-hop*] [**size** *octets*] [**src-ip-address** *ip-address*] [**timeout** *timeout*]

Context **[Tree]** (oam lsp-trace)
[Tree] (config>saa>test>type lsp-trace)

Full Context configure saa test type lsp-trace
oam lsp-trace

Description This command performs an LSP traceroute using the protocol and data structures defined in IETF RFC 8029.

The LSP trace operation is modeled after the IP traceroute utility which uses ICMP echo request and reply packets with increasing TTL values to determine the hop-by-hop route to a destination IP.

In an LSP trace, the originating device creates an MPLS echo request packet for the LSP to be tested with increasing values of the TTL in the outermost label. The MPLS echo request packet is sent through the data plane and awaits a TTL exceeded response or the MPLS echo reply packet from the device terminating the LSP. The devices that reply to the MPLS echo request packets with the TTL exceeded and the MPLS echo reply are displayed.

The downstream mapping TLV is used in **lsp-trace** to provide a mechanism for the sender and responder nodes to exchange and validate interface and label stack information for each downstream hop in the path of the LDP FEC an RSVP LSP, or a BGP IPv4 label route.

Two downstream mapping TLVs are supported. The original Downstream Mapping (DSMAP) TLV defined in RFC 4379 (obsoleted by RFC 8029) and the new Downstream Detailed Mapping (DDMAP) TLV defined in RFC 6424 AND RFC 8029. More details are provided in the DDMAP TLV sub-section below.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In addition, when the responder node has multiple equal cost next hops for an LDP FEC, a BGP label IPv4 prefix, an SR-ISIS node SID, an SR-OSPF node SID, or an SR-TE LSP, it replies in the Downstream Mapping TLV with the downstream information for each outgoing interface which is part of the ECMP next-hop set for the prefix. The downstream mapping TLV can further be used to exercise a specific path of the ECMP set using the **path-destination** option.

This command, when used with the **static** option, performs in-band on-demand LSP traceroute tests for static MPLS-TP LSPs. For other LSP types, the **static** option should be excluded and these are described elsewhere in this user guide.

The **lsp-trace static** command performs an LSP trace using the protocol and data structures defined in the RFC 8029, Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, as extended by RFC 6426, MPLS On-Demand Connectivity Verification and Route Tracing.

In MPLS-TP, the echo request and echo reply messages are always sent in-band over the LSP, either in a G-ACh channel or encapsulated as an IP packet below the LSP label.

The timestamp format to be sent, and to be expected when received in a PDU, is as configured by the **config>test-oam>mpls-time-stamp-format** command. If RFC 4379 (obsoleted by RFC 8029) is selected, then the timestamp is in seconds and microseconds since 1900, otherwise it is in seconds and microseconds since 1970.

Parameters *lsp-name* — Specifies the name of the target RSVP-TE LSP, up to 64 characters.

rsvp-te *lsp-name* — Specifies the name of the target RSVP-TE LSP, up to 64 characters.

Note: The **rsvp-te** explicit target FEC type is not supported under the SAA context.

path-name — Specifies the LSP path name along which to send the LSP trace request.

Values Any path name associated with the LSP.

Default The active LSP path.

bgp-label prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target BGP IPv4 /32 label route or the target IPv6 /128 label route.

Values

<ipv4-prefix>/32 | <ipv6-prefix>/128

ipv4-prefix a.b.c.d

ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

path-destination *ip-address* — Specifies the IP address of the path destination from the range 127/8. When the LDP FEC prefix is IPv6, the user must enter a 127/8 IPv4 mapped IPv6 address, that is, in the range ::ffff:127/104.

if-name — Specifies the name of an IP interface, up 32 characters, to send the MPLS echo request to. The name must already exist in the **config>router>interface** context.

next-hop *ip-address* — Specifies the next-hop to send the MPLS echo request message to.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target LDP FEC.

Values

<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix - a.b.c.d
ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

ldp prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target LDP FEC.

Values

<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix a.b.c.d
ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

sr-isis prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target node SID of the SR-ISIS tunnel.

Values

<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-prefix x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

igp-instance — Specifies the IGP instance of the node SID prefix.

Values isis-inst: 0 to 127
ospf3-inst: 0 to 31, 64 to 95
ospf-inst: 0 to 31

sr-ospf prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target node SID of the SR-OSPF tunnel.

Values
<ipv4-prefix>/32 | <ipv6-prefix>/128
ipv4-prefix - a.b.c.d
ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

sr-ospf3 prefix *ip-prefix/prefix-length* — Specifies the address prefix and subnet mask of the target node SID of the SR-OSPF3 tunnel. Note that only IPv6 prefixes in OSPFv3 instance ID 0-31 are supported.

Values
ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

sr-policy color *color-id* **endpoint** *ip-address* **segment-list** *segment-list-id* — Specifies the name of the target IPv4 or IPv6 SR policy.

Note: The **sr-policy** target FEC type is supported under the OAM context and under **type-multi-line node** in the SAA context.

color *color-id* — Specifies the color ID.

Values 0 to 4294967295

endpoint *ip-address* — Specifies the endpoint address.

Values

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

segment-list *segment-list-id* — Specifies the segment list ID.

Values 1 to 32

detail — Displays detailed information.

sr-te *lsp-name* — Specifies the name of the target SR-TE LSP, up to 64 characters.

static — Specifies to select the target FEC Stack sub-type 'Static LSP'.

assoc-channel {ipv4 | non-ip | none} — Specifies the launched echo request's usage of the Associated Channel (ACH) mechanism, when testing an MPLS-TP LSP.

Values **ipv4** — Use the Associated Channel mechanism with IP encapsulation, as described in RFC 6426, Section 3.2.

non-ip — Do not use an Associated Channel, as described in RFC 6426, Section 3.1.

none — Use the Associated Channel mechanism described in RFC 6426, Section 3.3.

path-type {active | working | protect} — Specifies the LSP path to test.

Values **active** — Specifies the currently active path. If MPLS-TP linear protection is configured on the LSP, then this is the path that is selected by the MPLS-TP PSC protocol for sending user plane traffic. If MPLS-TP linear protection is not configured, then this is the working path.

working — Specifies the working path of the MPLS-TP LSP.

protect — Specifies the protect path of the MPLS-TP LSP.

Default active

downstream-map-tlv — Specifies which format of the downstream mapping TLV to use in the LSP trace packet. The DSMAP TLV is the original format in RFC 4379 (obsoleted by RFC 8029). The DDMAP is the new enhanced format specified in RFC 6424 and RFC 8029. The user can also choose not to include the downstream mapping TLV by entering the value none. When lsp-trace is used on a MPLS-TP LSP (static option), it can only be executed if the control-channel is set to none. In addition, the DSMAP/DDMAP TLV is only included in the echo request message if the egress interface is either a numbered IP interface, or an unnumbered IP interface. The TLV is not included if the egress interface is of type **unnumbered-mpls-tp**.

Values ddmap: Sends a detailed downstream mapping TLV.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dsmap: Sends a downstream mapping TLV.

none: No mapping TLV is sent.

Default Inherited from global configuration of downstream mapping TLV in option **mpls-echo-request-downstream-map {dsmap | ddmap}**.

fc-name — Specifies the FC and profile parameters are used to indicate the forwarding class and profile of the MPLS echo request packet.

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified FC and profile parameter values. The marking of the packet EXP is dictated by the LSP-EXP mappings on the outgoing interface.

When the MPLS echo request packet is received on the responding node, The FC and profile parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the fc and profile parameter values determined by the classification of the echo request packet, which is being replied to, at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. The ToS byte is not modified. Table 78 summarizes this behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 78 **lsp-trace Request Packet and Behavior**

CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • pkt queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet {tos=1, fc2, profile2}
Outgoing interface (responder node)	Echo reply packet: • pkt queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | **out}** — Specifies the profile state of the MPLS echo request packet.

Default out

interval — Specifies the number of seconds to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the **interval** is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default **1**

no-response-count — Specifies the maximum number of consecutive MPLS echo requests, expressed as a decimal integer that do not receive a reply before the trace operation fails for a given TTL.

Values 1 to 255

Default 5

max-label-ttl — Specifies the maximum TTL value in the MPLS label for the LDP treetrace test, expressed as a decimal integer.

Values 1 to 255

Default 30

min-label-ttl — Specifies the minimum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Values 1 to 255

Default 1

probes-per-hop — Specifies the probes per hop.

Values 1 to 10

Default 1

octets — Specifies the size in octets, expressed as a decimal integer, of the MPLS echo request packet, including the IP header but not the label stack. The request payload is padded with zeros to the specified size. Note that an OAM command is not failed if the user entered a size lower than the minimum required to build the packet for the echo request message. The payload is automatically padded to meet the minimum size.

Values 1 to 9786

Default 1

src-ip-address *ip-address* — Specifies the source IP address. This option is used when an OAM packet must be generated from a different address than the node's system interface address. An example is when the OAM packet is sent over an LDP LSP and the LDP LSR-ID of the corresponding LDP session to the next-hop is set to an address other than the system interface address.

Values

ipv4-address: a.b.c.d

ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x - [0 to FFFF]H
d - [0 to 255]D

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

Values 1 to 60

Default 3

Output

Sample Output

```
*A:Dut-A# oam lsp-trace prefix 10.20.1.6/32 downstream-map-tlv ddmap path-
destination 127.0.0.1 detail lsp-trace to 10.20.1.6/
32: 0 hops min, 0 hops max, 152 byte packets
1  10.20.1.2  rtt=3.44ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=127.0.0.1 ifaddr=0 iftype=ipv4Unnumbered MRU=1500
           label[1]=131070 protocol=3(LDP)
2  10.20.1.4  rtt=4.65ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=127.0.0.1 ifaddr=0 iftype=ipv4Unnumbered MRU=1500
           label[1]=131071 protocol=3(LDP)
3  10.20.1.6  rtt=7.63ms rc=3(EgressRtr) rsc=1 *A:Dut-A#


*A:Dut-C# oam lsp-trace "p_1" detail
lsp-trace to p_1: 0 hops min, 0 hops max, 116 byte packets
1  10.20.1.2  rtt=3.46ms rc=8(DSRtrMatchLabel)
     DS 1: ipaddr 10.20.1.4 ifaddr 3 iftype 'ipv4Unnumbered' MRU=1500 label=131071
proto=4(RSVP-TE)
2  10.20.1.4  rtt=3.76ms rc=8(DSRtrMatchLabel)
     DS 1: ipaddr 10.20.1.6 ifaddr 3 iftype 'ipv4Unnumbered' MRU=1500 label=131071
proto=4(RSVP-TE)
3  10.20.1.6  rtt=5.68ms rc=3(EgressRtr)
*A:Dut-C#
```

lsp-trace over a numbered IP interface

```
A:Dut-C#
A:Dut-C# oam lsp-trace prefix 5.5.5.5/32 detail
lsp-trace to 5.5.5.5/32: 0 hops min, 0 hops max, 104 byte packets
1  6.6.6.6  rtt=2.45ms rc=8(DSRtrMatchLabel)
     DS 1: ipaddr=5.6.5.1 ifaddr=5.6.5.1 iftype=ipv4Numbered MRU=1564 label=131071
proto=3(LDP)
2  5.5.5.5  rtt=4.77ms rc=3(EgressRtr)
A:Dut-C#
```

lsp-trace over an unnumbered IP interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
*A:Dut-A# oam lsp-trace prefix 10.20.1.6/32 downstream-map-tlv ddmap path-
destination 127.0.0.1 detail lsp-trace to 10.20.1.6/
32: 0 hops min, 0 hops max, 152 byte packets
1  10.20.1.2  rtt=3.44ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=127.0.0.1 ifaddr=0 iftype=ipv4Unnumbered MRU=1500
           label[1]=131070 protocol=3(LDP)
2  10.20.1.4  rtt=4.65ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=127.0.0.1 ifaddr=0 iftype=ipv4Unnumbered MRU=1500
           label[1]=131071 protocol=3(LDP)
3  10.20.1.6  rtt=7.63ms rc=3(EgressRtr) rsc=1 *A:Dut-A#

*A:Dut-A# oam ldp-treetrace prefix 10.20.1.6/32

ldp-treetrace for Prefix 10.20.1.6/32:

         127.0.0.1, ttl =   3 dst =      127.1.0.255 rc = EgressRtr status = Done
    Hops:         127.0.0.1         127.0.0.1

         127.0.0.1, ttl =   3 dst =      127.2.0.255 rc = EgressRtr status = Done
    Hops:         127.0.0.1         127.0.0.1

ldp-treetrace discovery state: Done
ldp-treetrace discovery status: ' OK '
Total number of discovered paths: 2
Total number of failed traces: 0

lsp-trace of a LDP IPv6 prefix FEC



*A:Dut-A# oam lsp-trace prefix fc00::a14:106/128 path-destination ::ffff:127.0.0.1

lsp-trace to fc00::a14:106/128: 0 hops min, 0 hops max, 224 byte packets

1  fc00::a14:102  rtt=1.61ms rc=8(DSRtrMatchLabel) rsc=1

2  fc00::a14:103  rtt=3.51ms rc=8(DSRtrMatchLabel) rsc=1

3  fc00::a14:104  rtt=4.65ms rc=8(DSRtrMatchLabel) rsc=1

4  fc00::a14:106  rtt=7.02ms rc=3(EgressRtr) rsc=1



*A:Dut-A# oam lsp-trace prefix fc00::a14:106/128 path-destination ::ffff:127.0.0.2

lsp-trace to fc00::a14:106/128: 0 hops min, 0 hops max, 224 byte packets

1  fc00::a14:102  rtt=1.90ms rc=8(DSRtrMatchLabel) rsc=1

2  fc00::a14:103  rtt=3.10ms rc=8(DSRtrMatchLabel) rsc=1

3  fc00::a14:105  rtt=4.61ms rc=8(DSRtrMatchLabel) rsc=1

4  fc00::a14:106  rtt=6.45ms rc=3(EgressRtr) rsc=1
```

lsp-trace over SR-ISIS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
*A:Dut-A# oam lsp-trace sr-isis prefix 10.20.1.6/32 igp-instance 0 detail
lsp-trace to 10.20.1.6/32: 0 hops min, 0 hops max, 108 byte packets
1  10.20.1.2  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.4.4 ifaddr=10.10.4.4 iftype=ipv4Numbered MRU=1496
           label[1]=26406 protocol=6(ISIS)
2  10.20.1.4  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.9.6 ifaddr=10.10.9.6 iftype=ipv4Numbered MRU=1496
           label[1]=26606 protocol=6(ISIS)
3  10.20.1.6  rtt=1220324ms rc=3(EgressRtr) rsc=1


*A:Dut-E# oam lsp-trace prefix 10.20.1.2/32 detail downstream-map-tlv ddmap
lsp-trace to 10.20.1.2/32: 0 hops min, 0 hops max, 108 byte packets
1  10.20.1.3  rtt=3.25ms rc=15(LabelSwitchedWithFecChange) rsc=1
     DS 1: ipaddr=10.10.3.2 ifaddr=10.10.3.2 iftype=ipv4Numbered MRU=1496
           label[1]=26202 protocol=6(ISIS)
           fecchange[1]=POP  fectype=LDP IPv4 prefix=10.20.1.2 remotepeer=0.0.0.0 (U
nknown)
           fecchange[2]=PUSH fectype=SR Ipv4 Prefix prefix=10.20.1.2 remotepeer=10.1
0.3.2
2  10.20.1.2  rtt=4.32ms rc=3(EgressRtr) rsc=1
*A:Dut-E#


*A:Dut-B# oam lsp-trace prefix 10.20.1.5/32 detail downstream-map-tlv ddmap sr-isis
lsp-trace to 10.20.1.5/32: 0 hops min, 0 hops max, 108 byte packets
1  10.20.1.3  rtt=2.72ms rc=15(LabelSwitchedWithFecChange) rsc=1
     DS 1: ipaddr=10.11.5.5 ifaddr=10.11.5.5 iftype=ipv4Numbered MRU=1496
           label[1]=262143 protocol=3(LDP)
           fecchange[1]=POP  fectype=SR Ipv4 Prefix prefix=10.20.1.5 remotepeer=0.0.
0.0 (Unknown)
           fecchange[2]=PUSH fectype=LDP IPv4 prefix=10.20.1.5 remotepeer=10.11.5.5
2  10.20.1.5  rtt=4.43ms rc=3(EgressRtr) rsc=1
```

lsp-trace over SR Policy

```
# ipv4 sr-policy lsp-trace
*A:Dut-A# oam lsp-trace sr-policy color 2 endpoint 10.20.1.6 downstream-map-tlv ddma
p path-destination 127.1.1.1 detail lsp-trace to color 2 endpoint 10.20.1.6: 0 hops
min, 0 hops max, 188 byte packets
1  10.20.1.2  rtt=1220323ms rc=3(EgressRtr) rsc=4
1  10.20.1.2  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=3
     DS 1: ipaddr=10.10.3.3 ifaddr=10.10.3.3 iftype=ipv4Numbered MRU=1496
           label[1]=28303 protocol=6(ISIS)
           label[2]=28305 protocol=0(Unknown)
           label[3]=28506 protocol=0(Unknown)
     DS 2: ipaddr=10.10.12.3 ifaddr=10.10.12.3 iftype=ipv4Numbered MRU=1496
           label[1]=28303 protocol=6(ISIS)
           label[2]=28305 protocol=0(Unknown)
           label[3]=28506 protocol=0(Unknown)
2  10.20.1.3  rtt=1220323ms rc=3(EgressRtr) rsc=3
2  10.20.1.3  rtt=1220324ms rc=8(DSRtrMatchLabel) rsc=2
     DS 1: ipaddr=10.10.5.5 ifaddr=10.10.5.5 iftype=ipv4Numbered MRU=1496
           label[1]=28505 protocol=6(ISIS)
           label[2]=28506 protocol=0(Unknown)
     DS 2: ipaddr=10.10.11.5 ifaddr=10.10.11.5 iftype=ipv4Numbered MRU=1496
           label[1]=28505 protocol=6(ISIS)
           label[2]=28506 protocol=0(Unknown)
3  10.20.1.5  rtt=1220325ms rc=3(EgressRtr) rsc=2
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
3  10.20.1.5  rtt=1220325ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.10.6 ifaddr=10.10.10.6 iftype=ipv4Numbered MRU=1496
           label[1]=28606 protocol=6(ISIS)
4  10.20.1.6  rtt=1220325ms rc=3(EgressRtr) rsc=1


# ipv6 sr-policy lsp-trace
*A:Dut-A# oam lsp-trace sr-policy color 500 endpoint fc00::a14:106 lsp-trace to colo
r 500 endpoint fc00::a14:106: 0 hops min, 0 hops max, 204 byte packets
1  fc00::a14:102  rtt=1220323ms rc=3(EgressRtr) rsc=4
1  fc00::a14:102  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=3
2  fc00::a14:103  rtt=1220323ms rc=3(EgressRtr) rsc=3 ^C *A:Dut-A# oam lsp-trace sr-
policy color 500 endpoint fc00::a14:106 downstream-map-tlv ddmap path-destination ::
ffff:127.1.1.1 detail lsp-trace to color 500 endpoint fc00::a14:106: 0 hops min, 0 h
ops max, 260 byte packets
1  fc00::a14:102  rtt=1220323ms rc=3(EgressRtr) rsc=4
1  fc00::a14:102  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=3
     DS 1: ipaddr=fe80::c617:1ff:fe01:2 ifaddr=fe80::c617:1ff:fe01:2 iftype=ipv6Numb
ered MRU=1496
           label[1]=28363 protocol=6(ISIS)
           label[2]=28365 protocol=0(Unknown)
           label[3]=28566 protocol=0(Unknown)
     DS 2: ipaddr=fe80::c415:ffff:fe00:141 ifaddr=fe80::c415:ffff:fe00:141 iftype=ip
v6Numbered MRU=1496
           label[1]=28363 protocol=6(ISIS)
           label[2]=28365 protocol=0(Unknown)
           label[3]=28566 protocol=0(Unknown)
2  fc00::a14:103  rtt=1220323ms rc=3(EgressRtr) rsc=3
2  fc00::a14:103  rtt=1220324ms rc=8(DSRtrMatchLabel) rsc=2
     DS 1: ipaddr=fe80::c61e:1ff:fe01:1 ifaddr=fe80::c61e:1ff:fe01:1 iftype=ipv6Numb
ered MRU=1496
           label[1]=28565 protocol=6(ISIS)
           label[2]=28566 protocol=0(Unknown)
     DS 2: ipaddr=fe80::c61e:1ff:fe01:5 ifaddr=fe80::c61e:1ff:fe01:5 iftype=ipv6Numb
ered MRU=1496
           label[1]=28565 protocol=6(ISIS)
           label[2]=28566 protocol=0(Unknown)
3  fc00::a14:105  rtt=1220325ms rc=3(EgressRtr) rsc=2
3  fc00::a14:105  rtt=1220325ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=fe80::c420:1ff:fe01:2 ifaddr=fe80::c420:1ff:fe01:2 iftype=ipv6Numb
ered MRU=1496
           label[1]=28666 protocol=6(ISIS)
4  fc00::a14:106  rtt=1220326ms rc=3(EgressRtr) rsc=1 *A:Dut-A#
```

lsp-trace over SR-TE

```
*A:Dut-A# oam lsp-trace sr-te "srteABCEDF" downstream-map-tlv ddmap detail
lsp-trace to srteABCEDF: 0 hops min, 0 hops max, 252 byte packets
1  10.20.1.2  rtt=1220323ms rc=3(EgressRtr) rsc=5
1  10.20.1.2  rtt=1220322ms rc=8(DSRtrMatchLabel) rsc=4
     DS 1: ipaddr=10.10.33.3 ifaddr=10.10.33.3 iftype=ipv4Numbered MRU=1520
           label[1]=3 protocol=6(ISIS)
           label[2]=262135 protocol=6(ISIS)
           label[3]=262134 protocol=6(ISIS)
           label[4]=262137 protocol=6(ISIS)
2  10.20.1.3  rtt=1220323ms rc=3(EgressRtr) rsc=4
2  10.20.1.3  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=3
     DS 1: ipaddr=10.10.5.5 ifaddr=10.10.5.5 iftype=ipv4Numbered MRU=1496
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
           label[1]=3 protocol=6(ISIS)
           label[2]=262134 protocol=6(ISIS)
           label[3]=262137 protocol=6(ISIS)
3  10.20.1.5  rtt=1220325ms rc=3(EgressRtr) rsc=3
3  10.20.1.5  rtt=1220325ms rc=8(DSRtrMatchLabel) rsc=2
     DS 1: ipaddr=10.10.11.4 ifaddr=10.10.11.4 iftype=ipv4Numbered MRU=1496
           label[1]=3 protocol=6(ISIS)
           label[2]=262137 protocol=6(ISIS)
4  10.20.1.4  rtt=1220324ms rc=3(EgressRtr) rsc=2
4  10.20.1.4  rtt=1220325ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.9.6 ifaddr=10.10.9.6 iftype=ipv4Numbered MRU=1496
           label[1]=3 protocol=6(ISIS)
5  10.20.1.6  rtt=1220325ms rc=3(EgressRtr) rsc=1


*A:Dut-A# oam lsp-trace sr-te "srteABCE_loose" downstream-map-tlv ddmap detail
lsp-trace to srteABCE_loose: 0 hops min, 0 hops max, 140 byte packets
1  10.20.1.2  rtt=1220323ms rc=3(EgressRtr) rsc=3
1  10.20.1.2  rtt=1220322ms rc=8(DSRtrMatchLabel) rsc=2
     DS 1: ipaddr=10.10.3.3 ifaddr=10.10.3.3 iftype=ipv4Numbered MRU=1496
           label[1]=26303 protocol=6(ISIS)
           label[2]=26305 protocol=6(ISIS)
     DS 2: ipaddr=10.10.12.3 ifaddr=10.10.12.3 iftype=ipv4Numbered MRU=1496
           label[1]=26303 protocol=6(ISIS)
           label[2]=26305 protocol=6(ISIS)
     DS 3: ipaddr=10.10.33.3 ifaddr=10.10.33.3 iftype=ipv4Numbered MRU=1496
           label[1]=26303 protocol=6(ISIS)
           label[2]=26305 protocol=6(ISIS)
2  10.20.1.3  rtt=1220323ms rc=3(EgressRtr) rsc=2
2  10.20.1.3  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.5.5 ifaddr=10.10.5.5 iftype=ipv4Numbered MRU=1496
           label[1]=26505 protocol=6(ISIS)
     DS 2: ipaddr=10.10.11.5 ifaddr=10.10.11.5 iftype=ipv4Numbered MRU=1496
           label[1]=26505 protocol=6(ISIS)
3  10.20.1.5  rtt=1220324ms rc=3(EgressRtr) rsc=1


*A:Dut-F# oam lsp-trace sr-te "srteFECBA_eth" path-destination ::ffff:127.1.1.1 deta
il
lsp-trace to srteFECBA_eth: 0 hops min, 0 hops max, 336 byte packets
1  fc00::a14:105  rtt=1220323ms rc=3(EgressRtr) rsc=4
1  fc00::a14:105  rtt=1220323ms rc=8(DSRtrMatchLabel) rsc=3
     DS 1: ipaddr=fe80::c618:2ff:fe01:1 ifaddr=fe80::c618:2ff:fe01:1 iftype=ipv6Numb
ered MRU=1496
           label[1]=28363 protocol=6(ISIS)
           label[2]=74032 protocol=6(ISIS)
           label[3]=28261 protocol=6(ISIS)
     DS 2: ipaddr=fe80::c618:2ff:fe01:2 ifaddr=fe80::c618:2ff:fe01:2 iftype=ipv6Numb
ered MRU=1496
           label[1]=28363 protocol=6(ISIS)
           label[2]=74032 protocol=6(ISIS)
           label[3]=28261 protocol=6(ISIS)
2  fc00::a14:103  rtt=1220324ms rc=3(EgressRtr) rsc=3
2  fc00::a14:103  rtt=1220324ms rc=8(DSRtrMatchLabel) rsc=2
     DS 1: ipaddr=fe80::c613:1ff:fe01:3 ifaddr=fe80::c613:1ff:fe01:3 iftype=ipv6Numb
ered MRU=1496
           label[1]=3 protocol=6(ISIS)
           label[2]=28261 protocol=6(ISIS)
3  fc00::a14:102  rtt=1220325ms rc=3(EgressRtr) rsc=2
3  fc00::a14:102  rtt=1220325ms rc=8(DSRtrMatchLabel) rsc=1
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
     DS 1: ipaddr=fe80::c0ea:1ff:fe01:1 ifaddr=fe80::c0ea:1ff:fe01:1 iftype=ipv6Numb
ered MRU=1496
           label[1]=28161 protocol=6(ISIS)
4  fc00::a14:101  rtt=1220325ms rc=3(EgressRtr) rsc=1
```

lsp-trace with sr-ospf3

```
# sr-ospf3 lsp-trace
*A:Dut-A# oam lsp-trace sr-ospf3 prefix fc00::a14:106/
128 detail lsp-trace to fc00::a14:106/128: 0 hops min, 0 hops max, 164 byte packets
1  fc00::a14:102  rtt=1.33ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=fe80::c61c:1ff:fe01:1 ifaddr=fe80::c61c:1ff:fe01:1 iftype=ipv6Numb
ered MRU=1496
           label[1]=29466 protocol=5(OSPF)
2  fc00::a14:104  rtt=2.27ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=fe80::c420:1ff:fe01:1 ifaddr=fe80::c420:1ff:fe01:1 iftype=ipv6Numb
ered MRU=1496
           label[1]=29666 protocol=5(OSPF)
3  fc00::a14:106  rtt=2.50ms rc=3(EgressRtr) rsc=1
```

Platforms All

lsp-trace

Syntax **lsp-trace**

Context **[Tree]** (config>saa>test>type-multi-line lsp-trace)

Full Context configure saa test type-multi-line lsp-trace

Description This command creates the context to perform an LSP traceroute using the protocol and data structures defined in IETF RFC 4379 (obsoleted by RFC 8029).

Platforms All

16.278 lsp-wait

lsp-wait

Syntax **lsp-wait** *lsp-wait* [**lsp-initial-wait** *lsp-initial-wait*] [**lsp-second-wait** *lsp-second-wait*]
no lsp-wait

Context **[Tree]** (config>service>vpls>spb>timers lsp-wait)

Full Context configure service vpls spb timers lsp-wait

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to customize LSP generation throttling. Timers that determine when to generate the first, second and subsequent LSPs can be controlled with this command. Subsequent LSPs are generated at increasing intervals of the second **lsp-wait** timer until a maximum value is reached.

Note: The IS-IS timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Parameters *lsp-wait* — Specifies the maximum interval in milliseconds between two consecutive occurrences of an LSP being generated.

Values 10 to 120000

Default 5000

lsp-initial-wait — Specifies the initial LSP generation delay in milliseconds. Values < 100 ms are internally rounded down to 0, so that there is no added initial LSP generation delay.

Values 10 to 100000

Default 10

lsp-second-wait — Specifies the hold time in milliseconds between the first and second LSP generation.

Values 10 to 100000

Default 1000

Platforms All

lsp-wait

Syntax **lsp-wait** *lsp-wait***lsp-initial-wait** [*initial-wait*] [**lsp-second-wait** *second-wait*]

Context **[Tree]** (config>service>vprn>isis>timers lsp-wait)

Full Context configure service vprn isis timers lsp-wait

Description This command is used to customize LSP generation throttling. Timers that determine when to generate the first, second, and subsequent LSPs can be controlled with this command. Subsequent LSPs are generated at increasing intervals of the second **lsp-wait** timer until a maximum value is reached.

Note: The timer granularity is 10 ms if the value is < 500 ms, and 100 ms if the value is ≥ 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *lsp-wait* — Specifies the maximum interval, in milliseconds, between two consecutive occurrences of an LSP being generated.

Values 10 to 120000

Default 5000

initial-wait — Specifies the initial LSP generation delay, in milliseconds. Values less than 100 ms are internally rounded down to 0, so that there is no added initial LSP generation delay.

Values 10 to 100000

Default 10

second-wait — Specifies the hold time, in milliseconds, between the first and second LSP generation.

Values 10 to 100000

Default 1000

Platforms All

lsp-wait

Syntax **lsp-wait** *lsp-wait* [**lsp-initial-wait** *initial-wait*] [**lsp-second-wait** second-wait]

Context **[Tree]** (config>router>isis>timers lsp-wait)

Full Context configure router isis timers lsp-wait

Description This command customizes LSP generation throttling. Timers that determine when to generate the first, second and subsequent LSPs can be controlled with this command. Subsequent LSPs are generated at increasing intervals of the second **lsp-wait** timer until a maximum value is reached.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is greater than or equal to 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default lsp-wait 5000 lsp-initial-wait 10 lsp-second-wait 1000

Parameters *lsp-max-wait* — Specifies the maximum interval in milliseconds between two consecutive occurrences of an LSP being generated.

Values 10 to 120000

initial-wait — Specifies the initial LSP generation delay in milliseconds. Values less than 100 ms are internally rounded down to 0, so that there is no added initial LSP generation delay.

Values 10 to 100000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

second-wait — Specifies the hold time in milliseconds between the first and second LSP generation.

Values 10 to 100000

Platforms All

16.279 lsr-label-route

lsr-label-route

Syntax **lsr-label-route** [{**none** | **all**}]

Context **[Tree]** (config>router>ttl-propagate lsr-label-route)

Full Context configure router ttl-propagate lsr-label-route

Description This command configures the TTL propagation for transit packets at a router acting as an LSR for a BGP label route.

When an LSR swaps the BGP label for a ipv4 prefix packet, therefore acting as a ABR, ASBR, or data-path Route-Reflector (RR) in the base routing instance, or swaps the BGP label for a vpn-ipv4 or vpn-ipv6 prefix packet, therefore acting as an inter-AS Option B VPRN ASBR or VPRN data path Route-Reflector (RR), the all value of this command enables TTL propagation of the decremented TTL of the swapped BGP label into all outgoing LDP or RSVP transport labels.

When an LSR swaps a label or stitches a label, it always writes the decremented TTL value into the outgoing swapped or stitched label. What this feature controls is whether this decremented TTL value is also propagated to the transport label stack pushed on top of the swapped or stitched label.

The none value reverts to the default mode which disables TTL propagation. This changes the existing default behavior which propagates the TTL to the transport label stack. When a customer upgrades, the new default becomes in effect. This command does not have a no version.

This feature also controls the TTL propagation at an LDP-BGP stitching LSR in the LDP to BGP stitching direction. It also controls the TTL propagation in Carrier Supporting Carrier (CsC) VPRN at both the CsC CE and CsC PE.

SR OS does not support ASBR or data path RR functionality for labeled IPv6 routes in the global routing instance (6PE). As such the CLI command of this feature has no impact on prefix packets forwarded in this context.

Default lsr-label-route none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **none** — Specifies that the TTL of the swapped label is not propagated into the transport label stack.

all — Specifies that the TTL of the swapped label is propagated into all labels of the transport label stack.

Platforms All

16.280 lsr-load-balancing

lsr-load-balancing

Syntax **lsr-load-balancing** *hashing-algorithm*
no lsr-load-balancing

Context **[Tree]** (config>service>vprn>nw-if>load-balancing lsr-load-balancing)

Full Context configure service vprn network-interface load-balancing lsr-load-balancing

Description This command specifies whether the IP header is used in the LAG and ECMP LSR hashing algorithm. This is the per interface setting.

Default no lsr-load-balancing

Parameters **lbl-only** — Only the label is used in the hashing algorithm.

lbl-ip — The IP header is included in the hashing algorithm.

ip-only — The IP header is used exclusively in the hashing algorithm.

eth-encap-ip — The hash algorithm parses down the label stack and once it hits the bottom, the stack assumes Ethernet II non-tagged/dot1q or qinq header follows. At the expected Ethertype offset location, algorithm checks whether the value present is IPv4/v6 (0x0800 or 0x86DD). If the check passes, the hash algorithm checks the first nibble at the expected IP header location for IPv4/IPv6 (0x0100/0x0110). If the secondary check passes, the hash is performed using IP SA/DA fields in the expected IP header; otherwise (if any of the checks failed) label-stack hash is performed.

Platforms All

lsr-load-balancing

Syntax **lsr-load-balancing** {**lbl-only** | **lbl-ip** | **ip-only** | **eth-encap-ip** | **lbl-ip-l4-teid**}
no lsr-load-balancing

Context **[Tree]** (config>router>if>load-balancing lsr-load-balancing)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface load-balancing lsr-load-balancing

Description This command specifies whether the IP header is used in the LAG and ECMP LSR hashing algorithm. This is the per interface setting.

Default no lsr-load-balancing

Parameters **lbl-only** — Specifies that only the label is used in the hashing algorithm

lbl-ip — Specifies that only the IP header is included in the hashing algorithm.

ip-only — Specifies that only the IP header is used exclusively in the hashing algorithm

eth-encap-ip — Specifies that the hash algorithm parses down the label stack and once it hits the bottom, the stack assumes Ethernet II non-tagged/dot1q or qinq header follows. At the expected Ethertype offset location, algorithm checks whether the value present is IPv4/v6 (0x0800 or0x86DD). If the check passes, the hash algorithm checks the first nibble at the expected IP header location for IPv4/IPv6 (0x0100/ 0x0110). If the secondary check passes, the hash is performed using IP SA/DA fields in the expected IP header; otherwise (any of the check failed) label-stack hash is performed.

lbl-ip-l4-teid — Specifies that this hashing algorithm hashes based on label, IP header, Layer 4 header and GTP header (TEID) in order. The algorithm uses all the supported headers that are found in the header fragment of incoming traffic.

Platforms All

lsr-load-balancing

Syntax **lsr-load-balancing** *hashing-algorithm*
no lsr-load-balancing

Context **[Tree]** (config>system>load-balancing lsr-load-balancing)

Full Context configure system load-balancing lsr-load-balancing

Description This command configures system-wide LSR load balancing. Hashing can be enabled on the label stack and/or IP header at an LSR for spraying labeled IP packets over multiple equal cost paths and/or over multiple links of a LAG group.

The LSR hash routine operates on the label stack and the IP header if a packet is IPv4. An LSR will consider a packet to be IPv4 if the first nibble following the bottom of the label stack is 4. The hash on label and IPv4 and IPv6 headers can be enabled or disabled at the system level or incoming network IP interface level.

Default no lsr-load-balancing

Parameters **lbl-only** — Specifies that only the label is used in the hashing algorithm

lbl-ip — Specifies that the IP header is included in the hashing algorithm

ip-only — Specifies that the IP header is used exclusively in the hashing algorithm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

eth-encap-ip — Specifies that the hash algorithm parses down the label stack and once it hits the bottom, the stack assumes Ethernet II non-tagged/dot1q or qinq header follows. At the expected Ethertype offset location, the algorithm checks whether the value present is IPv4/v6 (0x0800 or 0x86DD). If the check passes, the hash algorithm checks the first nibble at the expected IP header location for IPv4/IPv6 (0x0100/ 0x0110). If the secondary check passes, the hash is performed using IP SA/DA fields in the expected IP header; if any of the checks fail, the label-stack hash is performed.

lbl-ip-l4-teid — Specifies that this hashing algorithm hashes based on label, IP header, Layer 4 header and GTP header (TEID) in order. The algorithm uses all the supported headers that are found in the header fragment of incoming traffic.

Platforms All

16.281 lub-init-min-pir

lub-init-min-pir

Syntax [**no**] **lub-init-min-pir**

Context **[Tree]** (config>qos>adv-config-policy>child-control>bandwidth-distribution lub-init-min-pir)

Full Context configure qos adv-config-policy child-control bandwidth-distribution lub-init-min-pir

Description This command enables new queues associated with a LUB context to use a minimum PIR similar to the effect of the **limit-pir-zero-drain** command. When a queue is initially created in a LUB context, it defaults to a zero value PIR until H-QoS has an opportunity to configure an offered rate based operational PIR. Enabling this command forces a minimum rate operational PIR to be applied to the queue for use by enqueued packets prior to an H-QoS iteration.

The **no** form of this command reverts to default behavior.

Default no lub-init-min-pir

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17 m Commands

17.1 ma-index-range

ma-index-range

Syntax **ma-index-range start** *ma-index* **end** *ma-index*
no ma-index-range

Context **[Tree]** (config>eth-cfm>md-auto-id ma-index-range)

Full Context configure eth-cfm md-auto-id ma-index-range

Description This command specifies the range of indexes used by SR OS to automatically assign an index to ETH-CFM associations that are created in model-driven interfaces without an index explicitly specified by the user or client.

An association created with an explicitly-specified index cannot use an index in this range. In classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed, which causes any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **md-auto-id** command for further details.

Parameters **start** *ma-index* — Specifies the lower value of the index range. The value must be less than or equal to the **end** value.

Values 1 to 4294967295

end *ma-index* — Specifies the upper value of the index range. The value must be greater than or equal to the **start** value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.2 mac

mac

Syntax **mac** *ieee-address*
no mac

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident mac)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-ident mac)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification mac
configure subscriber-mgmt local-user-db ppp host host-identification mac

Description This command specifies the MAC address to match for a host lookup.

Note: This command is only used when **mac** is configured as one of the **match-list** parameters.

The **no** form of this command removes the MAC address from the configuration.

Parameters *ieee-address* — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac

Syntax [**no**] **mac** *ieee-mac-address*

Context [Tree] (config>service>vprn>if mac)
[Tree] (config>service>vprn>if>ipv6>vrrp mac)
[Tree] (config>service>vprn>if>vrrp mac)
[Tree] (config>service>vprn>sub-if>grp-if mac)
[Tree] (config>service>vprn>nw-if mac)
[Tree] (config>service>vprn>if>sap>eth-cfm>mep mac)

Full Context configure service vprn interface ipv6 vrrp mac
configure service vprn interface mac
configure service vprn interface sap eth-cfm mep mac
configure service vprn interface vrrp mac
configure service vprn network-interface mac
configure service vprn subscriber-interface group-interface mac

Description This command assigns a specific MAC address to a VPRN IP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default The physical MAC address associated with the Ethernet interface on which the SAP is configured.

Parameters *ieee-mac-address* — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface mac

All

- configure service vprn interface ipv6 vrrp mac
- configure service vprn interface vrrp mac
- configure service vprn interface mac
- configure service vprn network-interface mac

mac

Syntax [**no**] **mac** *ieee-address*

Context **[Tree]** (debug>service>id>ppp mac)

Full Context debug service id ppp mac

Description This command shows PPP packets for the specified MAC address.

Parameters *ieee-address* — Enables debugging for the specified MAC address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac

Syntax [**no**] **mac** *ieee-address*

Context **[Tree]** (config>service>vpls>mac-protect mac)

Full Context configure service vpls mac-protect mac

Description This command specifies the 48-bit IEEE 802.3 MAC address.

The **no** form of the command reverts to the default.

Default none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ieee-address* — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers.

Platforms All

mac

Syntax **mac** *ieee-address*
no mac [*ieee-address*]

Context **[Tree]** (config>service>ies>if mac)
[Tree] (config>service>ies>sub-if>grp-if mac)

Full Context configure service ies interface mac
configure service ies subscriber-interface group-interface mac

Description This command assigns a specific MAC address to an IES IP interface.

For Routed Central Office (CO), a group interface has no IP address explicitly configured but inherits an address from the parent subscriber interface when needed. For example, a MAC will respond to an ARP request when an ARP is requested for one of the IPs associated with the subscriber interface through the group interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default The physical MAC address associated with the Ethernet interface that the SAP is configured on (the default MAC address assigned to the interface, assigned by the system).

Parameters *ieee-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff, where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface mac

All

- configure service ies interface mac

mac

Syntax **mac** *ieee-address*
no mac

Context **[Tree]** (config>service>vpls>mcr-default-gtw mac)

Full Context configure service vpls mcr-default-gtw mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command relates to a system configured for Dual Homing in L2-TPSDA. It defines the MAC address used when the system sends out a gratuitous ARP on an active SAP after a ring heals or fails in order to attract traffic from subscribers on the ring with connectivity to that SAP.

The **no** form of this command reverts to the default.

Default no mac

Parameters *ieee-address* — Specifies the address in xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format (cannot be all zeros).

Platforms All

mac

Syntax **mac** *ieee-address*
no mac

Context **[Tree]** (config>eth-tunnel mac)
[Tree] (config>lag mac)
[Tree] (config>port>ethernet mac)
[Tree] (config>port>sonet-sdh>path mac)
[Tree] (config>port>tdm>ds1>channel-group mac)
[Tree] (config>port>tdm>ds3 mac)
[Tree] (config>port>tdm>e1>channel-group mac)
[Tree] (config>port>tdm>e3 mac)

Full Context configure eth-tunnel mac
configure lag mac
configure port ethernet mac
configure port sonet-sdh path mac
configure port tdm ds1 channel-group mac
configure port tdm ds3 mac
configure port tdm e1 channel-group mac
configure port tdm e3 mac

Description This command assigns a specific MAC address to an Ethernet port, Link Aggregation Group (LAG), Ethernet tunnel, or BCP-enabled port or sub-port.

Only one MAC address can be assigned to a port. When multiple **mac** commands are entered, the last command overwrites the previous command. When the command is issued while the port is operational, IP will issue an ARP, if appropriate, and BPDUs are sent with the new MAC address.

The **no** form of this command returns the MAC address to the default value.

By default, a MAC address is assigned by the system from the chassis MAC address pool. The use of an all-zeroes MAC address indicates that an operational MAC address should be assigned from the chassis MAC address pool.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default mac 00:00:00:00:00:00

Parameters *ieee-address* — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path mac

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 mac
- configure port tdm ds1 channel-group mac
- configure port tdm ds3 mac
- configure port tdm e1 channel-group mac

All

- configure port ethernet mac
- configure lag mac

mac

Syntax **mac** *ieee-address*
no mac

Context **[Tree]** (config>eth-tunnel>ethernet mac)

Full Context configure eth-tunnel ethernet mac

Description This command assigns a specific MAC address to an Ethernet port, Link Aggregation Group (LAG), Ethernet tunnel, or BCP-enabled port or sub-port.

Only one MAC address can be assigned to a port. When multiple **mac** commands are entered, the last command overwrites the previous command. When the command is issued while the port is operational, IP will issue an ARP, if appropriate, and BPDUs are sent with the new MAC address.

The **no** form of this command returns the MAC address to the default value.

Default no mac

Parameters *ieee-address* — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses6-byte unicast mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) of the MEP. Using the all zeros address is equivalent to the **no** form of this command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac

Syntax **[no] mac** *ieee-address*

Context **[Tree]** (config>service>proxy-arp-nd>mac-list mac)

Full Context configure service proxy-arp-nd mac-list mac

Description This command configures the proxy ARP or ND MAC address information.

The **no** form of the command deletes the MAC address.

Parameters *ieee-address* — Specifies the MAC address added to the list. The MAC list can be empty or contain up to 10 addresses.

Values xx:xx:xx:xx:xx:xx
xx-xx-xx-xx-xx-xx

Platforms All

mac

Syntax **mac** *ieee-address* [**create**] **black-holemac** *ieee-address* [**create**] **sap** *sap-id* **monitor** {**fwd-status**}
mac *ieee-address* [**create**] **spoke-sdp** *sdp-id:vc-id* **monitor** {**fwd-status**}
no mac ieee-address

Context **[Tree]** (config>service>vpls>static-mac mac)

Full Context configure service vpls static-mac mac

Description This command assigns a conditional static MAC address entry to an SPBM B-VPLS SAP/spoke-SDP allowing external MACs for single and multi-homed operation.

For the 7450 ESS or 7750 SR, this command also assigns a conditional static MAC address entry to an EVPN VPLS SAP/spoke-SDP.

Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

Parameters *ieee-address* — Specifies the static MAC address to an SPBM/sdp-binding interface

Values 6-byte mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) Cannot be all zeros.

sap-id — Specifies the SAP identifier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sdp-id — Specifies the SDP identifier

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier

Values 1 to 4294967295

create — This keyword is mandatory while creating a static MAC

fwd-status — Specifies that this static mac is based on the forwarding status of the SAP or spoke-SDP for multi-homed operation.

black-hole — Specifies for TLS FDB entries defined on a local SAP the value 'sap', remote entries defined on an SDP have the value 'sdp'.

Platforms All

mac

Syntax [**no**] **mac** *ieee-address*

Context **[Tree]** (config>service>ipipe>sap mac)

Full Context configure service ipipe sap mac

Description This command assigns a specific MAC address to an Ipipe SAP.

The **no** form of this command returns the MAC address of the SAP to the default value.

Default The physical MAC address associated with the Ethernet interface where the SAP is configured.

Parameters *ieee-address* — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers.

Platforms All

mac

Syntax **mac** *mac-filter-id*
no mac

Context **[Tree]** (config>service>template>epipe-sap-template>egress>filter mac)
[Tree] (config>service>template>epipe-sap-template>ingress>filter mac)

Full Context configure service template epipe-sap-template egress filter mac
configure service template epipe-sap-template ingress filter mac

Description This command associates an existing MAC filter policy with the template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

Parameters *mac-filter-id* — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mac

Syntax **mac** *name*
no mac

Context **[Tree]** (config>service>template>epipe-sap-template>egress>filter-name mac)
[Tree] (config>service>template>epipe-sap-template>ingress>filter-name mac)

Full Context configure service template epipe-sap-template egress filter-name mac
configure service template epipe-sap-template ingress filter-name mac

Description This command associates an existing IP filter policy with the template.

Parameters *name* — Specifies the MAC filter policy name, up to 64 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mac

Syntax **mac** *ieee-address* [**mask** *six-byte-mask*]
no mac *ieee-address*

Context **[Tree]** (config>service>mac-list mac)

Full Context configure service mac-list mac

Description This command adds a protected MAC address entry.

The **no** form of this command removes the protected MAC address entry.

Parameters *ieee-address* — Specifies the address in xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format (cannot be all zeros), up to 30 characters.

six-byte-mask — Specifies the mask address in xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format (cannot be all zeros), up to 30 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac

Syntax **mac** *ieee-address*
no mac

Context **[Tree]** (config>service>vpls>interface mac)

Full Context configure service vpls interface mac

Description This command assigns a specific MAC address to a VPLS IP interface.

For Routed Central Office (CO), a group interface has no IP address explicitly configured but inherits an address from the parent subscriber interface when needed. For example, a MAC will respond to an ARP request when an ARP is requested for one of the IPs associated with the subscriber interface through the group interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default mac

Parameters *ieee-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Default The system chassis MAC address.

Platforms All

mac

Syntax **mac** *name*
no mac

Context **[Tree]** (config>service>template>vpls-sap-template>egress>filter-name mac)
[Tree] (config>service>template>vpls-sap-template>ingress>filter-name mac)

Full Context configure service template vpls-sap-template egress filter-name mac
configure service template vpls-sap-template ingress filter-name mac

Description This command associates an existing IP filter policy with the template.

Parameters *name* — Specifies the MAC filter policy name, up to 64 characters.

Platforms All

mac

Syntax [**no**] **mac** *ieee-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>service>id>arp-host mac)

Full Context debug service id arp-host mac

Description This command displays ARP host events for a particular MAC address.

Parameters *mac-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx (cannot be all zeros)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac

Syntax [**no**] **mac** *ieee-address*

Context [Tree] (debug>service>id>igmp-snooping mac)

Full Context debug service id igmp-snooping mac

Description This command shows IGMP packets for the specified MAC address.

The **no** form of this command disables the MAC debugging.

Platforms All

mac

Syntax [**no**] **mac** *ieee-address*

Context [Tree] (debug>service>id>mld mac)

Full Context debug service id mld-snooping mac

Description This command shows MLD packets for the specified MAC address.

The **no** form of this command disables the MAC debugging.

Platforms All

mac

Syntax [**no**] **mac** *ieee-address*

Context [Tree] (debug>service>id>host-connectivity-verify mac)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug service id host-connectivity-verify mac

Description This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular MAC address.

Parameters *mac-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx (cannot be all zeros)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac

Syntax **mac** *mac-address*
no mac

Context **[Tree]** (config>service>ies>if>ipv6>vrrp mac)

Full Context configure service ies interface ipv6 vrrp mac

Description This command assigns a specific MAC address to an IES IP interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default The physical MAC address associated with the Ethernet interface that the SAP is configured on (the default MAC address assigned to the interface, assigned by the system).

Parameters *mac-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms All

mac

Syntax **mac** *mac-address*
no mac

Context **[Tree]** (config>service>ies>if>vrrp mac)

Full Context configure service ies interface vrrp mac

Description This command assigns a specific MAC address to an IES IP interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default The physical MAC address associated with the Ethernet interface that the SAP is configured on (the default MAC address assigned to the interface, assigned by the system).

Parameters *mac-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff, where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms All

mac

Syntax **mac** *ieee-address*
no mac

Context **[Tree]** (config>router>if mac)

Full Context configure router interface mac

Description This command assigns a specific MAC address to an IP interface. Only one MAC address can be assigned to an IP interface. When multiple **mac** commands are entered, the last command overwrites the previous command.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default no mac

Parameters *ieee-address* — Specifies the 48-bit MAC address for the IP interface in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff,* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms All

mac

Syntax **mac** *mac-address*
no mac

Context **[Tree]** (config>router>if>vrrp mac)
[Tree] (config>router>if>ipv6>vrrp mac)

Full Context configure router interface ipv6 vrrp mac
configure router interface vrrp mac

Description This command sets an explicit MAC address used by the virtual router instance overriding the VRRP default derived from the VRID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Changing the default MAC address is useful when an existing HSRP or other non-VRRP default MAC is in use by the IP hosts using the virtual router IP address. Many hosts do not monitor unessential ARPs and continue to use the cached non-VRRP MAC address after the virtual router becomes master of the host's gateway address.

The **mac** command sets the MAC address used in ARP responses when the virtual router instance is master. Routing of IP packets with *mac-address* as the destination MAC is also enabled. The **mac** setting must be the same for all virtual routers participating as a virtual router or indeterminate connectivity by the attached IP hosts will result. All VRRP advertisement messages are transmitted with *mac-address* as the source MAC.

The command can be configured in both non-owner and owner **vrrp** nodal contexts.

The **mac** command can be executed at any time and takes effect immediately. When the virtual router MAC on a master virtual router instance changes, a gratuitous ARP is immediately sent with a VRRP advertisement message. If the virtual router instance is disabled or operating as backup, the gratuitous ARP and VRRP advertisement message is not sent.

The **no** form of the command restores the default VRRP MAC address to the virtual router instance.

Default no mac — The virtual router instance uses the default VRRP MAC address derived from the VRID.

Parameters *mac-address* — The 48-bit MAC address for the virtual router instance in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC, and non-IEEE reserved MAC addresses.

Platforms All

mac

Syntax **mac** *index* **name** *mac-name*
no mac *index*

Context **[Tree]** (config>system>security>ssh>client-mac-list mac)
[Tree] (config>system>security>ssh>server-mac-list mac)

Full Context configure system security ssh client-mac-list mac
configure system security ssh server-mac-list mac

Description This command allows the user to configure SSH MAC algorithms for SR OS as an SSH server or an SSH client.

The **no** form of this command removes the specified **mac** index.

Default no mac *index*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *index* — Specifies the index of the algorithm in the list.

Values 1 to 255

mac-name — Specifies the algorithm for calculating the message authentication code.

Values Table 79 lists the default client/server algorithms used for SSHv2.

Table 79 **SSHv2 Default client/server algorithms**

index	mac-name
200	hmac-sha2-512
210	hmac-sha2-256
215	hmac-sha1
220	hmac-sha1-96
225	hmac-md5
230	hmac-ripemd160
235	hmac-ripemd160-openssh-com
240	hmac-md5-96

Platforms All

mac

Syntax **mac** *mac-id* [**create**]
no mac *mac-id*

Context **[Tree]** (config>card>mda>xconnect mac)
[Tree] (config>card>xiom>mda>xconnect mac)

Full Context configure card mda xconnect mac
configure card xiom mda xconnect mac

Description This command creates a loopback in the MAC chip. It does not require the allocation of a faceplate. After the loopback is instantiated, a PXC can be configured on top of it.

For a list of MAC chip IDs per forwarding complex (datapath), use the **show datapath datapath-id** *datapath-id* command.

When considering loopback creation, the operation should consider the MAC chip's bandwidth capacity and the bandwidth utilization of all the faceplate ports connected to it.The selection of MAC chips for loopback creation should be taken into consideration.

The **no** form of this command removes the MAC ID from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac-id* — Specifies the MAC ID.

Values 1 to 12

create — Keyword used to create the MAC ID instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

- configure card mda xconnect mac

7750 SR-s

- configure card xiom mda xconnect mac

17.3 mac-address

mac-address

Syntax [**no**] **mac-address**

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute mac-address)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute mac-address)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute mac-address
configure subscriber-mgmt authentication-policy include-radius-attribute mac-address

Description This command enables the generation of the client MAC address RADIUS attribute.

The **no** form of this command disables the generation of the client MAC address RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac-address

Syntax **mac-address** *ieee-address*
no mac-address

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query mac-address)

Full Context configure subscriber-mgmt wlan-gw ue-query mac-address

Description This command enables matching on UEs with the specified MAC address.

The **no** form of this command disables matching on the MAC address.

Default no mac-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ieee-address* — Specifies the ethernet MAC address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep mac-address)
[Tree] (config>eth-tunnel>path>eth-cfm>mep mac-address)

Full Context configure eth-ring path eth-cfm mep mac-address
configure eth-tunnel path eth-cfm mep mac-address

Description This command specifies the MAC address of the MEP.

The **no** form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke SDP).

Parameters *mac-address* — Specifies the MAC address of the MEP.

Values 6-byte unicast mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) of the MEP. Using the all zeros address is equivalent to the **no** form of this command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context **[Tree]** (config>lag>eth-cfm>mep mac-address)
[Tree] (config>port>ethernet>eth-cfm>mep mac-address)
[Tree] (config>router>if>eth-cfm>mep mac-address)

Full Context configure lag eth-cfm mep mac-address
configure port ethernet eth-cfm mep mac-address
configure router interface eth-cfm mep mac-address

Description This command specifies the MAC address of the MEP.

The **no** form of this command reverts to the MAC address of the MEP back to the default, that of the port, since this is SAP based.

Default no mac-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac-address* — Specifies the MAC address of the MEP.

Values 6-byte unicast mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) of the MEP. Using the all zeros address is equivalent to the no form of this command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context **[Tree]** (config>service>epipe>spoke-sdp>eth-cfm>mep mac-address)

Full Context configure service epipe spoke-sdp eth-cfm mep mac-address

Description This command specifies the MAC address of the MEP.

The **no** form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke).

Parameters *mac-address* — Specifies the MAC address of the MEP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MEP. Must be unicast. Using the all zeros address is equivalent to the no form of this command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context **[Tree]** (config>service>vpls>eth-cfm>mep mac-address)
[Tree] (config>service>vpls>sap>eth-cfm>mep mac-address)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep mac-address)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep mac-address)

Full Context configure service vpls eth-cfm mep mac-address
configure service vpls mesh-sdp eth-cfm mep mac-address
configure service vpls sap eth-cfm mep mac-address
configure service vpls spoke-sdp eth-cfm mep mac-address

Description This command specifies the MAC address of the MEP.

The **no** form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac-address* — Specifies the MAC address of the MEP

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MEP. Must be unicast. Using the all zeros address is equivalent to the no form of this command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac-address

Syntax **mac-address** *mac-address*

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep mac-address)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep mac-address)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm mac-address)

Full Context configure service vprn interface sap eth-cfm mep mac-address
configure service vprn interface spoke-sdp eth-cfm mep mac-address
configure service vprn subscriber-interface group-interface sap eth-cfm mac-address

Description This command assigns a specific MAC address to an IP interface.

The **no** form of this command returns the MAC address of the IP interface to the default value.

Default The physical MAC address associated with the Ethernet interface that the SAP is configured on.

Parameters *mac-address* — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac-address

Syntax [**no**] **mac-address**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes mac-address)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes mac-address)

Full Context configure aaa isa-radius-policy acct-include-attributes mac-address
configure aaa isa-radius-policy auth-include-attributes mac-address

Description This command enables the generation of the client MAC address RADIUS attribute.

Default no mac-address

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context **[Tree]** (config>system>satellite>eth-sat mac-address)
[Tree] (config>system>satellite>tdm-sat mac-address)

Full Context configure system satellite eth-sat mac-address
configure system satellite tdm-sat mac-address

Description This command configures the MAC address for the associated satellite chassis. This MAC address is used to validate the identity of an satellite that attempts to associate with the local host.

The **no** form of the command deletes the MAC address for the associated satellite.

Parameters *mac-address* — Specifies the MAC address of the associated satellite chassis; do not use a broadcast or multicast MAC. Enter the MAC address in either of the following formats: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure system satellite eth-sat mac-address

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure system satellite tdm-sat mac-address

mac-address

Syntax **mac-address** *ieee-address*
no mac-address *ieee-address*

Context **[Tree]** (config>port>ethernet>dot1x>per-host-authentication>allowed-source-macs mac-address)

Full Context configure port ethernet dot1x per-host-authentication allowed-source-macs mac-address

Description This command configures the host MAC address on the allowed MAC list.

The **no** form of the command deletes the MAC address from the list.

Default no mac

Parameters *ieee-address* — Specifies the MAC address.

Values xx:xx:xx:xx:xx:xx

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.4 mac-advertisement

mac-advertisement

Syntax [**no**] **mac-advertisement**

Context **[Tree]** (config>service>vpls>bgp-evpn mac-advertisement)

Full Context configure service vpls bgp-evpn mac-advertisement

Description The mac-advertisement command enables the advertisement in BGP of the learned macs on SAPs and SDP bindings. When the mac-advertisement is disabled, the local macs will be withdrawn in BGP.

Default mac-advertisement

Platforms All

17.5 mac-criteria

mac-criteria

Syntax [**no**] **mac-criteria**

Context **[Tree]** (config>qos>sap-ingress mac-criteria)

Full Context configure qos sap-ingress mac-criteria

Description The **mac-criteria** based SAP ingress policies are used to select the appropriate ingress queue and corresponding forwarding class for matched traffic.

This command is used to enter the node to create or edit policy entries that specify MAC criteria.

Router implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit.

The **no** form of this command deletes all the entries specified under this node. When mac-criteria entries are removed from a SAP ingress policy, the mac-criteria is removed from all services where that policy is applied.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.6 mac-da-hashing

mac-da-hashing

Syntax [**no**] **mac-da-hashing**

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only mac-da-hashing)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters mac-da-hashing

Description This command specifies whether subscriber traffic egressing a LAG SAP has its egress LAG link selected by a function of the MAC destination address instead of the subscriber ID.

This command is only meaningful if subscriber management is enabled and can be configured for a VPLS service.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac-da-hashing

Syntax **mac-da-hashing**
no mac-da-hashing

Context **[Tree]** (config>service>vpls>sap>sub-sla-mgmt mac-da-hashing)

Full Context configure service vpls sap sub-sla-mgmt mac-da-hashing

Description This command specifies whether subscriber traffic egressing a LAG SAP has its egress LAG link selected by a function of the MAC destination address instead of the subscriber ID.

The **no** form of this command reverts to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.7 mac-duplication

mac-duplication

Syntax **mac-duplication**

Context **[Tree]** (config>service>vpls>bgp-evpn mac-duplication)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls bgp-evpn mac-duplication

Description Commands in this context configure the BGP EVPN MAC duplication parameters.

Platforms All

17.8 mac-filter

mac-filter

Syntax **mac-filter** *mac-filter-id* **entry** *entry-id* [*entry-id*]
no mac-filter *mac-filter-id* [**entry** *entry-id*]

Context **[Tree]** (config>mirror>mirror-source mac-filter)

Full Context configure mirror mirror-source mac-filter

Description This command enables mirroring of packets that match specific entries in an existing MAC filter.

The **mac-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The MAC filter must already exist in order for the command to execute. Filters are configured in the config>filter context. If the MAC filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IP interface, an error is not be generated but mirroring will not be enabled (there are no packets to mirror). Once the filter is defined to a SAP or MAC interface, mirroring is enabled.

If the MAC filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

If the MAC filter is defined as egress, only egress packets are mirrored. Egress mirrored packets are mirrored to the mirror destination after all egress packet modifications.

An *entry-id* within a MAC filter can only be mirrored to a single mirror destination. If the same *entry-id* is defined multiple times, an error occurs and only the first **mirror-source** definition is in effect.

By default, no packets matching any MAC filters are mirrored. Mirroring of MAC filter entries must be explicitly defined.

The **no mac-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *mac-filter-id*.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring of that list of *entry-id*'s is terminated within the *mac-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

Parameters *mac-filter-id* — Specifies the MAC filter ID whose entries are mirrored. If the *mac-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *mac-filter-id* is defined on a SAP.

entry-id — Specifies the MAC filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. Multiple *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space. Up to 8 entry IDs may be specified in a single command.

Each *entry-id* must exist within the *mac-filter-id*. If the *entry-id* is renumbered within the MAC filter definition, the old *entry-id* is removed from the list and the new *entry-id* will need to be manually added to the list if mirroring is still desired.

If no *entry-id* entries are specified in the command, mirroring will not occur for that MAC filter ID. The command will have no effect.

Platforms All

mac-filter

Syntax [**no**] **mac-filter** *mac-filter-id*

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block mac-filter)

Full Context configure li li-filter-block-reservation li-reserved-block mac-filter

Description This command configures to which normal MAC filters the entry reservation is applied.

This command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**).

Parameters *mac-filter-id* — The filter identification identifies the normal MAC filters.

Values {*filter-id* | *filter-name*}

filter-id:	1 to 65535
filter-name:	up to 64 characters (*filter-name* is an alias for input only. The *filter-name* gets replaced with an id automatically by SR OS in the configuration).

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-filter

Syntax [**no**] **mac-filter** *mac-filter-id*

Context **[Tree]** (config>li>li-filter-assoc>li-mac-fltr mac-filter)

Full Context configure li li-filter-associations li-mac-filter mac-filter

Description Specifies the MAC filter(s) into which the entries from the specified **li-mac-filter** are to be inserted. The **li-mac-filter** and **mac-filter** must already exist before the association is made. If the normal MAC filter is deleted then the association is also removed (and not re-created if the MAC filter comes into existence in the future).

The **no** form of this command removes the MAC filter ID from the configuration.

Parameters *mac-filter-id* — Specifies a filter identification to identify the MAC filter.

Values 1 to 65536, *name*: up to 64 characters

Platforms All

mac-filter

Syntax **mac-filter** *mac-filter-id* **entry** *entry-id* [*entry-id*] [**intercept-id** *intercept-id* [*intercept-id*]] [**session-id** [*session-id*] [[*session-id*]]]
no mac-filter *mac-filter-id*

Context **[Tree]** (config>li>li-source mac-filter)

Full Context configure li li-source mac-filter

Description This command enables lawful interception (LI) of packets that match specific entries in an existing MAC filter. Multiple entries can be created using unique *entry-id* numbers within the filter. The router implementation exits the filter on the first match found and executes the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword **action** for it to be considered complete. Entries without the **action** keyword will be considered incomplete and hence will be rendered inactive.

An *entry-id* within an MAC filter can only be intercepted to a single destination. If the same *entry-id* is defined multiple times, an error occurs and only the first definition is in effect.

The **no** form of this command removes the specified entry from the IP or MAC filter. Entries removed from the IP or MAC filter are immediately removed from all services or network ports where that filter is applied.

Parameters *mac-filter-id* — Specifies the MAC filter ID. If the *mac-filter-id* does not exist, an error will occur and the command will not execute.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

entry-id — The MAC filter entries to use as match criteria.

intercept-id — Specifies the intercept-id that is inserted into the packet header for all mirrored packets of the associated li-source entry. This *intercept-id* can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. For all types of **li-source** entries (filter, nat, sap, subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, an *intercept-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *intercept-id* configured for an **li-source** entry, then the default value will be inserted. When the mirror service is configured with **ip-gre** routable encap, no *intercept-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4294967295 (32b) — For nat li-source entries that are using a mirror service that is not configured with routable encapsulation

Values 1 to 1,073,741,824 (30b) — For all types of li-source entries that are using a mirror service with routable **ip-udp-shim** encapsulation and no direction-bit.

Values 1 to 536,870,912 (29b) — For all types of li-source entries that are using a mirror service with routable **ip-udp-shim** encapsulation and with the direction-bit enabled.

session-id — Specifies the *session-id* that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This *session-id* can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. The *session-id* is only valid and used for mirror services that are configured with **ip-udp-shim** routable encap (**config>mirror>mirror-dest>encap>ip-udp-shim**). For all types of **li-source** entries (filter, nat, sap, or subscriber), when the mirror service is configured with **ip-udp-shim** routable encap, a *session-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *session-id* configured for an **li-source** entry, then the default value will be inserted. When a mirror service is configured with **ip-gre** routable encap, no *session-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4,294,967,295 (32b)

Platforms All

mac-filter

Syntax **mac-filter** *mac-filter-id* **entry** *entry-id* [*entry-id*]
no mac-filter *mac-filter-id* [**entry** *entry-id*]

Context **[Tree]** (debug>mirror-source mac-filter)

Full Context debug mirror-source mac-filter

Description This command enables mirroring of packets that match specific entries in an existing MAC filter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **mac-filter** command directs packets which match the defined list of entry IDs to be mirrored to the mirror destination referenced by the *mirror-dest-service-id* of the **mirror-source**.

The MAC filter must already exist in order for the command to execute. Filters are configured in the config>filter context. If the MAC filter does not exist, an error will occur. If the filter exists but has not been associated with a SAP or IP interface, an error is not be generated but mirroring will not be enabled (there are no packets to mirror). Once the filter is defined to a SAP or MAC interface, mirroring is enabled.

If the MAC filter is defined as ingress, only ingress packets are mirrored. Ingress mirrored packets are mirrored to the mirror destination prior to any ingress packet modifications.

If the MAC filter is defined as egress, only egress packets are mirrored. Egress mirrored packets are mirrored to the mirror destination after all egress packet modifications.

An *entry-id* within a MAC filter can only be mirrored to a single mirror destination. If the same *entry-id* is defined multiple times, an error occurs and only the first **mirror-source** definition is in effect.

By default, no packets matching any MAC filters are mirrored. Mirroring of MAC filter entries must be explicitly defined.

The **no mac-filter** command, without the **entry** keyword, removes mirroring on all *entry-id*'s within the *mac-filter-id*.

When the **no** command is executed with the **entry** keyword and one or more *entry-id*'s, mirroring of that list of *entry-id*'s is terminated within the *mac-filter-id*. If an *entry-id* is listed that does not exist, an error will occur and the command will not execute. If an *entry-id* is listed that is not currently being mirrored, no error will occur for that *entry-id* and the command will execute normally.

Parameters *mac-filter-id* — The MAC filter ID whose entries are mirrored. If the *mac-filter-id* does not exist, an error will occur and the command will not execute. Mirroring of packets will commence once the *mac-filter-id* is defined on a SAP.

entry-id — The MAC filter entries to use as match criteria for packet mirroring. The **entry** keyword begins a list of *entry-id*'s for mirroring. Multiple *entry-id* entries may be specified with a single command. Each *entry-id* must be separated by a space. Up to 8 entry IDs may be specified in a single command.

Each *entry-id* must exist within the *mac-filter-id*. If the *entry-id* is renumbered within the MAC filter definition, the old *entry-id* is removed from the list and the new *entry-id* will need to be manually added to the list if mirroring is still desired.

If no *entry-id* entries are specified in the command, mirroring will not occur for that MAC filter ID. The command will have no effect.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-filter

Syntax **mac-filter** *filter-id* [**create**] [**name** *name*]
mac-filter {*filter-id* | *filter-name*}
no mac-filter {*filter-id* | *filter-name*}

Context **[Tree]** (config>filter mac-filter)

Full Context configure filter mac-filter

Description This command, creates a configuration context for the specified MAC filter policy.

The **no** form of the command deletes the MAC filter policy. A filter policy cannot be deleted until it is removed from all objects where it is applied.

Parameters *filter-id* — Specifies the MAC filter policy ID expressed as a decimal integer.

Values 1 to 65535

create — This keyword is required to create the configuration context. After it is created, the context can be enabled with or without the **create** keyword.

name — Configures an optional filter name, up to 64 characters in length, to a given filter. This filter name can then be used in configuration references, display, and show commands throughout the system. A defined filter name can help the service provider or administrator to identify and manage filters within the SR OS platforms.

To create a filter, you must assign a filter ID, however, after it is created, either the filter ID or filter name can be used to identify and reference a filter.

If a name is not specified at creation time, then SR OS assigns a string version of the *filter-id* as the name.

Filter names may not begin with an integer (0 to 9).

Values *name*: 64 characters maximum

filter-name — A string of up to 64 characters uniquely identifying this MAC filter policy

Platforms All

mac-filter

Syntax [**no**] **mac-filter**

Context **[Tree]** (config>system>security>mgmt-access-filter mac-filter)

Full Context configure system security management-access-filter mac-filter

Description This command configures a management access MAC-filter.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-filter

Syntax [**no**] **mac-filter**

Context **[Tree]** (config>system>security>cpm-filter mac-filter)

Full Context configure system security cpm-filter mac-filter

Description Commands in this context configure CPM MAC-filter parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mac-filter

Syntax **ip-filter** *src-filter-id* [**src-entry** *src-entry-id*] **to** *dst-filter-id* [**dst-entry** *dst-entry-id*] [**overwrite**]

Context **[Tree]** (config>filter>copy mac-filter)

Full Context configure filter copy mac-filter

Description This command copies an existing filter entry for a specific filter ID to another filter ID. The **copy** command is a configuration level maintenance tool used to create new entries using an existing filter policy. If **overwrite** is not specified, an error will occur if the destination filter entry exists.

Parameters *src-filter-id* — Identifies the source filter policy from which the copy command will attempt to copy. The filter policy must exist within the context of the preceding keyword (**mac-filter**).

dst-filter-id — Identifies the destination filter policy to which the copy command will attempt to copy. If the **overwrite** keyword is not specified, the filter entry ID cannot already exist in the destination filter policy. If the **overwrite** keyword is present, the destination entry ID may or may not exist.

overwrite — Specifies that the destination filter entry may exist. If it does, everything in the existing destination filter entry will be completely overwritten with the contents of the source filter entry. If the destination filter entry exists, either **overwrite** must be specified or an error message will be returned. If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.9 mac-filter-name

mac-filter-name

Syntax [**no**] **mac-filter-name** *filter-name*

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block mac-filter-name)

Full Context configure li li-filter-block-reservation li-reserved-block mac-filter-name

Description This command configures a MAC filter in which the reservation is done through name.

The **no** form of this command removes the MAC filter name.

Parameters *filter-name* — Specifies the MAC filter name, up to 64 characters.

Platforms All

mac-filter-name

Syntax [**no**] **mac-filter-name** *filter-name*

Context **[Tree]** (config>li>li-filter-assoc>li-mac-fltr mac-filter-name)

Full Context configure li li-filter-associations li-mac-filter mac-filter-name

Description This command associates a MAC filter with a specified LI MAC filter through its name.

The **no** form of this command removes the MAC filter name.

Parameters *filter-name* — Specifies the MAC filter name, up to 64 characters.

Platforms All

17.10 mac-format

mac-format

Syntax **mac-format** *format*
no mac-format

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>match-radprox-cache mac-format)

Full Context configure subscriber-mgmt local-user-db ipoe host match-radius-proxy-cache mac-format

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the format of MAC address used for matching incoming DHCP DISCOVER against the RADIUS proxy cache.

The **no** form of this command reverts to the default.

Default mac-format "aa:"

Parameters *format* — Specifies the format string that specifies the format of MAC address.

Values
mac-format: (only when match is equal to mac)
like ab: for 00:0c:f1:99:85:b8
or XY- for 00-0C-F1-99-85-B8
or mmmm. for 0002.03aa.abff
or xx for 000cf19985b8

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mac-format

Syntax **mac-format** *mac-format*
no mac-format

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx mac-format)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq mac-format)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy mac-format)

Full Context configure subscriber-mgmt diameter-application-policy gx mac-format
configure subscriber-mgmt diameter-application-policy gy mac-format
configure subscriber-mgmt diameter-application-policy nasreq mac-format

Description This command configures the format of the MAC address when reported in Gx, Gy, or NASREQ application message AVPs such as Calling-Station-Id or User-Name.

The **no** form of this command resets the command to the default setting.

Default mac-format ab

Parameters *mac-format* — Specifies the MAC address format.

Values like ab: for 00:0c:f1:99:85:b8
or XY- for 00-0C-F1-99-85-B8
or mmmm. for 0002.03aa.abff
or xx for 000cf19985b8

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-format

Syntax **mac-format** *mac-format*
no mac-format

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>track-mobility mac-format)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>track-mobility mac-format)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range track-mobility mac-format
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range track-mobility mac-format

Description This command configures how the MAC address is represented by the RADIUS proxy server.

Default no mac-format "aa:"

Parameters *mac-format* — Specifies how the MAC address is represented by the RADIUS proxy server.

Values

mac-format	like ab: for 00:0c:f1:99:85:b8
	or XY- for 00-0C-F1-99-85-B8
	or mmmm. for 0002.03aa.abff
	or xx for 000cf19985b8

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.11 mac-learning-options

mac-learning-options

Syntax [**no**] mac-learning-options

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host-mgmt mac-learning-options)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host-mgmt mac-learning-options)

Full Context configure service ies subscriber-interface group-interface sap static-host-mgmt mac-learning-options
configure service vprn subscriber-interface group-interface sap static-host-mgmt mac-learning-options

Description This command configures additional methods by which the BNG learns the subscriber host MAC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.12 mac-linking

mac-linking

Syntax **mac-linking** *ip-address*
no mac-linking

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host mac-linking)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host mac-linking)

Full Context configure service ies subscriber-interface group-interface sap static-host mac-linking
configure service vprn subscriber-interface group-interface sap static-host mac-linking

Description This command associates this IPv6 host to the specified IPv4 host through the learned MAC address. A learned MAC from the IPv6 host is associated with the IPv4 host and vice versa.

The **no** form of this command removes the IP address from the configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.13 mac-list

mac-list

Syntax **mac-list** *name* [**create**]
no mac-list *name*

Context **[Tree]** (config>service>proxy-arp-nd mac-list)

Full Context configure service proxy-arp-nd mac-list

Description This command creates a list of MAC addresses that can be pointed at from the service for a specified IP. The list may contain up to 10 MAC addresses; an empty list is also allowed.

The MAC list allows on-the-fly changes, but a change in the list deletes the proxy entries for all the IPs using that list.

The **no** form of the command deletes the entire MAC-list. Deleting a MAC list is only possible if it is not referenced in the configuration.

Parameters *name* — Specifies the name of the MAC address list, which can be up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Mandatory keyword to create a MAC list.

Platforms All

mac-list

Syntax **mac-list** *name*
no mac-list

Context **[Tree]** (config>service>vpls>proxy-arp>dynamic mac-list)
[Tree] (config>service>vpls>proxy-nd>dynamic mac-list)

Full Context configure service vpls proxy-arp dynamic mac-list
configure service vpls proxy-nd dynamic mac-list

Description This command associates a previously created MAC list to a dynamic IP. The MAC list is created using the **config**>**service**>**proxy-arp-nd**>**mac-list** command.

The **no** form of the command deletes the association of the MAC list and the dynamic IP.

Parameters *name* — The name of the MAC list previously created using the **config**>**service**>**proxy-arp-nd**>**mac-list** command.

Platforms All

mac-list

Syntax **mac-list** *name* [**create**]
no mac-list *name*

Context **[Tree]** (config>service mac-list)

Full Context configure service mac-list

Description This command configures a MAC list name. The MAC list is composed of a list of MAC addresses and masks, which along with Auto-Learn Mac Protect (ALMP) can be used to exclude certain MACs from being protected in a given object. This is typically used on SAPs and spoke SDPs configured with ALMP where certain MACs must be able to move to other objects (for example, VRRP virtual MACs).

The **no** form of this command removes the MAC list name.

Parameters *name* — Specifies the MAC list name, up to 32 characters.

create — Keyword used to create the MAC list.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.14 mac-move

mac-move

Syntax [**no**] **mac-move**

Context **[Tree]** (config>service>vpls mac-move)
[Tree] (config>service>template>vpls-template mac-move)

Full Context configure service template vpls-template mac-move
configure service vpls mac-move

Description Commands in this context configure MAC move attributes. A sustained high re-learn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the mac-move feature is an alternative way to protect your network against loops.

When enabled in a VPLS, **mac-move** monitors the re-learn rate of each MAC. If the rate exceeds the configured maximum allowed limit, it disables the SAP where the source MAC was last seen. The SAP can be disabled permanently (until a **shutdown**/**no shutdown** command is executed) or for a length of time that grows linearly with the number of times the specified SAP was disabled. You have the option of marking a SAP as non-blockable in the **config>service>vpls>sap>limit-mac-move** or **config>service>vpls>spoke-sdp>limit-mac-move** contexts. This means that when the re-learn rate has exceeded the limit, another (blockable) SAP will be disabled instead.

The **mac-move** command enables the feature at the service level for SAPs and spoke-SDPs, as only those objects can be blocked by this feature. Mesh SDPs are never blocked, but their re-learn rates (sap-to-mesh/spoke-to-mesh or vice versa) are still measured.

The operation of this feature is the same on the SAP and spoke-SDP. For example, if a MAC address moves from SAP to SAP, from SAP to spoke-SDP, or between spoke-SDPs, one will be blocked to prevent thrashing. If the MAC address moves between a SAP and mesh SDP or spoke-SDP and mesh SDP combinations, the respective SAP or spoke-SDP will be blocked.

mac-move will disable a VPLS port when the number of relearns detected has reached the number of relearns needed to reach the move-frequency in the 5-second interval. For example, when the move-frequency is configured to 1 (relearn per second) mac-move will disable one of the VPLS ports when 5 relearns were detected during the 5-second interval because then the average move-frequency of 1 relearn per second has been reached. This can already occur in the first second if the real relearn rate is 5 relearns per second or higher.

The **no** form of this command disables MAC move.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.15 mac-move-level

mac-move-level

Syntax **mac-move-level** {**primary** | **secondary**| **tertiary**}

Context **[Tree]** (config>service>template>vpls-sap-template mac-move-level)

Full Context configure service template vpls-sap-template mac-move-level

Description When a sap is instantiated using vpls-sap-template, if the MAC move feature is enabled at VPLS level, the command mac-move-level indicates whether the sap should be populated as primary-port, secondary-port or tertiary-port in the instantiated VPLS.

Default no mac-move-level; SAP is populated as a tertiary-port

Platforms All

17.16 mac-name

mac-name

Syntax **mac-name** *name ieee-address*
no mac-name *name*

Context **[Tree]** (config>service>pbb mac-name)

Full Context configure service pbb mac-name

Description This command configures the MAC name for the MAC address. It associates an ASCII name with an IEEE MAC to improve the PBB Epipe configuration. It can also change the dest-BMAC in one place instead of 1000s of Epipe.

Parameters *name* — Specifies the MAC name up to 32 characters in length.

ieee-address — The MAC address assigned to the MAC name. The value should be input in either a xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.17 mac-notification

mac-notification

Syntax **mac-notification**

Context **[Tree]** (config>service mac-notification)

Full Context configure service mac-notification

Description This command controls the settings for the MAC notification message.

The mac-notification message must be generated under the following events:

1. When enabled in the BVPLS using **no shutdown**, a MAC notification will be sent for every active MC-LAG link. The following 3 cases assume no shutdown in the BVPLS.
2. Whenever a related MC-LAG link becomes active (the related MC-LAG link has at least 1 SAP associated with the BVPLS) if the MC-LAG peering is initialized and the PE peers are synchronized.
3. First SAP on an active MC-LAG is associated (via IVPLS/Epipe) with the BVPLS
4. The link between IVPLS/Epipe and BVPLS is configured and there are I-SAPs configured on an active MC-LAG link.

The MAC notification is not sent for the following events:

1. Change of source-bmac or source-bmac-lsb
2. On changes of use-sap-bmac parameter
3. If MC-LAG peering is not (initialized and in sync).

Platforms All

mac-notification

Syntax **mac-notification**

Context **[Tree]** (config>service>vpls mac-notification)

Full Context configure service vpls mac-notification

Description This command controls the settings for the MAC notification message.

The mac-notification message must be generated under the following events:

1. When enabled in the BVPLS using **no shutdown**, a MAC notification will be sent for every active MC-LAG link. The following three cases assume no shutdown in the BVPLS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2. Whenever a related MC-LAG link becomes active (the related MC-LAG link has at least 1 SAP associated with the BVPLS) if the MC-LAG peering is initialized and the PE peers are synchronized.
3. First SAP on an active MC-LAG is associated (via IVPLS/Epipe) with the BVPLS
4. The link between IVPLS/Epipe and BVPLS is configured and there are I-SAPs configured on an active MC-LAG link.

The MAC notification is not sent for the following events:

1. Change of source-bmac or source-bmac-lsb
2. On changes of use-sap-bmac parameter
3. If MC-LAG peering is not (initialized and in sync).

Platforms All

17.18 mac-ping

mac-ping

Syntax **mac-ping service** *service-id* **destination** *dst-ieee-address* [**source** *src-ieee-address*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**ttl** *vc-label-ttl*] [**count** *send-count*] [**return-control**] [**interval** *interval*] [**timeout** *timeout*]

Context **[Tree]** (oam mac-ping)
[Tree] (config>saa>test>type mac-ping)

Full Context configure saa test type mac-ping
oam mac-ping

Description This command determines the existence of an egress SAP binding of a given MAC within a VPLS service.

A **mac-ping** packet is sent via the data plane.

A **mac-ping** is forwarded along the flooding domain if no MAC address bindings exist. If MAC address bindings exist, then the packet is forwarded along those paths, provided they are active. A response is generated only when there is an egress SAP binding for that MAC address or if the MAC address is a “local” OAM MAC address associated with the device’s control plan.

A **mac-ping** reply can be sent using the data plane or the control plane. The **return-control** option specifies the reply be sent using the control plane. If **return-control** is not specified, the request is sent using the data plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A **mac-ping** with data plane reply can only be initiated on nodes that can have an egress MAC address binding. A node without a FDB and without any SAPs cannot have an egress MAC address binding, so it is not a node where replies in the data plane are trapped and sent up to the control plane.

A control plane request is responded to via a control plane reply only.

By default, MAC OAM requests are sent with the system or chassis MAC address as the source MAC. The **source** option allows overriding of the default source MAC for the request with a specific MAC address.

When a **source** *ieee-address* value is specified and the source MAC address is locally registered within a split horizon group (SHG), then this SHG membership is used as if the packet originated from this SHG. In all other cases, SHG 0 (zero) is used. If the **mac-trace** is originated from a non-zero SHG, such packets do not go out to the same SHG.

Parameters *service-id* — Specifies the service ID of the service to diagnose or manage.

Values 1 to 2147483647
service-name: up to 64 characters

dst-ieee-address — Specifies the destination MAC address for the OAM MAC request.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

src-ieee-address — Specifies the source MAC address from which the OAM MAC request originates. By default, the system MAC address for the chassis is used.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

Default The system MAC address.

fc-name — Specifies that the **fc** parameter be used to test the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile state of the MPLS echo request encapsulation.

Default out

octets — Specifies the MAC OAM request packet size in octets, expressed as a decimal integer. The request payload is padded to the specified size with a 6 byte PAD header and a byte payload of 0xAA as necessary. If the octet size specified is less than the minimum packet, the minimum sized packet necessary to send the request is used.

Values 1 to 9198

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vc-label-ttl — Specifies the TTL value in the VC label for the OAM MAC request, expressed as a decimal integer.

Values 1 to 255

Default 255

send-count — Specifies the number of messages to send, expressed as a decimal integer. The **count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message *interval* value must be expired before the next message request is sent.

Values 1 to 100

Default 1

return-control — Specifies the MAC OAM reply to a data plane MAC OAM request be sent using the control plane instead of the data plane.

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second where the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded.

Values 1 to 10

Default 5

Platforms All

17.19 mac-pinning

mac-pinning

Syntax [**no**] **mac-pinning**

Context **[Tree]** (config>service>vpls>sap mac-pinning)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>spoke-sdp mac-pinning)
[Tree] (config>service>vpls>mesh-sdp mac-pinning)
[Tree] (config>service>vpls>endpoint mac-pinning)

Full Context configure service vpls endpoint mac-pinning
configure service vpls mesh-sdp mac-pinning
configure service vpls sap mac-pinning
configure service vpls spoke-sdp mac-pinning

Description This command disables re-learning of MAC addresses on other SAPs within the VPLS. The MAC address will remain attached to a given SAP for duration of its age-timer.

The age of the MAC address entry in the FDB is set by the age timer. If **mac-aging** is disabled on a given VPLS service, any MAC address learned on a SAP or SDP with **mac-pinning** enabled will remain in the FDB on this SAP or SDP forever.

Every event that would otherwise result in re-learning is logged (MAC address; original-SAP; new-SAP).

The **no** form of the command enables re-learning of MAC addresses.

Note: MAC addresses learned during DHCP address assignment (DHCP snooping enabled) are not impacted by this command. MAC-pinning for such addresses is implicit.

Default no mac-pinning — When a SAP or spoke SDP is part of a Residential Split Horizon Group (RSHG), MAC pinning is activated at creation of the SAP. Otherwise MAC pinning is not enabled by default.

Platforms All

mac-pinning

Syntax [**no**] **mac-pinning**

Context [Tree] (config>service>pw-template mac-pinning)

Full Context configure service pw-template mac-pinning

Description Enabling this command will disable re-learning of MAC addresses on other SAPs within the service. The MAC address will remain attached to a given SAP for duration of its age-timer.

The age of the MAC address entry in the FDB is set by the age timer. If **mac-aging** is disabled on a given VPLS service, any MAC address learned on a SAP or SDP with **mac-pinning** enabled will remain in the FDB on this SAP or SDP forever. Every event that would otherwise result in re-learning will be logged (MAC address; original-SAP; new-SAP).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: For 7750 SR and 7450 ESS, MAC addresses learned during DHCP address assignment (DHCP snooping enabled) are not impacted by this command. MAC-pinning for such addresses is implicit.

Default When a SAP or spoke SDP is part of a Residential Split Horizon Group (RSHG), MAC pinning is activated at creation of the SAP. Otherwise MAC pinning is not enabled by default.

Platforms All

17.20 mac-policy

mac-policy

Syntax **mac-policy** *mac-policy-id* [**create**]
no mac-policy *mac-policy-id*

Context **[Tree]** (config>macsec mac-policy)

Full Context configure macsec mac-policy

Description This command configures MAC address policy groups.

The **no** form of this command removes the MAC address policy group configuration.

Parameters *mac-policy-id* — Specifies the value of the MAC address policy.

Values 0 to 4294967295

create — Mandatory to create the configuration.

Platforms All

17.21 mac-populate

mac-populate

Syntax **mac-populate** {*service-id* | **service** *service-name*} **mac** *ieee-address* [**flood**] [**age** *seconds*] [**force**] [**target-sap** *sap-id*]

Context **[Tree]** (oam mac-populate)

Full Context oam mac-populate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command populates the FDB with an OAM-type MAC entry indicating the node is the egress node for the MAC address and optionally floods the OAM MAC association throughout the service. The **mac-populate** command installs an OAM MAC into the service FDB indicating the device is the egress node for a MAC address. The MAC address can be bound to a SAP (the **target-sap**) or can be associated with the control plane in that any data destined to the MAC address is forwarded to the control plane (CPM). As a result, if the service on the node has neither a FDB nor an egress SAP, then it is not allowed to initiate a **mac-populate**.

The MAC address that is populated in the FDBs in the provider network is given a type OAM, so that it can be treated distinctly from regular dynamically learned or statically configured MACs. Note that OAM MAC addresses are operational MAC addresses and are not saved in the device configuration. An exec file can be used to define OAM MACs after system initialization.

The **force** option in **mac-populate** forces the MAC in the table to be type OAM in the case it already exists as a dynamic, static or an OAM induced learned MAC with some other type binding.

An OAM-type MAC cannot be overwritten by dynamic learning and allows customer packets with the MAC to either ingress or egress the network while still using the OAM MAC entry.

The **flood** option causes each upstream node to learn the MAC (that is, populate the local FDB with an OAM MAC entry) and to flood the request along the data plane using the flooding domain. The flooded **mac-populate** request is sent via the data plane.

An **age** can be provided to age an OAM MAC using a specific interval. By default, OAM MAC addresses are not aged and can be removed with a **mac-purge** or with an FDB clear operation.

When split horizon group (SHG) is configured, the flooding domain depends on which SHG the packet originates from. The **target-sap** *sap-id* value dictates the originating SHG information.

Parameters *service-id* — Specifies the service ID of the service to diagnose or manage.

Values 1 to 2147483647

service-name — Specifies the name of the service to diagnose or manage. 64 characters maximum.

ieee-address — Specifies the MAC address to be populated.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

flood — Sends the OAM MAC populate to all upstream nodes.

seconds — Specifies the age for the OAM MAC, in seconds, expressed as a decimal integer.

Values 1 to 65535

Default 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

force — Converts the MAC to an OAM MAC.

sap-id — Specifies the local target SAP bound to a service on which to associate the OAM MAC. By default, the OAM MAC is associated with the control place, that is, it is associated with the CPU on the router.

When the **target-sap** *sap-id* value is not specified the MAC is bound to the CPM or CFM. The originating SHG is 0 (zero). When the **target-sap** *sap-id* value is specified, the originating SHG is the SHG of the target-sap.

Values

:null	*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id*		
	dot1q	*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *aps-id* | *pw-id*:[qtag1| cp-conn-prof-id]	
	qinq	*port-id* | *bundle-id* | *bpgrp-id* | *lag-id* | *pw-id*:[qtag1 **cp**-*conn-prof-id*].[qtag2 | **cp**-conn-prof-id]	
		cp	keyword
		conn-prof-id	1 to 8000
	atm	*port-id* | *aps-id* [:vpi/vci | vpi | vpi1.vpi2 | **cp**.*conn-prof-id*]	
		cp	keyword
		conn-prof-id	1 to 8000
	frame	*port-id* | *aps-id*:dlci	
	cisco-hdlc	*slot/mda/port.channel*	
	cem	*slot/mda/port.channel*	
	ima-grp	bundle-id [:vpi/vci | vpi | vpi1.vpi2 | **cp**.*conn-prof-id*]	
		cp	keyword
		conn-prof-id	1 to 8000
	port-id	*slot/mda/port*[.channel]	
		esat-*id*/*slot*/*port*	
		pxc-*id*.*sub-port*	
	bundle-id	**bundle**-*type*-slot/mda.-*bundle-num*	
		bundle	keyword
		type	ima | fr | ppp
		bundle-num	1 to 336
	bpgrp-id	**bpgrp**-*type*-*bpgrp-num*	
		bgrp	keyword
		type	ima | ppp
		bgrp-num	1 to 2000
	aps-id	**aps**-*group-id*[.channel]	
		aps	keyword
		group-id	1 to 128
	ccag-id	**ccag**-*id*.*path-id*[*cc-type*]:*cc-id*	
		ccag	keyword

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	id	1 to 8
	path-id	a | b
	cc-type	.sap-net | .net-sap
	cc-id	1 to 4094
eth-tunnel	eth-tunnel-*id*[:*eth-tun-sap-id*]	
	id	1 to 1024
	eth-tun-sap-id	0 to 4094
lag-id	**lag**-*id*	
	lag	keyword
	id	1 to 800
pw-id	**pw**-*id*	
	pw	keyword
	id	1 to 10239
qtag1	* | 0 to 4094	
qtag2	* | null | 0 to 4094	
vpi	0 to 4095 (NNI)	
	0 to 255 (UNI)	
vci	1 | 2 | 5 to 65535	
dlci	16 to 1022	
tunnel-id	**tunnel**-*id*.*private* | *public*:*tag*	
	tunnel	keyword
	id	1 to 16
	tag	0 to 4094

Platforms All

17.22 mac-prefix

mac-prefix

Syntax **mac-prefix** *mac-prefix*
no mac-prefix

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain mac-prefix)

Full Context configure subscriber-mgmt isa-service-chaining mac-prefix

Description This command configures the unique MAC prefix per ISA and per outside service for all NAT group configured for service-chaining.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the MAC prefix from the configuration.

Parameters *mac-prefix* — Specifies the MAC prefix, up to eight characters, including separators.

Values format AA:BB:CC

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.23 mac-protect

mac-protect

Syntax [**no**] **mac-protect**

Context **[Tree]** (config>service>vpls mac-protect)

Full Context configure service vpls mac-protect

Description This command indicates if this MAC is protected on the MAC protect list. When enabled, the agent will protect the MAC from being learned or re-learned on a SAP, spoke SDP or mesh SDP that has restricted learning enabled. The MAC protect list is used in conjunction with **restrict-protected-src**, **restrict-unprotected-dst** and **auto-learn-mac-protect**.

The **no** form of the command reverts to the default.

Default none

Platforms All

17.24 mac-purge

mac-purge

Syntax **mac-purge** {*service-id* | **service** *service-name*} **target** *ieee-address* [**flood**] [**force**] [**register**]

Context **[Tree]** (oam mac-purge)

Full Context oam mac-purge

Description This command removes an OAM-type MAC entry from the FDB and optionally floods the OAM MAC removal throughout the service. A **mac-purge** can be sent via the forwarding path or via the control plane.

When sending the MAC purge using the data plane, the TTL in the VC label is set to 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A MAC address is purged only if it is marked as OAM. A mac-purge request is an HVPLS OAM packet, with the following fields. The Reply Flags is set to 0 (since no reply is expected), the Reply Mode and Reserved fields are set to 0. The Ethernet header has source set to the (system) MAC address, the destination set to the broadcast MAC address. There is a VPN TLV in the FEC Stack TLV to identify the service domain.

If the **register** option is provided, the R bit in the Address Delete flags is turned on.

The **flood** option causes each upstream node to be sent the OAM MAC delete request and to flood the request along the data plane using the flooding domain. The flooded **mac-purge** request is sent via the data plane.

The **register** option reserves the MAC for OAM testing where it is no longer an active MAC in the FDB for forwarding, but it is retained in the FDB as a registered OAM MAC. Registering an OAM MAC prevents relearns for the MAC based on customer packets. Relearning a registered MAC can only be done through a **mac-populate** request. The originating SHG is always 0 (zero).

Parameters *service-id* — Specifies the service ID of the service to diagnose or manage.

Values 1 to 2147483647

service-name — Specifies the name, up to 64 characters, of the service to diagnose or manage.

ieee-address — Specifies the MAC address to be purged.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

flood — Sends the OAM MAC purge to all upstream nodes.

force — Purges the entry regardless of the entry's originating node.

register — Reserves the MAC for OAM testing.

Platforms All

17.25 mac-refresh

mac-refresh

Syntax **mac-refresh** *refresh interval*
no mac-refresh

Context **[Tree]** (config>service>ipipe>sap mac-refresh)

Full Context configure service ipipe sap mac-refresh

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the interval between ARP requests sent on this Ipipe SAP. When the SAP is first enabled, an ARP request will be sent to the attached CE device and the received MAC address will be used in addressing unicast traffic to the CE. Although this MAC address will not expire while the Ipipe SAP is enabled and operational, it is verified by sending periodic ARP requests at the specified interval.

The **no** form of this command restores mac-refresh to the default value.

Default mac-refresh 14400

Parameters *refresh interval* — Specifies the interval, in seconds, between ARP requests sent on this Ipipe SAP.

Values 0 to 65535

Platforms All

17.26 mac-subnet-length

mac-subnet-length

Syntax **mac-subnet-length** *subnet-length*
no mac-subnet-length

Context **[Tree]** (config>service>vpls mac-subnet-length)

Full Context configure service vpls mac-subnet-length

Description This command specifies the number of bits to be considered when performing MAC learning (MAC source) and MAC switching (MAC destination). Specifically, this value identifies how many bits, starting from the beginning of the MAC address are used. For example, if the mask-value of 28 is used, MAC learning only performs a lookup for the first 28 bits of the source MAC address when comparing with existing FDB entries. Then, it installs the first 28 bits in the FDB while zeroing out the last 20 bits of the MAC address. When performing switching in the reverse direction, only the first 28 bits of the destination MAC address are used to perform a FDB lookup to determine the next hop.

The **no** form of this command switches back to full MAC lookup.

Default mac-subnet-length 48

Parameters *subnet-length* — Specifies the number of bits to be considered when performing MAC learning or MAC switching.

Values 24 to 48

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.27 mac-trace

mac-trace

Syntax **mac-trace service** *service-id* **destination** *ieee-address* [**source** *ieee-address*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**min-ttl** *vc-label-ttl*] [**max-ttl** *vc-label-ttl*] [**probe-count** *send-count*] [**return-control**] [**interval** *interval*] [**timeout** *timeout*]

Context **[Tree]** (oam mac-trace)
[Tree] (config>saa>test>type mac-trace)

Full Context configure saa test type mac-trace
oam mac-trace

Description This command displays the hop-by-hop path for a destination MAC address within a VPLS.

The MAC traceroute operation is modeled after the IP traceroute utility which uses ICMP echo request and reply packets with increasing TTL values to determine the hop-by-hop route to a destination IP. The MAC traceroute command uses Nokia OAM packets with increasing TTL values to determine the hop-by-hop route to a destination MAC.

In a MAC traceroute, the originating device creates a MAC ping echo request packet for the MAC to be tested with increasing values of the TTL. The echo request packet is sent via the data plane and awaits a TTL exceeded response or the echo reply packet from the device with the destination MAC. The devices that reply to the echo request packets with the TTL exceeded and the echo reply are displayed.

When a **source** *ieee-address* value is specified and the source MAC address is locally registered within a split horizon group (SHG), then this SHG membership is used as if the packet originated from this SHG. In all other cases, SHG 0 (zero) is used. Note that if the **mac-ping** is originated from a non-zero SHG, such packets do not go out to the same SHG.

Parameters *service-id* — Specifies the service ID of the service to diagnose or manage.

This variant of the command is only supported in the classic configuration-mode (**configure system management-interface configuration-mode classic**).

Values {*id* | *svc-name*}

service-id: 1 to 2147483647
svc-name: up to 64 characters

destination *ieee-address* — Specifies the destination MAC address to be traced.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

source *ieee-address* — The source MAC address from which the OAM MAC request originates. By default, the system MAC address for the chassis is used.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx
All zeros and multicast is not allowed.

Default The system MAC address

fc-name — Specifies the forwarding class to test the forwarding class of the ICMP echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile state of the ICMP echo request encapsulation.

Default out

octets — Specifies the MAC OAM request packet size in octets, expressed as a decimal integer. The request payload is padded to the specified size with a 6 byte PAD header and a byte payload of 0xAA as necessary. If the octet size specified is less than the minimum packet, the minimum sized packet necessary to send the request is used.

Values 1 to 9198

min-ttl *vc-label-ttl* — Specifies the minimum TTL value in the VC label for the MAC trace test, expressed as a decimal integer.

Values 1 to 255

Default 1

max-ttl *vc-label-ttl* — Specifies the maximum TTL value in the VC label for the MAC trace test, expressed as a decimal integer.

Values 1 to 255

Default 4

send-count — Specifies the number of MAC OAM requests sent for a TTL value, expressed as a decimal integer.

Values 1 to 100

Default 1

return-control — Specifies the MAC OAM reply to a data plane MAC OAM request be sent using the control plane instead of the data plane.

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the *interval* is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded.

Values 1 to 60

Default 5

Platforms All

17.28 mac-translation

mac-translation

Syntax [**no**] **mac-translation**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext mac-translation)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext mac-translation)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext mac-translation
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext mac-translation

Description This command enables MAC address translation for HLE services.

The **no** form of this command disables MAC address translation for HLE services.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.29 macsec

macsec

Syntax **macsec**

Context **[Tree]** (config macsec)

Full Context configure macsec

Description Commands in this context configure MACsec, including the MACsec MKA profile.

Platforms All

macsec

Syntax [**no**] **macsec**

Context **[Tree]** (config>port>ethernet>dot1x macsec)

Full Context configure port ethernet dot1x macsec

Description This command configures MACsec under this port.

Platforms All

17.30 macsec-encrypt

macsec-encrypt

Syntax [**no**] **macsec-encrypt**

Context **[Tree]** (config>macsec>connectivity-association macsec-encrypt)

Full Context configure macsec connectivity-association macsec-encrypt

Description This command specifies that all PDUs are encrypted and authenticated (ICV payload).

The **no** form of this command specifies that all PDUs are transmitted with clear text, but still authenticated and have the trailing ICV.

Default macsec-encrypt

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.31 magic-number

magic-number

Syntax [**no**] **magic-number**

Context **[Tree]** (config>port>ml-bundle>mlppp magic-number)

Full Context configure port multilink-bundle mlppp magic-number

Description This command allows loopback detection to be enabled and disabled for MLPPP bundles. It is disabled by default. When the magic number option is disabled, the magic number option will not be requested when a member is trying to bring up the LCP layer on a member link; if the remote peer requests this option, it will be rejected. When transmitting echo-requests a magic number of 0 is used. When responding to echo-requests a magic number of 0 is sent.

The magic number option is sent to the remote peer during protocol negotiation. If this option is rejected by the remote peer, the router will bring the link up but will be unable to detect loopbacks since the router will always send a magic number of 0 in the echo messages. If this option is accepted by the remote peer, the router will send echo messages with randomly generated magic-numbers. If the SR receives a config-req with the same magic number that was sent out, the router will calculate a new magic number to use and send out another config-request. If the router is persistently seeing the randomly generated magic number in the received config-req, the router will declare a loopback.

The **no** form of this command disables the loopback detection.

Default no magic-number

Platforms 7450 ESS, 7750 SR-7/12/12e

17.32 main-ct-retry-limit

main-ct-retry-limit

Syntax **main-ct-retry-limit** *number*
no main-ct-retry-limit

Context **[Tree]** (config>router>mpls>lsp main-ct-retry-limit)
[Tree] (config>router>mpls>lsp-template main-ct-retry-limit)

Full Context configure router mpls lsp main-ct-retry-limit
configure router mpls lsp-template main-ct-retry-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of retries the LSP primary path should be retried with the LSP Diff-Serv main Class Type (CT).

When an unmapped LSP primary path goes into retry, it uses the main CT until the number of retries reaches the value of the new main-ct-retry-limit parameter. If the path did not come up, it must start using the backup CT at that point in time. By default, this parameter is set to infinite value. The new main-ct-retry-limit parameter has no effect on an LSP primary path which retries due to a failure event.

An unmapped LSP primary path is a path which has never received a Resv in response to the first Path message sent. This can occur when performing a “shut/no-shut” on the LSP or LSP primary path or when the node reboots. An unmapped LSP primary path goes into retry if the retry timer expired or the head-end node received a PathErr message before the retry timer expired.

If the user entered a value of the main-ct-retry-limit parameter that is greater than the value of the LSP retry-limit, the number of retries will still stop when the LSP primary path reaches the value of the LSP retry-limit. In other words, the meaning of the LSP retry-limit parameter is not changed and always represents the upper bound on the number of retries. The unmapped LSP primary path behavior applies to both CSPF and non-CSPF LSPs.

The **no** form of this command sets the parameter to the default value of zero (0) which means the LSP primary path will retry forever.

Default no main-ct-retry-limit

Parameters *number* — Specifies the number of times MPLS will attempt to re-establish the LSP primary path using the Diff-Serv main CT. Allowed values are integers in the range of zero (0) to 10,000, where zero indicates to retry infinitely.

Values 0 to 1000, integer

Platforms All

17.33 maintenance-policy

maintenance-policy

Syntax [**no**] **maintenance-policy** *maintenance-policy-name*

Context **[Tree]** (config>router>segment-routing maintenance-policy)

Full Context configure router segment-routing maintenance-policy

Description This command configures a named maintenance policy that can be applied to SR Policy candidate paths that are either statically configured or imported via BGP. A maintenance policy is used to configure seamless BFD and protection for an SR Policy candidate path.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A maintenance policy must be administratively disabled in order to change any of the parameters.

A maintenance policy cannot be enabled unless a **mode**, **bfd-enable**, and **bfd-template** are configured.

If a maintenance-template is administratively disabled, then all candidate paths to which it is applied are deprogrammed from the data path.

The **no** form of this command removes the specified maintenance policy.

Parameters *maintenance-policy-name* — Specifies the name of the maintenance policy, up to 32 characters and cannot start with a space or underscore.

Platforms All

maintenance-policy

Syntax [**no**] **maintenance-policy** *maintenance-policy-name*

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy maintenance-policy)

Full Context configure router segment-routing sr-policies static-policy maintenance-policy

Description This command applies a named maintenance policy to the static SR policy path. The maintenance policy must exist under the **config**>**router**>**segment-routing** context.

The **no** form of this command removes the specified maintenance policy.

Parameters *maintenance-policy-name* — Specifies the name of the maintenance policy, up to 32 characters and cannot start with a space or underscore.

Platforms All

17.34 managed-configuration

managed-configuration

Syntax [**no**] **managed-configuration**

Context **[Tree]** (config>router>router-advert>if managed-configuration)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 managed-configuration)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv managed-configuration)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv managed-configuration)
[Tree] (config>service>vprn>router-advert>if managed-configuration)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 managed-configuration)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv managed-configuration)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv managed-configuration)
[Tree] (config>subscr-mgmt>rtr-adv-plcy managed-configuration)

Full Context

configure router router-advertisement interface managed-configuration
configure service ies subscriber-interface group-interface ipv6 managed-configuration
configure service ies subscriber-interface group-interface ipv6 router-advertisements managed-configuration
configure service ies subscriber-interface ipv6 router-advertisements managed-configuration
configure service vprn router-advertisement interface managed-configuration
configure service vprn subscriber-interface group-interface ipv6 managed-configuration
configure service vprn subscriber-interface group-interface ipv6 router-advertisements managed-configuration
configure service vprn subscriber-interface ipv6 router-advertisements managed-configuration
configure subscriber-mgmt router-advertisement-policy managed-configuration

Description

This command sets or resets managed address configuration flag for this group-interface. This flag indicates that DHCPv6 is available for address configuration in addition to any address auto-configured using stateless address auto-configuration. See RFC 3315 for additional details.

The **no** form of this command reverts to the default.

Default

no managed-configuration

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface ipv6 router-advertisements managed-configuration
- configure service vprn subscriber-interface group-interface ipv6 router-advertisements managed-configuration
- configure service vprn subscriber-interface ipv6 router-advertisements managed-configuration
- configure subscriber-mgmt router-advertisement-policy managed-configuration
- configure service ies subscriber-interface ipv6 router-advertisements managed-configuration

All

- configure router router-advertisement interface managed-configuration
- configure service vprn router-advertisement interface managed-configuration

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.35 managed-routes

managed-routes

Syntax **managed-routes**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host managed-routes)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host managed-routes)

Full Context configure service ies subscriber-interface group-interface sap static-host managed-routes
configure service vprn subscriber-interface group-interface sap static-host managed-routes

Description Commands in this context configure managed route parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.36 managed-vlan-list

managed-vlan-list

Syntax **managed-vlan-list**

Context **[Tree]** (config>service>vpls>sap managed-vlan-list)

Full Context configure service vpls sap managed-vlan-list

Description Commands in this context configure VLAN ranges to be managed by a management VPLS. The list indicates, for each SAP, the ranges of associated VLANs that will be affected when the SAP changes state. This managed-vlan-list is not used when STP mode is MSTP in which case the vlan-range is taken from the **config>service>vpls>stp>msti** configuration.

This command is only valid when the VPLS in which it is entered was created as a management VPLS.

Platforms All

17.37 management

management

Syntax **management** [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no management

Context [Tree] (config>service>vprn management)

Full Context configure service vprn management

Description Commands in this context configure node management within the VPRN.

Parameters **create** — Creates a management server entry.

Platforms All

management

Syntax **management**

Context [Tree] (config>system>security management)

Full Context configure system security management

Description Commands in this context allow access to management servers.

Platforms All

17.38 management-access-filter

management-access-filter

Syntax [**no**] **management-access-filter**

Context [Tree] (config>system>security management-access-filter)

Full Context configure system security management-access-filter

Description This command creates the context to edit management access filters and to reset match criteria.

Management access filters control all traffic in and out of the CPM. They can be used to restrict management of the router by other nodes outside either specific (sub)networks or through designated ports.

Management filters, as opposed to other traffic filters, are enforced by system software.

The **no** form of this command removes management access filters from the configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.39 management-interface

management-interface

Syntax **management-interface**

Context **[Tree]** (config>system management-interface)

Full Context configure system management-interface

Description Commands in this context configure management interface parameters.

Platforms All

management-interface

Syntax **management-interface**

Context **[Tree]** (config>system>security management-interface)

Full Context configure system security management-interface

Description Commands in this context configure the selection of a management interface for hash configuration. The management interfaces are **classic-cli**, **md-cli**, **netconf**, or **grpc**.

Platforms All

17.40 manager

manager

Syntax **manager** *manager-name* [**create**]
no manager *manager-name*

Context **[Tree]** (config>system>management-interface>remote-management manager)

Full Context configure system management-interface remote-management manager

Description This command configures a name for the manager. This name identifies the specified SR OS node in the network.

The **no** form of this command removes the remote manager configuration.

Default system-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *manager-name* — Specifies the name of the remote manager, up to 32 characters.

Platforms All

17.41 manager-address

manager-address

Syntax **manager-address** *ip-address* | *fqdn*
no manager-address

Context **[Tree]** (config>system>management-interface>remote-management>manager manager-address)

Full Context configure system management-interface remote-management manager manager-address

Description This command configures the destination IP address or FQDN of the manager.

The no form of this command removes the configured IP address or FQDN of the configured manager.

Parameters *ip-address* — Specifies the IP address, up to 255 characters.

fqdn — Specifies the FQDN, up to 255 characters.

Platforms All

17.42 manager-port

manager-port

Syntax **manager-port** *port*
no manager-port

Context **[Tree]** (config>system>management-interface>remote-management>manager manager-port)

Full Context configure system management-interface remote-management manager manager-port

Description This command assigns a destination TCP port to be used for opening gRPC connections to the specified remote manager.

The **no** form of this command reverts the destination TCP port for the remote manager to the default gRPC port (57400).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port* — Specifies the TCP destination port.

Values 1 to 65535

Default 57400

Platforms All

17.43 manual

manual

Syntax **manual**

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>service-carving manual)

Full Context configure service system bgp-evpn ethernet-segment service-carving manual

Description Commands in this context manually configure the service-carving algorithm, that is, configure the EVIs or ISIDs for which the PE is DF.

Platforms All

17.44 manual-keying

manual-keying

Syntax [**no**] **manual-keying**

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel manual-keying)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel manual-keying)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel manual-keying)
[Tree] (config>router>if>ipsec>ipsec-tunnel manual-keying)

Full Context configure router interface ipsec ipsec-tunnel manual-keying
configure service ies interface ipsec ipsec-tunnel manual-keying
configure service vprn interface ipsec ipsec-tunnel manual-keying
configure service vprn interface sap ipsec-tunnel manual-keying

Description This command configures Security Association (SA) for manual keying. When enabled, the command specifies whether this SA entry is created manually, by the user, or dynamically by the IPsec sub-system.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface sap ipsec-tunnel manual-keying

VSR

- configure service ies interface ipsec ipsec-tunnel manual-keying
- configure router interface ipsec ipsec-tunnel manual-keying
- configure service vprn interface ipsec ipsec-tunnel manual-keying

17.45 map

map

Syntax **map start** *lsn-sub-address* **end** *lsn-sub-address* **to** *outside-ip-address*
no map start *lsn-sub-address* **end** *lsn-sub-address*

Context **[Tree]** (config>service>vprn>nat>inside>deterministic>prefix map)
[Tree] (config>router>nat>inside>deterministic>prefix map)

Full Context configure router nat inside deterministic prefix map
configure service vprn nat inside deterministic prefix map

Description This command is applicable to prefixes in deterministic NAT (LSN44 and DS-Lite) and static 1:1 NAT (LSN44). In deterministic NAT, its purpose is to split the number of subscribers within the configured prefix over available sequence of outside IP addresses. In static 1:1 NAT, its purpose it to statically map source IPv4 address of an LSN44 subscriber to a configured IPv4 address on the public side.

In deterministic NAT, there are several rules guiding the usage of the map statement:

- If the number of subscribers per configured prefix is greater than the subscriber-limit per outside IP parameter (2^n), then the lowest n bits of the map start <i*nside-addr-start*> must be set to 0.

  Subscriber in LSN44 is equals to an inside IPv4 address, while in DS-Lite, the subscriber can be an IPv6 address or IPv6 prefix. If the **subscriber-prefix-length** command is set to 128, then the subscriber in DS-Lite is an IPv6 address. Otherwise it will be an IPv6 prefix with length in the range [32 to 64] as set by the **subscriber-prefix-length** command.
- If the number of subscribers per configured prefix is equal or less than the subscriber-limit per outside IP parameter (2^n), then only one map command for this prefix is allowed. In this case there is no restriction on the lower n bits of the map start *lsn-sub-address*. The range of the inside IP addresses in such map statement represents the prefix itself.
- *outside-ip-address* in the map statements must be unique amongst all map statements referencing the same pool. In other words, two map statements cannot reference the same *outside-ip-address* in a pool.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To modify map statements in classic CLI, the corresponding prefix must be in a shutdown mode.

In classic CLI, **map** statements can be configured automatically by the system, as soon as the prefix is enabled (no shutdown state) or they can be configured manually by the operator while the prefix is disabled.

In MD-CLI, the **map** statement must be configured by the operator, but the t**ools perform nat deterministic calculate-maps** command can be used to produce system-generated maps. The **calculate-maps** command outputs a set of system-generated map statements. The **map** parameters can then be copied and pasted into an MD-CLI candidate configuration by the operator.

The following is an example of the map statement for the LSN44 case:

- The subscriber-limit in the pool is 128
- The pool has an address range 192.168.0.1 - 192.168.0.10
- The prefix is 10.0.0.0/24
- The map statement is configured as:

  map start 10.0.0.0 end 10.0.0.255 to 192.168.0.1

Since each outside IP address can accommodate only 128 hosts, the subscribers (IPv4 addresses in LSN44) from the 10.0.0.0/24 prefix will be split and mapped into two outside IP addresses

10.0.0.0 – 10.0.0.127 (10.0.0.0/25) - 192.168.0.1

10.0.0.128 – 10.0.0.255 (10.0.0.128/25) - 192.168.0.2

The first IP address range will be mapped to the ‘to’ address in the map statement => 192.168.0.1. The second IP address range will be mapped into the next consecutive IP address in the pool assuming that this IP address is free. In this case this consecutive address (192.168.0,2) would not be shown in the map statement.

For Deterministic DS-Lite, the example would be:

- The subscriber-limit in the pool is 128
- The pool has an address range 192.168.0.1 - 192.168.0.10
- The prefix is 2001:db8::/56
- The subscriber-prefix-length = 64
- The map statement is configured as:

  map start 2001:db8::/64 end 2001:db8::FF:0:0:0:0/64 to 192.168.0.1

There are 256 DS-Lite subscribers within the 2001:db8::/56 prefix. Each subscriber will be a /64 IPv6 prefix as dictated by the subscriber-prefix-length command.

Since each outside IP address can accommodate only 128 hosts, the subscribers from the 2001:db8::/56 prefix will be split and mapped into two outside IP addresses

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2001:db8:: – 2001:db8:0:7F:: (2001:db8::/57) - 192.168.0.1

2001:db8:0:80:: – 2001:db8:0:FF::(2001:db8:0:FF::/57) - 192.168.0.2

The first IP prefix range will be mapped to the 'to' address in the map statement => 192.168.0.1. The second IP prefix range will be mapped into the next consecutive IP address in the pool assuming that this IP address is free. In this case this consecutive address (192.168.0,2) would not be shown in the map statement.

Default By default in classic CLI only, the system will automatically divide the prefix and create the map statements when the prefix command is enabled (no shutdown). However, this automatic map provisioning can be overruled by manual configuration in classic CLI, and must be provided in MD-CLI..

Parameters *inside-ip-start* — Start IPv4/v6 address or IPv6 prefix on the inside.

inside-ip-end — End IPv4/v6 address or IPv6 prefix on the inside. The number of subscribers (range of inside IPv4 addresses in LSN44 or IPv6 addresses or prefixes in DS-Lite) in the map statement does not have to be a power of 2. Rather it has to be a multiple of a power of two ? m * 2^n, where m is the number of consecutive outside IP addresses to which the subscribers are mapped and the 2^n is the subscriber-limit per outside IP.

outside-ip-start — The first outside IPv4 address in the pool to which the subscribers are mapped. In case that the number of subscribers in the map statement is larger than the subscriber-limit for the *outside-ip address*, the consecutive outside IP addresses will be used for additional mappings. Those additional (consecutive) outside IP addresses are not shown in the map statement (only the first address is shown in the map statement).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

map

Syntax [**no**] **map**

Context **[Tree]** (config>service>nat>pcp-server-policy>opcode map)

Full Context configure service nat pcp-server-policy opcode map

Description This command enables/disables support for the **map** opcode.

Default no map

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.46 map-domain

map-domain

Syntax **map-domain** *domain-name* [**create**]
no map-domain

Context **[Tree]** (config>service>nat map-domain)

Full Context configure service nat map-domain

Description This command creates a MAP domain template, which is used to define MAP rules and parameters specific to the MAP domain. A MAP domain represents a set of CEs that share the same default gateway (BR's IPv6 prefix - DMR rule) and a set of basic MAP rules (BMRs). As a bordering node between the IPv6 and IPv4 realm, the BR performs stateless IPv4 and IPv6 translation based on MAP rules.

A MAP domain can be instantiated within a routing context by referencing an existing MAP domain template in the context.

Parameters *domain-name* — Specifies the name of the MAP domain, up to 32 characters. The MAP domain name has local significance.

Platforms VSR

map-domain

Syntax **map-domain** *domain-name*
no map-domain *domain-name*

Context **[Tree]** (config>service>vprn>nat>map map-domain)
[Tree] (config>router>nat>map map-domain)

Full Context configure router nat map map-domain
configure service vprn nat map map-domain

Description This command instantiates a MAP-T domain within a routing context, assuming that the MAP-T domain template is administratively enabled (**no shutdown**). When the MAP-T is instantiated, the forwarding for the MAP-T domain is enabled and its routes can be exported in routing protocols.

Multiple MAP-T domains can be instantiated within a routing context.

Interactions:

The referenced MAP domain is defined under the **config**>**service**>**nat** hierarchy.

Parameters *domain-name* — Specifies the name of the MAP domain template, up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms VSR

17.47 mapping

mapping

Syntax **mapping** *mapping*

Context **[Tree]** (config>port>tdm>ds3>atm mapping)

Full Context configure port tdm ds3 atm mapping

Description This command configures the ATM cell mapping for DS-3 channels. The mapping value specifies the cell mapping that is to be used on this ATM interface.

Default mapping direct

Parameters *mapping* — The mapping value specifies the cell mapping that is to be used on this ATM interface.

Values direct — Specifies direct cell mapping. plcp — Specifies PLCP cell mapping.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

17.48 mapping-limit

mapping-limit

Syntax **mapping-limit** *limit*
no mapping-limit

Context **[Tree]** (config>service>upnp>upnp-policy mapping-limit)

Full Context configure service upnp upnp-policy mapping-limit

Description This command specifies the maximum number of UPnP mapping per subscriber.

The **no** form of the command reverts to the default.

Default mapping-limit 256

Parameters *limit* — Specifies the upper limit of the number of UPnP mappings per subscriber.

Values 1 to 256

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.49 mapping-rule

mapping-rule

Syntax **mapping-rule** *map-rule-name* [**create**]
no mapping-rule *map-rule-name*

Context **[Tree]** (config>service>nat>map-domain mapping-rule)

Full Context configure service nat map-domain mapping-rule

Description This command provides a CLI context for configuring MAP rules.

Parameters *map-rule-name* — Specifies the name of the MAP rule; the name has a local significance.

Platforms VSR

17.50 mapping-server

mapping-server

Syntax [**no**] **mapping-server**

Context **[Tree]** (config>router>isis>segment-routing mapping-server)

Full Context configure router isis segment-routing mapping-server

Description Commands in this context configures the Segment Routing mapping server feature in an IS-IS instance.

SR mapping server enables the configuration and advertisement, via IS-IS, of the node SID index for IS-IS prefixes of routers which are in the LDP domain. This is performed in the router acting as a mapping server, which uses a prefix-SID sub-TLV within the SID/Label binding TLV in IS-IS.

The **no** form of this command deletes all node SID entries in the IS-IS instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mapping-server

Syntax [**no**] **mapping-server**

Context **[Tree]** (config>router>ospf>segm-rtng mapping-server)

Full Context configure router ospf segment-routing mapping-server

Description Commands in this context configure the Segment Routing mapping server feature in an OSPF instance.

The mapping server feature allows the configuration and advertisement in OSPF of the node SID index for OSPF prefixes of routers which are in the LDP domain. This is performed in the router acting as a mapping server and using a prefix-SID sub-TLV within the Extended Prefix Range TLV in OSPF.

The **no** form of this command deletes all node SID entries in the OSPF instance.

Platforms All

17.51 maps-to

maps-to

Syntax **maps-to fc** *fc-name* **profile** *profile*

Context **[Tree]** (config>qos>post-policer-mapping>fc maps-to)

Full Context configure qos post-policer-mapping fc maps-to

Description This command remaps the forwarding class and profile state of an egress policed packet that is to be mapped to another forwarding class and profile, where the profile state is that of the resulting profile after the packet has been processed by the egress policer.

The new forwarding class is used to select the egress queue on which the post-policer traffic is placed. The new profile is used to determine the congestion control handling in that queue, specifically the drop tail or slope that is applied to the traffic.

The **maps-to** command parameters can be overwritten by reissuing the command with a different FC or profile.

The traffic remarking is based on the marking configured for the forwarding class and profile of the traffic after being policed but before it is remapped.

Parameters *fc-name* — Specifies one of the eight forwarding classes supported by the system.

Values be, l2, af, l1, h2, ef, h1, nc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

profile — Specifies one of the egress packet profile states.

Values exceed, in, inplus, out

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

17.52 mark

mark

Syntax **mark** *entity* **high** *percentage-high* **low** *percentage-low*
no mark *entity*

Context **[Tree]** (config>isa>wlan-gw-group>watermarks mark)

Full Context configure isa wlan-gw-group watermarks mark

Description This command enables a watermark notification. If the watermark is set, it generates a notification when the corresponding resource consumption goes above the high percentage. No additional notifications are sent until resource consumption goes under the low watermark, upon which, a notification is sent indicating the high watermark is no longer hit.

The **no** form of this command disables the watermark notification.

Parameters *entity* — Specifies which watermark to set.

Values user-equipment | bridge-domain | radius-proxy-client

percentage-high — Specifies the high watermark in percentage of total resources available.

Values 1 to 100

percentage-low — Specifies the low watermark in percentage of total resources available.

Values 0 to 99

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.53 mask

mask

Syntax **mask type** *match-type* {[**prefix-string** *prefix-string* | **prefix-length** *prefix-length*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[**suffix-string** *suffix-string* | **suffix-length** *suffix-length*]}
no mask type *match-type*
mask type *dhcp-match-type* {[**prefix-string** *prefix-string* | **prefix-length** *prefix-length*]
[**suffix-string** *suffix-string* | **suffix-length** *suffix-length*]}
no mask type *dhcp-match-type*

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp mask)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe mask)

Full Context configure subscriber-mgmt local-user-db ipoe mask
configure subscriber-mgmt local-user-db ppp mask

Description This command configures the IPoE mask.

The **no** form of this command removes the mask parameters from the configuration.

Parameters *ppp-match-type* — Specifies the sub-option inserted by the PPPoE intermediate agent.

Values circuit-id, remote-id, sap-id, service-name, username

dhcp-match-type — The data type represents the type of matching done to identify a DHCP host.

Values circuit-id, option60, remote-id, sap-id, string, system-id

prefix-string — Specifies a substring that is stripped of the start of the incoming circuit ID before it is matched against the value configured in the DHCP or PPPoE circuit ID.

This string can only contain printable ASCII characters. The “*” character is a wildcard that matches any substring. If a "\" character is masked, use the escape key so it becomes "\\".

Values up to 127 characters, “*”

prefix-length — Specifies the number of characters to remove from the start of the incoming circuit ID before it is matched against the value configured in the circuit ID.

Values 1 to 127

suffix-string — Specifies a substring that is stripped of the end of the incoming circuit ID before it is matched against the value configured in circuit ID.

This string can only contain printable ASCII characters. The “*” character is a wildcard that matches any substring. If a "\" character is masked, use the escape key so it becomes "\\".

Values up to 127 characters

suffix-length — Specifies the number of characters to remove from the end of the incoming circuit ID before it is matched against the value configured in the circuit ID.

Values 1 to 127

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mask

Syntax **mask** *mask-value* [**type** {**included** | **excluded**}]
no mask

Context **[Tree]** (config>system>security>snmp>view>view-name mask)

Full Context configure system security snmp view view-name mask

Description The mask value and the mask type, along with the *oid-value* configured in the **view** command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view.

Each bit in the mask corresponds to a sub-identifier position. For example, the most significant bit for the first sub-identifier, the next most significant bit for the second sub-identifier, and so on. If the bit position on the sub-identifier is available, it can be included or excluded.

For example, the MIB subtree that represents MIB-II is 1.3.6.1.2.1. The mask that catches all MIB-II would be 0xfc or 0b11111100.

Only a single mask may be configured per view and OID value combination. If more than one entry is configured, each subsequent entry overwrites the previous entry.

The **no** form of this command removes the mask from the configuration.

Parameters *mask-value* — The mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view. (Default: all 1s)

The mask can be entered either:

- In hex. For example, 0xfc.
- In binary. For example, 0b11111100.

Note: If the number of bits in the bit mask is less than the number of sub-identifiers in the MIB subtree, then the mask is extended with ones until the mask length matches the number of sub-identifiers in the MIB subtree.

type — Specifies to include or exclude MIB subtree objects.

Values **included** - All MIB subtree objects that are identified with a 1 in the mask are available in the view.

excluded - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view.

Default **included**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.54 mask-reply

mask-reply

Syntax [**no**] **mask-reply**

Context **[Tree]** (config>service>ies>if>icmp mask-reply)
[Tree] (config>service>ies>sub-if>grp-if mask-reply)
[Tree] (config>service>vprn>if mask-reply)
[Tree] (config>service>vprn>if>icmp mask-reply)
[Tree] (config>service>vprn>nw-if>icmp mask-reply)

Full Context configure service ies interface icmp mask-reply
configure service ies subscriber-interface group-interface mask-reply
configure service vprn interface icmp mask-reply
configure service vprn interface mask-reply
configure service vprn network-interface icmp mask-reply

Description This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the **mask-reply** command configures the router interface to reply to the request.

By default, the router instance replies to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default mask-reply — Specifies to reply to ICMP mask requests.

Platforms All

mask-reply

Syntax [**no**] **mask-reply**

Context **[Tree]** (config>subscr-mgmt>git>ipv4>icmp mask-reply)

Full Context configure subscriber-mgmt group-interface-template ipv4 icmp mask-reply

Description This command enables responses to ICMP mask requests on the router interface. If a local node sends an ICMP mask request to the router interface, the router interface replies to the request.

By default, the router instance replies to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default mask-reply

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mask-reply

Syntax [**no**] **mask-reply**

Context **[Tree]** (config>router>if>icmp mask-reply)

Full Context configure router interface icmp mask-reply

Description This command enables responses to ICMP mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the **mask-reply** command configures the router interface to reply to the request.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default mask-reply — Replies to ICMP mask requests.

Platforms All

17.55 master-int-inherit

master-int-inherit

Syntax [**no**] **master-int-inherit**

Context **[Tree]** (config>service>ies>if>ipv6>vrrp master-int-inherit)

Full Context configure service ies interface ipv6 vrrp master-int-inherit

Description This command allows the master instance to dictate the master down timer (non-owner context only).

Default no master-int-inherit

Platforms All

master-int-inherit

Syntax [**no**] **master-int-inherit**

Context **[Tree]** (config>service>ies>if>vrrp master-int-inherit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface vrrp master-int-inherit

Description This command allows the master instance to dictate the master down timer (non-owner context only).

Default no master-int-inherit

Platforms All

master-int-inherit

Syntax [**no**] **master-int-inherit**

Context **[Tree]** (config>service>vprn>if>vrrp master-int-inherit)
[Tree] (config>service>vprn>if>ipv6>vrrp master-int-inherit)

Full Context configure service vprn interface ipv6 vrrp master-int-inherit
configure service vprn interface vrrp master-int-inherit

Description This command allows the master instance to dictate the master down timer (non-owner context only).

Default no master-int-inherit

Platforms All

master-int-inherit

Syntax [**no**] **master-int-inherit**

Context **[Tree]** (config>router>if>vrrp master-int-inherit)
[Tree] (config>router>if>ipv6>vrrp master-int-inherit)

Full Context configure router interface ipv6 vrrp master-int-inherit
configure router interface vrrp master-int-inherit

Description This command enables the virtual router instance to inherit the master VRRP router's advertisement interval timer which is used by backup routers to calculate the master down timer.

The **master-int-inherit** command is only available in the non-owner nodal context and is used to allow the current virtual router instance master to dictate the master down timer for all backup virtual routers. The **master-int-inherit** command has no effect when the virtual router instance is operating as master.

If **master-int-inherit** is not enabled, the locally configured **message-interval** must match the master's VRRP advertisement message advertisement interval field value or the message is discarded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command restores the default operating condition which requires the locally configured **message-interval** to match the received VRRP advertisement message advertisement interval field value.

Default no master-int-inherit — The virtual router instance does not inherit the master VRRP router's advertisement interval timer and uses the locally configured message interval.

Platforms All

17.56 master-only

master-only

Syntax **master-only** {**true** | **false**}

Context **[Tree]** (config>system>ptp>port master-only)

Full Context configure system ptp port master-only

Description This command is used to restrict the local port to never enter the slave state. Use the command to ensure that the 7750 SR never draws synchronization from the attached external device.

This parameter is only effective when the profile is set to g8275dot1-2014.

Note: The ITU-T G.8275.1 (07/2014) recommendation used the term notSlave for this functionality; however, the IEEE has added this capability into the next edition of the 1588 standard using the term masterOnly. These are equivalent.

Default master-only true

Parameters **true** — Enables the **master-only** parameter of the PTP port.

false — Disables the **master-only** parameter of the PTP port.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.57 master-selection-mode

master-selection-mode

Syntax **master-selection-mode** *mode*

Context **[Tree]** (config>app-assure>aarp master-selection-mode)

Full Context configure application-assurance aarp master-selection-mode

Description This command configures the AARP mode of operation with the peer instance. The modes affect the AARP state machine behavior according to the desired behavior. Minimize-switchover will change AARP state based on Master ISA failure, and be non-revertive in that when the priority ISA returns a switch does not occur, which is optimal for AA flow identification. Inter-chassis efficiency mode considers both priority (revertive) and the endpoint status of the AARP instance and will switch activity in case of EP failure in order to avoid sending all the traffic over the ICL. The priority-based-balance mode will be revertive after a priority master returns to service, but excludes EP status. The master-selection-mode configuration must match on both peer AARP instances, or the AARP operational status will stay down.

Default master-selection-mode minimize-switchovers

Parameters *mode* — Specifies the AARP master selection mode.

Values **minimize-switchovers** — Optimal AA flow detection continuity by minimizing AARP switchovers.

inter-chassis-efficiency — Minimizes inter-chassis traffic.

priority-based-balance — AA load balance between AARP peers based on configured priority.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.58 match

match

Syntax **match** {**circuit-id** | **mac** | **remote-id**}
match option [*number*] [**option6** [*number*]
match option6 [*number*]
no match

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>match-radprox-cache match)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt local-user-db ipoe host match-radius-proxy-cache match

Description This command specifies in what DHCPv6 option to retrieve the value to be used as lookup key in the RADIUS proxy cache.

The **no** form of this command reverts to the default.

Default match mac

Parameters **circuit-id** — Specifies to use the circuit Id to match against.

mac — Specifies the MAC address to match against.

remote-id — Specifies the remote ID to match against.

option *number* — Specifies the option number that the DHCP server uses to send the identification strings to the client.

Values 1 to 254

option6 *number* — Specifies the DHCPv6 option to retrieve the value to be used as lookup key in the RADIUS proxy cache.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match**

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry match)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry match

Description Commands in this context configure the match criterion for a VAS filter entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match** [**next-header** *next-header*]
no match

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry match)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry match)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the match criteria for this IP filter entry.

The **no** form of this command reverts to the default.

Parameters *next-header — protocol-number*, *protocol-name*

protocol-number — Specifies the protocol number accepted in DBH for IPv6 filter entries.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name accepted in DBH for IPv6 filter entries.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry match)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry match)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match

Description This command configures the match criteria for this IP filter entry.

The **no** form of this command reverts to the default.

Parameters *protocol-id* — Specifies the protocol ID or protocol name accepted in DHB.

Values *protocol-number* — [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match protocol** {**any** | **icmp** | **tcp** | **udp** | **gre**}
no match

Context **[Tree]** (config>subscr-mgmt>isa-filter>ipv6>entry match)

Full Context configure subscriber-mgmt isa-filter ipv6 entry match

Description This command creates a match context for this entry. The **protocol** value specifies which Layer-4 protocol the packet should match.

The **no** form of this command removes the match context of this entry.

Default match protocol any

Parameters *protocol* — Specifies that the only supported match context is **protocol**.

any — Specifies to match any protocol.

icmp — Specifies to match ICMP packets in a v4 filter.

tcp — Specifies to match TCP packets.

udp — Specifies to match UDP packets.

gre — Specifies to match GRE over IP packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

match

Syntax [**no**] **match**

Context **[Tree]** (config>service>mrp>mrp-policy>entry match)

Full Context configure service mrp mrp-policy entry match

Description This command creates the context for entering/editing match criteria for the mrp-policy entry. When the match criteria have been satisfied the action associated with the match criteria is executed. In the current implementation just one match criteria (ISID based) is possible in the entry associated with the mrp-policy. Only one match statement can be entered per entry.

The **no** form of this command removes the match criteria for the entry-id.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

match

Syntax **match**

Context **[Tree]** (config>service>vprn>bgp>group>dynamic-neighbor match)

Full Context configure service vprn bgp group dynamic-neighbor match

Description This command configures match conditions for the dynamic neighbors.

Platforms All

match

Syntax [**no**] **match**

Context **[Tree]** (config>service>vprn>log>filter>entry match)

Full Context configure service vprn log filter entry match

Description This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.

If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied (AND functional) before the action associated with the match is executed.

Use the **match** command to display a list of the valid applications.

Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple **match** statements cannot be entered per entry.

The **no** form of this command removes the match criteria for the *entry-id*.

Default no match

Platforms All

match

Syntax **match**

Context **[Tree]** (config>app-assure>group>policy>aqp>entry match)

Full Context configure application-assurance group policy app-qos-policy entry match

Description Commands in this context configure flow match rules for this AQP entry. A flow matches this AQP entry only if it matches all the match rules defined (logical and of all rules). If no match rule is specified, the entry will match all flows.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match**

Context **[Tree]** (config>app-assure>group>sess-fltr>entry match)

Full Context configure application-assurance group session-filter entry match

Description Commands in this context configure session conditions for this entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match**

Context **[Tree]** (config>app-assure>group>transit-prefix-policy>entry match)

Full Context configure application-assurance group transit-prefix-policy entry match

Description Commands in this context configure transit prefix policy entry match criteria.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match

Syntax [**no**] **match**

Context **[Tree]** (debug>app-assure>group>traffic-capture match)

Full Context debug application-assurance group traffic-capture match

Description This command configures debugging for traffic match criteria.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match protocol** *ip-protocol*
no match

Context **[Tree]** (config>service>nat>nat-classifier>entry match)

Full Context configure service nat nat-classifier entry match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an IP protocol to be used as a nat-classifier match criterion. When the match criteria have been satisfied the action associated with the match criteria is executed.

The **no** form of the command removes the match criteria for the entry-id.

Default match protocol udp

Parameters **protocol** *ip-protocol* — Specifies the text value representing the IP protocol to be used as a match criterion.

Values udp, tcp

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match

Syntax **match** [**frame-type** *frame-type*]
no match

Context **[Tree]** (config>li>li-filter>li-mac-filter>entry match)

Full Context configure li li-filter li-mac-filter entry match

Description Commands in this context configure match criteria for the filter entry and specifies an Ethernet frame type for the entry.

If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (and function) for a match to occur.

A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry.

The **no** form of this command removes the match criteria for the entry.

Parameters *frame-type* — Filters can continue to be edited by all users even when an li-source references an entry in that filter.

Values 802dot3, 802dot2-llc, 802dot2-snap, ethernet_II

Default 802dot3

Platforms All

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context **[Tree]** (config>li>li-filter>li-ip-filter>entry match)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure li li-filter li-ip-filter entry match

Description This command enables context to enter match criteria for LI IPv4 filter and optionally allows specifying protocol value to match on.

If more than one match criterion are configured then all criteria must be satisfied for a match to occur (logical “AND”). Multiple criteria must be configured within a single match context for a given entry.

The **no** form of this command removes the match criteria for the entry.

Parameters *protocol-id* — Configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP(1), TCP(6), UDP(17).

Values 0 to 255 (values can be expressed in decimal, hexadecimal, or binary - DHB)

Keywords for the 7750 SR:

none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

Keywords for the 7450 ESS:

none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

* — udp/tcp wildcard

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Protocol	Protocol ID	Description
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

Platforms All

match

Syntax **match** [**next-header** *next-header*]
no match

Context **[Tree]** (config>li>li-filter>li-ipv6-filter>entry match)

Full Context configure li li-filter li-ipv6-filter entry match

Description Commands in this context enter match criteria for an LI IPv6 filter and optionally allows specification IPv6 next-header value to match on.

If more than one match criterion are configured, then all criteria must be satisfied for a match to occur (logical “AND”). Multiple criteria must be configured within a single match context for a given entry.

The **no** form removes the match criteria for the entry.

Parameters *next-header — protocol-number*, *protocol-name*

Specifies the IPv6 next header to match. This parameter is analogous to the protocol parameter used in IP filter match criteria.

protocol-number — Specifies the protocol number value to be configured as a match criterion.

Values [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

Platforms All

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context **[Tree]** (config>qos>sap-egress>ip-criteria>entry match)
[Tree] (config>qos>sap-ingress>ip-criteria>entry match)

Full Context configure qos sap-egress ip-criteria entry match
configure qos sap-ingress ip-criteria entry match

Description This command creates a context to configure match criteria for SAP QoS policy match criteria. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.

A **match** context can consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

It is possible that a SAP policy includes the **dscp** map command, the **dot1p** map command, and an IP match criteria. When multiple matches occur for the traffic, the order of precedence is used to arrive at the final action. The order of precedence is as follows:

1. 802.1p bits
2. DSCP
3. IP quintuple or MAC headers

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters **protocol** *protocol-id* — Specifies an IP protocol to be used as a SAP QoS policy match criterion.

The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 80 lists the IP protocols and their respective IDs and descriptions.

Values The following values apply to the 7750 SR and 7950 XRS:

protocol-id: 0 to 255 protocol numbers accepted in decimal, hexadecimal, or binary

keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

Values The following values apply to the 7450 ESS:

keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

* — udp/tcp wildcard

Table 80 **IP Protocol Names**

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for their IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 80 **IP Protocol Names**

Protocol	Protocol ID	Description
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Schedule Transfer Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

Platforms All

match

Syntax **match** [**next-header** *next-header*]
no match

Context **[Tree]** (config>qos>sap-ingress>ipv6-criteria>entry match)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry match)

Full Context configure qos sap-egress ipv6-criteria entry match
configure qos sap-ingress ipv6-criteria entry match

Description This command creates a context to configure match criteria for ingress SAP QoS policy match IPv6 criteria. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured, all criteria must be satisfied (logical AND) before the action associated with the match is executed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A **match** context can consist of multiple match criteria, but multiple **match** statements cannot be created per entry.

A SAP ingress policy may include the **dscp** map command, the **dot1p** map command, and an IPv6 match criteria. When multiple matches occur for the traffic, the following order of precedence is used to arrive at the final action.

1. 802.1p bits
2. DSCP
3. IP quintuple or MAC headers

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters *next-header — protocol-number*, *protocol-name*

Specifies the IPv6 next header to match.

On the 7750 SR and 7950 XRS, the protocol type such as TCP, UDP, or OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6) and UDP(17).

protocol-number — Specifies the protocol number value to be configured as a match criterion.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

Platforms All

match

Syntax **match** [**frame-type** {**802dot3** | **802dot2-llc** | **802dot2-snap** | **ethernet-II** | **atm**}]
no match

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry match)

Full Context configure qos sap-ingress mac-criteria entry match

Description This command creates a context for entering/editing match MAC criteria for ingress SAP QoS policy match criteria. When the match criteria have been satisfied, the action associated with the match criteria is executed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If more than one match criteria (within one match statement) are configured, all criteria must be satisfied (AND function) before the action associated with the match will be executed.

A **match** context can consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters **frame-type** — The **frame-type** keyword configures an Ethernet frame type or an ATM frame type to be used for the MAC filter match criteria.

Values 802dot3, 802dot2-llc, 802dot2-snap, ethernet_II, atm

Default 802dot3

802dot3 — Specifies the frame type is Ethernet IEEE 802.3.

802dot2-llc — Specifies the frame type is Ethernet IEEE 802.2 LLC.

802dot2-snap — Specifies the frame type is Ethernet IEEE 802.2 SNAP.

ethernet-II — Specifies the frame type is Ethernet Type II.

atm — Specifies the frame type as ATM cell. The user is not allowed to configure entries with frame type of atm and a frame type of other supported values in the same QoS policy. This parameter applies only to the 7750 SR and 7950 XRS.

Platforms All

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry match)
[Tree] (config>qos>network>egress>ip-criteria>entry match)

Full Context configure qos network egress ip-criteria entry match
configure qos network ingress ip-criteria entry match

Description This command creates a context to configure match criteria for a network QoS policy. When the match criteria have been satisfied, the action associated with it is executed.

If more than one match criteria (within one match statement) are configured, then all criteria must be satisfied before the associated action with the match is executed.

A match context can consist of multiple match criteria, but multiple match statements cannot be entered per entry.

A network QoS policy can include the DSCP map command, the dot1p map command (ingress only), the prec map command (egress only), and an IP match criteria. When multiple matches occur for the traffic, the order of precedence is used to arrive at the final action. The order of precedence is as follows:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- 802.1p bits (ingress only)
- DSCP
- prec (egress only)
- IP quintuple

The **no** form of this command removes the match criteria for the entry identifier.

Parameters **protocol** *protocol-id* — Specifies an IP protocol to be used as an ingress or egress network QoS policy match criterion.

The protocol type is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), and UDP(17).

Values *protocol-id*: 0 to 255 protocol numbers accepted in decimal, hexadecimal, or binary

keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

* — udp/tcp wildcard

Table 81 lists the protocols and their protocol IDs and descriptions.

Table 81 **Protocol ID Descriptions**

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for their IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 81 **Protocol ID Descriptions**

Protocol	Protocol ID	Description
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Schedule Transfer Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

Platforms All

match

Syntax **match** [**next-header** *next-header*]
no match

Context **[Tree]** (config>qos>network>ingress>ipv6-criteria>entry match)
[Tree] (config>qos>network>egress>ipv6-criteria>entry match)

Full Context configure qos network egress ipv6-criteria entry match
configure qos network ingress ipv6-criteria entry match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a context to configure match criteria for a network QoS policy match IPv6 criteria. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured, all criteria must be satisfied (logical AND) before the action associated with the match is executed.

A match context can consist of multiple match criteria, but multiple match statements cannot be created per entry.

A network policy can include the DSCP map command, the dot1p map command (ingress only), the prec map command (egress only), and an IPv6 match criteria. When multiple matches occur for the traffic, the following order of precedence is used to arrive at the final action.

- 802.1p bits (ingress only)
- DSCP
- prec (egress only)
- IP quintuple

The **no** form of this command removes the match criteria for the entry identifier.

Parameters *next-header — protocol-number*, *protocol-name*

Specifies the next header to match.

The protocol type is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), and UDP(17).

protocol-number — Specifies the protocol number value to be configured as a match criterion.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

Platforms All

match

Syntax **match** *field-value* **instance** *instance-id*
no match *field-value*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>queue-group-redirect-list match)

Full Context configure qos queue-group-redirect-list match

Description This command configures the value of the field in the ingress or egress packet which, when matched, will cause the packet to be redirected to the specified queue group instance. The *field-value* is dependent on the setting of the **type** and therefore must be a valid VXLAN VNI.

A maximum of 16 match statements are supported in a queue group redirect list.

The **no** form of this command removes the match statement from the redirect list.

Parameters *field-value* — Specifies the value of the field in the ingress or egress packet which, when matched, will cause the packet to be redirected to the specified queue group instance. Because the only permitted **type** is **vxlan-vni**, the field must be a valid VXLAN VNI. The VNI can be specified in any of the available formats but is always shown in decimal.

Values 1 to 16777215 (Decimal)
0x1 to 0xFFFFFF (Hexadecimal)
0b1 to 0b111111111111111111111111 (Binary)

instance-id — Specifies the instance of the queue group template to which the VXLAN traffic is redirected. The traffic can be redirected to the default instance, which is the instance specified with the QoS policy under the SAP ingress or egress.

Values 1 to 65535

Platforms All

match

Syntax **match** [**protocol** *protocol-id*]
match protocol none
no match

Context [Tree] (config>filter>ip-exception>entry match)

Full Context configure filter ip-exception entry match

Description Commands in this context enter match criteria for the filter entry. When the match criteria have been satisfied the action associated with the match criteria is executed.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry. More precisely, the command can be entered multiple times but this only results in modifying the *protocol-id*. and does not affect the underlying match criteria configuration.

The **no** form of the command removes all the match criteria from the filter entry and sets the *protocol-id* of the match command to **none** (keyword). As per above, **match protocol none** is however not equivalent to **no match**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default match protocol none

Parameters *protocol-id* — Configures and IP protocol to be used as an IP filter match criterion. The protocol type, such as TCP or UDP, is identified by its respective protocol number.

Values protocol-number: [0..255]D

[0x0..0xFF]H

[0b0..0b11111111]B

protocol-name:0 to 255 in decimal format. Values can also be specified in hexadecimal format, in binary format, or using the following keywords:

IPv4 filter keywords: none (default), icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp

IP exception filter keywords: none, icmp, igmp, ospf-igp, pim, rsvp, tcp, udp, vrrp

* — udp/tcp wildcard

Table 82 **Protocol ID Descriptions**

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 82 **Protocol ID Descriptions**

Protocol	Protocol ID	Description
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram
sctp	132	Stream Control Transmission Protocol

Platforms VSR

match

Syntax **match** [{**protocol** *protocol-id* | **protocol-list** *protocol-list-name*}]
match protocol none
no match

Context **[Tree]** (config>filter>ip-filter>entry match)

Full Context configure filter ip-filter entry match

Description Commands in this context enter match criteria for the filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A match context may consist of multiple match criteria, but multiple match statements cannot be created per entry. More precisely, the **protocol** command can be entered multiple times but this only results in modifying the *protocol-id*. Matching on more than one protocol can be achieved using the protocol-list match criteria in an IP filter policy.

The **no** form of the command removes all the match criteria from the filter entry and sets the *protocol-id* of the match command to **none**. However, **match protocol none** is not equivalent to **no match**.

Default match protocol none

Parameters *protocol-id* — *protocol-number* | *protocol-name*

protocol-number — Specifies the protocol number value to be configured as a match criterion. The value can be expressed as a decimal integer, or in hexadecimal or binary format.

Values [0..255]D, [0x0..0xFF]H, [0b0..0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values IPv4 filter keywords: none (default), icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp

***** — udp/tcp

Table 83 **Protocol ID Descriptions**

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 83 **Protocol ID Descriptions**

Protocol	Protocol ID	Description
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram
sctp	132	Stream Control Transmission Protocol

protocol-list-name — Specifies the name of the protocol list, up to 32 characters.

Platforms All

match

Syntax **match** [**next-header** *next-header*]
no match

Context **[Tree]** (config>filter>ipv6-exception>entry match)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter ipv6-exception entry match

Description Commands in this context enter match criteria for the IPv6 filter exception. When the match criteria have been satisfied, the action associated with the match criteria is executed.

The **no** form of the command removes all the match criteria from the IPv6 filter exception.

Parameters *next-header — protocol-number*, *protocol-name*

Specifies the next header to match.

protocol-number — Specifies the protocol number value to be configured as a match criterion.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

Platforms VSR

match

Syntax **match** [{**next-header** *protocol-id* | **next-header-list** *protocol-list-name*}]
match next-header none
no match

Context **[Tree]** (config>filter>ipv6-filter>entry match)

Full Context configure filter ipv6-filter entry match

Description Commands in this context enter match criteria for the filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

A match context may consist of multiple match criteria, but multiple match statements cannot be created per entry. More precisely, the **next-header** command can be entered multiple times, but this only results in modifying the *protocol-id*. Matching on more than one protocol can be achieved using the **next-header-list** match criteria.

The **no** form of the command removes all the match criteria from the filter entry and sets the *protocol-id* of the match command to **none**. However, **match next-header none** is not equivalent to **no match**.

Default match next-header none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *next-header — protocol-number*, *protocol-name*

Specifies the IPv6 next header to match. This parameter is analogous to the protocol parameter used in IPv4 filter match command.

protocol-number — Specifies the protocol number value to be configured as a match criterion.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

protocol-list-name — Specifies the name of the protocol list, up to 32 characters.

Platforms All

match

Syntax **match** [**frame-type** {**802dot3** | **802dot2-llc** | **802dot2-snap** | **ethernet_II**}]
no match

Context **[Tree]** (config>filter>mac-filter>entry match)

Full Context configure filter mac-filter entry match

Description This command creates the context for entering/editing match criteria for the filter entry and specifies an Ethernet frame type for the entry.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Parameters **frame-type** — The **frame-type** keyword configures an Ethernet frame type to be used for the MAC filter match criteria.

Default **802dot3**

Values 802dot3, 802dot2-llc, 802dot2-snap, ethernet_II

802dot3 — Specifies the frame type is Ethernet IEEE 802.3.

802dot2-llc — Specifies the frame type is Ethernet IEEE 802.2 LLC.

802dot2-snap — Specifies the frame type is Ethernet IEEE 802.2 SNAP.

ethernet_II — Specifies the frame type is Ethernet Type II.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

match

Syntax [**no**] **match**

Context **[Tree]** (config>log>filter>filter-id>entry match)

Full Context configure log filter filter-id entry match

Description This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.

If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied (AND functional) before the action associated with the match is executed.

Use the **application** command to display a list of the valid applications.

Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple **match** statements cannot be entered per entry.

The **no** form of this command removes the match criteria for the *entry-id*.

match

Syntax **match** [**frame-type** *frame-type*]
no match

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry match)

Full Context configure system security management-access-filter mac-filter entry match

Description This command configures math criteria for this MAC filter entry.

Parameters *frame-type* — Specifies the type of MAC frame to use as match criteria.

Values 802dot3 | 802dot2-llc | 802dot2-snap | 802dot1ag | ethernet_II

Default 802dot3

Platforms All

match

Syntax **match** [**protocol** *protocol-id*]
no match

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (cfg>sys>sec>cpm>ip-filter>entry match)

Full Context configure system security cpm-filter ip-filter entry match

Description Commands in this context enter match criteria for the filter entry. When the match criteria have been satisfied the action associated with the match criteria is executed. If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (AND function) before the action associated with the match is executed.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters **protocol** — Configures an IP protocol to be used as an IP filter match criterion. The protocol type such as TCP or UDP is identified by its respective protocol number.

protocol-id — Configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form the command removes the protocol from the match criteria.

Values 1 to 255 (values can be expressed in decimal, hexadecimal, or binary) keywords - none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp, * — udp/tcp wildcard

Table 84 **IP Protocol Names**

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	any private interior gateway (used by Cisco for their IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 84 **IP Protocol Names**

Protocol	Protocol ID	Description
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

match

Syntax **match** [**next-header** *next-header*]
no match

Context **[Tree]** (cfg>sys>sec>cpm>ipv6-filter>entry match)

Full Context configure system security cpm-filter ipv6-filter entry match

Description This command specifies match criteria for the IP filter entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters *next-header — protocol-number*, *protocol-name*

Specifies the next header to match.

The protocol type such as TCP, UDP or OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6) and UDP(17).

protocol-number — Specifies the protocol number value to be configured as a match criterion.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be configured as a match criterion.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp
* - udp/tcp wildcard

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

match

Syntax **match** *command-string*
no match

Context **[Tree]** (config>system>security>profile>entry match)

Full Context configure system security profile entry match

Description This command configures a command or subtree commands in subordinate command levels are specified.

Because the OS exits when the first match is found, subordinate levels cannot be modified with subsequent action commands. More specific action commands should be entered with a lower entry number or in a profile that is evaluated prior to this profile.

All commands below the hierarchy level of the matched command are denied.

The **no** form of this command removes a match condition.

Parameters *command-string* — Specifies the CLI command or CLI tree level that is the scope of the profile entry.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

match

Syntax **match**

Context **[Tree]** (config>router>bgp>group>dynamic-neighbor match)

Full Context configure router bgp group dynamic-neighbor match

Description This command configures match conditions for the dynamic neighbors.

Platforms All

17.59 match-circuit-id

match-circuit-id

Syntax [**no**] **match-circuit-id**

Context **[Tree]** (config>service>ies>sub-if>grp-if>dhcp match-circuit-id)
[Tree] (config>service>vprn>sub-if>dhcp match-circuit-id)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp match-circuit-id)

Full Context configure service ies subscriber-interface group-interface dhcp match-circuit-id
configure service vprn subscriber-interface dhcp match-circuit-id
configure service vprn subscriber-interface group-interface dhcp match-circuit-id

Description This command enables Option 82 circuit ID on relayed DHCP packet matching. For routed CO, the group interface DHCP relay process is stateful. When packets are relayed to the server the virtual router ID, transaction ID, SAP ID, and client hardware MAC address of the relayed packet are tracked.

When a response is received from the server the virtual router ID, transaction ID, and client hardware MAC address must be matched to determine the SAP on which to send the packet out. In some cases, the virtual router ID, transaction ID, and client hardware MAC address are not guaranteed to be unique.

When the **match-circuit-id** command is enabled this as part of the key is used to guarantee correctness in our lookup. This is only needed when dealing with an IP aware DSLAM that proxies the client hardware MAC address.

The **no** form of this command disables Option 82 circuit ID on relayed DHCP packet matching.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.60 match-list

match-list

Syntax **match-list** *ppp-match-type-1* [*ppp-match-type-2*]
no match-list

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp match-list)

Full Context configure subscriber-mgmt local-user-db ppp match-list

Description This command specifies the type of matching done to identify a host. There are different match-types for PPPoE hosts of which a maximum of three can be specified.

The **no** form of this command reverts to the default.

Parameters *match-type-x* — Specifies up to three matching types to identify a host.

Values For PPP: circuit-id, derived-id, mac, remote-id, sap-id, encap-tag-range, encap-tag-separate-range, service-name, username

Note: The format of *remote-id* in IPv6 is different that the format of *remote-id* in IPv4; IPv6 *remote-id* contains *enterprise-id* filed that is also honored in matching.

circuit-id — Specifies to use the circuit ID to match against.

derived-id — Specifies the value extracted by Python script during processing of DHCP Discover/Solicit/Request/Renew/Rebind Messages (client to server bound messages). The value is stored in the DHCP Transaction Cache (DTC) in a variable named alc.dtc.derivedId. This value has a lifespan of a DHCP transaction (a single pair of messages exchanged between the client and the server, for example DHCP Discover and DHCP Offer).

encap-tag-separate-range — Specifies the match encapsulation inner and outer tag in two separate ranges.

encap-tag-range — Specifies to match tag ranges for inner and outer tags.

mac — Specifies to use the MAC address to match against.

remote-id — Specifies to use the remote ID to match against.

sap-id — Specifies the SAP ID on which DHCPv4 packet are received. The SAP ID is inserted as ALU VSO (82,9,4) by the DHCPv4 relay in router. This is enabled via configuration under the vendor-specific-option CLI hierarchy of the DHCPv4 relay. Since the **dhcp-relay** configuration is enabled under the group-interface CLI hierarchy, the group interface and the service ID must be known before the SAP ID can be used for LUDB match.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

service-id — Specifies the service ID of the ingress SAP for DHCPv4 packets. The service ID is inserted as ALU VSO (82,9,3) by the DHCPv4 relay in router. This is enabled via configuration under the vendor-specific-option CLI hierarchy of the DHCPv4 relay.

system-id — Specifies the system ID of the node name configured under the **system>name** CLI hierarchy. The system ID is inserted as ALU VSO (82,9,1) by the DHCPv4 relay in router. This is enabled via configuration under the vendor-specific-option CLI hierarchy of the DHCPv4 relay. Since the **dhcp-relay** configuration is enabled under the group interface CLI hierarchy, the group interface and the service-id must be known before the system ID can be used for LUDB match.

username — Specifies the user name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

match-list

Syntax **match-list** *ipoe-match-type-1* [*ipoe-match-type-2*]
no match-list

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe match-list)

Full Context configure subscriber-mgmt local-user-db ipoe match-list

Description This command specifies the type of matching done to identify a host. There are different match-types for IPoE hosts of which a maximum of four can be specified.

The **no** form of this command reverts to the default.

Parameters *match-type-x* — Specifies up to four matching types to identify a host.

Values For IPoE: circuit-id, derived-id, dual-stack-remote-id, encap-tag-range, encap-tag-separate-range, ip, mac, option60, remote-id, sap-id, service-id, string, system-id

Note: The format of *remote-id* in IPv6 is different that the format of remote-id in IPv4; IPv6 *remote-id* contains *enterprise-id* filed that is also honored in matching.

circuit-id — Specifies to use the circuit ID to match against.

derived-id — Specifies the value extracted by Python script during processing of DHCP Discover/Solicit/Request/Renew/Rebind Messages (client to server bound messages). The value is stored in the DHCP Transaction Cache (DTC) in a variable named alc.dtc.derivedId. This value has a lifespan of a DHCP transaction (a single pair of messages exchanged between the client and the server, for example DHCP Discover and DHCP Offer).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dual-stack-remote-id — Specifies the enterprise-id in IPv6 remote-id is stripped off before LUDB matching is performed. Processing of IPv4 remote ID remains unchanged. This will allow a single host entry in LUDB for dual-stack host where host identification is performed based on the remote ID field.

encap-tag-separate-range — Specifies the match encapsulation inner and outer tag in two separate ranges.

encap-tag-range — Specifies to match tag ranges for inner and outer tags.

ip — Specifies the source IPv4/IPv6 address of a data-trigger packet.

mac — Specifies to use the MAC address to match against.

option-60 — Specifies to use Option60 to match against.

remote-id — Specifies to use the remote ID to match against.

sap-id — Specifies the SAP ID on which DHCPv4 packet are received. The SAP ID is inserted as ALU VSO (82,9,4) by the DHCPv4 relay in router. This is enabled via configuration under the vendor-specific-option CLI hierarchy of the DHCPv4 relay. Since the **dhcp-relay** configuration is enabled under the group interface CLI hierarchy, the group interface and the service ID must be known before the SAP ID can be used for LUDB match.

service-id — Specifies the service ID of the ingress SAP for DHCPv4 packets. The service ID is inserted as ALU VSO (82,9,3) by the DHCPv4 relay in router. This is enabled via configuration under the vendor-specific-option CLI hierarchy of the DHCPv4 relay.

string — Specifies the custom string configured under the vendor-specific-option CLI hierarchy of the DHCPv4 relay. The string is inserted as ALU VSO (82,9,5) by the DHCPv4 relay in router. Since the **dhcp-relay** configuration is enabled under the group-interface CLI hierarchy, the group-interface and the service ID must be known before the string can be used for LUDB match.

system-id — Specifies the system ID of the node name configured under the **system>name** CLI hierarchy. The system ID is inserted as ALU VSO (82,9,1) by the DHCPv4 relay in router. This is enabled via configuration under the vendor-specific-option CLI hierarchy of the DHCPv4 relay. Since the **dhcp-relay** configuration is enabled under the group interface CLI hierarchy, the group interface and the service ID must be known before the system ID can be used for LUDB match.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

match-list

Syntax **match-list**

Context **[Tree]** (config>ipsec>client-db match-list)

Full Context configure ipsec client-db match-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the match list context on a client database. The match list defines the match input used during IPsec's tunnel setup. If there are multiple inputs configured in the match list, then they all must have matches before the system considers a client entry is a match.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

match-list

Syntax **match-list**

Context **[Tree]** (config>qos match-list)

Full Context configure qos match-list

Description This command is used to enter the context to create or edit match lists used in QoS policies.

Platforms All

match-list

Syntax **match-list**

Context **[Tree]** (config>filter match-list)

Full Context configure filter match-list

Description This command enables the configuration context for match lists to be used in filter policies (IOM/FP and CPM).

Platforms All

17.61 match-peer-id-to-cert

match-peer-id-to-cert

Syntax [**no**] **match-peer-id-to-cert**

Context **[Tree]** (config>ipsec>ike-policy match-peer-id-to-cert)

Full Context configure ipsec ike-policy match-peer-id-to-cert

Description This command enables checking the IKE peer's ID matches the peer's certificate when performing certificate authentication.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no match-peer-id-to-cert

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.62 match-qinq-dot1p

match-qinq-dot1p

Syntax **match-qinq-dot1p** {**top** | **bottom**}
no match-qinq-dot1p

Context **[Tree]** (config>service>ies>if>sap>ingress match-qinq-dot1p)
[Tree] (config>service>ies>sub-if>grp-if>sap>ingress match-qinq-dot1p)
[Tree] (config>service>vpls>sap>ingress match-qinq-dot1p)
[Tree] (config>service>vprn>sub-if>grp-if>sap>ingress match-qinq-dot1p)

Full Context configure service ies interface sap ingress match-qinq-dot1p
configure service ies subscriber-interface group-interface sap ingress match-qinq-dot1p
configure service vpls sap ingress match-qinq-dot1p
configure service vprn subscriber-interface group-interface sap ingress match-qinq-dot1p

Description This command specifies which dot1Q tag position dot1P bits in a QinQ encapsulated packet should be used to evaluate dot1P QoS classification.

The **match-qinq-dot1p** command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy's dot1P entries. The **top** and **bottom** keywords specify which position should be evaluated for QinQ encapsulated packets.

By default, the bottom-most service delineating dot1Q tag's dot1P bits are used. Table 85 defines the default behavior for dot1P evaluation when the **match-qinq-dot1p** command is not executed.

Table 85 **Default QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN-ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 85 **Default QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ/TopQ	TopQ	TopQ PBits
QinQ/TopQ	TopQ BottomQ	TopQ PBits
QinQ/TopQ	TopQ BottomQ	BottomQ PBits

The **no** form of this command restores the default dot1p evaluation behavior for the SAP.

Default no match-qinq-dot1p (no filtering based on p-bits)

(top or bottom must be specified to override the default QinQ dot1p behavior)

Parameters **top** — The top parameter is mutually exclusive to the bottom parameter. When the **top** parameter is specified, the topmost PBits are used (if existing) to match any dot1p dot1p-value entries. Table 86 defines the dot1p evaluation behavior when the **top** parameter is specified.

Table 86 **Top Position QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN-ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ/TopQ	TopQ	TopQ PBits
QinQ/TopQ	TopQ BottomQ	TopQ PBits
QinQ/QinQ	TopQ BottomQ	TopQ PBits

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bottom — The **bottom** parameter is mutually exclusive to the **top** parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. Table 87 defines the dot1p evaluation behavior when the bottom parameter is specified.

Table 87 **Bottom Position QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN-ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	BottomQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ/TopQ	TopQ	TopQ PBits
QinQ/TopQ	TopQ BottomQ	BottomQ PBits
QinQ/QinQ	TopQ BottomQ	BottomQ PBits

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap ingress match-qinq-dot1p
- configure service ies subscriber-interface group-interface sap ingress match-qinq-dot1p

All

- configure service vpls sap ingress match-qinq-dot1p
- configure service ies interface sap ingress match-qinq-dot1p

match-qinq-dot1p

Syntax **match-qinq-dot1p** {**top** | **bottom**}
no match-qinq-dot1p de

Context **[Tree]** (config>service>ipipe>sap>ingress match-qinq-dot1p)
[Tree] (config>service>epipe>sap>ingress match-qinq-dot1p)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service epipe sap ingress match-qinq-dot1p
configure service ipipe sap ingress match-qinq-dot1p

Description This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The **match-qinq-dot1p** command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy's Dot1P entries. The **top** and **bottom** keywords specify which position should be evaluated for QinQ encapsulated packets.

The setting also applies to classification based on the DE indicator bit.

The **no** form of this command reverts the dot1p and de bits matching to the default tag.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. Table 88 defines the default behavior for Dot1P evaluation.

Table 88 **Default QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits
QinQ / QinQ	TopQ BottomQ	BottomQ PBits

Default no match-qinq-dot1p (no filtering based on p-bits)

(top or bottom must be specified to override the default QinQ dot1p behavior)

Parameters **top** — The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. Table 89 defines the dot1p evaluation behavior when the top parameter is specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 89 **Top Position QinQ dpt1p Evaluation Behavior**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits
QinQ / QinQ	TopQ BottomQ	TopQ PBits

bottom — The bottom parameter and the top parameter are mutually exclusive. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. Table 90 defines the dot1p evaluation behavior when the bottom parameter is specified.

Table 90 **Bottom Position QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Null	None	None
Null	Dot1P (VLAN ID 0)	Dot1P PBits
Null	Dot1Q	Dot1Q PBits
Null	TopQ BottomQ	TopQ PBits
Null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	None (Default SAP)	None
Dot1Q	Dot1P (Default SAP VLAN ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	BottomQ PBits

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 90 **Bottom Position QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
QinQ / QinQ	TopQ BottomQ	BottomQ PBits

Table 91 **Egress SAP Types**

Egress SAP Type	Ingress Packet Preserved Dot1P State	Marked (or Remarked) PBits
Null	No preserved Dot1P bits	None
Null	Preserved Dot1P bits	Preserved tag PBits remarked using dot1p-value
Dot1Q	No preserved Dot1P bits	New PBits marked using dot1p-value
Dot1Q	Preserved Dot1P bits	Preserved tag PBits remarked using dot1p-value
TopQ	No preserved Dot1P bits	TopQ PBits marked using dot1p-value
TopQ	Preserved Dot1P bits (used as TopQ and BottomQ PBits)	TopQ PBits marked using dot1p-value, BottomQ PBits preserved
QinQ	No preserved Dot1P bits	TopQ PBits and BottomQ PBits marked using dot1p-value
QinQ	Preserved Dot1P bits (used as TopQ and BottomQ PBits)	TopQ PBits and BottomQ PBits marked using dot1p-value

The QinQ and TopQ SAP PBit/DEI bit marking follows the default behavior defined in the preceding table when **qinq-mark-top-only** is not specified.

The dot1p *dot1p-value* command must be configured without the qinq-mark-top-only parameter to remove the TopQ PBits only marking restriction.

A QinQ-encapsulated Ethernet port can have two different sap types:

For a TopQ SAP type, only the outer (top) tag is explicitly specified. For example, **sap 1/1/1:10.***

For QinQ SAP type, both inner (bottom) and outer (top) tags are explicitly specified. For example, **sap 1/1/1:10.100**.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

match-qinq-dot1p

Syntax **match-qinq-dot1p** {**top** | **bottom**}
no match-qinq-dot1p

Context **[Tree]** (config>service>vprn>if>sap>ingress match-qinq-dot1p)

Full Context configure service vprn interface sap ingress match-qinq-dot1p

Description This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The **match-qinq-dot1p** command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy's Dot1P entries. The **top** and **bottom** keywords specify which position should be evaluated for QinQ encapsulated packets.

The **no** form of this command restores the default dot1p evaluation behavior for the SAP.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. Table 92 defines the default behavior for Dot1P evaluation when the **match-qinq-dot1p** command is not executed.

Table 92 **Dot1P Default Behavior**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
null	none	none
null	Dot1P (VLAN-ID 0)	Dot1P PBits
null	—	Dot1Q PBits
null	TopQ BottomQ	TopQ PBits
null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	none (Default SAP)	none
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits
QinQ / QinQ	TopQ BottomQ	BottomQ PBits

Default no match-qinq-dot1p - No filtering based on p-bits.

top or **bottom** must be specified to override the default QinQ dot1p behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **top** — The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. Table 93 defines the dot1p evaluation behavior when the top parameter is specified.

Table 93 **Dot1P Evaluation Behavior**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
null	none	none
null	Dot1P (VLAN-ID 0)	Dot1P PBits
null	Dot1Q	Dot1Q PBits
null	TopQ BottomQ	TopQ PBits
null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	none (Default SAP)	none
Dot1Q	Dot1P (Default SAP VLAN-ID 0)	Dot1P PBits
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	TopQ PBits

bottom — The bottom parameter is mutually exclusive to the top parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any **dot1p** *dot1p-value* entries. The following tables define the bottom position QinQ and TopQ SAP dot1p evaluation and the default dot1p explicit marking actions.

Table 94 **Bottom Position QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
null	none	none
null	Dot1P (VLAN-ID 0)	Dot1P PBits
null	Dot1Q	Dot1Q PBits
null	TopQ BottomQ	BottomQ PBits
null	TopQ (No BottomQ)	TopQ PBits
Dot1Q	none (default SAP)	none
Dot1Q	Dot1P (default SAP VLAN-ID 0)	Dot1P PBits

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 94 **Bottom Position QinQ and TopQ SAP Dot1P Evaluation**

Port / SAP Type	Existing Packet Tags	PBits Used for Match
Dot1Q	Dot1Q	Dot1Q PBits
QinQ / TopQ	TopQ	TopQ PBits
QinQ / TopQ	TopQ BottomQ	BottomQ PBits
QinQ / QinQ	TopQ BottomQ	BottomQ PBits

Table 95 **Default Dot1P Explicit Marking Actions**

Egress SAP Type	Ingress Packet Preserved Dot1P State	Marked (or Remarked) PBits
null	no preserved Dot1P bits	none
null	preserved Dot1P bits	preserved tag PBits remarked using dot1p-value
Dot1Q	no preserved Dot1P bits	new PBits marked using dot1p-value
Dot1Q	preserved Dot1P bits	preserved tag PBits remarked using dot1p-value
TopQ	no preserved Dot1P bits	TopQ PBits marked using dot1p-value
TopQ	preserved Dot1P bits (used as TopQ and BottomQ PBits)	TopQ PBits marked using dot1p-value, BottomQ PBits preserved
QinQ	no preserved Dot1P bits	TopQ PBits and BottomQ PBits marked using dot1p-value
QinQ	preserved Dot1P bits (used as TopQ and BottomQ PBits)	TopQ PBits and BottomQ PBits marked using dot1p-value

The **dot1p** *dot1p-value* command must be configured without the **qinq-mark-top-only** parameter to remove the TopQ PBits only marking restriction.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.63 match-radius-proxy-cache

match-radius-proxy-cache

Syntax **match-radius-proxy-cache**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host match-radius-proxy-cache)

Full Context configure subscriber-mgmt local-user-db ipoe host match-radius-proxy-cache

Description Commands in this context configure RADIUS proxy cache match parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.64 max

max

Syntax **max** *num-sessions*
no max

Context **[Tree]** (config>service>nat>nat-policy>session-limits max)
[Tree] (config>service>nat>firewall-policy>session-limits max)
[Tree] (config>service>nat>up-nat-policy>session-limits max)

Full Context configure service nat firewall-policy session-limits max
configure service nat nat-policy session-limits max
configure service nat up-nat-policy session-limits max

Description This command configures the session limit of this policy. The session limit is the maximum number of sessions allowed for a subscriber associated with this policy.

Default max 65535

Parameters *num-sessions* — Specifies the session limit.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy session-limits max
- configure service nat nat-policy session-limits max

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy session-limits max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.65 max-admin-down-time

max-admin-down-time

Syntax **max-admin-down-time** [[*down-interval*] | **infinite**]
no max-admin-down-time

Context **[Tree]** (config>lag>bfd>family max-admin-down-time)

Full Context configure lag bfd family max-admin-down-time

Description This command specifies the maximum amount of time the router will continue to forward traffic over a link after the micro-BFD sessions has transitioned to a Down state because it received an ADMIN-DOWN state from the far-end. This timer provide the administrator the configured amount of time to disable or de-provision the micro-BFD session on the local node before forwarding is halted over the associated link(s).

The **no** form of this command removes the time interval from the configuration.

Default max-admin-down-time 0

Parameters *down-interval* — Specifies the amount of time, in seconds.

Values -1 to 3600

infinite — Specifies no end time to forward traffic.

Platforms All

17.66 max-advertisement

max-advertisement

Syntax **max-advertisement** *seconds*
no max-advertisement

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv max-advertisement)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 max-advertisement)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv max-advertisement)
[Tree] (config>service>vprn>router-advert>if max-advertisement)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv max-advertisement)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 max-advertisement)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv max-advertisement)
[Tree] (config>subscr-mgmt>rtr-adv-plcy max-advertisement)

Full Context configure service ies subscriber-interface group-interface ipv6 max-advertisement

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies subscriber-interface group-interface ipv6 router-advertisements max-advertisement
configure service ies subscriber-interface ipv6 router-advertisements max-advertisement
configure service vprn router-advert interface max-advertisement
configure service vprn subscriber-interface group-interface ipv6 max-advertisement
configure service vprn subscriber-interface group-interface ipv6 router-advertisements max-advertisement
configure service vprn subscriber-interface ipv6 router-advertisements max-advertisement
configure subscriber-mgmt router-advertisement-policy max-advertisement

Description This command specifies the maximum time allowed between sending unsolicited router advertisements from this interface.

The **no** form of this command reverts to the default.

Default max-advertisement 1800

Parameters *seconds* — Specifies the maximum advertisement interval, in seconds.

Values 900 to 1800

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.67 max-advertisement-interval

max-advertisement-interval

Syntax [**no**] **max-advertisement-interval** *seconds*

Context **[Tree]** (config>service>vprn>router-advert>if max-advertisement-interval)
[Tree] (config>router>router-advert>if max-advertisement-interval)

Full Context configure router router-advertisement interface max-advertisement-interval
configure service vprn router-advertisement interface max-advertisement-interval

Description This command configures the maximum interval between sending router advertisement messages.

Default max-advertisement-interval 600

Parameters *seconds* — Specifies the maximum interval in seconds between sending router advertisement messages.

Values 4 to 1800

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.68 max-age

max-age

Syntax **max-age** *max-age*
no max-age [*max-age*]

Context **[Tree]** (config>service>vpls>stp max-age)
[Tree] (config>service>template>vpls-template>stp max-age)

Full Context configure service template vpls-template stp max-age
configure service vpls stp max-age

Description This command indicates how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge will take the message_age value from BPDUs received on their root port and increment this value by 1. The message_age therefore reflects the distance from the root bridge. BPDUs with a message age exceeding max-age are ignored.

STP uses the max-age value configured in the root bridge. This value is propagated to the other bridges via the BPDUs.

The **no** form of this command returns the max age to the default value.

Default max-age 20

Parameters *max-age* — The max info age for the STP instance in seconds. Allowed values are integers in the range 6 to 40.

Platforms All

17.69 max-attempts

max-attempts

Syntax **max-attempts** *count*
max-attempts infinite
no max-attempts

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>efh>interim-c max-attempts)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling interim-credit max-attempts

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of attempts made to establish a new Diameter Gy session with the Online Charging Server (OCS) when Extended Failure Handling (EFH) is active.

A new attempt is made when the volume or time interim credit of a rating group is consumed or when the validity time expires for a rating group.

When the maximum number of attempts is reached, the user session associated with the Diameter session is terminated (the corresponding subscriber hosts are deleted from the system).

The **no** form of this command resets the value to the default value.

Default max-attempts 10

Parameters *count* — Specifies the maximum number attempts that is made to establish a Diameter Gy session with the OCS when EFH is active.

Values 1 to 4294967295

infinite — Specifies that an unlimited number of attempts is made to establish a Diameter Gy session with the OCS when EFH is active.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.70 max-auth-req

max-auth-req

Syntax **max-auth-req** *max-auth-request*

Context **[Tree]** (config>port>ethernet>dot1x max-auth-req)

Full Context configure port ethernet dot1x max-auth-req

Description This command configures the maximum number of times that the router will send an access request RADIUS message to the RADIUS server. If a reply is not received from the RADIUS server after the specified number attempts, the 802.1x authentication procedure is considered to have failed.

The **no** form of this command returns the value to the default.

Default max-auth-req 2

Parameters *max-auth-request* — The maximum number of RADIUS retries.

Values 1 to 10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.71 max-avg

max-avg

Syntax **max-avg** *percent*
no max-avg

Context **[Tree]** (config>qos>slope-policy>exceed-slope max-avg)
[Tree] (config>qos>slope-policy>highplus-slope max-avg)
[Tree] (config>qos>slope-policy>high-slope max-avg)
[Tree] (config>qos>slope-policy>low-slope max-avg)

Full Context configure qos slope-policy exceed-slope max-avg
configure qos slope-policy high-slope max-avg
configure qos slope-policy highplus-slope max-avg
configure qos slope-policy low-slope max-avg

Description Sets the exceed, low, high, or highplus Random Early Detection (RED) slope position for the shared buffer average utilization value where the packet discard probability rises directly to one. The percent parameter is expressed as a percentage of the shared buffer size.

The **no** form of this command restores the max-avg value to the default setting. If the current **start-avg** setting is larger than the default, an error will occur and the max-avg setting will not be changed to the default.

Default max-avg 100 - Highplus slope default is 100% buffer utilization before discard probability is 1.

max-avg 90 — High slope default is 90% buffer utilization before discard probability is 1.

max-avg 75 — Low slope default is 75% buffer utilization before discard probability is 1.

max-avg 55 — Exceed slope default is 55% buffer utilization before discard probability is 1.

Parameters *percent* — The percentage of the shared buffer space for the buffer pool at which point the drop probability becomes one. The value entered must be greater or equal to the current setting of **start-avg**. If the entered value is smaller than the current value of **start-avg**, an error will occur and no change will take place.

Values 0 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.72 max-bandwidth

max-bandwidth

Syntax **max-bandwidth** *number-links*
no max-bandwidth

Context **[Tree]** (config>port>ml-bundle>ima max-bandwidth)

Full Context configure port multilink-bundle ima max-bandwidth

Description This command specifies the number of links used to determine the maximum configurable bandwidth that is allowed to be used for this IMA group.

The maximum bandwidth is computed as:

Maximum Configurable ATM Bandwidth (MCAB) =

(number-links) * (M-1)/M * (2048/2049) * primary member link speed

Where: M is the IMA frame size (128)
Primary member link speed is either E-1 — 1920 kb/s or DS-1 — 1539 kb/s. E-1 speed is used for a group with no members.

The total ATM bandwidth of services over shaped VCs cannot exceed the MCAB value as result of adding more services or removing member links.

The **no** form of this command resets the max-bandwidth to its default value.

Default max-bandwidth 8

Parameters *number-links* — Specifies the number of links that determines the maximum configurable bandwidth that is allowed to be used for this IMA group.

Values 1 to 8

Platforms 7450 ESS, 7750 SR-7/12/12e

max-bandwidth

Syntax **max-bandwidth** *bandwidth-in-mbps*
no max-bandwidth

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth max-bandwidth)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth max-bandwidth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls lsp auto-bandwidth max-bandwidth
configure router mpls lsp-template auto-bandwidth max-bandwidth

Description This command configures the maximum bandwidth that auto-bandwidth allocation is allowed to request for an LSP.

The LSP maximum applies whether the bandwidth adjustment is triggered by normal adjust-interval expiry, the overflow limit having been reached, or manual request.

The **no** form of this command reverts to the default value.

The max-bandwidth must be greater than the min-bandwidth.

Default max-bandwidth 100000

Parameters *bandwidth-in-mbps* — Specifies the maximum bandwidth in Mb/s.

Values 0 to 6400000

Platforms All

17.73 max-burst

max-burst

Syntax **max-burst** *number*
no max-burst

Context **[Tree]** (config>router>rsvp>msg-pacing max-burst)

Full Context configure router rsvp msg-pacing max-burst

Description This command specifies the maximum number of RSVP messages that are sent in the specified period under normal operating conditions.

Default max-burst 650

Parameters *number* — Specifies the maximum number of RSVP messages to be sent in increments of 10.

Values 100 to 1000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.74 max-burst-size

max-burst-size

Syntax **max-burst-size** *size* [**bytes** | **kilobytes**]
no max-burst-size

Context **[Tree]** (config>router>policy-acct-template>policer max-burst-size)

Full Context configure router policy-acct-template policer max-burst-size

Description This command configures the MBS for the policer. When this threshold value is exceeded, packets are considered violating and are dropped.

When this value is not configured, the default value is dependent on the peak-rate setting. When peak-rate is set to max or is greater than or equal to the FP capacity (overriding an explicitly configured MBS value), the default value is 16 megabytes; otherwise the value is capped at 3988 kilobytes with a minimum of 256 bytes.

The **no** form of this command reverts to the default value.

Parameters *size* — Specifies the maximum number of RSVP messages to be sent in increments of 10.

Values 0 to 16777216 | **default**

bytes — Specifies that the value is in bytes.

kilobytes — Specifies that the value is in kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

17.75 max-bypass-associations

max-bypass-associations

Syntax **max-bypass-associations** *integer*
no max-bypass-associations

Context **[Tree]** (config>router>mpls max-bypass-associations)

Full Context configure router mpls max-bypass-associations

Description This command allows the user to set a maximum number of LSP primary path associations with each manual or dynamic bypass LSP that is created in the system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, a Point of Local Repair (PLR) node will associate a maximum of 1000 primary LSP paths with a given bypass before using the next available manual bypass or signaling a new dynamic bypass.

Note that a new bypass LSP may need to be signaled if the constraint of a given primary LSP path is not met by an existing bypass LSP even if the max-bypass-associations for this bypass LSP has not been reached.

The **no** form of this command reinstates the default value of this parameter.

Default max-bypass-associations 1000

Parameters *integer* — Configures the number of LSP primary path associations

Values 100 to 131072

Platforms All

17.76 max-bypass-plr-associations

max-bypass-plr-associations

Syntax **max-bypass-plr-associations** *plr-value*
no max-bypass-plr-associations

Context **[Tree]** (config>router>mpls max-bypass-plr-associations)

Full Context configure router mpls max-bypass-plr-associations

Description This command enables the configuration of the maximum number of Points of Local Repair (PLRs) per RSVP-TE bypass LSP.

A PLR summarizes the constraints applied to the computation of the path of the bypass LSP. It consists of the avoid link/node constraint, and potentially other TE constraints such as exclude SRLG, that are needed to protect against the failure of the primary path of the RSVP-TE LSP that is associated with this bypass LSP.

Additional PLRs with the same avoid link/node constraint are associated with the same bypass to minimize the number of bypass LSPs created. This command controls the maximum number of such PLRs.

Because MPLS saves only the PLR constraints of the first LSP that triggered the dynamic bypass creation, subsequent LSPs for the same avoid link/node and with the non-strict bypass SRLG disjointness enabled may be associated with the same bypass. This is even in cases where there exists a bypass LSP path that strictly satisfies the SRLG constraint.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the maximum PLRs per bypass is configured with a value of 1, MPLS triggers the signaling of a new dynamic bypass LSP for each new PLR and saves each PLR constraint separately with its own bypass. As a result, when MPLS re-optimizes a bypass LSP it guarantees that SRLG disjointness of that PLR are checked and enforced.

The **no** form of this command returns the command to its default value.

Default max-bypass-plr-associations 16

Parameters *plr-value* — Configures the number of LSP primary path associations

Values 1 to 16

Default 16

Platforms All

17.77 max-cells

max-cells

Syntax **max-cells** *cell-count*
no max-cells [*cell-count*]

Context **[Tree]** (config>service>apipe>spoke-sdp>cell-concat max-cells)

Full Context configure service apipe spoke-sdp cell-concatenation max-cells

Description This command enables the configuration of the maximum number of ATM cells to accumulate into an MPLS packet. The remote peer will also signal the maximum number of concatenated cells it is willing to accept in an MPLS packet. When the lesser of (the configured value and the signaled value) number of cells is reached, the MPLS packet is queued for transmission onto the pseudowire. It is ensured that the MPLS packet MTU conforms to the configured service MTU.

The **no** form of this command sets max-cells to the value '1' indicating that no concatenation will be performed.

Parameters *cell-count* — Specifies the maximum number of ATM cells to be accumulated into an MPLS packet before queuing the packet for transmission onto the pseudowire.

Values 1 to 128

Default 1

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.78 max-cleared

max-cleared

Syntax **max-cleared** *maximum*

Context **[Tree]** (config>system>alarms max-cleared)

Full Context configure system alarms max-cleared

Description This command configures the maximum number of cleared alarms that the system will store and display.

Default max-cleared 500

Parameters *maximum* — Specifies the maximum number of cleared alarms, up to 500.

Platforms All

17.79 max-completed

max-completed

Syntax **max-completed** *unsigned*

Context **[Tree]** (config>system>script-control>script-policy max-completed)

Full Context configure system script-control script-policy max-completed

Description This command is used to configure the maximum number of script run history status entries to keep.

Default max-completed 1

Parameters *unsigned* — Specifies the maximum number of script run history status entries to keep.

Values 1 to 1500

Default 1

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.80 max-conn-prefix

max-conn-prefix

Syntax **max-conn-prefix** *count*
no max-conn-prefix

Context **[Tree]** (config>test-oam>twamp>server>prefix max-conn-prefix)

Full Context configure test-oam twamp server prefix max-conn-prefix

Description This command configures the maximum number of control connections by clients with an IP address in a specific prefix. A new control connection is rejected if accepting it would cause either the prefix limit defined by this command or the server limit (max-conn-server) to be exceeded.

The **no** form of this command returns the value to the default.

Default max-conn-prefix 32

Parameters *count* — Specifies the maximum number of control connections.

Values 0 to 64

Default 32

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.81 max-conn-server

max-conn-server

Syntax **max-conn-server** *count*
no max-conn-server

Context **[Tree]** (config>test-oam>twamp>server max-conn-server)

Full Context configure test-oam twamp server max-conn-server

Description This command configures the maximum number of TWAMP control connections from all TWAMP clients. A new control connection is rejected if accepting it would cause either this limit or a prefix limit (max-conn-prefix) to be exceeded.

The **no** form of this command returns the value to the default.

Default max-conn-server 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the maximum number of control connections.

Values 0 to 64

Default 32

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.82 max-data-size

max-data-size

Syntax **max-data-size** *bytes*

Context **[Tree]** (config>sflow>receiver max-data-size)

Full Context configure sflow receiver max-data-size

Description This configures the maximum data size for sFlow UDP datagrams sent to the collector.

To restore default configuration, execute max-data-size 1400.

Default max-data-size 1400

Parameters *bytes* — Specifies the data size.

Values 200 to 1500

Platforms 7750 SR, 7750 SR-s, 7950 XRS

17.83 max-debounce-time

max-debounce-time

Syntax **max-debounce-time** *max-debounce-time*
no max-debounce-time

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring>in-band-control-path max-debounce-time)
[Tree] (config>redundancy>mc>peer>mc>l3-ring>in-band-control-path max-debounce-time)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring in-band-control-path max-debounce-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure redundancy multi-chassis peer mc-ring ring in-band-control-path max-debounce-time

Description This command configures the inband control path maximum debounce time.

The **no** form of this command reverts to the default.

Default max-debounce-time 10

Parameters *max-debounce-time* — Specifies the maximum debounce time on the transition of the operational state of the inband control connection.

Values 5 to 200 seconds

Platforms All

17.84 max-decrement

max-decrement

Syntax **max-decrement** {**percent** *percent-of-admin-pir* | **rate** *rate-in-kilobits-per-second*}
no max-decrement

Context **[Tree]** (config>qos>adv-config-policy>child-control>offered-measurement max-decrement)

Full Context configure qos adv-config-policy child-control offered-measurement max-decrement

Description This command is used to limit how fast a child queue or policer can 'give up' bandwidth that it has been allotted from the virtual scheduler in a single iteration. If the child's new offered rate has decreased by more than the maximum decrement limit, the system ignores the new offered rate and instead uses the old offered rate less the maximum decrement limit.

A possible reason to define a maximum decrement limit is to allow a child queue or policer to hold on to a portion of bandwidth that has been distributed by the parent virtual scheduler in case the child's offered rate fluctuates in an erratic manor. The max-decrement limit has a dampening effect to changes in the offered rate.

A side effect of using a maximum decrement limit is that unused bandwidth allocated to the child queue or policer will not be given to another child as quickly. This may result in an underrun of the virtual scheduler's aggregate rate.

The max-decrement limit has no effect on any increase in a child's offered rate. If the rate increase is above the change sensitivity, the new offered rate is immediately used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the max-decrement command is used with a percent-based value, the decrement limit will be a function of the configured PIR value on the policer or queue. In this case, care should be taken that the child is either configured with an explicit PIR rate (other than max) or the child's administrative PIR is defined using the percent-rate command with the local parameter enabled if an explicit value is not desired. When a maximum PIR is in use on the child, the system attempts to interpret the maximum child forwarding rate. This rate could be very large if the child is associated with multiple ingress or egress ports.

Except for the overall cap on the offered input into the virtual scheduler, the child's administrative PIR has no effect on the calculated sensitivity if an explicit rate is specified.

If the child's administrative PIR is modified while a percent based max-decrement is in effect, the system automatically uses the new relative maximum decrement limit value the next time the child's offered rate is determined.

When the max-decrement command is not specified or removed, the virtual scheduler does not limit a decreasing offered rate to a specific limit.

The **no** form of this command is used to remove any currently configured maximum decrement limit for all child policers and queues associated with the policy.

Parameters *percent-of-admin-pir* — When the percent qualifier is used, this parameter specifies the percentage of the child's administrative PIR that should be used as the decrement limit to offered rate change. If a value of 100 or 100.00 is used, the system will interpret this equivalent to **no max-decrement**.

Values 1.00 to 100.00

rate-in-kilobits-per-second — When the rate qualifier is used, this parameter specifies an explicit rate, in kb/s, that should be used as the child's offered rate change sensitivity value. If a rate sensitivity of 0 is specified, the system interprets this equivalent to **no max-decrement**.

Values 0 to 100,000,000

Platforms All

17.85 max-delay

max-delay

Syntax **max-delay** *delay-time*
no max-delay [*delay-time*]

Context **[Tree]** (config>service>apipe>spoke-sdp>cell-concat max-delay)

Full Context configure service apipe spoke-sdp cell-concatenation max-delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the configuration of the maximum amount of time to wait while performing ATM cell concatenation into an MPLS packet before transmitting the MPLS packet. This places an upper bound on the amount of delay introduced by the concatenation process. When this amount of time is reached from when the first ATM cell for this MPLS packet was received, the MPLS packet is queued for transmission onto the pseudowire.

The **no** form of this command resets max-delay to its default value.

Parameters *delay-time* — Specifies the maximum amount of time, in hundreds of microseconds, to wait before transmitting the MPLS packet with whatever ATM cells have been received. For example, to bound the delay to 1 ms the user would configure 10 (hundreds of microseconds). The delay-time is rounded up to one of the following values 1, 5, 10, 50, 100, 200, 300 and 400.

Values 1 to 400

Default 400

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

17.86 max-description-size

max-description-size

Syntax **max-description-size** *size*
no max-description-size

Context **[Tree]** (config>service>nat>pcp-server-policy max-description-size)

Full Context configure service nat pcp-server-policy max-description-size

Description This command specifies the maximum length of mapping descriptions made by the PCP servers using this PCP policy.

Default max-description-size 64

Parameters *size* — Specifies the maximum length of mapping descriptions made by the PCP servers.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.87 max-drop-count

max-drop-count

Syntax **max-drop-count** *count*
no max-drop-count

Context **[Tree]** (config>service>sdp>keep-alive max-drop-count)

Full Context configure service sdp keep-alive max-drop-count

Description This command configures the number of consecutive SDP keepalive failed request attempts or remote replies that can be missed after which the SDP is operationally downed. If the **max-drop-count** consecutive keepalive request messages cannot be sent or no replies are received, the SDP-ID will be brought operationally down by the keepalive SDP monitoring.

The **no** form of this command reverts the **max-drop-count** *count* value to the default settings.

Default max-drop-count 3

Parameters **count** — Specifies the number of consecutive SDP keepalive requests that are failed to be sent or replies missed, expressed as a decimal integer.

Values 1 to 5

Platforms All

17.88 max-ecmp-routes

max-ecmp-routes

Syntax **max-ecmp-routes** *max-routes*
no max-ecmp-routes

Context **[Tree]** (config>router>ldp max-ecmp-routes)

Full Context configure router ldp max-ecmp-routes

Description This command sets the maximum number of ECMP routes that LDP may use to resolve the next hop for a FEC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The system-wide maximum number of ECMP routes is limited by the **config**>**router**>**ecmp** command. This command, under the LDP context, simply allows LDP to use more than 32 routes, if they are available in RTM or TTM. When configured, the actual number of ECMP routes used by LDP is therefore min[**config**>**router**>**ecmp**, **config**>**router**>**ldp**>**max-ecmp-routes**].

The **no** form of this command reverts to the default value.

Default max-ecmp-routes 32

Parameters *max-routes* — Specifies the maximum number of routes.

Values 1 to 64

Platforms All

17.89 max-entries

max-entries

Syntax **max-entries** *count*
no max-entries

Context **[Tree]** (config>python>py-pol>cache max-entries)

Full Context configure python python-policy cache max-entries

Description This command configures the maximum number of Python cache entries that can be stored in the cache of this Python policy.

If the limit has been reached, a Python exception will be thrown when requested to store another data structure.

The **no** form of this command reverts to the default.

Default max-entries 128000

Parameters *count* — Specifies the maximum number of cache entries allowed.

Values 1 to 1000000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-entries

Syntax **max-entries** *max-entries*
no shutdown

Context **[Tree]** (config>app-assure>group>evt-log max-entries)

Full Context configure application-assurance group event-log max-entries

Description This command configures the number of entries in the buffer.

Default max-entries 500

Parameters *max-entries* — Specifies the maximum number of entries for the event log.

Values 1 to 100000

Default 500

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

max-entries

Syntax **max-entries** *max-entries*
no max-entries

Context **[Tree]** (conf>router>segment-routing>srv6>loc>static-function max-entries)

Full Context configure router segment-routing segment-routing-v6 locator static-function max-entries

Description This command configures the maximum number of entries from the function field that must be reserved for static End, End.X, or a service SID function assignment.

The **no** form of this command reverts to the default value.

Default max-entries 1

Parameters *max-entries* — Specifies the maximum number of entries for the SRv6 locator.

Values 1 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

17.90 max-entry-lifetime

max-entry-lifetime

Syntax **max-entry-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no max-entry-lifetime

Context [Tree] (config>python>py-pol>cache max-entry-lifetime)

Full Context configure python python-policy cache max-entry-lifetime

Description This command configures the maximum allowed lifetime for each entry of the Python cache of this Python policy.

When adding data to the Python cache the lifetime of the given object must always be specified. If the specified lifetime is bigger than the configured value, then the value of the **max-entry-lifetime** will be used instead of the lifetime that was specified.

The **no** form of this command reverts to the default.

Default max-entry-lifetime days 1

Parameters **days** *days* — Specifies the maximum lifetime that can be set on a cache entry in days.

Values 0 to 7

Default 1

hrs *hours* — Specifies the maximum lifetime that can be set on a cache entry in hours.

Values 0 to 23

min *minutes* — Specifies the maximum lifetime that can be set on a cache entry in minutes.

Values 0 to 59

sec *seconds* — Specifies the maximum lifetime that can be set on a cache entry in seconds.

Values 0 to 59

Platforms All

17.91 max-fail

max-fail

Syntax **max-fail** *no-response-count*
no max-fail

Context [Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy max-fail)

Full Context configure saa test type-multi-line lsp-trace sr-policy max-fail

Description This command configures the maximum number of consecutive MPLS echo requests that do not receive a reply before the trace operation fails for a TTL.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default max-fail 5

Parameters *no-response-count* — Specifies the maximum number of consecutive MPLS echo requests, expressed as a decimal integer, that do not receive a reply before the trace operation fails for a TTL.

Values 1 to 255

Default 5

Platforms All

17.92 max-files-number

max-files-number

Syntax **max-files-number** *number*

Context **[Tree]** (config>call-trace max-files-number)

Full Context configure call-trace max-files-number

Description This command configures the maximum number of files call trace can create.

Default max-files-number 200

Parameters *number* — Specifies the maximum number of all call trace log files stored on all compact flash cards together.

Values 1 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.93 max-fragment-delay

max-fragment-delay

Syntax **max-fragment-delay** *milliseconds*
no max-fragment-delay

Context **[Tree]** (config>router>l2tp>group>mlppp max-fragment-delay)
[Tree] (config>router>l2tp>group>tunnel>mlppp max-fragment-delay)
[Tree] (config>service>vprn>l2tp>group>mlppp max-fragment-delay)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp max-fragment-delay)

Full Context configure router l2tp group mlppp max-fragment-delay
configure router l2tp group tunnel mlppp max-fragment-delay
configure service vprn l2tp group mlppp max-fragment-delay
configure service vprn l2tp group tunnel mlppp max-fragment-delay

Description This command is applicable only to LNS. It determines the maximum fragment delay caused by the transmission that will be imposed on a link.

Fragmentation can be used to interleave high priority packet in-between low priority fragments on a MLPPPoX session with a single link or on a MLPPPoX session with multiple links to better load balance traffic over multiple member links.

Default no max-fragment-delay

Parameters *milliseconds* — Specifies the interval, in milliseconds.

Values 5 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

17.94 max-groups

max-groups

Syntax **max-groups** *max-groups*
no max-groups

Context [Tree] (config>service>vprn>igmp>grp-if max-groups)
[Tree] (config>service>vprn>igmp>if max-groups)

Full Context configure service vprn igmp group-interface max-groups
configure service vprn igmp interface max-groups

Description This command configures the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

The **no** form of this command removes the value.

Parameters *max-groups* — Specifies the maximum number of groups for this interface.

Values 1 to 16000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn igmp group-interface max-groups

All

- configure service vprn igmp interface max-groups

max-groups

Syntax **max-groups** *value*
no max-groups

Context **[Tree]** (config>service>vprn>mld>if max-groups)

Full Context configure service vprn mld interface max-groups

Description This command specifies the maximum number of groups for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default 0 (no limit to the number of groups)

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 to 16000

Platforms All

max-groups

Syntax **max-groups** *value*
no max-groups

Context **[Tree]** (config>service>vprn>pim>if max-groups)

Full Context configure service vprn pim interface max-groups

Description This command configures the maximum number of groups for which PIM can have downstream state based on received PIM Joins on this interface. This does not include IGMP local receivers on the interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. When this object has a value of 0, there is no limit to the number of groups.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 to 16000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-groups

Syntax **max-groups** *value*
no max-groups

Context **[Tree]** (config>router>igmp>group-interface max-groups)
[Tree] (config>router>igmp>if max-groups)

Full Context configure router igmp group-interface max-groups
configure router igmp interface max-groups

Description This command specifies the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. This command is applicable for IPv4 and IPv6.

The **no** form of the command sets no limit to the number of groups.

Default no max-groups

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 to 16000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface max-groups

All

- configure router igmp interface max-groups

max-groups

Syntax **max-groups** [*1..16000*]
no max-groups

Context **[Tree]** (config>router>mld>group-interface max-groups)
[Tree] (config>router>mld>if max-groups)

Full Context configure router mld group-interface max-groups
configure router mld interface max-groups

Description This command specifies the maximum number of groups for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. New groups are not allowed.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default max-groups 0 (no limit to the number of groups)

Parameters *1..16000* — Specifies the maximum number of groups for this interface.

Values 1 to 16000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router mld group-interface max-groups

All

- configure router mld interface max-groups

max-groups

Syntax **max-groups** [*value*]
no max-groups

Context **[Tree]** (config>router>pim>interface max-groups)

Full Context configure router pim interface max-groups

Description This command specifies the maximum number of groups for which PIM can have local receiver information based on received PIM reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. This command is applicable for IPv4 and IPv6.

The **no** form of this command sets no limit to the number of groups.

Default no max-groups

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 to 16000

Platforms All

17.95 max-grp-sources

max-grp-sources

Syntax **max-grp-sources** *max-group-sources*
no max-grp-sources

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>igmp>grp-if max-grp-sources)
[Tree] (config>service>vprn>igmp>if max-grp-sources)
[Tree] (config>service>vprn>mld>interface max-grp-sources)

Full Context configure service vprn igmp group-interface max-grp-sources
configure service vprn igmp interface max-grp-sources
configure service vprn mld interface max-grp-sources

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed.

The **no** form of this command reverts to the default.

Default max-grp-sources 0

Parameters *max-grp-sources* — Specifies the maximum number of group source.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface max-grp-sources

All

- configure service vprn mld interface max-grp-sources
- configure service vprn igmp interface max-grp-sources

max-grp-sources

Syntax **max-grp-sources** *value*
no max-grp-sources

Context [Tree] (config>router>igmp>group-interface max-grp-sources)
[Tree] (config>router>igmp>if max-grp-sources)

Full Context configure router igmp group-interface max-grp-sources
configure router igmp interface max-grp-sources

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed.

The **no** form of the command reverts to the default.

Default no max-grp-sources

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the maximum number of group sources.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface max-grp-sources

All

- configure router igmp interface max-grp-sources

max-grp-sources

Syntax **max-grp-sources** [*1..32000*]
no max-grp-sources

Context **[Tree]** (config>router>mld>group-interface max-grp-sources)
[Tree] (config>router>mld>if max-grp-sources)

Full Context configure router mld group-interface max-grp-sources
configure router mld interface max-grp-sources

Description This command configures the maximum number of group sources for which MLD can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed.

The **no** form of this command reverts to the default.

Default max-grp-sources 0 (no limit to the number of sources)

Parameters *1 .. 32000* — Specifies the maximum number of group source.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router mld group-interface max-grp-sources

All

- configure router mld interface max-grp-sources

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.96 max-held-sessions

max-held-sessions

Syntax **max-held-sessions** *max-held-sessions*
no max-held-sessions

Context **[Tree]** (config>subscr-mgmt>gtp max-held-sessions)

Full Context configure subscriber-mgmt gtp max-held-sessions

Description This command configures the maximum number of GTP sessions to be held while their UE is disconnected.

The **no** form of this command reverts to the default.

Default max-held-sessions 2000

Parameters *max-held-sessions* — Specifies the maximum number of GTP sessions.

Values 0 to 500000

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.97 max-history-esp-key-records

max-history-esp-key-records

Syntax **max-history-esp-key-records** *max-records*
no max-history-esp-key-records

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel max-history-esp-key-records)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel max-history-esp-key-records)
[Tree] (config>service>ies>if>sap>ipsec-gw max-history-esp-key-records)
[Tree] (config>service>vprn>if>sap>ipsec-gw max-history-esp-key-records)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel max-history-esp-key-records)
[Tree] (config>router>if>ipsec>ipsec-tunnel max-history-esp-key-records)
[Tree] (config>ipsec>trans-mode-prof max-history-esp-key-records)

Full Context configure ipsec ipsec-transport-mode-profile max-history-esp-key-records
configure router interface ipsec ipsec-tunnel max-history-esp-key-records
configure service ies interface ipsec ipsec-tunnel max-history-esp-key-records
configure service ies interface sap ipsec-gw max-history-esp-key-records
configure service vprn interface ipsec ipsec-tunnel max-history-esp-key-records
configure service vprn interface sap ipsec-gw max-history-esp-key-records

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ipsec-tunnel max-history-esp-key-records

Description This command enables the system to keep records of CHILD-SA keys. There is a system wide limit of maximum number of IPsec tunnels that save keys. If the number of tunnel exceeds that limit, the system does not save keys for the new tunnels. Contact Nokia support for details of the limitation.

This command is ignored if the **config>ipsec>no show-ipsec-keys** command is configured.

The **no** form of this command prevents the system from keeping records.

Default no max-history-esp-key-records

Parameters *max-records* — Specifies the maximum number of recent records.

Values 1 to 48

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec ipsec-transport-mode-profile max-history-esp-key-records
- configure service ies interface sap ipsec-gw max-history-esp-key-records
- configure service vprn interface sap ipsec-gw max-history-esp-key-records
- configure service vprn interface sap ipsec-tunnel max-history-esp-key-records

VSR

- configure service ies interface ipsec ipsec-tunnel max-history-esp-key-records
- configure router interface ipsec ipsec-tunnel max-history-esp-key-records
- configure service vprn interface ipsec ipsec-tunnel max-history-esp-key-records

17.98 max-history-ike-key-records

max-history-ike-key-records

Syntax **max-history-ike-key-records** *max-records*
no max-history-ike-key-records

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel max-history-ike-key-records)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel max-history-ike-key-records)
[Tree] (config>service>ies>if>sap>ipsec-gw max-history-ike-key-records)
[Tree] (config>service>vprn>if>sap>ipsec-gw max-history-ike-key-records)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel max-history-ike-key-records)
[Tree] (config>router>if>ipsec>ipsec-tunnel>manual-keying max-history-ike-key-records)
[Tree] (config>ipsec>trans-mode-prof max-history-ike-key-records)

Full Context configure ipsec ipsec-transport-mode-profile max-history-ike-key-records

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router interface ipsec ipsec-tunnel manual-keying max-history-ike-key-records
configure service ies interface ipsec ipsec-tunnel max-history-ike-key-records
configure service ies interface sap ipsec-gw max-history-ike-key-records
configure service vprn interface ipsec ipsec-tunnel max-history-ike-key-records
configure service vprn interface sap ipsec-gw max-history-ike-key-records
configure service vprn interface sap ipsec-tunnel max-history-ike-key-records

Description This command enables the system to keep records of IKE-SA keys for the corresponding **ipsec-gw**, **ipsec-tunnel**, or **ipsec-transport-mode-profile**.

This command is ignored if the **config>ipsec>no show-ipsec-keys** command is enabled. There is a system-wide limit for the maximum number of IPsec tunnels that save keys. If the number of tunnels exceeds that limit, the system does not save keys for the new tunnels. Contact Nokia support for details of the limitation.

The **no** form of this command prevents the system from keeping records.

Default no max-history-ike-key-records

Parameters *max-records* — Specifies the maximum number of recent records.

Values 1 to 3

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ipsec-gw max-history-ike-key-records
- configure ipsec ipsec-transport-mode-profile max-history-ike-key-records
- configure service vprn interface sap ipsec-tunnel max-history-ike-key-records
- configure service vprn interface sap ipsec-gw max-history-ike-key-records

VSR

- configure service ies interface ipsec ipsec-tunnel max-history-ike-key-records
- configure service vprn interface ipsec ipsec-tunnel max-history-ike-key-records

17.99 max-igmp-latency

max-igmp-latency

Syntax **max-igmp-latency** *milli-seconds*

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if max-igmp-latency)

Full Context configure mcast-management multicast-info-policy video-policy video-interface max-igmp-latency

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description After the subscriber requests a fast channel change using RTCP, the video ISA bursts the video content as unicast to the subscriber. When the unicasted content has caught up to the multicast, the video ISA sends a notification message using RTCP to the subscriber to switch over to multicast with an IGMP request. When the notification message from the video ISA is sent, the **max-igmp-latency** timer starts. The video ISA continues to send unicast video until the **max-igmp-latency** expires or until the subscriber, using RTCP, informs the video ISA of the exact sequence number to stop (whichever occurs first). The **max-igmp-latency** is the maximum delay that the multicast router takes to respond and deliver the multicast upon the subscriber IGMP request.

Parameters *milli-seconds* — The maximum delay in milli-seconds.

Values 10 to 1000

Default 100

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

17.100 max-lanext-bd

max-lanext-bd

Syntax **max-lanext-bd** [*value*]
no max-lanext-bd

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw max-lanext-bd)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw max-lanext-bd)

Full Context configure service ies subscriber-interface group-interface wlan-gw max-lanext-bd
configure service vprn subscriber-interface group-interface wlan-gw max-lanext-bd

Description This command specifies the maximum number of HLE BDs for this group interface.

The **no** form of this command disables HLE for the group interface.

Parameters *value* — Specifies the maximum number of Bridged Domains for this interface.

Values 1 to 131071

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.101 max-lease-time

max-lease-time

Syntax **max-lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no max-lease-time

Context **[Tree]** (config>router>dhcp>server>pool max-lease-time)

Full Context configure router dhcp local-dhcp-server pool max-lease-time

Description This command configures the maximum lease time.

The **no** form of this command reverts to the default.

Default max-lease-time days 10

Parameters *max-lease-time* — Specifies the maximum lease time.

Values

days	0 to 3650
hours	0 to 23
minutes	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.102 max-lifetime

max-lifetime

Syntax **max-lifetime** *hours*
no max-lifetime

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>ccrt-replay max-lifetime)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy>ccrt-replay max-lifetime)

Full Context configure subscriber-mgmt diameter-application-policy gx ccrt-replay max-lifetime
configure subscriber-mgmt diameter-application-policy gy ccrt-replay max-lifetime

Description This command specifies the maximum period of time that CCR-T messages for Diameter Gx or Gy sessions that belong to the Diameter application policy are replayed.

The **no** form of this command resets the maximum lifetime to the default value setting.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default max-lifetime 24

Parameters *hours* — Specifies the maximum lifetime after which the CCR-T messages are no longer replayed.

Values 1 to 24

Default 24

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.103 max-links

max-links

Syntax **max-links** *max-links*
no max-links

Context **[Tree]** (config>router>l2tp>group>mlppp max-links)
[Tree] (config>router>l2tp>group>tunnel>mlppp max-links)
[Tree] (config>service>vprn>l2tp>group>mlppp max-links)
[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp max-links)

Full Context configure router l2tp group mlppp max-links
configure router l2tp group tunnel mlppp max-links
configure service vprn l2tp group mlppp max-links
configure service vprn l2tp group tunnel mlppp max-links

Description This command is applicable only to LNS. It determines the maximum number of links that can be put in a bundle.

Any attempt of a session to join a bundle that is above the max-link limit will be rejected.

If interleaving is configured, it is recommended that max-links be set to 1 or a version of the command is used (no max-links). Both have the same effect.

The configuration under the tunnel hierarchy will override the configuration under the group hierarchy.

The **no** form of this command limits the number of links in the bundle to 1.

Default no max-links

Parameters *max-links* — Specifies the maximum number of links in a bundle.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.104 max-list-length

max-list-length

Syntax **max-list-length unlimited**
max-list-length *count*
no max-list-length

Context **[Tree]** (config>router>l2tp>tunnel-sel max-list-length)
[Tree] (config>service>vprn>l2tp>tunnel-sel max-list-length)

Full Context configure router l2tp tunnel-selection-blacklist max-list-length
configure service vprn l2tp tunnel-selection-blacklist max-list-length

Description This command specifies the number of tunnels or peers that can be in the **tunnel-selection-blacklist**. If a tunnel or peer needs to be added to the denylist and the denylist is full, the system removes the item (tunnel or peer) from the denylist that was in this denylist for the longest time.

The **no** form of this command reverts to the default.

Default max-list-length unlimited

Parameters **unlimited** — Specifies there is no limit.

count — Specifies how many items (tunnels or peers) can be in the denylist.

Values 1 to 65635

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.105 max-lockout-hosts

max-lockout-hosts

Syntax **max-lockout-hosts** *hosts*
no max-lockout-hosts

Context **[Tree]** (config>subscr-mgmt>host-lockout-plcy max-lockout-hosts)

Full Context configure subscriber-mgmt host-lockout-policy max-lockout-hosts

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When a client enters lockout, authentication and ESM host creation is suppressed. A lightweight context maintains the lockout state and the timeouts for the client in lockout. This command allows the number of lockout contexts to be configured per SAP. If the number of existing contexts reaches the configured count, incoming hosts that fail authentication or creation are not subject to lockout, and are retried as normal.

The **no** form of this command reverts to the default value.

Default max-lockout-hosts 100

Parameters *hosts* — Specifies the maximum number of lockout host.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.106 max-mac

max-mac

Syntax **max-mac** [*value*]
no max-mac

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>access max-mac)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>access max-mac)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access max-mac
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access max-mac

Description This command specifies the maximum number of allowed MAC addresses on the access side of HLE.

The **no** form of this command reverts to the default.

Default max-mac 20

Parameters *value* — Specifies the maximum number of MAC entries in bridged domains.

Values 1 to 128

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-mac

Syntax **max-mac** [*value*]
no max-mac

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>xconnect max-mac)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>xconnect max-mac)

Full Context configure service ies subscriber-interface group-interface wlan-gw ranges range vrgw lanext xconnect max-mac
configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext xconnect max-mac

Description This command specifies the maximum number of allowed MAC in the bridge domain.

The **no** form of this command reverts to the default.

Default max-mac 20

Parameters *value* — Specifies the maximum number of MAC entries in bridged domains.

Values 1 to 128

max-mac

Syntax **max-mac** [*value*]
no max-mac

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network max-mac)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network max-mac)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext network max-mac
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext network max-mac

Description This command specifies the maximum number of allowed VM MAC addresses on the access side of HLE.

The **no** form of this command reverts to the default.

Default max-mac 20

Parameters *value* — Specifies the maximum number of VM MAC entries in bridged domains.

Values 1 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.107 max-msg-count

max-msg-count

Syntax **max-msg-count** *count*

Context **[Tree]** (config>system>telemetry>notification-bundling max-msg-count)

Full Context configure system telemetry notification-bundling max-msg-count

Description This command sets the maximum number of notifications that can be bundled in a single telemetry message.

The **no** form of this command returns the message count to the default value.

Default max-msg-count 100

Parameters *count* — Specifies the maximum of notifications that can be bundled in a single telemetry message.

Values 2 to 1000

Platforms All

17.108 max-msg-size

max-msg-size

Syntax **max-msg-size** *number*
no max-msg-size

Context **[Tree]** (config>system>grpc max-msg-size)

Full Context configure system grpc max-msg-size

Description This command configures the maximum rx message size that can be received.

The **no** form of this command reverts to the default.

Default max-msg-size 512

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the message size, in MB.

Values 1 to 1024

Default 512

Platforms All

17.109 max-nbr-mac-addr

max-nbr-mac-addr

Syntax **max-nbr-mac-addr** *table-size*
no max-nbr-mac-addr

Context **[Tree]** (config>service>template>vpls-sap-template max-nbr-mac-addr)
[Tree] (config>service>vpls>endpoint max-nbr-mac-addr)
[Tree] (config>service>vpls>sap max-nbr-mac-addr)
[Tree] (config>service>vpls>spoke-sdp max-nbr-mac-addr)
[Tree] (config>service>vpls>vxlan max-nbr-mac-addr)

Full Context configure service template vpls-sap-template max-nbr-mac-addr
configure service vpls endpoint max-nbr-mac-addr
configure service vpls sap max-nbr-mac-addr
configure service vpls spoke-sdp max-nbr-mac-addr
configure service vpls vxlan max-nbr-mac-addr

Description This command specifies the maximum number of FDB entries for both learned and static MAC addresses for this SAP, spoke-SDP, endpoint, or VXLAN instance.

When the configured limit is reached, and **discard-unknown-source** is enabled for this SAP, spoke-SDP, or static VXLAN instance (see **config>service>vpls>sap discard-unknown-source** or **config>service>vpls>spoke-sdp discard-unknown-source**), then packets with unknown source MAC addresses are discarded.

The **no** form of the command restores the global MAC learning limitations for the SAP or spoke-SDP, or VXLAN instance.

Default no max-nbr-mac-addr

Parameters *table-size* — Specifies the maximum number of learned and static entries allowed in the FDB of this service.

Values 1 to 511999 for the 7750 SR
1 to 131071 for the 7450 ESS

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls vxlan max-nbr-mac-addr

All

- configure service vpls spoke-sdp max-nbr-mac-addr
- configure service vpls sap max-nbr-mac-addr
- configure service template vpls-sap-template max-nbr-mac-addr
- configure service vpls endpoint max-nbr-mac-addr

max-nbr-mac-addr

Syntax **max-nbr-mac-addr** *table-size*
no max-nbr-mac-addr

Context **[Tree]** (config>service>pw-template max-nbr-mac-addr)

Full Context configure service pw-template max-nbr-mac-addr

Description This command specifies the maximum number of FDB entries for both learned and static MAC addresses for this SAP or spoke SDP.

When the configured limit has been reached, and **discard-unknown-source** has been enabled for this SAP or spoke SDP (see **config>service>vpls>sap discard-unknown-source** or **config>service>vpls>spoke-sdp discard-unknown-source**), packets with unknown source MAC addresses will be discarded.

The **no** form of the command restores the global MAC learning limitations for the SAP or spoke SDP.

Default no max-nbr-mac-addr

Parameters *table-size* — Specifies the maximum number of learned and static entries allowed in the FDB of this service.

Values 1 to 511999

Platforms All

17.110 max-nbr-of-leases

max-nbr-of-leases

Syntax **max-nbr-of-leases** *max-nbr-of-leases*
no max-nbr-of-leases

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>ipv6>dhcp6-server max-nbr-of-leases)

Full Context configure service ies interface ipv6 dhcp6-server max-nbr-of-leases

Description This command configures the maximum number of lease states installed by the DHCPv6 server function allowed on this interface.

The **no** form of this command returns the value to the default.

Default max-nbr-of-leases 8000

Parameters *max-nbr-of-leases* — Specifies the maximum number of lease states installed by the DHCPv6 server function allowed on this interface.

Values 0 to 8000

Platforms All

17.111 max-num-groups

max-num-groups

Syntax **max-num-groups** *count*
no max-num-groups

Context [Tree] (config>service>vpls>sap>igmp-snooping max-num-groups)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping max-num-groups)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping max-num-groups)
[Tree] (config>service>vpls>sap>mld-snooping max-num-groups)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping max-num-groups)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping max-num-groups)

Full Context configure service vpls mesh-sdp igmp-snooping max-num-groups
configure service vpls mesh-sdp mld-snooping max-num-groups
configure service vpls sap igmp-snooping max-num-groups
configure service vpls sap mld-snooping max-num-groups
configure service vpls spoke-sdp igmp-snooping max-num-groups
configure service vpls spoke-sdp mld-snooping max-num-groups

Description This command defines the maximum number of multicast groups that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

The **no** form of this command reverts to the default value.

Default no max-num-groups

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the maximum number of groups that can be joined on this SAP or SDP.

Values 1 to 1000

Platforms All

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>igmp-trk max-num-groups)

Full Context configure service ies subscriber-interface group-interface sap igmp-host-tracking max-num-groups

Description This command configures the maximum number of multicast groups allowed to be tracked.

The **no** form of this command disables the check.

Default no max-num-groups

Parameters *max-num-groups* — Specifies the maximum number of multicast groups allowed to be tracked.

Values 1 to 196607

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>subscr-mgmt>igmp-policy max-num-groups)

Full Context configure subscriber-mgmt igmp-policy max-num-groups

Description This command configures the maximum number of multicast groups.

The **no** form of this command reverts to the default value.

Parameters *max-num-groups* — Specifies the maximum number of multicast groups.

Values 0 to 16000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-trk max-num-groups)

Full Context configure service vprn subscriber-interface group-interface sap igmp-host-tracking max-num-groups

Description This command configures the maximum number of multicast groups allowed to be tracked.

The **no** form of this command removes the values from the configuration.

Default no max-num-groups

Parameters *max-num-groups* — Specifies the maximum number of multicast groups allowed to be tracked.

Values 1 to 196607

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>subscr-mgmt>msap-policy>igmp-host-tracking max-num-groups)

Full Context configure subscriber-mgmt msap-policy igmp-host-tracking max-num-groups

Description This command configures the maximum number of multicast groups allowed to be tracked.

The **no** form of this command removes the values from the configuration.

Parameters *max-num-groups* — Specifies the maximum number of multicast groups allowed to be tracked.

Values 1 to 196607

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp max-num-groups)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping max-num-groups

Description This command configures the maximum number of multicast groups that can be joined on an MSAP or SDP. If the router receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

Parameters *max-num-groups* — Specifies the maximum number of groups that can be joined on an MSAP or SDP.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-groups

Syntax **max-num-groups** *count*
no max-num-groups

Context **[Tree]** (config>subscr-mgmt>mld-policy max-num-groups)

Full Context configure subscriber-mgmt mld-policy max-num-groups

Description This command defines the maximum number of multicast groups that can be joined. If the router receives a join message that would exceed the configured number of groups, the request is ignored.

The **no** form of this command reverts to the default.

Parameters *count* — Specifies the maximum number of groups that can be joined.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-snooping max-num-groups)

Full Context configure service vprn subscriber-interface group-interface sap igmp-snooping max-num-groups

Description This command configures the maximum number of multicast groups allowed to be tracked.

The **no** form of this command removes the values from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *max-num-groups* — Specifies the maximum number of multicast groups allowed to be tracked.

Values 1 to 196607

max-num-groups

Syntax **max-num-groups** *max-num-groups*
no max-num-groups

Context **[Tree]** (config>service>vpls>sap>igmp-host-tracking max-num-groups)

Full Context configure service vpls sap igmp-host-tracking max-num-groups

Description This command configures the maximum number of multicast groups allowed to be tracked.

The **no** form of this command removes the values from the configuration.

Default no max-num-groups

Parameters *max-num-groups* — Specifies the maximum number of multicast groups allowed to be tracked

Values 1 to 196607

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-groups

Syntax **max-num-groups** *num-groups*
no max-num-groups

Context **[Tree]** (config>service>vpls>spoke-sdp>pim-snooping max-num-groups)
[Tree] (config>service>vpls>sap>pim-snooping max-num-groups)

Full Context configure service vpls sap pim-snooping max-num-groups
configure service vpls spoke-sdp pim-snooping max-num-groups

Description This command configures the maximum groups for PIM snooping.

Parameters *num-groups* — Specifies the maximum groups for PIM snooping

Values 1 to 16000

Platforms All

max-num-groups

Syntax **max-num-groups** *count*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no max-num-groups

Context **[Tree]** (config>service>pw-template>igmp-snooping max-num-groups)

Full Context configure service pw-template igmp-snooping max-num-groups

Description This command defines the maximum number of multicast groups that can be joined. If the router receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

Default no max-num-groups

Parameters *count* — Specifies the maximum number of groups that can be joined.

Values 1 to 1000

Platforms All

17.112 max-num-grp-sources

max-num-grp-sources

Syntax **max-num-grp-sources** [*max-num-grp-sources*]
no max-num-grp-sources

Context **[Tree]** (config>subscr-mgmt>igmp-policy max-num-grp-sources)

Full Context configure subscriber-mgmt igmp-policy max-num-grp-sources

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed. When this object has a value of 0, there is no limit to the number of group sources.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-grp-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-num-grp-sources

Syntax **max-num-grp-sources** [*max-num-grp-sources*]
no max-num-grp-sources

Context **[Tree]** (config>subscr-mgmt>msap-policy>igmp-trk max-num-grp-sources)

Full Context configure subscriber-mgmt msap-policy igmp-host-tracking max-num-grp-sources

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed. When this object has a value of 0, there is no limit to the number of group sources.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-grp-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-grp-sources

Syntax **max-num-grp-sources** [*max-num-grp-sources*]
no max-num-grp-sources

Context **[Tree]** (config>subscr-mgmt>mld-policy max-num-grp-sources)

Full Context configure subscriber-mgmt mld-policy max-num-grp-sources

Description This command configures the maximum number of group sources for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources are not allowed. When this object has a value of 0, there is no limit to the number of group sources.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-grp-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-num-grp-sources

Syntax [**no**] **max-num-grp-sources** [*number*]

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-snooping max-num-grp-sources)

Full Context configure service vprn subscriber-interface group-interface sap igmp-snooping max-num-grp-sources

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources are not allowed. When this object has a value of 0, there is no limit to the number of group sources.

The **no** form of this command removes the value from the configuration.

Parameters *number* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 32000

max-num-grp-sources

Syntax **max-num-grp-sources** [1 to 32000]
no max-num-grp-sources

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping max-num-grp-sources)
[Tree] (config>service>vpls>sap>igmp-host-tracking max-num-grp-sources)
[Tree] (config>service>vpls>sap>igmp-snooping max-num-grp-sources)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping max-num-grp-sources)

Full Context configure service vpls mesh-sdp igmp-snooping max-num-grp-sources
configure service vpls sap igmp-host-tracking max-num-grp-sources
configure service vpls sap igmp-snooping max-num-grp-sources
configure service vpls spoke-sdp igmp-snooping max-num-grp-sources

Description This command defines the maximum number of multicast SGs that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of SGs, the request is ignored.

The **no** form of this command disables the check.

Default no max-num-grp-sources

Parameters **1 to 32000** — Specifies the maximum number of multicast sources allowed to be tracked per group

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls sap igmp-host-tracking max-num-grp-sources

All

- configure service vpls mesh-sdp igmp-snooping max-num-grp-sources
- configure service vpls spoke-sdp igmp-snooping max-num-grp-sources
- configure service vpls sap igmp-snooping max-num-grp-sources

max-num-grp-sources

Syntax **max-num-grp-sources** *max-num-sources*
no max-num-grp-sources

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>igmp-host-tracking max-num-grp-sources)

Full Context configure service ies subscriber-interface group-interface sap igmp-host-tracking max-num-grp-sources

Description This command configures the max number of multicast (S,G)s allowed to be tracked.

The **no** form of this command disables the check.

Default no max-num-grp-sources

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 32000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.113 max-num-sources

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context **[Tree]** (config>subscr-mgmt>igmp-policy max-num-sources)

Full Context configure subscriber-mgmt igmp-policy max-num-sources

Description This command configures the maximum number of multicast sources.

The **no** form of this command disables the command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *max-num-sources* — Specifies the maximum number of multicast sources.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context **[Tree]** (config>subscr-mgmt>msap-policy>igmp-host-tracking max-num-sources)

Full Context configure subscriber-mgmt msap-policy igmp-host-tracking max-num-sources

Description This command configures the maximum number of multicast sources allowed to be tracked per group.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context **[Tree]** (config>subscr-mgmt>mld-policy max-num-sources)

Full Context configure subscriber-mgmt mld-policy max-num-sources

Description This command configures the maximum number of multicast sources allowed per group.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed per group.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>igmp-snooping max-num-sources)

Full Context configure service vprn subscriber-interface group-interface sap igmp-snooping max-num-sources

Description This command configures the maximum number of multicast sources allowed to be tracked per group.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 1000

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping max-num-sources)
[Tree] (config>service>vpls>sap>igmp-host-tracking max-num-sources)
[Tree] (config>service>vpls>sap>igmp-snooping max-num-sources)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping max-num-sources)

Full Context configure service vpls mesh-sdp igmp-snooping max-num-sources
configure service vpls sap igmp-host-tracking max-num-sources
configure service vpls sap igmp-snooping max-num-sources
configure service vpls spoke-sdp igmp-snooping max-num-sources

Description This command defines the maximum number of multicast sources that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of sources, the request is ignored.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed per group

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vpls sap igmp-host-tracking max-num-sources

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls mesh-sdp igmp-snooping max-num-sources
- configure service vpls spoke-sdp igmp-snooping max-num-sources
- configure service vpls sap igmp-snooping max-num-sources

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>igmp-host-tracking max-num-sources)

Full Context configure service ies subscriber-interface group-interface sap igmp-host-tracking max-num-sources

Description This command configures the maximum number of multicast sources allowed to be tracked per group.

The **no** form of this command removes the value from the configuration.

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed to be tracked per group.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.114 max-num-ue

max-num-ue

Syntax **max-num-ue** *maximum*

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query max-num-ue)

Full Context configure subscriber-mgmt wlan-gw tunnel-query max-num-ue

Description This command enables matching only on tunnels that have, at most, the specified number of UEs connected.

Default max-num-ue 4294967295

Parameters *maximum* — Specifies the maximum number of UEs.

Values 0 to 4294967295

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.115 max-path

max-path

Syntax **max-path** *max-paths*
no max-path

Context **[Tree]** (config>test-oam>ldp-treetrace>path-discovery max-path)

Full Context configure test-oam ldp-treetrace path-discovery max-path

Description This command configures the maximum number of ECMP paths the path discovery attempts to discover for each run every **interval** minute.

The **no** form of this command resets the time out to its default value.

Default no max-path

Parameters *max-paths* — Specifies the tree discovery maximum path.

Values 1 to 128

Platforms All

17.116 max-payload-length

max-payload-length

Syntax **max-payload-length direction** *direction* [**create**]
no max-payload-length direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter max-payload-length)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter max-payload-length

Description This command configures a TCA for the counter capturing drops due to the GTP filter maximum payload length. A maximum payload length drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a maximum payload length drop TCA.

Default none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

max-payload-length

Syntax **max-payload-length** *bytes*
no max-payload-length

Context **[Tree]** (config>app-assure>group>gtp>gtp-filter max-payload-length)

Full Context configure application-assurance group gtp gtp-filter max-payload-length

Description This command specifies the maximum allowed GTP payload size.

The **no** form of this command removes this GTP message length filter.

Default no max-payload-length

Parameters *bytes* — Specifies the packet length in bytes.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.117 max-peer

max-peer

Syntax **max-peer** *max-peer*
no max-peer

Context **[Tree]** (config>port>ethernet>dot1x>macsec>sub-port max-peer)

Full Context configure port ethernet dot1x macsec sub-port max-peer

Description This command configures the max peer allowed under this MACsec instance.

Note: The peer establishment is a race condition and first come first serve. On any security zone, only 32 peers can be supported. See SA Exhaustion Behavior for more details.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the value to the default.

Default no max-peer

Parameters *max-peer* — The maximum number of peers supported on this port.

Values 0 to 32

Platforms All

17.118 max-percent-rate

max-percent-rate

Syntax **max-percent-rate** *percentage* [**local-limit** | **reference-port-limit**]
no max-percent-rate

Context **[Tree]** (config>qos>plcr-ctrl-plcy>root max-percent-rate)

Full Context configure qos policer-control-policy root max-percent-rate

Description This command configures the maximum percentage rate for the policer control policy.

The **no** form of this command removes the configuration.

Parameters *percentage* — Specifies the percentage.

Values 0.01 to 100.00

local-limit — Keyword used to specify the local limit.

reference-port-limit — Keyword used to specify the reference port limit.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

17.119 max-prob

max-prob

Syntax **max-prob** *percent*
no max-prob

Context **[Tree]** (config>qos>slope-policy>exceed-slope max-prob)
[Tree] (config>qos>slope-policy>highplus-slope max-prob)
[Tree] (config>qos>slope-policy>high-slope max-prob)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>qos>slope-policy>low-slope max-prob)

Full Context configure qos slope-policy exceed-slope max-prob
configure qos slope-policy high-slope max-prob
configure qos slope-policy highplus-slope max-prob
configure qos slope-policy low-slope max-prob

Description Sets the exceed, low, high, or highplus Random Early Detection (RED) slope position for the maximum non-one packet discard probability value before the packet discard probability rises directly to one. The percent parameter is expressed as a percentage of packet discard probability where always discard is a probability of 1. A **max-prob** value of 80 represents 80% of 1, or a packet discard probability of 0.8.

The **no** form of this command restores the **max-prob** value to the default setting.

Default max-prob 80

Parameters *percent* — The maximum drop probability percentage corresponding to the **max-avg,** expressed as a decimal integer.

Values 0 to 100

Platforms All

17.120 max-queue-size

max-queue-size

Syntax **max-queue-size** *queue-size*
no max-queue-size

Context [Tree] (config>qos>mlppp-profile-egress>class max-queue-size)

Full Context configure qos mlppp-profile-egress class max-queue-size

Description This command configures the maximum queue size for each MLPPP class queue for this profile.

Parameters *queue-size* — Specifies the maximum queue size in ms of buffer space.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

max-queue-size

Syntax **max-queue-size** *queue-size*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no max-queue-size

Context [Tree] (config>qos>mc-fr-profile-egress>class max-queue-size)

Full Context configure qos mc-fr-profile-egress class max-queue-size

Description This command configures the maximum size for each Frame Relay scheduling class queue for this profile.

Default max-queue-size 10 — class 0

max-queue-size 50 — class 1

max-queue-size 150 — class 2

max-queue-size 750 — class 3

Parameters *queue-size* — Specifies the number, in ms, of the available link or bundle rate.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.121 max-rate

max-rate

Syntax **max-rate percent** *percent-rate*
max-rate *pir-rate*
no max-rate

Context [Tree] (config>qos>hw-agg-shap-sched-plcy max-rate)

Full Context configure qos hw-agg-shaper-scheduler-policy max-rate

Description This command configures the maximum frame-based rate of the hardware aggregate shaper scheduler policy expressed as a percentage of the port rate or as the PIR rate.

The **no** form of this command removes the rate from the configuration.

Parameters *percent-rate* — Specifies the percentage rate.

Values 0.01 to 100.00

pir-rate — Specifies the PIR rate in kb/s.

Values 1 to 6400000000, max

Platforms 7750 SR-1, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-rate

Syntax **max-rate** {*rate* | **max**}
no max-rate

Context **[Tree]** (config>subscr-mgmt>sub-prof>ingress>policer-control-policy max-rate)
[Tree] (config>subscr-mgmt>sub-prof>egress>policer-control-policy max-rate)

Full Context configure subscriber-mgmt sub-profile egress policer-control-policy max-rate
configure subscriber-mgmt sub-profile ingress policer-control-policy max-rate

Description The **max-rate** command defines the parent policer's PIR leaky bucket's decrement rate. A parent policer is created for each time the policer-control-policy is applied to either a SAP or subscriber instance. Packets that are not discarded by the child policers associated with the SAP or subscriber instance are evaluated against the parent policer's PIR leaky bucket.

For each packet, the bucket is first decremented by the correct amount based on the decrement rate to derive the current bucket depth. The current depth is then compared to one of two discard thresholds associated with the packet. The first discard threshold (discard-unfair) is applied if the FIR (Fair Information Rate) leaky bucket in the packet's child policer is in the confirming state. The second discard threshold (discard-all) is applied if the child policer's FIR leaky bucket is in the exceed state. Only one of the two thresholds is applied per packet. If the current depth of the parent policer PIR bucket is less than the threshold value, the parent PIR bucket is in the conform state for that particular packet. If the depth is equal to or greater than the applied threshold, the bucket is in the violate state for the packet.

If the result is "conform," the bucket depth is increased by the size of the packet (plus or minus the per-packet-offset setting in the child policer) and the packet is not discarded by the parent policer. If the result is "violate," the bucket depth is not increased and the packet is discarded by the parent policer. When the parent policer discards a packet, any bucket depth increases (PIR, CIR and FIR) in the parent policer caused by the packet are canceled. This prevents packets that are discarded by the parent policer from consuming the child policers PIR, CIR and FIR bandwidth.

The **policer-control-policy root max-rate** setting may be overridden on each SAP or sub-profile where the policy is applied.

The **no** form of this command reverts to the default.

Default max-rate max

Parameters *rate* — Specifies the max rate in kilobits per second. Defining the *rate* value is mutually exclusive with the **max** parameter. The *rate* (in kilobits per second) value must be defined as an integer that represents the number of kilobytes that the parent policer is decremented per second. The actual decrement is performed per packet based on the time that has elapsed since the last packet associated with the parent policer.

Values 0 to 2000000000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max — Specifies the maximum frame-based bandwidth limit of this policer. The **max** parameter is mutually exclusive with defining a *rate* (in kilobits per second) value. When max is specified, the parent policer does not enforce a maximum rate on the aggregate throughput of the child policers. This is the default setting when the **policer-control-policy** is first created and is the value that the parent policer returns to when a **no max-rate** command is executed. In order for the parent policer to be effective, a *rate* (in kilobits per second) value should be specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

max-rate

Syntax **max-rate** {*rate* | **max**}
no max-rate

Context **[Tree]** (config>card>fp>ingress>acc>qgrp>policer-ctrl-over max-rate)
[Tree] (config>card>fp>ingress>network>qgrp>policer-ctrl-over max-rate)

Full Context configure card fp ingress access queue-group policer-control-override max-rate
configure card fp ingress network queue-group policer-control-override max-rate

Description This command defines the parent policer's PIR leaky bucket's decrement rate. A parent policer is created for each time the policer-control-policy is applied to either a SAP or subscriber instance. Packets that are not discarded by the child policers associated with the SAP or subscriber instance are evaluated against the parent policer's PIR leaky bucket.

For each packet, the bucket is first decremented by the correct amount based on the decrement rate to derive the current bucket depth. The current depth is then compared to one of two discard thresholds associated with the packet. The first discard threshold (discard-unfair) is applied if the FIR (Fair Information Rate) leaky bucket in the packet's child policer is in the confirming state. The second discard threshold (discard-all) is applied if the child policer's FIR leaky bucket is in the exceed state. Only one of the two thresholds is applied per packet. If the current depth of the parent policer PIR bucket is less than the threshold value, the parent PIR bucket is in the conform state for that particular packet. If the depth is equal to or greater than the applied threshold, the bucket is in the violate state for the packet.

If the result is "conform," the bucket depth is increased by the size of the packet (plus or minus the per-packet-offset setting in the child policer) and the packet is not discarded by the parent policer. If the result is "violate," the bucket depth is not increased and the packet is discarded by the parent policer. When the parent policer discards a packet, any bucket depth increases (PIR, CIR and FIR) in the parent policer caused by the packet are canceled. This prevents packets that are discarded by the parent policer from consuming the child policers PIR, CIR and FIR bandwidth.

The **policer-control-policy root max-rate** setting may be overridden on each SAP or sub-profile where the policy is applied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the policer-control-policy's parent policer maximum rate to **max**.

Default max-rate max

Parameters *rate* — Specifies that a kilobits-per-second value is mutually exclusive with the **max** keyword. The kilobits-per-second value must be defined as an integer that represents the number of kilobytes that the parent policer will be decremented per second. The actual decrement is performed per packet based on the time that has elapsed since the last packet associated with the parent policer.

Values 0 to 2000000000

max — The **max** keyword is mutually exclusive with defining a kilobits-per-second value. When max is specified, the parent policer does not enforce a maximum rate on the aggregate throughput of the child policers. This is the default setting when the **policer-control-policy** is first created and is the value that the parent policer returns to when no max-rate is executed. In order for the parent policer to be effective, a kilobits-per-second value should be specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

max-rate

Syntax **max-rate** *pir-rate*
max-rate percent *percent-rate*
no max-rate

Context **[Tree]** (config>port>ethernet>egr-scheduler-override max-rate)
[Tree] (config>port>sonet-sdh>path>egr-scheduler-override max-rate)
[Tree] (config>port>tdm>ds1>channel-group>egr-scheduler-override max-rate)
[Tree] (config>port>tdm>ds3>egr-scheduler-override max-rate)
[Tree] (config>port>tdm>e1>channel-group>egr-scheduler-override max-rate)
[Tree] (config>port>tdm>e3>egr-scheduler-override max-rate)

Full Context configure port ethernet egress-scheduler-override max-rate
configure port sonet-sdh path egress-scheduler-override max-rate
configure port tdm ds1 channel-group egress-scheduler-override max-rate
configure port tdm ds3 egress-scheduler-override max-rate
configure port tdm e1 channel-group egress-scheduler-override max-rate
configure port tdm e3 egress-scheduler-override max-rate

Description This command overrides the **max-rate** parameter found in the port-scheduler-policy associated with the port. When a max-rate is defined at the port or channel level, the port scheduler policies max-rate parameter is ignored.

The egress-scheduler-override **max-rate** command supports a parameter that allows the override command to restore the default of not having a rate limit on the port scheduler. This is helpful when the port scheduler policy has an explicit maximum rate defined and it is desirable to remove this limit at the port instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the maximum rate override from the egress port or channels port scheduler context. Once removed, the max-rate parameter from the port scheduler policy associated with the port or channel will be used by the local scheduler context.

Parameters *pir-rate* — Specifies the explicit maximum frame based bandwidth limit, in kilobits per second. This value overrides the QoS scheduler policy rate.

Values **For Ethernet:** 1 to 6400000000, **max**
For SONET-SDH and TDM: 1 to 3200000000, **max**

percent-rate — Specifies the percent rate.

Values 0.01 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path egress-scheduler-override max-rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group egress-scheduler-override max-rate
- configure port tdm e3 egress-scheduler-override max-rate
- configure port tdm ds1 channel-group egress-scheduler-override max-rate
- configure port tdm ds3 egress-scheduler-override max-rate

All

- configure port ethernet egress-scheduler-override max-rate

max-rate

Syntax **max-rate** *rate*
no max-rate

Context **[Tree]** (config>port>ethernet>egress>hs-sched-ovr max-rate)

Full Context configure port ethernet egress hs-scheduler-overrides max-rate

Description This command overrides the max-rate configured in the HS scheduler policy applied to the port egress.

The **no** form of this command removes the **max-rate** override from the port egress configuration.

Parameters *rate* — Specifies the explicit maximum frame based bandwidth limit, in megabits per second. This parameter is required when executing this command..

Values 1 to 100000, max

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-rate

Syntax **max-rate** {*rate* | **max**}

Context **[Tree]** (config>service>cpipe>sap>egress>policer-control-override max-rate)
[Tree] (config>service>cpipe>sap>ingress>policer-control-override max-rate)
[Tree] (config>service>epipe>sap>egress>policer-control-override max-rate)
[Tree] (config>service>epipe>sap>ingress>policer-control-override max-rate)
[Tree] (config>service>ipipe>sap>egress>policer-control-override max-rate)
[Tree] (config>service>ipipe>sap>ingress>policer-control-override max-rate)

Full Context configure service cpipe sap egress policer-control-override max-rate
configure service cpipe sap ingress policer-control-override max-rate
configure service epipe sap egress policer-control-override max-rate
configure service epipe sap ingress policer-control-override max-rate
configure service ipipe sap egress policer-control-override max-rate
configure service ipipe sap ingress policer-control-override max-rate

Description This command, within the SAP ingress and egress contexts, overrides the root arbiter parent policer max-rate that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy max-rate parameter have no effect on the SAP's parent policer until the override is removed using the **no max-rate** command within the SAP.

The **no** form of this command returns the policer-control-policy's parent policer maximum rate to **max**.

Parameters *rate* — Specifies the rate override in kilobits per second.

Values 1 to 6400000000

max — Specifies the maximum rate override.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress policer-control-override max-rate
- configure service cpipe sap ingress policer-control-override max-rate

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap ingress policer-control-override max-rate
- configure service epipe sap ingress policer-control-override max-rate
- configure service ipipe sap egress policer-control-override max-rate
- configure service epipe sap egress policer-control-override max-rate

max-rate

Syntax **max-rate** {*rate* | **max**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap>egress>policer-ctrl-over max-rate)
[Tree] (config>service>vpls>sap>ingress>policer-ctrl-over max-rate)

Full Context configure service vpls sap egress policer-control-override max-rate
configure service vpls sap ingress policer-control-override max-rate

Description This command, within the SAP ingress and egress contexts, overrides the root arbiter parent policer max-rate that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy max-rate parameter have no effect on the SAP's parent policer until the override is removed using the **no max-rate** command within the SAP.

The **no** form of this command removes an explicit rate value from the aggregate rate therefore returning it to its default value.

Parameters *rate* **| max** — Specifies the max rate override in kilobits per second or use the maximum

Values 1 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

max-rate

Syntax **max-rate** {*rate* | **max**}

Context [Tree] (config>service>ies>if>sap>egress>policer-ctrl-over max-rate)
[Tree] (config>service>ies>if>sap>ingress>policer-ctrl-over max-rate)

Full Context configure service ies interface sap egress policer-control-override max-rate
configure service ies interface sap ingress policer-control-override max-rate

Description This command, within the SAP ingress and egress contexts, overrides the root arbiter parent policer max-rate that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy max-rate parameter have no effect on the SAP's parent policer until the override is removed using the **no max-rate** command within the SAP.

Parameters *rate* **| max** — Specifies the rate override in kilobits per second or use the maximum override value.

Values 1 to 6400000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

max-rate

Syntax **max-rate** {*rate* | **max**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>if>sap>egress>policer-ctrl-over max-rate)
[Tree] (config>service>vprn>if>sap>ingress>policer-ctrl-over max-rate)

Full Context configure service vprn interface sap egress policer-control-override max-rate
configure service vprn interface sap ingress policer-control-override max-rate

Description This command, within the SAP ingress and egress contexts, overrides the root arbiter parent policer max-rate that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy max-rate parameter have no effect on the SAP's parent policer until the override is removed using the **no max-rate** command within the SAP.

The **no** form of this command returns the policer-control-policy's parent policer maximum rate to **max**.

Parameters *rate* **| max** — Specifies the rate override in kilobits per second or use the maximum override value.

Values 1 to 6400000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

max-rate

Syntax **max-rate** *rate*
no max-rate

Context [Tree] (config>qos>plcr-ctrl-plcy>root max-rate)

Full Context configure qos policer-control-policy root max-rate

Description The **max-rate** command defines the parent policer's PIR leaky bucket's decrement rate. A parent policer is created for each time the policer-control-policy is applied to either a SAP or subscriber instance for the 7450 ESS and 7750 SR, or multiservice site instance for the 7950 XRS. Packets that are not discarded by the child policers associated with the SAP or subscriber or multiservice site instances are evaluated against the parent policer's PIR leaky bucket.

For each packet, the bucket is first decremented by the correct amount based on the decrement rate to derive the current bucket depth. The current depth is then compared to one of two discard thresholds associated with the packet. The first discard threshold (discard-unfair) is applied if the FIR (Fair Information Rate) leaky bucket in the packet's child policer is in the confirming state. The second discard threshold (discard-all) is applied if the child policer's FIR leaky bucket is in the exceed state. Only one of the two thresholds is applied per packet. If the current depth of the parent policer PIR bucket is less than the threshold value, the parent PIR bucket is in the conform state for that particular packet. If the depth is equal to or greater than the applied threshold, the bucket is in the violate state for the packet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the result is “conform,” the bucket depth is increased by the size of the packet (plus or minus the per-packet-offset setting in the child policer) and the packet is not discarded by the parent policer. If the result is “violate,” the bucket depth is not increased and the packet is discarded by the parent policer. When the parent policer discards a packet, any bucket depth increases (PIR, CIR and FIR) in the parent policer caused by the packet are canceled. This prevents packets that are discarded by the parent policer from consuming the child policers PIR, CIR, and FIR bandwidth.

The **policer-control-policy root max-rate** setting may be overridden on each SAP or sub-profile where the policy is applied.

The **no** form of this command returns the policer-control-policy’s parent policer maximum rate to **max**.

Parameters *rate* — The kilobits-per-second value must be defined as an integer that represents the number of kilobytes that the parent policer will be decremented per second. The actual decrement is performed per packet, based on the time that has elapsed since the last packet associated with the parent policer.

Values 1 to 6400000000, **max**

max — When **max** is specified, the parent policer does not enforce a maximum rate on the aggregate throughput of the child policers. This is the default setting when the **policer-control-policy** is first created and is the value that the parent policer returns to when no max-rate is executed. In order for the parent policer to be effective, a kilobits-per-second value should be specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

max-rate

Syntax **max-rate** *rate*
no max-rate

Context **[Tree]** (config>qos>hs-scheduler-policy max-rate)

Full Context configure qos hs-scheduler-policy max-rate

Description This command defines an explicit maximum frame-based bandwidth limit for the HS scheduler policy scheduler context. If a maximum rate is defined that is smaller than the port rate, the port is rate-limited to the configured megabits per second value. This command can be executed at any time for any non-default existing HS scheduler policy.

The **no** form of the command removes an explicit rate value from the HS scheduler policy. After the explicit rate value is removed, all instances of the scheduler policy on HSQ egress ports are allowed to run at the available line rate unless the instance has a max rate override in place.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *rate* — Specifies the explicit maximum frame-based bandwidth limit, in megabits per second. This parameter is required when executing this command.

Values 1 to 100000, max

Platforms 7750 SR-7/12/12e

max-rate

Syntax **max-rate** *pir-rate*
max-rate percent *percent-rate*
no max-rate

Context **[Tree]** (config>qos>port-scheduler-policy max-rate)

Full Context configure qos port-scheduler-policy max-rate

Description This command defines an explicit maximum frame-based bandwidth limit for the port scheduler policies scheduler context. By default, when a scheduler policy is associated with a port or channel, the instance of the scheduler on the port automatically limits the bandwidth to the lesser of port or channel line rate and a possible egress-rate value (for Ethernet ports). If a max-rate is defined that is smaller than the port or channel rate, the expressed kilobits per second value is used instead. The max-rate command is another way to sub-rate the port or channel. This command can be used on channels only on the 7450 ESS and 7750 SR.

The **max-rate** command may be executed at any time for an existing port-scheduler-policy. When a new max-rate is given for a policy, the system evaluates all instances of the policy to see if the configured rate is smaller than the available port or channel bandwidth. If the rate is smaller and the maximum rate is not currently overridden on the scheduler instance, the scheduler instance is updated with the new maximum rate value.

The max-rate value defined in the policy may be overridden on each scheduler instance. If the maximum rate is explicitly defined as an override on a port or channel, the policies max-rate value has no effect.

The **no** form of this command removes an explicit rate value from the port scheduler policy. When removed, all instances of the scheduler policy on egress ports or channel are allowed to run at the available line rate unless the instance has a max-rate override in place.

Parameters *pir-rate* — Specifies the PIR rate, in kilobits per second.

Values 1 to 6400000000, **max**

percent *percent-rate* — Specifies the percent rate.

Values 0.01 to 100.00

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.122 max-retries-estab

max-retries-estab

Syntax **max-retries-estab** *max-retries*
no max-retries-estab

Context **[Tree]** (config>router>l2tp max-retries-estab)
[Tree] (config>router>l2tp>group max-retries-estab)
[Tree] (config>router>l2tp>group>tunnel max-retries-estab)
[Tree] (config>service>vprn>l2tp max-retries-estab)
[Tree] (config>service>vprn>l2tp>group max-retries-estab)
[Tree] (config>service>vprn>l2tp>group>tunnel max-retries-estab)

Full Context configure router l2tp group max-retries-estab
configure router l2tp group tunnel max-retries-estab
configure router l2tp max-retries-estab
configure service vprn l2tp group max-retries-estab
configure service vprn l2tp group tunnel max-retries-estab
configure service vprn l2tp max-retries-estab

Description This command configures the number of retries allowed for this L2TP tunnel while it is established, before its control connection goes down.

The **no** form of this command removes the value from the configuration.

Default no max-retries-estab

Parameters *max-retries* — Specifies the maximum number of retries for an established tunnel.

Default no max-retries-estab

Values 2 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.123 max-retries-not-estab

max-retries-not-estab

Syntax **max-retries-not-estab** *max-retries*
no max-retries-not-estab

Context **[Tree]** (config>router>l2tp max-retries-not-estab)
[Tree] (config>router>l2tp>group max-retries-not-estab)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>l2tp>group>tunnel max-retries-not-estab)
[Tree] (config>service>vprn>l2tp max-retries-not-estab)
[Tree] (config>service>vprn>l2tp>group max-retries-not-estab)
[Tree] (config>service>vprn>l2tp>group>tunnel max-retries-not-estab)

Full Context configure router l2tp group max-retries-not-estab
configure router l2tp group tunnel max-retries-not-estab
configure router l2tp max-retries-not-estab
configure service vprn l2tp group max-retries-not-estab
configure service vprn l2tp group tunnel max-retries-not-estab
configure service vprn l2tp max-retries-not-estab

Description This command configures the number of retries allowed for this L2TP tunnel while it is not established, before its control connection goes down.

The **no** form of this command removes the value from the configuration.

Default no max-retries-not-estab

Parameters *max-retries* — Specifies the maximum number of retries for non-established tunnels.

Default no max-retries-not-estab

Values 2 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.124 max-routes

max-routes

Syntax **max-routes** *routes*
no max-routes

Context [Tree] (config>aaa>route-downloader max-routes)

Full Context configure aaa route-downloader max-routes

Description This command determines the upper limits for total number of routes to be received and accepted by the system. The total number is inclusive of both IPv4 and IPv6 addresses and no differentiation is needed across protocols. It includes the sum of both. Once this limit is reached, the download process stops sending new access-requests until the next download-interval expires.

The **no** form of this command reverts to the default value.

Default max-routes 200000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *routes* — Specifies the maximum number of the routes imported.

Values 1 to 200000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.125 max-rx-defect-window

max-rx-defect-window

Syntax **max-rx-defect-window** *seconds*
no max-rx-defect-window

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>lag>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>port>ethernet>eth-cfm>mep>grace>eth-ed max-rx-defect-window)

Full Context configure eth-ring path eth-cfm mep grace eth-ed max-rx-defect-window
configure eth-tunnel path eth-cfm mep grace eth-ed max-rx-defect-window
configure lag eth-cfm mep grace eth-ed max-rx-defect-window
configure port ethernet eth-cfm mep grace eth-ed max-rx-defect-window

Description This command limits the duration of the received ETH-ED expected defect window to the lower value of either the received value from the peer or this parameter.

The **no** form of this command removes the limitation, and any valid defect window value received from a peer MEP in the ETH-ED PDU will be used.

Default no max-rx-defect-window

Parameters *seconds* — Specifies the duration, in seconds, of the maximum expected defect window.

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

max-rx-defect-window

Syntax **max-rx-defect-window** *seconds*
no max-rx-defect-window

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service epipe sap eth-cfm mep grace eth-ed max-rx-defect-window
configure service epipe spoke-sdp eth-cfm mep grace eth-ed max-rx-defect-window
configure service ipipe sap eth-cfm mep grace eth-ed max-rx-defect-window

Description This command limits the duration of the received ETH-ED expected defect window to the lower value of either the received value from the peer or this parameter.

The **no** form of this command removes the limitation, and any valid defect window value received from a peer MEP in the ETH-ED PDU will be used.

Default no max-rx-defect-window

Parameters *seconds* — Specifies the duration, in seconds, of the maximum expected defect window.

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

max-rx-defect-window

Syntax **max-rx-defect-window** *seconds*
no max-rx-defect-window

Context **[Tree]** (config>service>vpls>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)

Full Context configure service vpls eth-cfm mep grace eth-ed max-rx-defect-window
configure service vpls mesh-sdp eth-cfm mep grace eth-ed max-rx-defect-window
configure service vpls sap eth-cfm mep grace eth-ed max-rx-defect-window
configure service vpls spoke-sdp eth-cfm mep grace eth-ed max-rx-defect-window

Description This command limits the duration of the received ETH-ED expected defect window to the lower value of either the received value from the peer or this parameter.

The **no** form of this command removes the limitation, and any valid defect window value received from a peer MEP in the ETH-ED PDU will be used.

Default no max-rx-defect-window

Parameters *seconds* — Specifies the duration, in seconds, of the maximum expected defect window.

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max-rx-defect-window

Syntax **max-rx-defect-window** *seconds*
no max-rx-defect-window

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)

Full Context configure service ies interface sap eth-cfm mep grace eth-ed max-rx-defect-window
configure service ies interface spoke-sdp eth-cfm mep grace eth-ed max-rx-defect-window
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed max-rx-defect-window

Description This command limits the duration of the received ETH-ED expected defect window to the lower value of either the received value from the peer or this parameter.

The **no** form of this command removes the limitation, and any valid defect window value received from a peer MEP in the ETH-ED PDU will be used.

Default no max-rx-defect-window

Parameters *seconds* — Specifies the duration, in seconds, of the maximum expected defect window

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed max-rx-defect-window

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep grace eth-ed max-rx-defect-window
- configure service ies interface spoke-sdp eth-cfm mep grace eth-ed max-rx-defect-window

max-rx-defect-window

Syntax **max-rx-defect-window** *seconds*
no max-rx-defect-window

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace>eth-ed max-rx-defect-window)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed max-rx-defect-window)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap eth-cfm mep grace eth-ed max-rx-defect-window
configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed max-rx-defect-window
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed max-rx-defect-window

Description This command limits the duration of the received ETH-ED expected defect window to the lower value of either the received value from the peer or this parameter.

The **no** form of this command removes the limitation, and any valid defect window value received from a peer MEP in the ETH-ED PDU will be used.

Default no max-rx-defect-window

Parameters *seconds* — Specifies the duration, in seconds, of the maximum expected defect window

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed max-rx-defect-window

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed max-rx-defect-window
- configure service vprn interface sap eth-cfm mep grace eth-ed max-rx-defect-window

max-rx-defect-window

Syntax **max-rx-defect-window** *seconds*
no max-rx-defect-window

Context **[Tree]** (config>router>if>eth-cfm>mep>grace>eth-ed max-rx-defect-window)

Full Context configure router interface eth-cfm mep grace eth-ed max-rx-defect-window

Description This command limits the duration of the received ETH-ED expected defect window to the lower value of either the received value from the peer or this parameter.

The **no** form of this command removes the limitation, and any valid defect window value received from a peer MEP in the ETH-ED PDU will be used.

Default no max-rx-defect-window

Parameters *seconds* — Specifies the duration, in seconds, of the maximum expected defect window.

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.126 max-sess-prefix

max-sess-prefix

Syntax **max-sess-prefix** *count*
no max-sess-prefix

Context **[Tree]** (config>test-oam>twamp>server>prefix max-sess-prefix)

Full Context configure test-oam twamp server prefix max-sess-prefix

Description This command configures the maximum number of concurrent TWAMP-Test sessions by clients with an IP address in a specific prefix. A new test session (described by a Request-TW-Session message) is rejected if accepting it would cause either the limit defined by this command or the server limit (max-sess-server) to be exceeded.

The **no** form of this command returns the value to the default.

Default max-sess-prefix 32

Parameters *count* — Specifies the maximum number of concurrent test sessions.

Values 0 to 128

Default 32

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.127 max-sess-server

max-sess-server

Syntax **max-sess-server** *count*
no max-sess-server

Context **[Tree]** (config>test-oam>twamp>server max-sess-server)

Full Context configure test-oam twamp server max-sess-server

Description This command configures the maximum number of concurrent TWAMP-Test sessions across all allowed clients. A new test session (described by a Request-TW-Session message) is rejected if accepting it would cause either the limit defined by this command or a prefix limit (max-sess-prefix) to be exceeded.

The **no** form of this command returns the value to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default max-sess-server 32

Parameters *count* — Specifies the maximum number of concurrent test sessions.

Values 0 to 128

Default 32

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.128 max-sessions

max-sessions

Syntax **max-sessions** *sessions*
no max-sessions

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if max-sessions)

Full Context configure mcast-management multicast-info-policy video-policy video-interface max-sessions

Description This command configures the per-client maximum number of sessions.

The **no** form of the command reverts to the default value.

Default max-sessions 256

Parameters *sessions* — Specifies the per-client maximum number of sessions.

Values 1 to 65536

Default 256

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

17.129 max-sessions-per-cid

max-sessions-per-cid

Syntax **max-sessions-per-cid** *sessions* [**allow-sessions-without-cid**]
no max-sessions-per-cid

Context **[Tree]** (config>subscr-mgmt>ppp-policy max-sessions-per-cid)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt ppp-policy max-sessions-per-cid

Description This command configures the maximum number of PPPoE sessions with the same Agent Circuit ID that can be active on the same SAP or MSAP. The limit is enforced in the discovery phase, prior to PAP or CHAP authentication and is based on the Agent Circuit ID sub-option that is present in the vendor-specific PPPoE access loop identification tag added in PADI and PADR messages by a PPPoE intermediate agent.

When the optional **allow-sessions-without-cid** keyword is specified, PPPoE sessions without an Agent Circuit ID can be established. The configured sessions limit does not apply to these sessions.

By default, there is no limit for the number of PPPoE sessions with the same Agent Circuit ID that are active on the same SAP or MSAP. Sessions without Agent Circuit ID can be established.

The **no** form of this command reverts to the default value.

Default no max-sessions-per-cid

Parameters *sessions* — Specifies the maximum number of sessions with the same circuit ID that can be active on the same SAP or MSAP.

Values 1 to 8190

allow-sessions-without-cid — Specifies to enable support for PPPoE sessions without a circuit ID while a **max-sessions-per-cid** limit is configured on a SAP or MSAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.130 max-sessions-per-mac

max-sessions-per-mac

Syntax **max-sessions-per-mac** *sessions* [**allow-same-circuit-id-for-dhcp**]
no max-sessions-per-mac

Context **[Tree]** (config>subscr-mgmt>ppp-policy max-sessions-per-mac)

Full Context configure subscriber-mgmt ppp-policy max-sessions-per-mac

Description This command sets the maximum PPP sessions that can be opened for a given MAC address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To enable IPv4 address allocation using the internal DHCPv4 client for multiple PPPoE sessions on a single SAP and having the same MAC address and circuit-ID, the optional CLI parameter **allow-same-circuit-id-for-dhcp** should be added. The SR OS local DHCP server detects the additional vendor-specific options inserted by the internal DHCPv4 client and use an extended unique key for lease allocation.

The **no** form of this command reverts to the default value.

Parameters *sessions* — Specifies the maximum PPP sessions that can be opened for the given MAC address.

Values 1 to 8191

allow-same-circuit-id-for-dhcp — Enables support for IPv4 address allocation using the internal DHCPv4 client for multiple PPPoE sessions on a single SAP that have the same MAC address and circuit ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.131 max-setup-time

max-setup-time

Syntax **max-setup-time** [[*up-interval*] | **infinite**]
no max-setup-time

Context **[Tree]** (config>lag>bfd>family max-setup-time)

Full Context configure lag bfd family max-setup-time

Description This command specifies the maximum amount of time the router will forward traffic over a link that has transitioned from Standby to Active, before the micro-BFD session must be fully established (Up state).

The **no** form of this command returns the timer value to the default (0) which indicates that forwarding will not start until the BFD session is established.

Default max-setup-time infinite

Parameters *up-interval* — Specifies the amount of time, in milliseconds.

Values -1 to 60000

infinite — Specifies no end time to forward traffic.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.132 max-size

max-size

Syntax **max-size** *size*
no max-size

Context **[Tree]** (config>open-flow>of-switch>flowtable max-size)

Full Context configure open-flow of-switch flowtable max-size

Description This command configures the size for the specified flow table. The OpenFlow switch instance must be shutdown to modify this parameter.

The **no** form of this command restores the default size.

Default max-size 1000

Parameters *size* — Specifies the maximum size limit for the flow table. The size limit is a total for both IPv4 and IPv6.

Values 1 to 262144

Default 1000

Platforms All

17.133 max-sources

max-sources

Syntax **max-sources** *max-sources*
no max-sources

Context **[Tree]** (config>service>vprn>igmp>grp-if max-sources)
[Tree] (config>service>vprn>igmp>if max-sources)
[Tree] (config>service>vprn>mld>interface max-sources)

Full Context configure service vprn igmp group-interface max-sources
configure service vprn igmp interface max-sources
configure service vprn mld interface max-sources

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the maximum number of sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of sources, the sources that are already accepted are not deleted. Only new sources will not be allowed.

Parameters *sources* — Specifies the maximum number of sources for this interface.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface max-sources

All

- configure service vprn mld interface max-sources
- configure service vprn igmp interface max-sources

max-sources

Syntax **max-sources** *value*
no max-sources

Context **[Tree]** (config>router>igmp>group-interface max-sources)
[Tree] (config>router>igmp>if max-sources)

Full Context configure router igmp group-interface max-sources
configure router igmp interface max-sources

Description This command configures the maximum number of group sources for this group-interface.

Parameters *value* — Specifies the maximum number of group sources.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface max-sources

All

- configure router igmp interface max-sources

max-sources

Syntax **max-sources** [*1..1000*]
no max-sources

Context **[Tree]** (config>router>mld>group-interface max-sources)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>mld>if max-sources)

Full Context configure router mld group-interface max-sources
configure router mld interface max-sources

Description This command configures the maximum number of group sources for this interface.

The **no** form of this command reverts to the default.

Default no max-sources

Parameters *1 .. 1000* — Specifies the maximum number of group sources for this interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router mld group-interface max-sources

All

- configure router mld interface max-sources

17.134 max-sr-labels

max-sr-labels

Syntax **max-sr-labels** *label-stack-size* [**additional-frr-labels** *labels*]
no max-sr-labels

Context [Tree] (config>router>mpls>lsp max-sr-labels)
[Tree] (config>router>mpls>lsp-template max-sr-labels)

Full Context configure router mpls lsp max-sr-labels
configure router mpls lsp-template max-sr-labels

Description This command configures the maximum number of labels which the ingress LER can push for a given SR-TE LSP.

This command is used to allow room to insert additional transport, service, and other labels when packets are forwarded in a given context.

The **max-sr-labels** *label-stack-size* value should reflect the desired maximum label stack of the primary path of the SR-TE LSP.

The value in **additional-frr-labels** *labels* should reflect additional labels inserted by remote LFA for the backup next-hop of the SR-TE LSP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The sum of both label values represents the worst case transport of SR label stack size for this SR-TE LSP and is populated by MPLS in the TTM such that services and shortcut applications can check it to decide if a service can be bound or a route can be resolved to this SR-TE LSP.

The maximum label stack supported by the router is always signaled by PCC in the PCEP Open object as part of the as SR-PCE-CAPABILITY TLV. It is referred to as the Maximum Stack Depth (MSD).

In addition, the per-LSP value for the max-sr-labels option, if configured, is signaled by PCC to PCE in the Segment-ID (SID) Depth value in a METRIC object for both a PCE computed LSP and a PCE controlled LSP. PCE will compute and provide the full explicit path with TE-links specified. If there is no path with the number of hops lower than the MSD value, or the Segment-ID (SID) Depth value if signaled, a reply with no path will be returned to PCC.

For a PCC controlled LSP, if the label stack returned by the TE-DB's hop-to-label translation exceeds the per LSP maximum SR label stack size, the LSP is brought down.

The **no** form of this command reverts to the default value.

Default max-sr-labels 6 additional-frr-labels 1

Parameters *label-stack-size* — Specifies the label stack size.

Values 1 to 11

additional-frr-labels *labels* — Specifies the addition FRR labels.

Values 0 to 3

Platforms All

17.135 max-srte-pce-init-lsps

max-srte-pce-init-lsps

Syntax **max-srte-pce-init-lsps** *max-number*
no max-srte-pce-init-lsps

Context **[Tree]** (config>router>pcep>pcc max-srte-pce-init-lsps)

Full Context configure router pcep pcc max-srte-pce-init-lsps

Description This command configures the maximum number of PCE-initiated SR-TE LSPs that can be created by the router.

The **no** form of the command sets this value to the default.

Default max-srte-pce-init-lsps 8191

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *max-number* — Specifies the maximum number of SR-TE PCE-initiated LSPs.

Values 0 to 8191

Platforms All

17.136 max-stats

max-stats

Syntax [**no**] **max-stats**

Context **[Tree]** (config>router>mpls>ingr-stats>p2mp-template-lsp max-stats)
[Tree] (config>router>mpls>ingr-stats>p2p-template-lsp max-stats)
[Tree] (config>router>mpls>lsp>egr-stats max-stats)
[Tree] (config>router>mpls>lsp-template>egr-stats max-stats)

Full Context configure router mpls ingress-statistics p2mp-template-lsp max-stats
configure router mpls ingress-statistics p2p-template-lsp max-stats
configure router mpls lsp egr-stats max-stats
configure router mpls lsp-template egr-stats max-stats

Description This command enables accounting and statistical data collection. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

The config>router>mpls>ingr-stats>p2mp-template-lsp>max-stats command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

When the **no max-stats** command is issued the statistics are still accumulated by the forwarding engine. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **max-stats** command is issued then the counters written to the billing file include all the traffic while the **no max-stats** command was in effect.

Default max-stats

Platforms All

17.137 max-suppress

max-suppress

Syntax **max-suppress** *minutes*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no max-suppress

Context [Tree] (config>router>policy-options>damping max-suppress)

Full Context configure router policy-options damping max-suppress

Description This command configures the maximum suppression parameter for the route damping profile.

This value indicates the maximum time, expressed in minutes, that a route can remain suppressed.

The **no** form of this command removes the maximum suppression parameter from the damping profile.

Default no max-suppress

Parameters *minutes* — Specifies the maximum suppression time, in minutes, expressed as a decimal integer.

Values 1 to 720

Platforms All

17.138 max-throughput-octet-count

max-throughput-octet-count

Syntax [**no**] **max-throughput-octet-count**

Context [Tree] (config>log>acct-policy>cr>aa>aa-from-sub-cntr max-throughput-octet-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr max-throughput-octet-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters max-throughput-octet-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters max-throughput-octet-count

Description This command includes the maximum throughput as measured in the octet count. This command only applies to the 7750 SR.

The **no** form of this command excludes the maximum throughput octet count.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.139 max-throughput-packet-count

max-throughput-packet-count

Syntax [**no**] m**ax-throughput-packet-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr max-throughput-packet-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr max-throughput-packet-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters max-throughput-packet-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters max-throughput-packet-count

Description This command includes the maximum throughput as measured in the packet count. This command only applies to the 7750 SR.

The **no** form of this command excludes the maximum throughput packet count.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.140 max-throughput-stats

max-throughput-stats

Syntax [**no**] **max-throughput-stats**

Context **[Tree]** (config>app-assure>group>statistics>aa-sub max-throughput-stats)

Full Context configure application-assurance group statistics aa-sub max-throughput-stats

Description This command enables the collection of max-throughput statistics.

The **no** form of this command disables the collection.

Default no max-throughput-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.141 max-throughput-timestamp

max-throughput-timestamp

Syntax [**no**] **max-throughput-timestamp**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr max-throughput-timestamp)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr max-throughput-timestamp)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters max-throughput-timestamp
configure log accounting-policy custom-record aa-specific to-aa-sub-counters max-throughput-timestamp

Description This command includes the timestamp of the maximum throughput. This command only applies to the 7750 SR.

The **no** form of this command excludes the timestamp.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.142 max-time

max-time

Syntax **max-time** *minutes*
no max-time

Context **[Tree]** (config>router>l2tp>tunnel-selection-blacklist max-time)
[Tree] (config>service>vprn>l2tp>tunnel-selection-blacklist max-time)

Full Context configure router l2tp tunnel-selection-blacklist max-time
configure service vprn l2tp tunnel-selection-blacklist max-time

Description This command configures time for which an entity (peer or a tunnel) are kept in the denylist.

The **no** form of this command reverts to the default.

Default max-time 5

Parameters *minutes* — Specifies the maximum time a tunnel or peer may remain in the denylist.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.143 max-time-granularity

max-time-granularity

Syntax **[no] max-time-granularity** *time*

Context **[Tree]** (config>system>telemetry>notification-bundling max-time-granularity)

Full Context configure system telemetry notification-bundling max-time-granularity

Description This command sets the maximum time interval during which telemetry notifications are bundled. All bundled notifications will have the same timestamp, which is the timestamp of the bundle.

The **no** form of this command returns the time granularity to the default value.

Default max-time-granularity 100

Parameters *time* — Specifies the maximum time interval during which telemetry notifications are bundled, in milliseconds.

Values 1 to 1000

Platforms All

17.144 max-ttl

max-ttl

Syntax **max-ttl** *ttl-value*
no max-ttl

Context **[Tree]** (config>test-oam>ldp-treetrace>path-discovery max-ttl)

Full Context configure test-oam ldp-treetrace path-discovery max-ttl

Description This command configures the maximum number of hops the path discovery traces in the path of each FEC to be discovered.

The **no** form of this command resets the time out to its default value.

Default no max-ttl

Parameters *ttl-value* — Specifies the maximum label time-to-live value for an LSP trace request during the tree discovery.

Values 1 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.145 max-tx-delay

max-tx-delay

Syntax **max-tx-delay** *deci-seconds*
no max-tx-delay

Context **[Tree]** (config>mcast-mgmt>mcast-rprt-dest max-tx-delay)

Full Context configure mcast-management mcast-reporting-dest max-tx-delay

Description This command specifies the time interval before the packet starts transmitting towards the destination. When an IGMP event is encoded and ready to be transported, a buffer for the packet is allocated (if not already existent). The events are written into this buffer. Along with the initial buffer creation, a timer is started. The trigger for the transmission of the packet is either the TX buffer being filled up to 1400 B, or the timer expiry, whichever comes first.

The **no** form of this command reverts to the default.

Parameters *deci-seconds* — Specifies the maximum delay after which any cached reports are flushed to the reporting destination.

Values 0 to 100

Platforms All

max-tx-delay

Syntax **max-tx-delay** *deciseconds*
no max-tx-delay

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy max-tx-delay)

Full Context configure service nat syslog syslog-export-policy max-tx-delay

Description This command enables aggregation of flow log messages within a syslog frame. It introduces a delay during which logs are collected in each BB-ISA so they can be sent in a single syslog message to conserve system resources and network bandwidth.

When aggregation is enabled, generation of a syslog frame carrying multiple flow logs is triggered by one of the two events (whichever occurs first):

- Expiry of the max-tx-delay timer
- Exceeding MTU size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command reverts to the default.

Default max-tx-delay 3

Parameters *deciseconds* — Specifies the maximum time a syslog message is delayed in the system's output buffer.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.146 max-ve-id

max-ve-id

Syntax **max-ve-id** *value*
no max-ve-id

Context **[Tree]** (config>service>vpls>bgp-vpls max-ve-id)

Full Context configure service vpls bgp-vpls max-ve-id

Description This command configures the allowed range for the VE-id value: locally configured and received in a NLRI. Configuration of a VE-id higher than the value specified in this command is not allowed.

Also upon reception of a higher VE-id in an NLRI imported in this VPLS instance (RT is the configured import RT) the following action must be taken:

- a trap must be generated informing the operator of the mismatch.
- NLRI must be dropped
- no service labels are to be installed for this VE-id
- no new NLRI must be generated if a new offset is required for VE-id.

The **no** form of this command sets the max-ve-id to un-configured. The BGP VPLS status should be administratively down for “no max-ve-id” to be used.

The max-ve-id value can be changed without shutting down bgp-vpls if the newly provisioned value does not conflict with the already configured local VE-ID. If the value of the local-VE-ID is higher than the new max-ve-id value the command is rejected. The operator needs to decrease first the VE-ID before running the command.

The actions taken for other max-ve-id values are as follows:

- max-ve-id value higher than all VE-IDs (local and received) is allowed and there are no effects.
- max-ve-id higher than the local VE-ID but smaller than the remote VE-IDs:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Provisioning is allowed
- A warning message will be generated stating that “Higher VE-ID values were received in the BGP VPLS context. Related pseudowires will be removed.”
- The pseudowires associated with the higher VE-IDs will be removed locally.
- This is a situation that should be corrected by the operator as the pseudowire may be down just at the local PE, consuming unnecessarily core bandwidth. The higher VE-IDs should be removed or lowered.

If the max-ve-id has increased a BGP route refresh is sent to the VPLS community to get the routes which might have been rejected earlier due to max-ve-id check. A max-ve-id value needs to be provisioned for BGP VPLS to be in “no shutdown” state.

Default no max-ve-id

Parameters *value* — Specifies the allowed range of [1-value] for the VE-id. The configured value must be bigger than the existing VE-ids

Values 1 to 65535

Platforms All

17.147 max-wait-to-advertise

max-wait-to-advertise

Syntax **max-wait-to-advertise** *seconds*
no max-wait-to-advertise

Context **[Tree]** (config>service>vprn>bgp>convergence>family max-wait-to-advertise)

Full Context configure service vprn bgp convergence family max-wait-to-advertise

Description This command configures the maximum amount of time that BGP waits until it starts advertising IPv4-unicast or IPv6-unicast routes to its BGP peers. For IPv4-unicast routes, *seconds* is measured from the time when the first peer that supports the IPv4-unicast address family comes up. For IPv6-unicast routes *seconds* is measured from the time when the first peer that negotiates the IPv6-unicast address family comes up.

The time limit configured by this command should allow sufficient time for all important peers to re-establish their sessions with the restarting router and advertise their complete set of IPv4-unicast or IPv6-unicast routes (followed by the applicable End of RIB marker).

The **no** form of this command implements the default value, which is three times the value of the **min-wait-to-advertise** time limit.

Default no max-wait-to-advertise

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the maximum amount of time, in seconds, that BGP waits until IPv4-unicast or IPv6-unicast routes are advertised to peers.

Values 0 to 3600

Platforms All

max-wait-to-advertise

Syntax **max-wait-to-advertise** *seconds*
no max-wait-to-advertise

Context **[Tree]** (config>router>bgp>convergence>family max-wait-to-advertise)

Full Context configure router bgp convergence family max-wait-to-advertise

Description This command configures the maximum amount of time that BGP waits until it starts advertising IPv4-unicast or IPv6-unicast routes to its BGP peers. For IPv4-unicast routes, the time limit value is measured from the time when the first peer that supports the IPv4-unicast address family comes up. For IPv6-unicast routes the time limit value is measured from the time when the first peer that negotiates the IPv6-unicast address family comes up.

The time limit configured by this command should allow sufficient time for all important peers to re-establish their sessions with the restarting router and advertise their complete set of IPv4-unicast or IPv6-unicast routes (followed by the applicable End of RIB marker).

The **no** form of this command implements the default value, which is three times the value of the **min-wait-to-advertise** time-limit.

Default no max-wait-to-advertise

Parameters *seconds* — Specifies the maximum amount of time, in seconds, that BGP waits until IPv4-unicast or IPv6-unicast routes are advertised to peers.

Values 0 to 3600

Platforms All

17.148 maximum-cert-chain-depth

maximum-cert-chain-depth

Syntax **maximum-cert-chain-depth** *level*
no maximum-cert-chain-depth

Context **[Tree]** (config>system>security>pki maximum-cert-chain-depth)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security pki maximum-cert-chain-depth

Description This command defines the maximum depth of certificate chain verification. This number is applied system wide.

The **no** form of this command reverts to the default.

Default maximum-cert-chain-depth 7

Parameters *level* — Specifies the maximum depth level of certificate chain verification, range from 1 to 7. the certificate under verification is not counted in. for example, if this parameter is set to 1, then the certificate under verification must be directly signed by trust anchor CA.

Values 1 to 7

Platforms All

17.149 maximum-client-lead-time

maximum-client-lead-time

Syntax **maximum-client-lead-time** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no maximum-client-lead-time

Context **[Tree]** (config>router>dhcp>server>failover maximum-client-lead-time)
[Tree] (config>router>dhcp>server>pool>failover maximum-client-lead-time)
[Tree] (config>service>vprn>dhcp>server>failover maximum-client-lead-time)
[Tree] (config>service>vprn>dhcp>server>pool>failover maximum-client-lead-time)
[Tree] (config>router>dhcp6>server>failover maximum-client-lead-time)
[Tree] (config>router>dhcp6>server>pool>failover maximum-client-lead-time)
[Tree] (config>service>vprn>dhcp6>server>failover maximum-client-lead-time)
[Tree] (config>service>vprn>dhcp6>server>pool>failover maximum-client-lead-time)

Full Context configure router dhcp local-dhcp-server failover maximum-client-lead-time
configure router dhcp server pool failover maximum-client-lead-time
configure router dhcp6 local-dhcp-server failover maximum-client-lead-time
configure router dhcp6 server pool failover maximum-client-lead-time
configure service vprn dhcp local-dhcp-server failover maximum-client-lead-time
configure service vprn dhcp local-dhcp-server pool failover maximum-client-lead-time
configure service vprn dhcp6 local-dhcp-server failover maximum-client-lead-time
configure service vprn dhcp6 local-dhcp-server pool failover maximum-client-lead-time

Description The **maximum-client-lead-time** (MCLT) is the maximum time that a DHCP server can extend client's lease time beyond the lease time currently known by the DHCP partner node. In dual-homed environment, the initial lease time for all DHCP clients is by default restricted to MCLT. Consecutive DHCP renews can extend the lease time beyond the MCLT.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The MCLT is a safeguard against IP address/prefix duplication in cases of a lease synchronization failure when local-remote failover model is deployed.

Once the intercommunication link failure between the redundant DHCP servers is detected, the DHCP IP address range configured as remote will not be allowed to start delegating new leases until the MCLT + partner-down-delay intervals expire. This is to ensure that the new lease that was delegated from the local IP address-range/prefix on one node but was never synchronized due to the intercommunication link failure, will expire before the same IP address/prefix is allocated from the remote IP address-range/prefix on the other node.

However, the already existing (and synchronized) lease times can be renewed from the remote IP address range at any time, regardless of the state of the intercommunication link (operational or failed).

Lease synchronization failure can be caused either by a node failure, or a failure of the link over which the DHCP leases are synchronized (intercommunication link). Synchronization failure detection can take up to 3 seconds.

During the failure, the DHCP lease time for the new clients is restricted to MCLT while for the existing clients the lease time will over time (by consecutive DHCP renews) be gradually reduced to the MCLT.

The **no** form of this command reverts to the default.

Default maximum-client-lead-time min 10

Parameters *maximum-client-lead-time* — Specifies the maximum client lead time.

Values

hrs *hours*	1 to 23
min *minutes*	1 to 59
sec *seconds*	1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.150 maximum-declined

maximum-declined

Syntax **maximum-declined** *maximum-declined*
no maximum-declined

Context **[Tree]** (config>router>dhcp>server>pool>subnet maximum-declined)
[Tree] (config>service>vprn>dhcp>server>pool>subnet maximum-declined)

Full Context configure router dhcp local-dhcp-server pool subnet maximum-declined

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn dhcp local-dhcp-server pool subnet maximum-declined

Description This command configures the maximum number of declined addresses allowed.

The **no** form of the reverts to the default.

Default maximum-declined 64

Parameters *maximum-declined* — Specifies the maximum number of declined addresses allowed.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.151 maximum-ipv6-routes

maximum-ipv6-routes

Syntax **maximum-ipv6-routes** *number* [**log-only**] [**threshold** *percentage*]
no maximum-ipv6-routes

Context **[Tree]** (config>service>vprn maximum-ipv6-routes)

Full Context configure service vprn maximum-ipv6-routes

Description This command specifies the maximum number of remote IPv6 routes that can be held within a VPN routing/ forwarding (VRF) context. The **local**, **host**, **static** and **aggregate** routes are not counted.

The VPRN service ID must be in a shutdown state in order to modify maximum-routes command parameters.

If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering will remain up but the exceeding BGP routes will not be added to the VRF.

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols will resubmit their routes which were initially rejected.

The **no** form of this command disables any limit on the number of routes within a VRF context. Issue the **no** form of this command only when the VPRN instance is shutdown.

Default 0 or disabled — The threshold will not be raised.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — An integer that specifies the maximum number of routes to be held in a VRF context.

Values 1 to 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold *percentage* — The percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set and the second is a high-level warning at level between the maximum number of routes and the mid-level rate ([mid+max] / 2).

Values 0 to 100

Platforms All

17.152 maximum-p2mp-spmsi

maximum-p2mp-spmsi

Syntax **maximum-p2mp-spmsi** *range*
no maximum-p2mp-spmsi

Context **[Tree]** (config>service>vprn>mvpn>pt>selective maximum-p2mp-spmsi)

Full Context configure service vprn mvpn provider-tunnel selective maximum-p2mp-spmsi

Description This command specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the mVPN. When the limit is reached, no more RSVP P2MP S-PMSI or LDP P2MP S-PMSI is created and traffic over the data-threshold will stay on I-PMSI.

Default 10

Parameters *range* — Specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnel for the mVPN.

Values 1 to 4000

Default 10

Platforms All

maximum-p2mp-spmsi

Syntax **maximum-p2mp-spmsi** *range*
no maximum-p2mp-spmsi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>gtm>provider-tunnel>selective maximum-p2mp-spmsi)

Full Context configure router gtm provider-tunnel selective maximum-p2mp-spmsi

Description This command specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the GTM. When the limit is reached, no more RSVP P2MP S-PMSI or LDP P2MP S-P MSI tunnels are created and traffic over the data-threshold will stay on I-PMSI.

The **no** form of this command reverts to the default values.

Default maximum-p2mp-spmsi 10

Parameters *range* — Specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the GTM.

Values 1 to 4000

Default 10

Platforms All

17.153 maximum-paths

maximum-paths

Syntax **maximum-paths** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no maximum-paths

Context [Tree] (config>service>vprn>bgp>multi-path maximum-paths)

Full Context configure service vprn bgp multi-path maximum-paths

Description This command sets ECMP multi-path parameters that apply to all address families for that BGP multi-path. For some address families it is possible to override these settings on a per address family basis.

When multi-path is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

To qualify as a multi-path, a non-best route must meet the following criteria (some criteria are controlled by this command):

- The multi-path route must be the same type of route as the best path (same AFI/SAFI and, in some cases, same next-hop resolution method).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The multi-path route must be tied with the best path for all criteria of greater significance than next-hop cost, except for criteria that are configured to be ignored.
- If the best path selection reaches the next-hop cost comparison, the multi-path route must have the same next-hop cost as the best route unless the **unequal-cost** option is configured.
- The multi-path route must not have the same BGP next-hop as the best path or any other multi-path route.
- The multi-path route must not cause the ECMP limit of the routing instance to be exceeded (configured using the **ecmp** command with a value in the range 1 to 64).
- The multi-path route must not cause the applicable *max-paths* limit to be exceeded. If the best path is an EBGP learned route and the **ebgp** option is used, the *ebgp-max-paths* limit overrides the *max-paths* limit. If the best path is an IBGP-learned route and the **ibgp** option is used, the *ibgp-max-paths* limit overrides the *max-paths* limit. All path limits are configurable up to a maximum of 64. Multi-path is effectively disabled if a value is set to 1.
- The multi-path route must have the same neighbor AS in its AS path as the best path if the **restrict same-neighbor-as** option is configured. By default, any path with the same AS path length as the best path (regardless of neighbor AS) is eligible for multi-path.
- The route must have the same AS path as the best path if the **restrict exact-as-path** option is configured. By default, any path with the same AS path length as the best path (regardless of the actual AS numbers) is eligible for multi-path.

The **no** form of this command disables BGP multi-path.

Default no maximum-paths

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

egp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path-as — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

maximum-paths

Syntax **maximum-paths** *max-paths* [**ebgp** *ebgp-max-paths*] [**ibgp** *ibgp-max-paths*] [**restrict** {**same-neighbor-as** | **exact-as-path**}] [**unequal-cost**]
no maximum-paths

Context **[Tree]** (config>router>bgp>multi-path maximum-paths)

Full Context configure router bgp multi-path maximum-paths

Description This command sets ECMP multipath parameters that apply to all address families for that BGP multipath. For some address families it is possible to override these settings on a per address family basis.

When multipath is enabled, traffic to the destination is load-shared across a set of paths (BGP routes) that the BGP decision process considers equal to the best path. The actual distribution of traffic over the multiple paths may be equal or unequal (that is, based on weights derived from the Link Bandwidth Extended Community).

The **no** form of this command disables BGP multipath.

Default no maximum-paths

Parameters *max-paths* — Specifies the maximum number of multipaths per prefix/NLRI if *ebgp-max-paths* or *ibgp-max-paths* does not apply.

Values 1 to 64

ebgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an EBGP learned route.

Values 1 to 64

ibgp-max-paths — Specifies the maximum number of multipaths per prefix or NLRI when the best path is an IBGP learned route.

Values 1 to 64

restrict same-neighbor-as — Specifies that the non-best path must have the same neighbor AS in its AS path as the best path.

restrict exact-as-path — Specifies that the non-best path must have the same AS path as the best path.

unequal-cost — Instructs BGP to ignore differences in the next-hop cost only when determining eligible multipaths.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.154 maximum-recovery-time

maximum-recovery-time

Syntax **maximum-recovery-time** *interval*
no maximum-recovery-time

Context **[Tree]** (config>router>ldp>graceful-restart maximum-recovery-time)

Full Context configure router ldp graceful-restart maximum-recovery-time

Description This command configures the local maximum recovery time.

The **no** form of this command returns the default value.

Default no maximum-recovery-time (which equals a value of 120 seconds)

Parameters *interval* — Specifies the length of time in seconds.

Values 15 to 1800

Platforms All

17.155 maximum-routes

maximum-routes

Syntax **maximum-routes** *number* [**log-only**] [**threshold** *percentage*]
no maximum-routes

Context **[Tree]** (config>service>vprn maximum-routes)

Full Context configure service vprn maximum-routes

Description This command specifies the maximum number of remote routes that can be held within a VPN routing/ forwarding (VRF) context. The **local**, **host**, **static** and **aggregate** routes are not counted.

The VPRN service ID must be in a shutdown state in order to modify maximum-routes command parameters.

If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering will remain up but the exceeding BGP routes will not be added to the VRF.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols will resubmit their routes which were initially rejected.

The **no** form of this command disables any limit on the number of routes within a VRF context. Issue the **no** form of this command only when the VPRN instance is shutdown.

Default 0 or disabled — The threshold will not be raised.

Parameters *number* — An integer that specifies the maximum number of routes to be held in a VRF context.

Values 1 to 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold *percentage* — The percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set and the second is a high-level warning at level between the maximum number of routes and the mid-level rate ([mid+max] / 2).

Values 0 to 100

Platforms All

17.156 maximum-sid-depth

maximum-sid-depth

Syntax **maximum-sid-depth**

Context **[Tree]** (config>router>isis>segm-rtng maximum-sid-depth)

Full Context configure router isis segment-routing maximum-sid-depth

Description Commands in this context configure a manual override of the Maximum Segment Depths (MSD) that is announced by the router.

Platforms All

maximum-sid-depth

Syntax **maximum-sid-depth**

Context **[Tree]** (config>router>ospf>segm-rtng maximum-sid-depth)

Full Context configure router ospf segment-routing maximum-sid-depth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure a manual override of the Maximum Segment Depths (MSD) that is announced by the router.

Platforms All

17.157 mbb

mbb

Syntax **mbb** [**detail**]
no mbb

Context **[Tree]** (debug>router>mpls>event mbb)

Full Context debug router mpls event mbb

Description This command debugs the state of the most recent invocation of the make-before-break (MBB) functionality.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about MBB events.

Platforms All

17.158 mbb-prefer-current-hops

mbb-prefer-current-hops

Syntax [**no**] **mbb-prefer-current-hops**

Context **[Tree]** (config>router>mpls mbb-prefer-current-hops)

Full Context configure router mpls mbb-prefer-current-hops

Description This command implements a new option in the CSPF path computation during a Make-Before-Break (MBB) procedure of an RSVP LSP.

When MPLS performs an MBB for the primary or secondary path of a P2P LSP, or the S2L path of a P2MP LSP, and the new **mbb-prefer-current-hops** option is enabled in MPLS context, CSPF will select a path, among equal-cost candidate paths, with the most overlapping links with the current path. Normally, CSPF selects the path randomly.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The procedures of the new MBB CSPF path selection apply to LSP without the least-fill option enabled. If the least-fill rule results in a different path, the LSP path will be moved though. Users can still favor stability over least-fill condition by applying a larger value to the parameter **least-fill-min-thd** under the MPLS context such that a path will only be moved when the difference of the least-available bandwidth becomes significant enough between the most used links in the equal cost paths. If that difference is not significant enough, CSPF will select the path with the most overlapping links instead of selecting a path randomly.

The procedures when the new **mbb-prefer-current-hops** option is enabled apply to all MBB types. Thus, it applies to the auto-bandwidth MBB, the configuration change MBB, the soft preemption MBB, the TE graceful shutdown MBB, the delayed retry MBB (for SRLG secondary LSP path), the path change MBB, the timer resignal MBB, and the manual resignal MBB.

During the FRR global revertive MBB, CSPF selects a random link among the ones available between the PLR node and the Merge Point node, including the failed link if it has restored in the meantime. These links cannot be checked for overlap with the current path.

The TE graceful shutdown MBB will still avoid the link or node that is in maintenance and the soft preemption MBB will still avoid the link that is overbooked.

For an inter-area LSP, this feature applies to the subset of the path from the ingress LER to the exit ABR.

The procedures of this feature are not applied to a zero bandwidth CSPP LSP, including an auto-bandwidth CSPF LSP while its operational bandwidth is zero, and to a non-CSPF LSP.

Platforms All

17.159 mbs

mbs

Syntax **mbs** *percent-of-pool*
no mbs

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2-paths>primary-paths>queue-parameters mbs)
[Tree] (config>mcast-mgmt>bw-plcy>t2-paths>secondary-paths>queue-parameters mbs)

Full Context configure mcast-management bandwidth-policy t2-paths primary-paths queue-parameters mbs
configure mcast-management bandwidth-policy t2-paths secondary-paths queue-parameters mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the override for the default Maximum Buffer Size (MBS) for each individual path's queue. The queues MBS threshold defines the point at which all packets destined for the queue are discarded based on queue depth. The defined threshold also provides context for the queues drop-tail parameter.

The mbs *percent-of-pool* parameter is defined as a percentage of the total pool size. The system allows the sum of all MBS values to equal more than 100% allowing for oversubscription of the pool.

For the primary-path and secondary-path queues, the mbs percent is applied to a single queue for each path.

The **no** form of this command is used to restore the path queues default MBS value.

Parameters *percent-of-pool* — Specifies the percent of buffers from the total buffer pool space for the number of buffers, expressed as a decimal integer. If 10 MB is the total buffers in the buffer pool, a value of 10 would limit the maximum queue size to 1MB (10%) of buffer space for the forwarding class queue. If the total size is increased to 20MB, the existing value of 10 would automatically increase the maximum size of the queue to 2MB.

Values 0 to 100

Default

Primary:	7
Secondary:	40

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]
no mbs

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue mbs)

Full Context configure subscriber-mgmt sla-profile egress qos queue mbs

Description This command configures the maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer is available when needed or that the packet's RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

The **no** form of this command returns the MBS size to the size as configured in the QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — This required parameter specifies that the MBS is expressed as an integer representing the required size in either bytes or kilobytes. The default is **kilobytes**. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly to define the size. By specifying the keyword **default** sets the MBS to its default value.

Values 0 to 1073741824, **default**

bytes — Specifies that the value given for *size* is interpreted as the queue's MBS value in bytes.

kilobytes — Specifies that the value given for *size* is interpreted as the queue's MBS value in kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]
no mbs

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>queue mbs)

Full Context configure subscriber-mgmt sla-profile ingress qos queue mbs

Description The Maximum Burst Size (MBS) command configures the explicit definition of the maximum number of buffers allowed for a specific queue.

The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the number of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sap-ingress context for mbs provides a mechanism for overriding the default maximum size for the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer is available when needed or that the packet's RED slope does not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

The **no** form of this command returns the MBS size to the size as configured in the QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — This required parameter specifies that the MBS is expressed as an integer representing the required size in either bytes or kilobytes. The default is **kilobytes**. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly to define the size. By specifying the keyword **default** sets the MBS to its default value.

Values 0 to 1073741824, **default**

bytes — Specifies that the value given for *size* is interpreted as the queue's MBS value is in bytes.

kilobytes — Specifies that the value given for *size* is interpreted as the queue's MBS value is in kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]
no mbs

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>policer mbs)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>policer mbs)

Full Context configure subscriber-mgmt sla-profile egress qos policer mbs
configure subscriber-mgmt sla-profile ingress qos policer mbs

Description This command configures the MBS for the QoS policer.

The **no** form of this command returns the MBS to its default value. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

Parameters *size* — This required parameter specifies that the MBS is expressed as an integer representing the required size in either bytes or kilobytes. The default is **kilobytes**. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly to define the size. By specifying the keyword **default** sets the MBS to its default value.

Values 0 to 2683435456, **default**

bytes — Specifies that the value given for *size* is interpreted as the queue's MBS value in bytes.

kilobytes — Specifies that the value given for *size* is interpreted as the queue's MBS value in kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]
no mbs

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue mbs)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue mbs)
[Tree] (config>service>vprn>sap>egress>queue-override>queue mbs)
[Tree] (config>service>vprn>sap>ingress>queue-override>queue mbs)

Full Context configure service ies interface sap egress queue-override queue mbs
configure service ies interface sap ingress queue-override queue mbs
configure service vprn sap egress queue-override queue mbs
configure service vprn sap ingress queue-override queue mbs

Description This command overrides specific attributes of the specified queue's MBS parameters. The MBS is a mechanism to override the default maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer is available when needed or that the packets RED slope is not forced the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The **no** form of this command returns the MBS size assigned to the queue.

Default mbs default

Parameters *size* — This required parameter specifies that the MBS is expressed as an integer representing the required size in either bytes or kilobytes. The default is **kilobytes**. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly to define the size. By specifying the keyword **default** sets the MBS to its default value.

Values 0 to 1073741824, default

bytes — Specifies that the value given for *size* is interpreted as the queue's MBS value in bytes.

kilobytes — Specifies that the value given for *size* is interpreted as the queue's MBS value in kb/s.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]
no mbs

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue mbs)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue mbs)

Full Context configure service vpls sap egress queue-override queue mbs
configure service vpls sap ingress queue-override queue mbs

Description This command overrides specific attributes of the specified queue's MBS parameters. The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS is not guaranteed that a buffer will be available when needed or that the packets RED slope will not force the discard of the packet. Setting correct CBS parameters and controlling CBS over-subscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

The **no** form of this command returns the MBS assigned to the queue to the default value.

Default mbs default

Parameters *size* — The size parameter is required when specifying mbs and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **bytes** and **kilobytes** keywords are mutually exclusive and are used to explicitly define whether the size represents bytes or kilobytes.

Values 0 to 1073741824
default

bytes — When **byte** is defined, the value given for size is interpreted as the queue's MBS value given in bytes.

kilobytes — When **kilobytes** is defined, the value is interpreted as the queue's MBS value given in kilobytes.

Platforms All

mbs

Syntax **mbs** *burst-size*
no mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>isa-policer mbs)

Full Context configure subscriber-mgmt isa-policer mbs

Description This command specifies the maximum burst-size value of this policer.

The **no** form of this command reverts to its default.

Default mbs 0

Parameters *burst-size* — The maximum burst-size in kbytes.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mbs

Syntax **mbs** {*size* [**bytes** | **kilobyte**] | **default**}
no mbs

Context [Tree] (config>card>fp>ingress>access>qgrp>policer-over>plcr mbs)
[Tree] (config>card>fp>ingress>network>qgrp>policer-over>plcr mbs)

Full Context configure card fp ingress access queue-group policer-override policer mbs
configure card fp ingress network queue-group policer-override policer mbs

Description This command configures the policer's PIR leaky bucket's violate threshold. The **high-prio-only** command is applied to the MBS value to derive the bucket's low priority violate threshold. For ingress, trusted in-profile packets and untrusted high priority packets use the policer's high priority violate threshold while trusted out-of-profile and untrusted low priority packets use the policer's low priority violate threshold.

The PIR bucket's violate threshold represent the maximum burst tolerance allowed by the policer. If the policer's offered rate is equal to or less than the policer's defined rate, the PIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the offered rate increases beyond the metering rate, the amount of data allowed above the rate is capped by the threshold. The low priority violate threshold provides a smaller burst size for the lower priority traffic associated with the policer. Since all lower priority traffic is discarded at the lower burst tolerance size, the remaining burst tolerance defined by **high-prio-only** is available for the higher priority traffic.

The policer's mbs size defined in the QoS policy may be overridden on an sla-profile or SAP where the policy is applied.

The **no** form of this command reverts the policer to its default MBS size. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — The *size* parameter is required when specifying **mbs** and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **bytes** and **kilobytes** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

bytes — When **bytes** is defined, the value given for size is interpreted as the policer's MBS value given in bytes.

kilobytes — When **kilobytes** is defined, the value is interpreted as the policer's MBS value given in kilobytes.

default — Specifying the keyword **default** sets the MBS to its default value.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover>q mbs)
[Tree] (config>port>ethernet>access>ing>qgrp>qover>q mbs)
[Tree] (config>port>ethernet>network>egr>qgrp>qover>q mbs)

Full Context configure port ethernet access egress queue-group queue-overrides queue mbs
configure port ethernet access ingress queue-group queue-overrides queue mbs
configure port ethernet network egress queue-group queue-overrides queue mbs

Description The Maximum Burst Size (MBS) command specifies the default maximum buffer size for the template queue. The value is given in kilobytes.

The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The **queue-group** or network egress QoS context for mbs provides a mechanism for overriding the default maximum size for the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packets RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

This command applies to egress queue group queues as the queue-delay is only supported on egress queues. This command **the queue-delay** command are mutually exclusive.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the MBS size assigned to the queue to the value.

Default mbs default

Parameters *size* — The *size* parameter is required when specifying **mbs** and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 1073741824

bytes — When **byte** is defined, the value given for size is interpreted as the queue's MBS value given in bytes.

kilobytes — When **kilobytes** is defined, the value is interpreted as the queue's MBS value given in kilobytes.

default — Specifying the keyword **default** sets the MBS to its default value.

Platforms All

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]
no mbs

Context **[Tree]** (config>service>apipe>sap>egress>policer-over>plcr mbs)
[Tree] (config>service>apipe>sap>ingress>policer-over>plcr mbs)
[Tree] (config>service>cpipe>sap>egress>policer-over>plcr mbs)
[Tree] (config>service>cpipe>sap>ingress>policer-over>plcr mbs)
[Tree] (config>service>ipipe>sap>egress>policer-over>plcr mbs)
[Tree] (config>service>ipipe>sap>ingress>policer-over>plcr mbs)
[Tree] (config>service>epipe>sap>egress>policer-over>plcr mbs)
[Tree] (config>service>epipe>sap>ingress>policer-over>plcr mbs)

Full Context configure service apipe sap egress policer-override policer mbs
configure service apipe sap ingress policer-override policer mbs
configure service cpipe sap egress policer-override policer mbs
configure service cpipe sap ingress policer-override policer mbs
configure service epipe sap egress policer-override policer mbs
configure service epipe sap ingress policer-override policer mbs
configure service ipipe sap egress policer-override policer mbs
configure service ipipe sap ingress policer-override policer mbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured mbs parameter for the specified policer-id.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command is used to restore the MBS to the default value. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

Default no mbs

Parameters *size* — The size parameter is required when specifying mbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

bytes — When **bytes** is defined, the value given for *size* is interpreted as the policer MBS value in bytes.

kilobytes — When **kilobytes** is defined, the value given for *size* is interpreted as the policer MBS value in kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress policer-override policer mbs
- configure service cpipe sap ingress policer-override policer mbs

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service epipe sap egress policer-override policer mbs
- configure service ipipe sap ingress policer-override policer mbs
- configure service epipe sap ingress policer-override policer mbs
- configure service ipipe sap egress policer-override policer mbs

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap egress policer-override policer mbs
- configure service apipe sap ingress policer-override policer mbs

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue mbs)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue mbs)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue mbs)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue mbs)
[Tree] (config>service>epipe>sap>egress>queue-override>queue mbs)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue mbs)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue mbs)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>fpipe>sap>ingress>queue-override>queue mbs)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue mbs)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue mbs)

Full Context
configure service apipe sap egress queue-override queue mbs
configure service apipe sap ingress queue-override queue mbs
configure service cpipe sap egress queue-override queue mbs
configure service cpipe sap ingress queue-override queue mbs
configure service epipe sap egress queue-override queue mbs
configure service epipe sap ingress queue-override queue mbs
configure service fpipe sap egress queue-override queue mbs
configure service fpipe sap ingress queue-override queue mbs
configure service ipipe sap egress queue-override queue mbs
configure service ipipe sap ingress queue-override queue mbs

Description
This command overrides specific attributes of the specified queue's MBS parameters. A queue uses its MBS value to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the number of buffers allowed by the MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope associated with a packet. A queue that has not exceeded its MBS is not guaranteed to have buffer available when needed or that the packet's RED slope will not force the discard of the packet. Setting correct CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

The **no** form of this command returns the MBS assigned to the queue to the default value.

Default
mbs default

Parameters
size — The size parameter is an integer expression of the maximum number of kilobytes or bytes of buffering allowed for the queue. A value of 0 causes the queue to discard all packets.

Values 0 to 1073741824, default

bytes — Indicates that the *size* parameter value is expressed in bytes.

kilobytes — Indicates that the *size* parameter is expressed in kilobytes.

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress queue-override queue mbs
- configure service cpipe sap ingress queue-override queue mbs
- configure service fpipe sap ingress queue-override queue mbs
- configure service fpipe sap egress queue-override queue mbs

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe sap egress queue-override queue mbs
- configure service apipe sap ingress queue-override queue mbs

All

- configure service epipe sap egress queue-override queue mbs
- configure service epipe sap ingress queue-override queue mbs
- configure service ipipe sap egress queue-override queue mbs
- configure service ipipe sap ingress queue-override queue mbs

mbs

Syntax **mbs** *size* [{**bytes** | **kilobytes**}]
no mbs

Context **[Tree]** (config>service>vpls>sap>egress>policer-override>plcr mbs)
[Tree] (config>service>vpls>sap>ingress>policer-override>plcr mbs)

Full Context configure service vpls sap egress policer-override policer mbs
configure service vpls sap ingress policer-override policer mbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured mbs parameter for the specified policer-id.

The **no** form of this command restores the MBS to the default value. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

Default no mbs

Parameters *size* — This parameter is required when specifying MBS override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs

Syntax **mbs** *size* [{**bytes** | **kilobytes**}]
no mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>egress>policer-override>plcr mbs)
[Tree] (config>service>ies>if>sap>ingress>policer-override>plcr mbs)

Full Context configure service ies interface sap egress policer-override policer mbs
configure service ies interface sap ingress policer-override policer mbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured mbs parameter for the specified policer-id.

The **no** form of this command restores the MBS setting to the default value. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

Default no mbs

Parameters *size* — This parameter is required when specifying MBS override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs

Syntax **mbs** *size* [{**bytes** | **kilobytes**}]
no mbs

Context [Tree] (config>service>vprn>if>sap>egress>policer-override>plcr mbs)
[Tree] (config>service>vprn>if>sap>ingress>policer-override>plcr mbs)

Full Context configure service vprn interface sap egress policer-override policer mbs
configure service vprn interface sap ingress policer-override policer mbs

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured mbs parameter for the specified policer-id.

The **no** form of this command restores the MBS to the default value. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

Default no mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — This parameter is required when specifying MBS override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 2683435456, **default**

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue mbs)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue mbs)

Full Context configure service vprn interface sap egress queue-override queue mbs
configure service vprn interface sap ingress queue-override queue mbs

Description This command can be used to override specific attributes of the specified queue's MBS parameters. The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet's RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The **no** form of this command returns the MBS size assigned to the queue to the value.

Default mbs default

Parameters *size* — The size parameter is required when specifying **mbs** and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **bytes** and **kilobytes** keywords are mutually exclusive and are used to explicitly define whether the size represents bytes or kilobytes.

Values 0 to 1073741824
default

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bytes — When **byte** is defined, the value given for size is interpreted as the queue'sMBS value given in bytes.

kilobytes — When **kilobytes** is defined, the value is interpreted as the queue's MBSvalue given in kilobytes.

default — Specifying the keyword **default** sets the MBS to its default value.

Platforms All

mbs

Syntax **mbs** *congested-mbs*
no mbs

Context **[Tree]** (config>app-assure>group>policer>congestion-override mbs)

Full Context configure application-assurance group policer congestion-override mbs

Description This command configures the maximum burst size for the policer. It is recommended that MBS is configured larger than twice the MTU for the traffic handled by the policer to allow for some burstiness of the traffic. MBS is configurable for single-bucket, dual-bucket bandwidth and flow setup rate policers only.

The **no** form of this command removes the congested MBS value from the configuration.

Default mbs 0

Parameters *congested-mbs* — Specifies the maximum burst size, in kbytes, when the access-network-level, which the subscriber belongs to, is in a congested state.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mbs

Syntax **mbs** *maximum-burst-size*
no mbs

Context **[Tree]** (config>app-assure>group>tod-override mbs)

Full Context configure application-assurance group tod-override mbs

Description This command provides a mechanism to configure the maximum burst size for the policer. It is recommended that MBS is configured larger than twice the MTU for the traffic handled by the policer to allow for some burstiness of the traffic. MBS is configurable for single-bucket, dual-bucket bandwidth and flow setup rate policers only.

The **no** form of this command resets the MBS value to its default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default mbs 0

Parameters *maximum-burst-size* — Specifies an integer value defining either size, in kbytes, for the MBS of the bandwidth policer, or flow count for the MBS of the flow setup rate policers.

Values 0 to 131071

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>qos>sap-ingress>dyn-policer mbs)
[Tree] (config>qos>sap-egress>dyn-policer mbs)
[Tree] (config>qos>sap-ingress>policer mbs)
[Tree] (config>qos>sap-egress>policer mbs)

Full Context configure qos sap-egress dynamic-policer mbs
configure qos sap-egress policer mbs
configure qos sap-ingress dynamic-policer mbs
configure qos sap-ingress policer mbs

Description This command is used to configure the policer's PIR leaky bucket's high-priority violate threshold. The **high-prio-only** command is applied to the MBS value to derive the bucket's low-priority violate threshold. For ingress, trusted in-profile packets and untrusted high-priority packets use the policer's high-priority violate threshold while trusted out-of-profile and untrusted low-priority packets use the policer's low-priority violate threshold. At egress, inplus-profile, and in-profile packets use the policer's high-priority violate threshold and out-of-profile packets use the policer's low-priority violate threshold. Exceed-profile packets are discarded unless **enable-exceed-pir** is configured, in which case they are forwarded.

The PIR bucket's violate threshold represents the maximum burst tolerance allowed by the policer. If the policer's offered rate is equal to or less than the policer's defined rate, the PIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the offered rate increases beyond the metering rate, the amount of data allowed above the rate is capped by the threshold. The low-priority violate threshold provides a smaller burst size for the lower priority traffic associated with the policer. Since all lower priority traffic is discarded at the lower burst tolerance size, the remaining burst tolerance defined by **high-prio-only** is available for the higher priority traffic.

The policer's MBS size defined in the QoS policy may be overridden on an SLA profile or SAP where the policy is applied.

The **no** form of this command returns the queue to its default MBS size. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* **[bytes | kilobytes]** — The *size* parameter is required when specifying **mbs** and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **bytes** and **kilobytes** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 – 2683435456, **default**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure qos sap-ingress dynamic-policer mbs
- configure qos sap-egress dynamic-policer mbs

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-ingress policer mbs
- configure qos sap-egress policer mbs

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>qos>sap-egress>queue mbs)
[Tree] (config>qos>sap-ingress>queue mbs)

Full Context configure qos sap-egress queue mbs
configure qos sap-ingress queue mbs

Description This command configures the maximum number of buffers allowed for a specific queue. The value is given in bytes or kilobytes and overrides the default value for the context.

The **no** form of this command returns the policer to its default MBS.

Default no mbs

Parameters *size* — The *size* parameter is required when specifying **mbs** and is expressed as an integer representing the required size in either bytes or kilobytes.

Default **kilobyte**

default — Sets the MBS to its default value.

bytes — Specifies that the value given for size is interpreted as the queue's MBS value given in bytes.

Values 0 to 2688000

kilobytes — Specifies the value is interpreted as the queue's MBS value given in kilobytes.

Values 0 to 2625

Default kilobytes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

mbs

Syntax **mbs** *percent*
no mbs

Context **[Tree]** (config>qos>network-queue>queue mbs)

Full Context configure qos network-queue queue mbs

Description This command specifies the relative amount of buffer pool space for the maximum buffers for a specific ingress network FP forwarding class queue or egress network port forwarding class queue. The value is entered as a percentage.

The MBS value is used by a queue to determine whether it has exhausted its total allowed buffers while enqueuing packets. When the queue has exceeded its maximum amount of buffers, all packets are discarded until the queue transmits a packet. A queue that has not exceeded its MBS is not guaranteed to have a buffer available when needed or that the packet's RED slope will not force the discard of the packet. In order to safeguard against queue starvation (when a queue does not receive its fair share of buffers), set proper CBS parameters and control CBS oversubscription. Another safeguard is to properly set the RED slope parameters for the needs of the network queues.

The MBS can sometimes be smaller than the CBS. This will result in a portion of the CBS for the queue to be unused and should be avoided.

The **no** form of this command returns the MBS for the queue to the default for the forwarding class.

Special Cases **Forwarding Class Queue on Egress Network Port or Channel —** For network egress, each forwarding class is supported by an egress queue on a per network port basis. These forwarding class-based queues are automatically created when a port or channel is placed in network mode. The configuration parameters for each queue come from the applied egress policy on the network port or channel. Forwarding class queue on egress channel applies only to the 7450 ESS and 7750 SR.

The **mbs** value is used to calculate the queue's MBS size based on the total amount buffer space allocated for the buffer pool on the egress network port or channel. This buffer pool size will dynamically fluctuate based on the port or channels egress pool size setting.

The total MBS settings for all network egress queues on the port or channel based on the total percentages can exceed 100 percent. Some over-subscription can be desirable to allow exceptionally busy forwarding classes more access to buffer space. The proper use of CBS settings will ensure that oversubscribing MBS settings will not starve other queues of buffers when needed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Forwarding Class Queue on Ingress FP — For network ingress, each forwarding class is supported by an ingress queue per FP. These forwarding class queues are automatically created when a single port or channel is placed in the network mode on the FP and are removed when all network ports or channels are removed from the FP (defined as access). The configuration parameters for each queue come from the applied ingress policy under the network context of the FP.

The **mbs** value is used to calculate the queue's MBS size based on the total amount buffer space allocated for the network ingress buffer pool on the FP. This buffer pool will dynamically fluctuate based on the sum of all ingress pool sizes for all network ports and channels on the FP.

The total MBS settings for all network egress queues on the port or channel based on the total percentages can exceed 100 percent. Some over-subscription can be desirable to allow exceptionally busy forwarding classes more access to buffer space. The proper use of CBS settings will ensure that oversubscribing MBS settings will not starve other queues of buffers when needed.

Parameters *percent* — The percent of buffers from the total buffer pool space for the maximum number of buffers, expressed as a decimal integer. If 10 Mbytes is the total buffer space in the buffer pool, a value of 10 would limit the maximum queue size to 1 Mbyte (10%) of buffer space for the forwarding class queue. If the total size is increased to 20 Mbytes, the existing value of 10 would automatically increase the maximum size of the queue to 2 Mbytes.

Values 0 to 100

Platforms All

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer mbs)
[Tree] (config>qos>qgrps>ing>qgrp>policer mbs)

Full Context configure qos queue-group-templates egress queue-group policer mbs
configure qos queue-group-templates ingress queue-group policer mbs

Description This command specifies the default maximum buffer size for the template queue in bytes or kilobytes.

The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. When the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The **port>ethernet>access>ingress>queue-group** and **port>ethernet>access>egress>queue-group** contexts for **mbs** provides a mechanism for overriding the default maximum size for the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope that a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet's RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard against queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

When configured on an egress queue group queue, this command and the **queue-delay** command are mutually exclusive. In order to change between the **mbs** and **queue-delay** parameters, the current parameter must be removed before adding the new parameter; that is, changing from **mbs** to **queue-delay** requires a **no mbs** before the **queue-delay** is configured and changing from **queue-delay** to **mbs** requires a **no queue-delay** before the **mbs** is configured. If **queue-delay** is configured for an egress queue group queue, it is not possible to override the MBS for that queue.

For policers, this command is used to configure the policer's PIR leaky bucket's high-priority violate threshold. The **high-prio-only** command is applied to the MBS value to derive the bucket's low-priority violate threshold.

At ingress, trusted in-profile packets and untrusted high-priority packets use the policer's high-priority violate threshold while trusted out-of-profile and untrusted low-priority packets use the policer's low-priority violate threshold.

At egress, inplus-profile and in-profile packets use the policer's high-priority violate threshold and out-of-profile packets use the policer's low-priority violate threshold. Exceed-profile packets are discarded unless **enable-exceed-pir** is configured, in which case they are forwarded.

The PIR bucket's violate threshold represents the maximum burst tolerance allowed by the policer. If the policer's offered rate is equal to or less than the policer's defined rate, the PIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the offered rate increases beyond the metering rate, the amount of data allowed above the rate is capped by the threshold. The low-priority violate threshold provides a smaller burst size for the lower priority traffic associated with the policer. Since all lower priority traffic is discarded at the lower burst tolerance size, the remaining burst tolerance defined by high-prio-only is available for the higher priority traffic.

The policer's mbs size defined in the QoS policy may be overridden on an SLA profile or SAP where the policy is applied.

The **no** form of this command returns the MBS size to its default value. By default, the MBS is 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicit configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

Default default

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — For queues, the size parameter is an integer expression of the maximum number of bytes or kilobytes of buffering allowed for the queue. For a value of 100 kbytes, enter the value 100. A value of 0 causes the queue to discard all packets. For policers, the size parameter is an integer expression of the maximum number of bytes for the policer's MBS. The queue MBS maximum value used is constrained by the pool size in which the queue exists and by the shared pool space in the corresponding megapool.

Values 0 to 2683435456

Default value: 16 Mbytes when PIR equals max or is greater than or equal to the FP capacity (this overrides an explicitly configured MBS value); otherwise, 10 ms volume of traffic for a configured non-zero/non-max PIR capped to 3968 kbytes, with a minimum of 256 bytes.

[bytes | kilobytes] — Select bytes or kilobytes.

Default kilobytes

default — Sets the MBS to its default value.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs

Syntax **mbs** {*size* [**bytes** | **kilobytes**] | **default**}
no mbs

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue mbs)
[Tree] (config>qos>qgrps>ing>qgrp>queue mbs)

Full Context configure qos queue-group-templates egress queue-group queue mbs
configure qos queue-group-templates ingress queue-group queue mbs

Description This command specifies the default maximum buffer size for the template queue in bytes or kilobytes.

The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. When the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The **port>ethernet>access>ingress>queue-group** and **port>ethernet>access>egress>queue-group** contexts for **mbs** provides a mechanism for overriding the default maximum size for the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope that a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet's RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard against queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

When configured on an egress queue group queue, this command and the **queue-delay** command are mutually exclusive. In order to change between the **mbs** and **queue-delay** parameters, the current parameter must be removed before adding the new parameter; that is, changing from **mbs** to **queue-delay** requires a **no mbs** before the **queue-delay** is configured and changing from **queue-delay** to **mbs** requires a **no queue-delay** before the **mbs** is configured. If **queue-delay** is configured for an egress queue group queue, it is not possible to override the MBS for that queue.

For policers, this command is used to configure the policer's PIR leaky bucket's high-priority violate threshold. The **high-prio-only** command is applied to the MBS value to derive the bucket's low-priority violate threshold.

At ingress, trusted in-profile packets and untrusted high-priority packets use the policer's high-priority violate threshold while trusted out-of-profile and untrusted low-priority packets use the policer's low-priority violate threshold.

At egress, inplus-profile and in-profile packets use the policer's high-priority violate threshold and out-of-profile packets use the policer's low-priority violate threshold. Exceed-profile packets are discarded unless **enable-exceed-pir** is configured, in which case they are forwarded.

The PIR bucket's violate threshold represents the maximum burst tolerance allowed by the policer. If the policer's offered rate is equal to or less than the policer's defined rate, the PIR bucket depth hovers around the 0 depth with spikes up to the maximum packet size in the offered load. If the offered rate increases beyond the metering rate, the amount of data allowed above the rate is capped by the threshold. The low-priority violate threshold provides a smaller burst size for the lower priority traffic associated with the policer. Since all lower priority traffic is discarded at the lower burst tolerance size, the remaining burst tolerance defined by high-prio-only is available for the higher priority traffic.

The policer's mbs size defined in the QoS policy may be overridden on an SLA profile or SAP where the policy is applied.

The **no** form of this command returns the MBS size assigned by the queue.

Default default

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — For queues, the size parameter is an integer expression of the maximum number of bytes or kilobytes of buffering allowed for the queue. For a value of 100 kbytes, enter the value 100. A value of 0 causes the queue to discard all packets. For policers, the size parameter is an integer expression of the maximum number of bytes for the policer's MBS. The queue MBS maximum value used is constrained by the pool size in which the queue exists and by the shared pool space in the corresponding megapool.

Values 0 to 1048576 or **default**

Minimum configurable non-zero value: 6 kbytes on an FP2, 7680 bytes on an FP3, and 16 kbytes on an FP4

Minimum non-zero default value: maximum of 10 ms of CIR, or 6 kbytes on an FP2, 7680 bytes on an FP3, and 16 kbytes on an FP4

[bytes | kilobytes] — Select bytes or kilobytes.

Default kilobytes

default — Sets the MBS to its default value.

Platforms All

mbs

Syntax **mbs** *percent*
no mbs

Context **[Tree]** (config>qos>shared-queue>queue mbs)

Full Context configure qos shared-queue queue mbs

Description This command specifies the relative amount of the buffer pool space for the maximum buffers for a specific ingress shared queue.

The MBS value is used by a queue to determine whether it has exhausted its total allowed buffers while enqueuing packets. When the queue has exceeded its maximum amount of buffers, all packets are discarded until the queue transmits a packet. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard against queue starvation (when a queue does not receive its fair share of buffers).

The MBS size can sometimes be smaller than the CBS. This will result in a portion of the CBS for the queue to be unused and should be avoided.

Default The queue MBS defaults are listed in Table 96.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 96 **Queue MBS Default Values**

Queue	Default MBS
1	50
2	50
3	50
4	25
5	50
6	50
7	25
8	25
9	50
10	50
11	50
12	25
13	50
14	50
15	25
16	25

Parameters *percent* — The percent of buffers from the total buffer pool space for the maximum amount of buffers, expressed as a decimal integer.

Values 0 to 100

Platforms All

mbs

Syntax **mbs** *mbs*
no mbs

Context **[Tree]** (config>system>security>cpm-queue>queue mbs)

Full Context configure system security cpm-queue queue mbs

Description This command specifies the maximum queue depth to which a queue can grow.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mbs* — Specifies the maximum burst size in kbytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.160 mbs-contribution

mbs-contribution

Syntax **mbs-contribution** *size* [**bytes** | **kilobytes**] [**fixed**]
no mbs-contribution

Context **[Tree]** (config>subscr-mgmt>sub-prof>ing>plcr-ctrl-plcy>mbs-thrshlds>prio mbs-contribution)
[Tree] (config>subscr-mgmt>sub-prof>egr>plcr-ctrl-plcy>mbs-thrshlds>prio mbs-contribution)

Full Context configure subscriber-mgmt sub-profile egress policer-control-policy priority-mbs-thresholds priority mbs-contribution
configure subscriber-mgmt sub-profile ingress policer-control-policy priority-mbs-thresholds priority mbs-contribution

Description The **mbs-contribution** command is used to configure the policy-based burst tolerance for a parent policer instance created when the policy is applied to a SAP or subscriber context. The system uses the parent policer's **min-thresh-separation** value, the priority level's **mbs-contribution** value and the number of child policers currently attached to the priority level to derive the priority level's shared-portion and fair-portion of burst tolerance within the local priority level. The shared-portion and fair-portions for each priority level are then used by the system to calculate each priority level's discard-unfair threshold and discard-all threshold.

The value for a priority level's **mbs-contribution** within the policer-control-policy may be overridden on the SAP or subscriber sub-profile where the policy is applied in order to allow fine tuning of the discard-unfair and discard-all thresholds relevant to the needs of the local child policers on the object.

Accumulative Nature of Burst Tolerance for a Parent Policer Priority Level

When defining **mbs-contribution**, the specified size may only be a portion of the burst tolerance associated with the priority level. The packets associated with the priority level share the burst tolerance of lower within the parent policer. As the parent policer PIR bucket depth increases during congestion, the lower priority packets eventually experience discard based on each priority's discard-unfair and discard-all thresholds. Assuming congestion continues once all the lower priority packets have been prevented from consuming bucket depth, the burst tolerance for the priority level is consumed by its own packets and any packets associated with higher priorities.

The Effect of Fair and Unfair Child Policer Traffic at a Parent Policer Priority Level

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The system continually monitors the offered rate of each child policer on each parent policer priority level and detects when the policer is in a congested state (the aggregate offered load is greater than the decrement rate defined on the parent policer). As previously stated, the result of congestion is that the parent policer's bucket depth will increase until it eventually hovers around either a discard-unfair or discard-all threshold belonging to one of the priority levels. This threshold is the point where enough packets are being discarded that the increment rate and decrement rate begin to even out. If only a single child policer is associated to the priority level, the discard-unfair threshold is not used since fairness is only applicable when multiple child policers are competing at the same priority level.

When multiple child policers are sharing the congested priority level, the system uses the offered rates and the parenting parameters of each child to determine the fair rate per child when the parent policer is unable to meet the bandwidth needs of each child. The fair rate represents the number of bandwidth that each child at the priority level should receive relative to the other children at the same level according to the policer control policy instance managing the child policers. This fair rate is applied as the decrement rate for each child's FIR bucket. Changing a child’s FIR rate does not modify the number of packets forwarded by the parent policer for the child’s priority level. It simply modifies the forwarded ratio between the children on that priority level. Since each child FIR bucket has some level of burst tolerance before marking its packets as unfair, the current parent policer bucket depth may at times rise above the discard-unfair threshold. The mbs-contribution value provides a means to define how much separation is provided between the priority level’s discard-unfair and discard-all threshold to allow the parent policer to absorb some of the FIR burst before reaching the priority’s discard-all threshold.

This level of fair aggregate burst tolerance is based on the decrement rate of the parent policer’s PIR bucket while the individual fair bursts making up the aggregate are based on each child’s FIR decrement rate. The aggregate fair rate of the priority level is managed by the system with consideration of the current rate of traffic in higher priority levels. In essence, the system ensures that for each iteration of the child FIR rate calculation, the sum of the child FIR decrement rates plus the sum of the higher priority traffic increment rates equals the parent policers decrement rate. This means that dynamic numbers of higher priority traffic can be ignored when sizing a lower priority’s fair aggregate burst tolerance. Consider the following:

- The parent policer decrement rate is set to 20 Mb/s (max-rate 20,000).
- A priority level’s fair burst size is set to 30 kbytes (mbs-contribution 30 kbytes).
- Higher priority traffic is currently taking 12 Mb/s.
- The priority level has three child policers attached.
- Each child’s PIR MBS is set to 10 kbytes, which makes each child’s FIR MBS 10 kbytes.
- The children want 10 Mb/s, but only 8 Mb/s is available,
- Based on weights, the children's FIR rates are set as follows:

	FIR Rate	**FIR MBS**
Child 1	4 Mb/s	10 kbytes
Child 2	3 Mb/s	10 kbytes
Child 3	1 Mb/s	10 kbytes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The 12 Mb/s of the higher priority traffic and the 8 Mb/s of fair traffic equal the 20 Mb/s decrement rate of the parent policer.

It is clear that the higher priority traffic is consuming 12 Mb/s of the parent policer's decrement rate, leaving 8 Mb/s of decrement rate for the lower priority's fair traffic.

- The burst tolerance of child 1 is based on 10 kbytes above 4 Mb/s,
- The burst tolerance of child 2 is based on 10 kbytes above 3 Mb/s,
- The burst tolerance of child 3 is based on 10 kbytes above 1 Mb/s.

If all three children burst simultaneously (unlikely), they will consume 30 kbytes above 8 Mb/s. This is the same as the remaining decrement rate after the higher priority traffic.

Parent Policer Total Burst Tolerance and Downstream Buffering

The highest in-use priority level's discard-all threshold is the total burst tolerance of the parent policer. In some cases the parent policer represents downstream bandwidth capacity and the max-rate of the parent policer is set to prevent overrunning the downstream bandwidth. The burst tolerance of the parent policer defines how much more traffic may be sent beyond the downstream scheduling capacity. In the worst case scenario, when the downstream buffering is insufficient to handle the total possible burst from the parent policer, downstream discards based on lack of buffering may occur. However, in all likelihood, this is not the case.

In most cases, lower priority traffic in the policer is responsible for the greater part of congestion above the parent policer rate. Since this traffic is discarded with a lower threshold, this lowers the effective burst tolerance even while the highest priority traffic is present.

Configuring a Priority Level's MBS Contribution Value

In the most conservative case, a priority level's **mbs-contribution** value may be set to be greater than the sum of child policer's mbs and one max-size-frame per child policer. This ensures that even in the absolute worst case where all the lower priority levels are simultaneously bursting to the maximum capacity of each child, enough burst tolerance for the priority's children will exist if they also burst to their maximum capacity.

Since simply adding up all the child policer's PIR MBS values may result in large overall burst tolerances that are not ever likely to be needed, you should consider some level of burst oversubscription when configuring the **mbs-contribution** value for each priority level. The number of oversubscription should be determined based on the needs of each priority level.

Using the Fixed Keyword to Create Deterministic Parent Policer Discard Thresholds

In the default behavior, the system ignores the **mbs-contribution** values for a priority level on a subscriber or SAP parent policer when a child policer is not currently associated with the level. This prevents additional burst tolerance from being added to higher priority traffic within the parent policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This does cause fluctuations in the defined threshold values when child policers are added or removed from a parent policer instance. If this behavior is undesirable, the fixed keyword may be used which causes the **mbs-contribution** value to always be included in the calculation of parent policer's discard thresholds. The defined **mbs-contribution** value may be overridden on a subscriber sla-profile or on a SAP instance, but the fixed nature of the contribution cannot be overridden.

If the defined **mbs-contribution** value for the priority level is zero, the priority level will have no effect on the parent policer's defined discard thresholds. A packet associated with the priority level will use the next lower priority level's discard-unfair and discard-all thresholds.

The **no mbs-contribution** command returns the policy's priority level's MBS contribution to the default value. When changed, the thresholds for the priority level and all higher priority levels for all instances of the parent policer is recalculated.

Parameters *size* [**bytes** | **kilobytes**] — The size parameter is required when executing the **mbs-contribution** command. It is expressed as an integer and specifies the priority's specific portion of accumulative MBS for the priority level in bytes or kilobytes which is selected by the trailing **bytes** or **kilobytes** keywords. If both **bytes** and **kilobytes** are missing, **kilobytes** is assumed. Setting this value has no effect on parent policer instances where the priority level's **mbs-contribution** value has been overridden.

Values 0 to 16777216

bytes | **kilobytes**: — The **bytes** keyword is optional and is mutually exclusive with the **kilobytes** keyword. When specified, size is interpreted as specifying the size of **min-thresh-separation** in bytes.

The **kilobytes** keyword is optional and is mutually exclusive with the **bytes** keyword. Size is interpreted as specifying the size of min-thresh-separation in kilobytes.

Default **kilobytes**

fixed — This optional fixed keyword is used to force the inclusion of the defined **mbs-contribution** value in the parent policer's discard threshold calculations. If the **mbs-contribution** command is executed without the **fixed** keyword, the fixed calculation behavior for the priority level is removed.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mbs-contribution

Syntax **mbs-contribution** *size* [**bytes** | **kilobytes**]
no mbs-contribution

Context **[Tree]** (config>card>fp>ingress>access>qgrp>policer-ctrl-over>mbs-thrshlds>prio mbs-contribution)
[Tree] (config>card>fp>ing>network>qgrp>policer-ctrl-over>mbs-thrshlds>prio mbs-contribution)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure card fp ingress network queue-group policer-control-override priority-mbs-thresholds priority mbs-contribution
configure card fp ingress access queue-group policer-control-override priority-mbs-thresholds priority mbs-contribution

Description This command configures the policy-based burst tolerance for a parent policer instance created when the policy is applied to a SAP or subscriber context. The system uses the parent policer's **min-thresh-separation** value, the priority level's **mbs-contribution** value and the number of child policers currently attached to the priority level to derive the priority level's shared-portion and fair-portion of burst tolerance within the local priority level. The shared-portion and fair-portions for each priority level are then used by the system to calculate each priority level's discard-unfair threshold and discard-all threshold.

The value for a priority level's **mbs-contribution** within the policer-control-policy may be overridden on the SAP or subscriber sub-profile where the policy is applied in order to allow fine tuning of the discard-unfair and discard-all thresholds relevant to the needs of the local child policers on the object.

Accumulative Nature of Burst Tolerance for a Parent Policer Priority Level

When defining **mbs-contribution**, the specified size may only be a portion of the burst tolerance associated with the priority level. The packets associated with the priority level share the burst tolerance of lower within the parent policer. As the parent policer PIR bucket depth increases during congestion, the lower priority packets eventually experience discard based on each priority's discard-unfair and discard-all thresholds. Assuming congestion continues once all the lower priority packets have been prevented from consuming bucket depth, the burst tolerance for the priority level will be consumed by its own packets and any packets associated with higher priorities.

The Effect of Fair and Unfair Child Policer Traffic at a Parent Policer Priority Level

The system continually monitors the offered rate of each child policer on each parent policer priority level and detects when the policer is in a congested state (the aggregate offered load is greater than the decrement rate defined on the parent policer). As previously stated, the result of congestion is that the parent policer's bucket depth will increase until it eventually hovers around either a discard-unfair or discard-all threshold belonging to one of the priority levels. This threshold is the point where enough packets are being discarded that the increment rate and decrement rate begin to even out. If only a single child policer is associated to the priority level, the discard-unfair threshold is not used since fairness is only applicable when multiple child policers are competing at the same priority level.

When multiple child policers are sharing the congested priority level, the system uses the offered rates and the parenting parameters of each child to determine the fair rate per child when the parent policer is unable to meet the bandwidth needs of each child. The fair rate represents the amount of bandwidth that each child at the priority level should receive relative to the other children at the same level according to the policer control policy instance managing the child policers. This fair rate is applied as the decrement rate for each child's FIR bucket. Changing a child's FIR rate does not modify the amount of packets forwarded by the parent policer for the child's priority level. It simply modifies the forwarded ratio between the children on that priority level. Since each child FIR bucket has some level of burst

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tolerance before marking its packets as unfair, the current parent policer bucket depth may at times rise above the discard-unfair threshold. The mbs-contribution value provides a means to define how much separation is provided between the priority level's discard-unfair and discard-all threshold to allow the parent policer to absorb some amount of FIR burst before reaching the priority's discard-all threshold.

This level of fair aggregate burst tolerance is based on the decrement rate of the parent policer's PIR bucket while the individual fair bursts making up the aggregate are based on each child's FIR decrement rate. The aggregate fair rate of the priority level is managed by the system with consideration of the current rate of traffic in higher priority levels. In essence, the system ensures that for each iteration of the child FIR rate calculation, the sum of the child FIR decrement rates plus the sum of the higher priority traffic increment rates equals the parent policers decrement rate. This means that dynamic amounts of higher priority traffic can be ignored when sizing a lower priority's fair aggregate burst tolerance. Consider the following:

- The parent policer decrement rate is set to 20 Mb/s (max-rate 20,000).
- A priority level's fair burst size is set to 30 kbytes (mbs-contribution 30 kilobytes).
- Higher priority traffic is currently taking 12 Mb/s.
- The priority level has three child policers attached.
- Each child's PIR MBS is set to 10 kbytes, which makes each child's FIR MBS 10 kbytes.
- The children want 10 Mb/s, but only 8 Mb/s is available,
- Based on weights, the children's FIR rates are set as follows:

	FIR Rate	**FIR MBS**
Child 1	4 Mb/s	10 kbytes
Child 2	3 Mb/s	10 kbytes
Child 3	1 Mb/s	10 kbytes

The 12 Mb/s of the higher priority traffic and the 8 Mb/s of fair traffic equal the 20 Mb/s decrement rate of the parent policer.

It is clear that the higher priority traffic is consuming 12 Mb/s of the parent policer's decrement rate, leaving 8 Mb/s of decrement rate for the lower priority's fair traffic.

- The burst tolerance of child 1 is based on 10 kbytes above 4 Mb/s,
- The burst tolerance of child 2 is based on 10 kbytes above 3 Mb/s,
- The burst tolerance of child 3 is based on 10 kbytes above 1 Mb/s.

If all three children burst simultaneously (unlikely), they will consume 30 kbytes above 8 Mb/s. This is the same as the remaining decrement rate after the higher priority traffic.

Parent Policer Total Burst Tolerance and Downstream Buffering

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The highest in-use priority level's discard-all threshold is the total burst tolerance of the parent policer. In some cases the parent policer represents downstream bandwidth capacity and the max-rate of the parent policer is set to prevent overrunning the downstream bandwidth. The burst tolerance of the parent policer defines how much more traffic may be sent beyond the downstream scheduling capacity. In the worst case scenario, when the downstream buffering is insufficient to handle the total possible burst from the parent policer, downstream discards based on lack of buffering may occur. However, in all likelihood, this is not the case.

In most cases, lower priority traffic in the policer will be responsible for the greater part of congestion above the parent policer rate. Since this traffic is discarded with a lower threshold, this lowers the effective burst tolerance even while the highest priority traffic is present.

Configuring a Priority Level's MBS Contribution Value

In the most conservative case, a priority level's **mbs-contribution** value may be set to be greater than the sum of child policer's MBS and one max-size-frame per child policer. This ensures that even in the absolute worst case where all the lower priority levels are simultaneously bursting to the maximum capacity of each child, enough burst tolerance for the priority's children will exist if they also burst to their maximum capacity.

Since simply adding up all the child policer's PIR MBS values may result in large overall burst tolerances that are not ever likely to be needed, you should consider some level of burst oversubscription when configuring the **mbs-contribution** value for each priority level. The amount of oversubscription should be determined based on the needs of each priority level.

Using the Fixed Keyword to Create Deterministic Parent Policer Discard Thresholds

In the default behavior, the system ignores the **mbs-contribution** values for a priority level on a subscriber or SAP parent policer when a child policer is not currently associated with the level. This prevents additional burst tolerance from being added to higher priority traffic within the parent policer.

This does cause fluctuations in the defined threshold values when child policers are added or removed from a parent policer instance. If this behavior is undesirable, the fixed keyword may be used which causes the **mbs-contribution** value to always be included in the calculation of parent policer's discard thresholds. The defined **mbs-contribution** value may be overridden on a subscriber SLA profile or on a SAP instance, but the fixed nature of the contribution cannot be overridden.

If the defined **mbs-contribution** value for the priority level is zero, the priority level will have no effect on the parent policer's defined discard thresholds. A packet associated with the priority level will use the next lower priority level's discard-unfair and discard-all thresholds.

The **no** form of this command reverts to the policy's priority level's MBS contribution to the default value. When changed, the thresholds for the priority level and all higher priority levels for all instances of the parent policer are recalculated.

Default no mbs-contribution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — Specifies that the size parameter is required when executing the **mbs-contribution** command. It is expressed as an integer and specifies the priority's specific portion amount of accumulative MBS for the priority level in bytes or kilobytes which is selected by the trailing **bytes** or **kilobytes** keywords. If both **bytes** and **kilobytes** are missing, **kilobytes** is assumed. Setting this value has no effect on parent policer instances where the priority level's **mbs-contribution** value has been overridden. Clearing an override on parent policer instance causes this value to be enforced.

Values 0 to 16777216

bytes, kilobytes — Specifies that the **bytes** keyword is optional and is mutually exclusive with the **kilobytes** keyword. When specified, size is interpreted as specifying the size of **min-thresh-separation** in bytes.

The **kilobytes** keyword is optional and is mutually exclusive with the **bytes** keyword. When specified, size is interpreted as specifying the size of min-thresh-separation in kilobytes.

Default **kilobytes**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs-contribution

Syntax **mbs-contribution** *size* [**bytes** | **kilobytes**]

Context **[Tree]** (config>service>apipe>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>apipe>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>cpipe>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>cpipe>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>epipe>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>epipe>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>fpipe>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>fpipe>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>ipipe>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>ipipe>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)

Full Context configure service apipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service apipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service cpipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service cpipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service epipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service epipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service fpipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service fpipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service ipipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service ipipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution

Description The mbs-contribution override command within the SAP ingress and egress contexts is used to override a parent policer's priority level's mbs-contribution parameter that is defined within the policer-control-policy applied to the SAP. This override allow the priority level's burst tolerance to be tuned based on the needs of the SAP's child policers attached to the priority level.

When the override is defined, modifications to the policer-control-policy priority level's mbs-contribution parameter have no effect on the SAP's parent policer priority level until the override is removed using the no mbs-contribution command within the SAP.

The **no** form of this command removes the override and allows the mbs-contribution setting from the policer-control-policy to control the parent policer's priority level's burst tolerance.

Default no mbs-contribution

Parameters *size* — The mbs-contribution override value.

Values 1 to 16777216 | default

bytes — Signifies that *size* is expressed in bytes. The bytes and kilobytes keywords are mutually exclusive and optional. The default is kilobytes.

kilobytes — Signifies that *size* is expressed in kilobytes. The bytes and kilobytes keywords are mutually exclusive and optional. The default is kilobytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
- configure service fpipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
- configure service cpipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
- configure service epipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
- configure service ipipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
- configure service epipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution
- configure service apipe sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution

mbs-contribution

Syntax **mbs-contribution** *size* [{**bytes** | **kilobytes**}]

Context **[Tree]** (config>service>vpls>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>vpls>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)

Full Context configure service vpls sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service vpls sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution

Description The mbs-contribution override command within the SAP ingress and egress contexts is used to override a parent policer's priority level's mbs-contribution parameter that is defined within the policer-control-policy applied to the SAP. This override allow the priority level's burst tolerance to be tuned based on the needs of the SAP's child policers attached to the priority level.

When the override is defined, modifications to the policer-control-policy priority level's mbs-contribution parameter have no effect on the SAP's parent policer priority level until the override is removed using the no mbs-contribution command within the SAP.

The **no** form of this command removes the override and allows the mbs-contribution setting from the policer-control-policy to control the parent policer's priority level's burst tolerance.

Default no mbs-contribution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — This parameter is required when specifying MBS contribution override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 16777216 or default

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs-contribution

Syntax **mbs-contribution** *size* [{**bytes** | **kilobytes**}]

Context **[Tree]** (config>service>ies>if>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>ies>if>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)

Full Context configure service ies interface sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service ies interface sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution

Description The mbs-contribution override command within the SAP ingress and egress contexts is used to override a parent policer's priority level's mbs-contribution parameter that is defined within the policer-control-policy applied to the SAP. This override allow the priority level's burst tolerance to be tuned based on the needs of the SAP's child policers attached to the priority level.

When the override is defined, modifications to the policer-control-policy priority level's mbs-contribution parameter have no effect on the SAP's parent policer priority level until the override is removed using the no mbs-contribution command within the SAP.

The **no** form of this command removes the override and allows the mbs-contribution setting from the policer-control-policy to control the parent policer's priority level's burst tolerance.

Default no mbs-contribution

Parameters *size* — This parameter is required when specifying MBS contribution override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 16777216 or default

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mbs-contribution

Syntax **mbs-contribution** *size* [**bytes** | **kilobytes**]

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)
[Tree] (config>service>vprn>if>sap>ingress>policer-ctrl-over>mbs-thrshlds>priority mbs-contribution)

Full Context configure service vprn interface sap egress policer-control-override priority-mbs-thresholds priority mbs-contribution
configure service vprn interface sap ingress policer-control-override priority-mbs-thresholds priority mbs-contribution

Description The mbs-contribution override command within the SAP ingress and egress contexts is used to override a parent policer's priority level's mbs-contribution parameter that is defined within the policer-control-policy applied to the SAP. This override allow the priority level's burst tolerance to be tuned based on the needs of the SAP's child policers attached to the priority level.

When the override is defined, modifications to the policer-control-policy priority level's mbs-contribution parameter have no effect on the SAP's parent policer priority level until the override is removed using the no mbs-contribution command within the SAP.

The **no** form of this command removes the override and allows the mbs-contribution setting from the policer-control-policy to control the parent policer's priority level's burst tolerance.

Default no mbs-contribution

Parameters *size* — This parameter is required when specifying MBS contribution override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 16777216 or default

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

mbs-contribution

Syntax **mbs-contribution** *size* [**bytes** | **kilobytes**] [**fixed**]
no mbs-contribution

Context **[Tree]** (config>qos>plcr-ctrl-plcy>root>priority-mbs-thresholds>priority mbs-contribution)

Full Context configure qos policer-control-policy root priority-mbs-thresholds priority mbs-contribution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **mbs-contribution** command is used to configure the policy-based burst tolerance for a parent policer instance created when the policy is applied to a SAP, or a subscriber context for the 7450 ESS and 7750 SR, or a 7950 XRS multiservice site. The system uses the parent policer's **min-thresh-separation** value, the priority level's **mbs-contribution** value, and the number of child policers currently attached to the priority level to derive the priority level's shared-portion and fair-portion of burst tolerance within the local priority level. The shared-portion and fair-portions for each priority level are then used by the system to calculate each priority level's discard-unfair threshold and discard-all threshold. The mbs-contribution is the minimum separation between two adjacent active discard-all thresholds.

The value for a priority level's **mbs-contribution** within the policer-control-policy may be overridden on the SAP, or subscriber sub-profile (applies to the 7450 ESS and 7750 SR) or multiservice site (for 7950 XRS) where the policy is applied in order to allow fine tuning of the discard-unfair and discard-all thresholds relevant to the needs of the local child policers on the object.

Accumulative Nature of Burst Tolerance for a Parent Policer Priority Level

When defining **mbs-contribution**, the specified size may only be a portion of the burst tolerance associated with the priority level. The packets associated with the priority level share the burst tolerance of lower within the parent policer. As the parent policer PIR bucket depth increases during congestion, the lower priority packets eventually experience discard based on each priority's discard-unfair and discard-all thresholds. Assuming congestion continues when all the lower priority packets have been prevented from consuming bucket depth, the burst tolerance for the priority level will be consumed by its own packets and any packets associated with higher priorities.

The Effect of Fair and Unfair Child Policer Traffic at a Parent Policer Priority Level

The system continually monitors the offered rate of each child policer on each parent policer priority level and detects when the policer is in a congested state (the aggregate offered load is greater than the decrement rate defined on the parent policer). As previously stated, the result of congestion is that the parent policer's bucket depth will increase until it eventually hovers around either a discard-unfair or discard-all threshold belonging to one of the priority levels. This threshold is the point where enough packets are being discarded that the increment rate and decrement rate begin to even out. If only a single child policer is associated with the priority level, the discard-unfair threshold is not used since fairness is only applicable when multiple child policers are competing at the same priority level.

When multiple child policers are sharing the congested priority level, the system uses the offered rates and the parenting parameters of each child to determine the fair rate per child when the parent policer is unable to meet the bandwidth needs of each child. The fair rate represents the amount of bandwidth that each child at the priority level should receive relative to the other children at the same level according to the policer control policy instance managing the child policers. This fair rate is applied as the decrement rate for each child's FIR bucket. Changing a child's FIR rate does not modify the number of packets forwarded by the parent policer for the child's priority level. It just modifies the forwarded ratio between the children on that priority level. Since each child FIR bucket has some level of burst tolerance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

before marking its packets as unfair, the current parent policer bucket depth may at times rise above the discard-unfair threshold. The mbs-contribution value provides a means to define how much separation is provided between the priority level's discard-unfair and discard-all threshold to allow the parent policer to absorb some amount of FIR burst before reaching the priority's discard-all threshold.

This level of fair aggregate burst tolerance is based on the decrement rate of the parent policer's PIR bucket while the individual fair bursts making up the aggregate are based on each child's FIR decrement rate. The aggregate fair rate of the priority level is managed by the system with consideration of the current rate of traffic in higher priority levels. In essence, the system ensures that for each iteration of the child FIR rate calculation, the sum of the child FIR decrement rates plus the sum of the higher priority traffic increment rates equals the parent policers decrement rate. This means that dynamic amounts of higher priority traffic can be ignored when sizing a lower priority's fair aggregate burst tolerance. Consider the following:

- The parent policer decrement rate is set to 20 Mb/s (max-rate 20,000).
- A priority level's fair burst size is set to 30 kbytes (mbs-contribution 30 kbytes).
- Higher priority traffic is currently taking 12 Mb/s.
- The priority level has three child policers attached.
- Each child's PIR MBS is set to 10 kbytes, which makes each child's FIR MBS 10 kbytes.
- The children want 10 Mb/s, but only 8 Mb/s is available
- Based on weights, the children's FIR rates are set as follows:

	FIR Rate	**FIR MBS**
Child 1	4 Mb/s	10 kbytes
Child 2	3 Mb/s	10 kbytes
Child 3	1 Mb/s	10 kbytes

The 12 Mb/s of the higher priority traffic and the 8 Mb/s of fair traffic equal the 20 Mb/s decrement rate of the parent policer.

It is clear that the higher priority traffic is consuming 12 Mb/s of the parent policer's decrement rate, leaving 8 Mb/s of decrement rate for the lower priority's fair traffic.

- The burst tolerance of child 1 is based on 10 kbytes above 4 Mb/s.
- The burst tolerance of child 2 is based on 10 kbytes above 3 Mb/s.
- The burst tolerance of child 3 is based on 10 kbytes above 1 Mb/s.

If all three children burst simultaneously (unlikely), they will consume 30 kbytes above 8 Mb/s. This is the same as the remaining decrement rate after the higher priority traffic.

Parent Policer Total Burst Tolerance and Downstream Buffering

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The highest in-use priority level's discard-all threshold is the total burst tolerance of the parent policer. In some cases, the parent policer represents downstream bandwidth capacity and the max-rate of the parent policer is set to prevent overrunning the downstream bandwidth. The burst tolerance of the parent policer defines how much more traffic may be sent beyond the downstream scheduling capacity. In the worst-case scenario, when the downstream buffering is insufficient to handle the total possible burst from the parent policer, downstream discards based on lack of buffering may occur. However, in all likelihood, this is not the case.

In most cases, lower priority traffic in the policer will be responsible for the greater part of congestion above the parent policer rate. Since this traffic is discarded with a lower threshold, this lowers the effective burst tolerance even while the highest priority traffic is present.

Configuring a Priority Level's MBS Contribution Value

In the most conservative case, a priority level's **mbs-contribution** value may be set to be greater than the sum of child policer's mbs and one max-size-frame per child policer. This ensures that even in the absolute worst case where all the lower priority levels are simultaneously bursting to the maximum capacity of each child, enough burst tolerance for the priority's children will exist if they also burst to their maximum capacity.

Since simply adding up all the child policer's PIR MBS values may result in large overall burst tolerances that are not ever likely to be needed, consider some level of burst oversubscription when configuring the **mbs-contribution** value for each priority level. The amount of oversubscription should be determined based on the needs of each priority level.

Using the Fixed Keyword to Create Deterministic Parent Policer Discard Thresholds

In the default behavior, the system ignores the **mbs-contribution** values for a priority level on a subscriber for 7450 ESS and 7750 SR, or a multiservice site for 7950 XRS, or SAP parent policer when a child policer is not currently associated with the level. This prevents additional burst tolerance from being added to higher priority traffic within the parent policer.

This does cause fluctuations in the defined threshold values when child policers are added or removed from a parent policer instance. If this behavior is undesirable, the fixed keyword may be used that causes the **mbs-contribution** value to always be included in the calculation of parent policer's discard thresholds. The defined **mbs-contribution** value may be overridden on a subscriber sla-profile for the 7450 ESS and 7750 SR, or on a multiservice site for the 7950 XRS, or on a SAP instance, but the fixed nature of the contribution cannot be overridden.

If the defined **mbs-contribution** value for the priority level is zero, the priority level will have no effect on the parent policer's defined discard thresholds. A packet associated with the priority level will use the next lower priority level's discard-unfair and discard-all thresholds.

The **no** form of this command returns the policy's priority level's MBS contribution to the default value. When changed, the thresholds for the priority level and all higher priority levels for all instances of the parent policer will be recalculated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — The size parameter is required when executing the **mbs-contribution** command. It is expressed as an integer and specifies the priority's specific portion amount of accumulative MBS for the priority level. Setting this value has no effect on parent policer instances where the priority level's **mbs-contribution** value has been overridden.

Values 0 to 4194304 or **default** (applies to the 7450 ESS)
0 to 16777216 or **default** (applies to the 7750 SR and 7950 XRS)

Default 8

bytes | kilobytes: — This parameter indicates whether the size is expressed in bytes or kilobytes.

Default **kilobytes**

fixed — The optional fixed keyword is used to force the inclusion of the defined **mbs-contribution** value in the parent policer's discard threshold calculations. If the **mbs-contribution** command is executed without the **fixed** keyword, the fixed calculation behavior for the priority level is removed.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

17.161 mbytes

mbytes

Syntax **mbytes** {*mbytes* | **disable**}
no mbytes

Context **[Tree]** (config>system>security>ssh>key-re-exchange>client mbytes)
[Tree] (config>system>security>ssh>key-re-exchange>server mbytes)

Full Context configure system security ssh key-re-exchange client mbytes
configure system security ssh key-re-exchange server mbytes

Description This command configures the maximum bytes to be transmitted before a key re-exchange is initiated by the server.

The **no** form of this command reverts to the default value.

Default mbytes 1024

Parameters *mbytes* — Specifies the number of megabytes, on a SSH session, after which the SSH client initiates the key-re-exchange.

Values 1 **to** 64000

Default 1024

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

disable — Specifies that a session will never timeout. To re-enable **mbytes**, enter the command without the **disable** option.

Platforms All

17.162 mc-constraints

mc-constraints

Syntax **mc-constraints**

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac mc-constraints)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac mc-constraints

Description Commands in this context configure the level and its associated bandwidth for a bundle or a logical interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mc-constraints

Syntax **mc-constraints**

Context **[Tree]** (config>service>vpls>sap>igmp-snooping>mcac mc-constraints)
[Tree] (config>service>vpls>sap>mld-snooping>mcac mc-constraints)

Full Context configure service vpls sap igmp-snooping mcac mc-constraints
configure service vpls sap mld-snooping mcac mc-constraints

Description Commands in this context configure multicast CAC constraints.

Platforms All

mc-constraints

Syntax **mc-constraints**

Context **[Tree]** (config>service>vprn>igmp>grp-if>mcac mc-constraints)
[Tree] (config>service>vprn>igmp>if>mcac mc-constraints)
[Tree] (config>service>vprn>mld>grp-if>mcac mc-constraints)
[Tree] (config>service>vprn>mld>if>mcac mc-constraints)
[Tree] (config>service>vprn>pim>if>mcac mc-constraints)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn igmp group-interface mcac mc-constraints
configure service vprn igmp interface mcac mc-constraints
configure service vprn mld group-interface mcac mc-constraints
configure service vprn mld interface mcac mc-constraints
configure service vprn pim interface mcac mc-constraints

Description Commands in this context configure multicast CAC constraints.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn mld group-interface mcac mc-constraints
- configure service vprn igmp group-interface mcac mc-constraints

All

- configure service vprn mld interface mcac mc-constraints
- configure service vprn igmp interface mcac mc-constraints
- configure service vprn pim interface mcac mc-constraints

mc-constraints

Syntax **mc-constraints**

Context **[Tree]** (config>router>mcac>policy>bundle mc-constraints)
[Tree] (config>router>igmp>grp-if>mcac mc-constraints)
[Tree] (config>router>igmp>interface>mcac mc-constraints)
[Tree] (config>router>mld>grp-if>mcac mc-constraints)
[Tree] (config>router>mld>interface>mcac mc-constraints)
[Tree] (config>router>pim>interface>mcac mc-constraints)

Full Context configure router igmp group-interface mcac mc-constraints
configure router igmp interface mcac mc-constraints
configure router mcac policy bundle mc-constraints
configure router mld group-interface mcac mc-constraints
configure router mld interface mcac mc-constraints
configure router pim interface mcac mc-constraints

Description Commands in this context configure the level and its associated bandwidth for a bundle or a logical interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router mld group-interface mcac mc-constraints
- configure router igmp group-interface mcac mc-constraints

All

- configure router igmp interface mcac mc-constraints
- configure router mld interface mcac mc-constraints

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router mcac policy bundle mc-constraints
- configure router pim interface mcac mc-constraints

17.163 mc-ecmp-balance

mc-ecmp-balance

Syntax [**no**] **mc-ecmp-balance**

Context **[Tree]** (config>router>pim mc-ecmp-balance)

Full Context configure router pim mc-ecmp-balance

Description This command enables multicast balancing of traffic over ECMP links based on the number of (S, G) distributed over each link. When enabled, each new multicast stream that needs to be forwarded over an ECMP link is compared to the count of (S, G) already using each link, so that the link with the fewest (S, G) is chosen.

This command cannot be used together with the **mc-ecmp-hashing-enabled** command.

The **no** form of this command disables multicast ECMP balancing.

Platforms All

mc-ecmp-balance

Syntax [**no**] **mc-ecmp-balance**

Context **[Tree]** (config>service>vprn>pim mc-ecmp-balance)

Full Context configure service vprn pim mc-ecmp-balance

Description This command enables multicast balancing of traffic over ECMP links based on the number of (S, G) distributed over each link. When enabled, each new multicast stream that needs to be forwarded over an ECMP link is compared to the count of (S, G) already using each link, so that the link with the fewest (S, G) is chosen.

This command cannot be used together with the **mc-ecmp-hashing-enabled** command.

The **no** form of this command disables multicast ECMP balancing.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.164 mc-ecmp-balance-hold

mc-ecmp-balance-hold

Syntax **mc-ecmp-balance-hold** *minutes*
no mc-ecmp-balance-hold

Context **[Tree]** (config>router>pim mc-ecmp-balance-hold)

Full Context configure router pim mc-ecmp-balance-hold

Description This command defines a hold period that applies after an interface has been added to the ECMP link. It is also used periodically to rebalance if channels have been removed from the ECMP link.

If the ECMP interface has not changed in the hold period and if no multicast streams have been removed, then no action is taken when the timer triggers.

This parameter should be used to avoid excessive changes to the multicast distribution.

A rebalance will not occur to multicast streams that have a priority greater than the configured **ecmp-opt-threshold**.

The **no** form of this command removes the minutes value from the configuration.

Parameters *minutes* — Specifies the hold time, in minutes, that applies after an interface has been added to the ECMP link.

Values 2 to 600

Platforms All

mc-ecmp-balance-hold

Syntax **mc-ecmp-balance-hold** *minutes*
no mc-ecmp-balance-hold

Context **[Tree]** (config>service>vprn>pim mc-ecmp-balance-hold)

Full Context configure service vprn pim mc-ecmp-balance-hold

Description This command configures the hold time for multicast balancing over ECMP links.

Parameters *minutes* — Specifies the hold time, in minutes, that applies after an interface has been added to the ECMP link.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.165 mc-ecmp-hashing-enabled

mc-ecmp-hashing-enabled

Syntax **mc-ecmp-hashing-enabled** [**rebalance**]
no mc-ecmp-hashing-enabled

Context **[Tree]** (config>service>vprn>pim mc-ecmp-hashing-enabled)

Full Context configure service vprn pim mc-ecmp-hashing-enabled

Description This command enables hash-based multicast balancing of traffic over ECMP links and causes PIM joins to be distributed over the multiple ECMP paths based on a hash of S and G (and possibly next-hop IP address). When a link in the ECMP set is removed, the multicast flows that were using that link are redistributed over the remaining ECMP links using the same hash algorithm. When a link is added to the ECMP set new joins may be allocated to the new link based on the hash algorithm, but existing multicast flows using the other ECMP links stay on those links until they are pruned.

Hash-based multicast balancing is supported for both IPv4 and IPv6.

This command cannot be used together with the **mc-ecmp-balance** command. Using this command and the **lag-usage-optimization** command on mixed port speed LAGs is not recommended, because some groups may be forwarded incorrectly.

The **no** form of this command disables the hash-based multicast balancing of traffic over ECMP links.

The **no** form of this command means that the use of multiple ECMP paths if enabled at the **config>router** or **config>service>vprn** context is controlled by the existing implementation and CLI commands **mc-ecmp-balance**.

Default no mc-ecmp-hashing-enabled

Parameters **rebalance** — Specifies to rebalance flows to newly added links immediately, instead of waiting until they are pruned.

Platforms All

mc-ecmp-hashing-enabled

Syntax [**no**] **mc-ecmp-hashing-enabled** [**rebalance**]

Context **[Tree]** (config>router>pim mc-ecmp-hashing-enabled)

Full Context configure router pim mc-ecmp-hashing-enabled

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables hash-based multicast balancing of traffic over ECMP links and causes PIM joins to be distributed over the multiple ECMP paths based on a hash of S and G (and possibly next-hop IP address). When a link in the ECMP set is removed, the multicast flows that were using that link are redistributed over the remaining ECMP links using the same hash algorithm. When a link is added to the ECMP set new joins may be allocated to the new link based on the hash algorithm, but existing multicast flows using the other ECMP links stay on those links until they are pruned.

Hash-based multicast balancing is supported for both IPv4 and IPv6.

This command cannot be used together with the **mc-ecmp-balance** command. Using this command and the **lag-usage-optimization** command on mixed port speed LAGs is not recommended, because some groups may be forwarded incorrectly.

The **no** form of this command disables the hash-based multicast balancing of traffic over ECMP links.

Default no mc-ecmp-hashing-enabled

Parameters **rebalance** — Specifies to rebalance flows to newly added links immediately, instead of waiting until they are pruned.

Platforms All

17.166 mc-endpoint

mc-endpoint

Syntax [**no**] **mc-endpoint**

Context **[Tree]** (config>redundancy>multi-chassis>peer mc-endpoint)

Full Context configure redundancy multi-chassis peer mc-endpoint

Description This command specifies that the endpoint is multi-chassis. This value should be the same on both MC-EP peers for the pseudowires that must be part of the same group.

The **no** form of this command removes the endpoint from the MC-EP. Single chassis behavior applies.

Default no mc-endpoint

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mc-endpoint

Syntax **mc-endpoint** *mc-ep-id*
no mc-endpoint

Context **[Tree]** (config>service>vpls>endpoint mc-endpoint)

Full Context configure service vpls endpoint mc-endpoint

Description This command specifies the identifier associated with the multi-chassis endpoint. This value should be the same on both MC-EP peers for the pseudowires that must be part of the same group.

The **no** form of this command removes the endpoint from the MC-EP. Single chassis behavior applies.

Default no mc-endpoint

Parameters *mc-ep-id* — Specifies a multi-chassis endpoint ID

Values 1 to 4294967295

Platforms All

17.167 mc-enh-load-balancing

mc-enh-load-balancing

Syntax [**no**] **mc-enh-load-balancing**

Context **[Tree]** (config>system>load-balancing mc-enh-load-balancing)

Full Context configure system load-balancing mc-enh-load-balancing

Description This command enables enhanced egress multicast load balancing behavior for Layer 3 multicast. When enabled, the router will spray the multicast traffic using as hash inputs from the packet based on lsr-load-balancing, l4-load-balancing and system-ip-load-balancing configurations. That is, an ingress LER or IP PE will spray traffic based on the IP hash criteria: SA/DA + optional Layer 4 port + optional system IP egress LER or LSR - will spray traffic based on label or IP hash criteria outlined above or both based on configuration of lsr-load-balancing, l4-load-balancing, and system-ip-load-balancing.

The **no** form of the command preserves the default behavior for per flow hashing of multicast traffic.

Default no mc-enh-load-balancing

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.168 mc-ep-peer

mc-ep-peer

Syntax **mc-ep-peer** *name*
mc-ep-peer *ip-address*
no mc-ep-peer

Context **[Tree]** (config>service>vpls>endpoint>mc-ep mc-ep-peer)

Full Context configure service vpls endpoint mc-endpoint mc-ep-peer

Description This command adds multi-chassis endpoint object.

The **no** form of this command removes the multi-chassis endpoint object.

Default no mc-ep-peer

Parameters *name* — Specifies the name of the multi-chassis endpoint peer

ip-address — Specifies the IP address of multi-chassis endpoint peer

Platforms All

17.169 mc-fr-profile-egress

mc-fr-profile-egress

Syntax **mc-fr-profile-egress** *profile-id* [**create**]
no mc-fr-profile-egress *profile-id*

Context **[Tree]** (config>qos mc-fr-profile-egress)

Full Context configure qos mc-fr-profile-egress

Description This command creates a profile for the user to configure the egress QoS parameters of an MLFR bundle or an FRF.12 UNI/NNI link. A maximum of 128 egress QoS profiles may be created on the system.

The no form of this command deletes the profile.

Parameters *profile-id* — Specifies the profile number.

Values 1 to 65535

create — Required parameter when creating a multi-class Frame Relay egress profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mc-fr-profile-egress

Syntax **mc-fr-profile-egress** *src-mc-fr-prof dst-mc-fr-prof* [**overwrite**]

Context **[Tree]** (config>qos>copy mc-fr-profile-egress)

Full Context configure qos copy mc-fr-profile-egress

Description This command copies an existing **mc-fr-profile-egress** profile ID to another multi-class frame-relay egress profile ID. The **copy** command is a configuration level maintenance tool used to create new entries using an existing profile ID. If **overwrite** is not specified, an error occurs if the destination profile ID exists.

Parameters *src-mc-fr-prof* — Specifies the existing source **mc-fr-profile-egress** profile ID from which the **copy** command attempts to copy.

Values 1 to 65535

src-mc-fr-prof — Specifies the destination **mc-fr-profile-egress** profile ID to which the copy command attempts to copy.

Values 1 to 65535

overwrite — Use this parameter when the **mc-fr-profile-egress** *dst-mc-fr-prof* already exists. If it does, everything in the existing destination **mc-fr-profile-egress** *dst-mc-fr-prof* is completely overwritten with the contents of the **mc-fr-profile-egress** *src-mc-fr-prof*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI use {overwrite}; destination mc-fr-egress-profile
"4" exists.
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.170 mc-fr-profile-ingress

mc-fr-profile-ingress

Syntax **mc-fr-profile-ingress** *profile-id* [**create**]
no mc-fr-profile-ingress *profile-id*

Context **[Tree]** (config>qos mc-fr-profile-ingress)

Full Context configure qos mc-fr-profile-ingress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a profile for the user to configure the ingress QoS parameters of a Multi-Link Frame Relay (MLFR) bundle. A maximum of 128 ingress QoS profiles may be created on the system.

The **no** form of this command deletes the profile.

Parameters *profile-id* — Specifies the profile number.

Values 1 to 65535

create — Required parameter when creating a multi-class Frame Relay ingress profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.171 mc-handover

mc-handover

Syntax **mc-handover** *percentage*
no mc-handover

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd mc-handover)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip mc-handover)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd mc-handover)

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd mc-handover
configure mcast-management multicast-info-policy video-policy video-interface pip mc-handover
configure mcast-management multicast-info-policy video-policy video-interface sd mc-handover

Description This command sets the rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client during the handover to the multicast stream.

The **no** form of the command returns the parameter to the default value.

Default mc-handover 25

Parameters *percentage* — Specifies the percentage of nominal bandwidth.

Values

HD:	0 to 100
SD and PIP:	0 to 600

Default 25

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.172 mc-ipsec

mc-ipsec

Syntax [**no**] **mc-ipsec**

Context **[Tree]** (config>redundancy>multi-chassis>peer mc-ipsec)

Full Context configure redundancy multi-chassis peer mc-ipsec

Description Commands in this context configure multi-chassis peer parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.173 mc-ipsec-non-forwarding

mc-ipsec-non-forwarding

Syntax [**no**] **mc-ipsec-non-forwarding tunnel-grp-id**

Context **[Tree]** (config>vrrp>policy>priority-event mc-ipsec-non-forwarding)

Full Context configure vrrp policy priority-event mc-ipsec-non-forwarding

Description This command configures an instance of a multi-chassis IPsec tunnel-group Priority Event used to override the base priority value of a VRRP virtual router instance depending on the operational state of the event.

Parameters *tunnel-grp-id* — Identifies the multi-chassis IPsec tunnel group whose non-forwarding state is monitored by this priority control event.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.174 mc-lag

mc-lag

Syntax [**no**] **mc-lag**

Context **[Tree]** (config>redundancy>multi-chassis>peer mc-lag)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure redundancy multi-chassis peer mc-lag

Description Commands in this context configure multi-chassis LAG operations and related parameters.

The **no** form of this command administratively disables multi-chassis LAG. MC-LAG can be issued only when mc-lag is shutdown.

Default no mc-lag

Platforms All

mc-lag

Syntax **mc-lag**

Context **[Tree]** (config>eth-cfm>redundancy mc-lag)

Full Context configure eth-cfm redundancy mc-lag

Description Commands in this context configure the MC-LAG specific ETH-CFM redundancy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.175 mc-maximum-routes

mc-maximum-routes

Syntax **mc-maximum-routes** *number* [**log-only**] [**threshold** *threshold*]

Context **[Tree]** (config>service>vprn mc-maximum-routes)

Full Context configure service vprn mc-maximum-routes

Description This command specifies the maximum number of multicast routes that can be held in the form of this command in a VPN routing or forwarding (VRF) context. When this limit is reached, a log and SNMP trap are sent. If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then no new joins are processed.

The **no** form of this command disables the limit of multicast routes within a VRF context. Issue the **no** form of this command only when the VPRN instance is shutdown.

Default no mc-maximum-routes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the maximum number of routes to be held in a VRF context.

Values 1 to 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold — Specifies the percentage at which a warning log message and SNMP trap should be sent.

Values 0 to 100

Default 10

Platforms All

mc-maximum-routes

Syntax **mc-maximum-routes** *number* [**log-only**] [**threshold** *threshold*]
no mc-maximum-routes

Context **[Tree]** (config>router mc-maximum-routes)

Full Context configure router mc-maximum-routes

Description This command specifies the maximum number of multicast routes that can be held within a VPN routing/forwarding (VRF) context. When this limit is reached, a log and SNMP trap are sent. If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then no new joins will be processed.

The **no** form of this command disables the limit of multicast routes within a VRF context. Issue the **no** form of this command only when the VPRN instance is shutdown.

Default no mc-maximum-routes

Parameters *number* — Specifies the maximum number of routes to be held in a VRF context

Values 1 to 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes

threshold — The percentage at which a warning log message and SNMP trap should be sent.

Values 0 to 100

Default 10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.176 mc-ring

mc-ring

Syntax **mc-ring**

Context **[Tree]** (config>redundancy>multi-chassis>peer mc-ring)

Full Context configure redundancy multi-chassis peer mc-ring

Description Commands in this context configure the multi-chassis ring parameters.

The **no** form of this command reverts to the default.

Default mc-ring

Platforms All

mc-ring

Syntax [**no**] **mc-ring**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync mc-ring)

Full Context configure redundancy multi-chassis peer sync mc-ring

Description This command specifies whether multi-chassis ring information shoud be synchronized with the multi-chassis peer.

Default no mc-ring

Platforms All

17.177 mcac

mcac

Syntax **mcac**

Context **[Tree]** (config>service>pw-template>igmp-snooping mcac)
[Tree] (config>service>vpls>mesh-sdp>snooping mcac)

Full Context configure service pw-template igmp-snooping mcac
configure service vpls mesh-sdp snooping mcac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure multicast CAC policy parameters and constraints for this interface.

mcac

Syntax **mcac**

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp mcac)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac

Description Commands in this context configure multicast CAC parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mcac

Syntax **mcac**

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping mcac)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping mcac)
[Tree] (config>service>vpls>sap>igmp-snooping mcac)
[Tree] (config>service>vpls>sap>mld-snooping mcac)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping mcac)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping mcac)

Full Context configure service vpls mesh-sdp igmp-snooping mcac
configure service vpls mesh-sdp mld-snooping mcac
configure service vpls sap igmp-snooping mcac
configure service vpls sap mld-snooping mcac
configure service vpls spoke-sdp igmp-snooping mcac
configure service vpls spoke-sdp mld-snooping mcac

Description This command configures multicast CAC policy and constraints for this interface.

Platforms All

mcac

Syntax **mcac**

Context **[Tree]** (config>service>vprn>igmp>grp-if mcac)
[Tree] (config>service>vprn>igmp>if mcac)
[Tree] (config>service>vprn>mld>grp-if mcac)
[Tree] (config>service>vprn>mld>if mcac)
[Tree] (config>service>vprn>pim>if mcac)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn igmp group-interface mcac
configure service vprn igmp interface mcac
configure service vprn mld group-interface mcac
configure service vprn mld interface mcac
configure service vprn pim interface mcac

Description This command configures multicast CAC policy and constraints for this interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn mld group-interface mcac
- configure service vprn igmp group-interface mcac

All

- configure service vprn pim interface mcac
- configure service vprn mld interface mcac
- configure service vprn igmp interface mcac

mcac

Syntax **mcac**

Context **[Tree]** (config>router mcac)
[Tree] (config>router>igmp>group-interface mcac)
[Tree] (config>router>igmp>interface mcac)
[Tree] (config>router>mld>group-interface mcac)
[Tree] (config>router>mld>interface mcac)
[Tree] (config>router>pim>if mcac)

Full Context configure router igmp group-interface mcac
configure router igmp interface mcac
configure router mcac
configure router mld group-interface mcac
configure router mld interface mcac
configure router pim interface mcac

Description Commands in this context configure multicast CAC parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface mcac
- configure router mld group-interface mcac

All

- configure router igmp interface mcac
- configure router mld interface mcac
- configure router pim interface mcac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router mcac

17.178 mcast-capacity

mcast-capacity

Syntax **mcast-capacity** *primary-percentage* **secondary** *secondary-percentage*
no mcast-capacity

Context **[Tree]** (config>mcast-mgmt>chassis-level>plane-capacity mcast-capacity)

Full Context configure mcast-management chassis-level per-mcast-plane-capacity mcast-capacity

Description This command configures the primary and secondary multicast plane capacities used when the full complement of possible switch fabrics in the system is not up (at least one possible switch fabric is not provisioned or is down). The rates are defined as a percentage of the total multicast plane capacity which is configured using the **total-capacity** command.

The **no** form of this command reverts to the default values.

Default mcast-capacity 87.50 secondary 87.50

Parameters *primary-percentage* — Specifies the percentage of the total multicast plane capacity to be used for primary multicast planes.

secondary-percentage — Specifies the percentage of the total multicast plane capacity to be used for secondary multicast planes.

Values 0.01 to 100

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

17.179 mcast-ipv4

mcast-ipv4

Syntax [**no**] **mcast-ipv4**

Context **[Tree]** (config>cflowd>collector>export-filter>family mcast-ipv4)

Full Context configure cflowd collector export-filter family mcast-ipv4

Description This command filters multicast IPv4 flow data from being sent to the associated collector.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the filter, allowing multicast IPv4 flow data to be sent to the associated collector.

Default no mcast-ipv4

Platforms All

17.180 mcast-ipv6

mcast-ipv6

Syntax [**no**] **mcast-ipv6**

Context **[Tree]** (config>cflowd>collector>export-filter>family mcast-ipv6)

Full Context configure cflowd collector export-filter family mcast-ipv6

Description This command filters multicast IPv6 flow data from being sent to the associated collector.

The **no** form of this command removes the filter, allowing multicast IPv6 flow data to be sent to the associated collector.

Default no mcast-ipv6

Platforms All

17.181 mcast-ipv6-snooping-scope

mcast-ipv6-snooping-scope

Syntax **mcast-ipv6-snooping-scope** {**mac-based** | **sg-based**}
no mcast-ipv6-snooping-scope

Context **[Tree]** (config>service>vpls mcast-ipv6-snooping-scope)

Full Context configure service vpls mcast-ipv6-snooping-scope

Description This command specifies the forwarding scope used for IPv6 multicast traffic when PIM snooping for IPv6 is enabled.

By default, the scope is **mac-based**; IPv6 snooped multicast traffic is forwarded is based on the low-order 32 bits of the destination IPv6 address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the scope is configured as **sg-based**, the IPv6 snooped multicast traffic is forwarded based on both its full source (if specified in the join) and destination IPv6 address. SG-based forwarding is only supported on FP3- (or higher) based line cards.

PIM snooping for IPv6 must be disabled to change the forwarding mode within a VPLS service between **mac-based** and **sg-based**.

Default mcast-ipv6-snooping-scope mac-based

Parameters **mac-based** — Enables forwarding for PIM-snooped IPv6 multicast traffic based on the low-order 32 bits of its destination IPv6 address.

sg-based — Enables forwarding for PIM-snooped IPv6 multicast traffic based on its full source (if specified in the join) and destination IPv6 address.

Platforms All

17.182 mcast-management

mcast-management

Syntax **mcast-management**

Context **[Tree]** (config mcast-management)

Full Context configure mcast-management

Description Commands in this context configure multicast management parameters. The **mcast-management** CLI node contains the **bandwidth-policy** and **multicast-info-policy** definitions. The bandwidth-policy is used to manage the ingress multicast paths into the switch fabric. The multicast-info-policy defines how each multicast channel is handled by the system. The policy may be used by the ingress multicast bandwidth manager, the ECMP path manager and the egress multicast CAC manager.

The **mcast-management** node always exists and contains the default bandwidth-policy and the default multicast-info-policy. Enter the mcast-management node when editing, deleting or creating a bandwidth policy or multicast info policy. The default bandwidth policy and multicast-info-policy cannot be edited or deleted.

A chassis-level node within multicast-management is used to control the switch fabric multicast planes replication limits. The switch fabric multicast planes are the individual multicast spatial replication contexts available in the system.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.183 mcast-path-management

mcast-path-management

Syntax **mcast-path-management**

Context **[Tree]** (config>card>fp>ingress mcast-path-management)

Full Context configure card fp ingress mcast-path-management

Description This CLI node contains the forwarding plane settings for ingress multicast path management. Enter the node to configure the bandwidth-policy and the administrative state of ingress multicast path management.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

17.184 mcast-pool

mcast-pool

Syntax **mcast-pool percent-of-total** *percent-of-buffers* **resv-cbs** *percent-of-pool* **slope-policy** *policy-name*
no mcast-pool

Context **[Tree]** (config>mcast-mgmt>bw-plcy mcast-pool)

Full Context configure mcast-management bandwidth-policy mcast-pool

Description This command configures the ingress multicast path management buffer pool. The pool is used by the primary and secondary path queues through which all ingress managed multicast traffic must flow. The parameters may be used to configure the size of the pool relative to the total ingress buffer space, the amount of reserved CBS buffers within the pool and the slope policy used to manage early congestion detection functions in the shared portion of the pool.

Care should be taken when managing the buffer pool space as changes to the systems buffer pool behavior can have negative effects on multicast and unicast forwarding.

Sizing the Pool

The percent-of-total command defines how much of the total ingress buffer pool space for the MDA is dedicated for multicast channels managed by the bandwidth policy. Since multicast typically has a higher scheduling priority through the switch fabric, the buffer pool does not need to be large. By default, the system reserves 10% of the buffers on the ingress side of the MDA once multicast path management is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Reserved CBS Portion of the Pool

The multicast pool is divided into two portions; reserved and shared. The reserved portion is used by the multicast path queues until they cross there individual CBS thresholds. Since the CBS thresholds are configured as percentages and the percentages can oversubscribe the reserved portion of the pool, it is possible for some of the queues CBS buffer allocation to be met by the shared portion of the pool. By default, 50% of the pool is defined as reserved. This may be changed using the resv-cbs percentage parameter.

Shared Portion WRED Slopes

The shared portion of the buffer pool is used by queues that have crossed over their CBS thresholds. Since the total MBS values for the multicast path queues may oversubscribe the pool size, a buffer congestion control mechanism is supported within the pool in the form of two WRED slopes. The **slope-policy** parameter defines how the slopes are configured and whether they are activated. Each packet entering a path queue is defined as high or low priority within the queue based on the channel's preference value relative to the **cong-priority-threshold** command. When getting a shared buffer of a high priority packet, the high WRED slope is used. Low priority packets use the low WRED slope.

The **no** form of this command returns the managed multicast path pool to its default settings.

Parameters *percent-of-buffers* — Specifies the percentage of ingress buffers that is allocated to the multicast pool.

Values 1 to 50

Default 10

percent-of-pool — Specifies the percentage of the pool that is reserved for multicast path queues within their CBS threshold.

Values 1 to 100

Default 50

slope-policy-name — Specifies the WRED slopes within the multicast pool. Once a slope policy is associated with a buffer pool, it cannot be deleted.

Default default

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

17.185 mcast-reporting

mcast-reporting

Syntax [**no**] **mcast-reporting**

Context **[Tree]** (config>subscr-mgmt>igmp-policy mcast-reporting)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt igmp-policy mcast-reporting

Description Commands in this context configure mcast reporting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.186 mcast-reporting-dest

mcast-reporting-dest

Syntax **mcast-reporting-dest** *dest-name* [**create**]
no mcast-reporting-dest *dest-name*

Context **[Tree]** (config>mcast-management mcast-reporting-dest)

Full Context configure mcast-management mcast-reporting-dest

Description This command creates a multicast reporting destination hierarchy in CLI under which parameters defining this destination can be specified. The destination refers to an external node that collects and analyze IGMP events.

The multicast reporting destination is associated with a name that each subscriber can reference to send the IGMP related events.

It can be also referenced in the host tracking policy in case that IGMP events are related to the host tracking feature.

The **no** form of this command removes the destination name from the configuration.

Parameters *dest-name* — Specifies the multicast reporting destination name.

Platforms All

mcast-reporting-dest

Syntax [**no**] **mcast-reporting-dest** [*dest-name*]

Context **[Tree]** (debug>mcast-mgmt mcast-reporting-dest)

Full Context debug mcast-management mcast-reporting-dest

Description This command debugs multicast path management reporting destinations and applies only to the 7750 SR.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mcast-reporting-dest

Syntax **mcast-reporting-dest** *dest-name*
no mcast-reporting-dest

Context **[Tree]** (config>subscr-mgmt>igmp-policy>mcast-reporting mcast-reporting-dest)

Full Context configure subscriber-mgmt igmp-policy mcast-reporting mcast-reporting-dest

Description This command references the multicast reporting destination to which IGMP-related events are exported. The multicast-reporting-destination is referenced within the IGMP policy for the subscriber.

The **no** form of this command reverts to the default value.

Parameters *dest-name* — Specifies the name of the multicast reporting destination, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.187 mcast-tunneling

mcast-tunneling

Syntax [**no**] **mcast-tunneling**

Context **[Tree]** (config>router>ldp>targ-session>peer mcast-tunneling)
[Tree] (config>router>ldp>targ-session>peer-template mcast-tunneling)

Full Context configure router ldp targeted-session peer mcast-tunneling
configure router ldp targeted-session peer-template mcast-tunneling

Description At the downstream router, the FEC is resolved and the result of the resolution is a Label Mapping advertisement to the upstream peer.

At the upstream router, if the RSVP LSP does not exist to the peer address, the upstream router does not use the T-LDP session for FEC resolution.

The **no** form of this command reverts to the default value.

Default no mcast-tunneling

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.188 mcast-upstream-asbr-frr

mcast-upstream-asbr-frr

Syntax [**no**] **mcast-upstream-asbr-frr**

Context **[Tree]** (config>router>ldp mcast-upstream-asbr-frr)

Full Context configure router ldp mcast-upstream-asbr-frr

Description This command enables ASBR MoFRR.

When ASBR MoFRR is enabled, the local leaf will perform MoFRR for multiple ASBRs; for example, if there are two ASBRs, the local leaf will select one ASBR as the primary and another ASBR as the backup.

The **no** form of the command disables ASBR MoFRR.

If the **mcast-upstream-frr** command is enabled, disabling ASBR MoFRR will only allow IGP MoFRR in the local AS; for example, a single ASBR will be selected and two separate, disjointed paths will be selected as the primary and backup LSPs from the local leaf to ASBR.

If the **mcast-upstream-frr** command is disabled, disabling ASBR MoFRR will disable MoFRR entirely.

Default no mcast-upstream-asbr-frr

Platforms All

17.189 mcast-upstream-frr

mcast-upstream-frr

Syntax [**no**] **mcast-upstream-frr**

Context **[Tree]** (config>router>ldp mcast-upstream-frr)

Full Context configure router ldp mcast-upstream-frr

Description This command enables the mLDP fast upstream switchover feature.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this command is enabled and LDP is resolving a mLDP FEC received from a downstream LSR, it checks if an ECMP next-hop or a LFA next-hop exist to the root LSR node. If LDP finds one, it programs a primary ILM on the interface corresponding to the primary next-hop and a backup ILM on the interface corresponding to the ECMP or LFA next-hop. LDP then sends the corresponding labels to both upstream LSR nodes. In normal operation, the primary ILM accepts packets while the backup ILM drops them. If the interface or the upstream LSR of the primary ILM goes down causing the LDP session to go down, the backup ILM will then start accepting packets.

In order to make use of the ECMP next-hop, the user must configure the **ecmp** value in the system to at least 2 using the following command:

config>router>ecmp

In order to make use of the LFA next-hop, the user must enable LFA using the following commands:

config>router>isis>loopfree-alternates

config>router>ospf>loopfree-alternates

Enabling IP FRR or LDP FRR features is not strictly required since LDP only needs to know where the alternate next-hop to the root LSR is to be able to send the Label Mapping message to program the backup ILM at the initial signaling of the tree. Thus enabling the LFA option is sufficient. If however, unicast IP and LDP prefixes need to be protected, then these features and the mLDP fast upstream switchover can be enabled concurrently.

The mLDP FRR fast switchover relies on the fast detection of loss of **LDP session** to the upstream peer to which the primary ILM label had been advertised. We strongly recommended to perform the following:

- Enable BFD on all LDP interfaces to upstream LSR nodes. When BFD detects the loss of the last adjacency to the upstream LSR, it will bring down immediately the LDP session which will cause the IOM to activate the backup ILM.
- If there is a concurrent TLDP adjacency to the same upstream LSR node, enable BFD on the T-LDP peer in addition to enabling it on the interface.
- Enable the **ldp-sync-timer** option on all interfaces to the upstream LSR nodes. If an LDP session to the upstream LSR to which the primary ILM is resolved goes down for any other reason than a failure of the interface or of the upstream LSR, routing and LDP will go out of sync. This means the backup ILM will remain activated until the next time SPF is rerun by IGP. By enabling IGP-LDP synchronization feature, the advertised link metric will be changed to max value as soon as the LDP session goes down. This in turn will trigger an SPF and LDP will likely download a new set of primary and backup ILMs.

The **no** form of this command disables the fast upstream switchover for mLDP FECs.

Default no mcast-upstream-frr

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.190 mcast-vpn-ipv4

mcast-vpn-ipv4

Syntax **mcast-vpn-ipv4 send** *send-limit* **receive** [**none**]
mcast-vpn-ipv4 send *send-limit*
no mcast-vpn-ipv4

Context **[Tree]** (config>router>bgp>add-paths mcast-vpn-ipv4)
[Tree] (config>router>bgp>group>add-paths mcast-vpn-ipv4)
[Tree] (config>router>bgp>group>neighbor>add-paths mcast-vpn-ipv4)

Full Context configure router bgp add-paths mcast-vpn-ipv4
configure router bgp group add-paths mcast-vpn-ipv4
configure router bgp group neighbor add-paths mcast-vpn-ipv4

Description This command configures the add-paths capability for multicast IPv4 VPN routes. By default, add-paths is not enabled for multicast IPv4 VPN routes.

The maximum number of multicast paths per IPv4 VPN prefix to send is the configured *send-limit*, which is a mandatory parameter. The capability to receive multiple multicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command, receive capability is enabled by default. The **none** option disables the receive capability.

The **no** form of this command disables add-paths support for multicast IPv4 VPN routes, causing sessions established using add-paths for multicast IPv4 VPN to go down and come back up without the add-paths capability.

Default no mcast-vpn-ipv4

Parameters *send-limit* — Specifies the maximum number of paths per multicast IPv4 VPN prefix that are allowed to be advertised to add-paths peers. The actual number of advertised routes may be less. If the value is **none**, the router does not negotiate the send capability with respect to multicast IPv4 VPN AFI/SAFI.

Values 1 to 16, none

receive — Specifies that the router negotiates to receive multiple multicast routes per IPv4 VPN prefix.

none — Specifies that the router does not negotiate to receive multiple multicast routes per IPv4 VPN prefix.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.191 mcast-vpn-ipv6

mcast-vpn-ipv6

Syntax **mcast-vpn-ipv6 send** *send-limit* **receive** [**none**]
mcast-vpn-ipv6 send *send-limit*
no mcast-vpn-ipv6

Context **[Tree]** (config>router>bgp>add-paths mcast-vpn-ipv6)
[Tree] (config>router>bgp>group>add-paths mcast-vpn-ipv6)
[Tree] (config>router>bgp>group>neighbor>add-paths mcast-vpn-ipv6)

Full Context configure router bgp add-paths mcast-vpn-ipv6
configure router bgp group add-paths mcast-vpn-ipv6
configure router bgp group neighbor add-paths mcast-vpn-ipv6

Description This command configures the add-paths capability for multicast IPv6 VPN routes. By default, add-paths is not enabled for multicast IPv6 VPN routes.

The maximum number of multicast paths per IPv6 VPN prefix to send is the configured *send-limit*, which is a mandatory parameter. The capability to receive multiple multicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command, receive capability is enabled by default. The **none** option disables the receive capability.

The **no** form of this command disables add-paths support for multicast IPv6 VPN routes, causing sessions established using add-paths for multicast IPv6 VPN to go down and come back up without the add-paths capability.

Default no mcast-vpn-ipv6

Parameters *send-limit* — Specifies the maximum number of paths per multicast IPv6 VPN prefix that are allowed to be advertised to add-paths peers. The actual number of advertised routes may be less. If the value is **none**, the router does not negotiate the send capability with respect to multicast IPv6 VPN AFI/SAFI.

Values 1 to 16, none

receive — Specifies that the router negotiates to receive multiple multicast routes per IPv6 VPN prefix.

none — Specifies that the router does not negotiate to receive multiple multicast routes per IPv6 VPN prefix.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.192 mcc-mnc-prefix

mcc-mnc-prefix

Syntax **mcc-mnc-prefix** *imsi-prefix-string*
no mcc-mnc-prefix

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>imsi-apn-fltr>entry mcc-mnc-prefix)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter entry mcc-mnc-prefix

Description This command configures a matching condition for the IMSI (MCC-MNC) prefix.

Parameters *imsi-prefix-string* — Specifies a string of 1 to 6 decimal digits representing the IMSI prefix to be matched against the IMSI IE of the packet, or the special value **ANY_IMSI** to indicate that an IMSI IE must be present as a matching condition regardless of the IMSI IE value.

If no MCC-MNC prefix is specified, the entry will match GTP packets that have an IMSI IE containing any value.

Values 0 to 999999, **ANY_IMSI**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.193 mcr-default-gtw

mcr-default-gtw

Syntax **mcr-default-gtw**

Context **[Tree]** (config>service>vpls mcr-default-gtw)

Full Context configure service vpls mcr-default-gtw

Description Commands in this context configure the default gateway information when using Dual Homing in L2-TPSDA. The IP and MAC address of the default gateway used for subscribers on an L2 MC-Ring are configured in this context. After a ring heals or fails, the system sends out a gratuitous ARP on an active ring SAP in order to attract traffic from subscribers on the ring with connectivity to that SAP.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.194 mcs

mcs

Syntax **mcs** [**detail**]
no mcs

Context **[Tree]** (debug>service>id>pim-snooping mcs)

Full Context debug service id pim-snooping mcs

Description This command enables or disables debugging for PIM snooping multi-chassis synchronization.

Parameters **detail** — Provides detailed debugging information

Platforms All

mcs

Syntax **mcs** [*ip-int-name*]
no mcs

Context **[Tree]** (debug>router>igmp mcs)

Full Context debug router igmp mcs

Description This command enables debugging for IGMP multicast servers (MCS).

The **no** form of the command disables the IGMP interface debugging for the specifies interface name.

Parameters *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IP interface address

Platforms All

17.195 mcs-interval

mcs-interval

Syntax **mcs-interval** *minutes*
mcs-interval use-update-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no mcs-interval

Context [Tree] (config>subscr-mgmt>acct-plcy mcs-interval)

Full Context configure subscriber-mgmt radius-accounting-policy mcs-interval

Description This command specifies the interval at which the active BNG in a dual-homed deployment synchronizes subscriber accounting data using MCS to the standby BNG. The MCS interval is a statically configured value or is equal to the configured RADIUS accounting update-interval.

The **no** form of the command reverts to the default value.

Default no mcs-interval

Parameters *minutes* — Specifies the interval, in minutes, at which accounting data of the subscriber is synchronized.

Values 5 to 60

use-update-interval — Synchronizes subscriber accounting data at the same time as the RADIUS interim-update. For this, the configured update-interval in the RADIUS accounting policy is used, ignoring RADIUS overrides.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.196 mcs-peer

mcs-peer

Syntax **mcs-peer** *ip-address* **sync-tag** [*sync-tag*]
no mcs-peer

Context [Tree] (config>python>py-pol>cache mcs-peer)

Full Context configure python python-policy cache mcs-peer

Description This command specifies the MCS peer's address and sync-tag for syncing the cached entries of the python-policy. The sync-tag must be match on both chassis.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IPv4 address of the MCS peer.

sync-tag — Specifies the tag for sync, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mcs-peer

Syntax **mcs-peer** *ip-address* **sync-tag** *name*
no mcs-peer

Context **[Tree]** (config>aaa>diam-peer-plcy>proxy mcs-peer)

Full Context configure aaa diameter-peer-policy proxy mcs-peer

Description This command configures the IP address and the synchronization tag for the multi-chassis synchronization (MCS) peer.

This command is applicable only to legacy implementations of Diameter base in SR OS.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the MCS peer.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

name — Specifies the sync tag name, up to 32 characters. The name must match on both nodes for the pair of redundant diameter proxies.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.197 md

md

Syntax **md** *file-url*

Context **[Tree]** (file md)

Full Context file md

Description This command creates a new directory in a file system.

Directories can only be created one level at a time.

Parameters *file-url* — Specifies the directory name to be created.

Values

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-url	[*cflash-id*/][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

17.198 md-auto-id

md-auto-id

Syntax **md-auto-id**

Context **[Tree]** (config>eth-cfm md-auto-id)

Full Context configure eth-cfm md-auto-id

Description This command automatically assigns numerical index values for ma-index and md-index in model-driven management interfaces.

Classic management interfaces use a numerical index as the primary key for ETH-CFM domains and associations. In model-driven interfaces, domains and associations use string names as keys. The domain and association can optionally be created without having to explicitly select and specify a numerical index in model-driven interfaces. In this case, SR OS assigns an index using the configured index range.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

md-auto-id

Syntax **md-auto-id**

Context **[Tree]** (config>qos md-auto-id)

Full Context configure qos md-auto-id

Description This command automatically assigns numerical ID values for QoS policies in model-driven (MD) management interfaces.

Classic management interfaces use a numerical policy ID as the primary key for sap-ingress, sap-egress, and network QoS policies. In model-driven interfaces, SAP and network policies use string names as keys. The SAP and network policies can optionally be created in MD interfaces without having to explicitly select and specify a numerical policy ID. In this case, SR OS assigns an ID using the configured ID range.

Platforms All

md-auto-id

Syntax **md-auto-id**

Context **[Tree]** (config>filter md-auto-id)

Full Context configure filter md-auto-id

Description This command automatically assigns numerical ID values for filter policies in model-driven management interfaces.

Classic management interfaces use a numerical filter ID as the primary key for IP filters, IPv6 filters, and MAC filters. In model-driven interfaces, IP, IPv6, and MAC filters use string names as keys. The filters can optionally be created in MD interfaces without having to explicitly select and specify a numerical filter ID. In this case, SR OS assigns an ID using the configured ID range.

Platforms All

md-auto-id

Syntax **md-auto-id**

Context **[Tree]** (config>service md-auto-id)

Full Context configure service md-auto-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command automatically assigns numerical ID values for services, customers, and PW templates in model-driven (MD) management interfaces.

Classic management interfaces use a numerical service ID, customer ID, and PW template ID as the primary key for services, customers, and PW templates. In model-driven interfaces, services, customers, and PW templates use string names as keys. The services, customers, and PW templates can optionally be created in MD interfaces without having to explicitly select and specify a numerical ID. In this case, SR OS assigns an ID using the configured ID range.

Platforms All

17.199 md-cli

md-cli

Syntax **md-cli**

Context **[Tree]** (config>system>management-interface>cli md-cli)

Full Context configure system management-interface cli md-cli

Description Commands in this context configure MD-CLI capabilities.

Platforms All

md-cli

Syntax **md-cli**

Context **[Tree]** (config>system>security>management-interface md-cli)

Full Context configure system security management-interface md-cli

Description Commands in this context configure hash-control for the MD-CLI interface.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.200 md-cli-session

md-cli-session

Syntax **md-cli-session** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization md-cli-session)

Full Context configure system security profile grpc rpc-authorization md-cli-session

Description This command configures the use of the MdCli Session RPC for the user profile.

The **no** form of this command reverts to the default value.

Default md-cli-session permit

Parameters **deny** — Specifies that the use of MdCli Session RPC is denied.

permit — Specifies that the use of MdCli Session RPC is permitted.

Platforms All

17.201 md-index-range

md-index-range

Syntax **md-index-range start** *md-index* **end** *md-index*
no md-index-range

Context **[Tree]** (config>eth-cfm>md-auto-id md-index-range)

Full Context configure eth-cfm md-auto-id md-index-range

Description This command specifies the range of indexes used by SR OS to automatically assign an index to ETH-CFM domains that are created in model-driven interfaces without an index explicitly specified by the user or client.

A domain created with an explicitly-specified index cannot use an index in this range. In classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed, which causes any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **md-auto-id** command for further details.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **start** *md-index* — Specifies the lower value of the index range. The value must be less than or equal to the **end** value.

Values 1 to 4294967295

end *md-index* — Specifies the upper value of the index range. The value must be greater than or equal to the **start** value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.202 md-interfaces

md-interfaces

Syntax [**no**] **md-interfaces**

Context **[Tree]** (config>system>security>management-interface>output-authorization md-interfaces)

Full Context configure system security management-interface output-authorization md-interfaces

Description This command controls output authorization of commands or RPCs for model-driven interfaces that display configuration or state.

When enabled, output authorization is performed for the following commands:

- MD-CLI **info** and **compare** commands
- NETCONF <get> and <get-config> RPCs
- gNMI Get RPC

When disabled, output authorization is not performed, which may significantly decrease the system response time by reducing command authorization requests, especially when remote AAA servers are used. Input to edit configuration is always authorized based on the AAA configuration.

By default, authorization checks are performed for configuration and state output.

The **no** form of this command disables authorization checks, allowing the output to be displayed immediately.

Default md-interfaces

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.203 mda

mda

Syntax [**no**] **mda** *mda-id*

Context **[Tree]** (config>isa>wlan-gw-group mda)

Full Context configure isa wlan-gw-group mda

Description This command enables an ISA for WLAN-GW functionality.

The **no** form of this command removes the ISA from the WLAN-GW configuration.

Parameters *mda-id* — Indicates the IOM and MDA slot in format *slot*/*mda*.

Values slot — 1 to 10
mda — 1 to 2

Platforms 7750 SR, 7750 SR-e, 7750 SR-s

mda

Syntax [**no**] **mda** *mda-slot*

Context **[Tree]** (config>card mda)

Full Context configure card mda

Description This mandatory command enables access to a card's MDA CLI context to configure MDAs.

Parameters *mda-slot* — Specifies the MDA slot number to be configured. Slots are numbered 1 and 2. On vertically oriented slots, the top MDA slot is number 1, and the bottom MDA slot is number 2. On horizontally oriented slots, the left MDA is number 1, and the right MDA slot is number 2.

Values 1, 2

Platforms All

mda

Syntax [**no**] **mda** *mda-slot*

Context **[Tree]** (config>card>xiom mda)

Full Context configure card xiom mda

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Configures an MDA-s in one of the slots of an XIOM.

Parameters *mda-slot* — Specifies the MDA-s slot number.

Values 1 or 2

Platforms 7750 SR-s

mda

Syntax [**no**] **mda** *mda-id*

Context **[Tree]** (config>service>vpls>mesh-sdp>egress>mfib-allowed-mda-destinations mda)
[Tree] (config>service>vpls>spoke-sdp>egress>mfib-allowed-mda-destinations mda)

Full Context configure service vpls mesh-sdp egress mfib-allowed-mda-destinations mda
configure service vpls spoke-sdp egress mfib-allowed-mda-destinations mda

Description This command specifies an MFIB-allowed MDA destination for an SDP binding configured in the system.

Parameters *mda-id* — Specifies an MFIB-allowed MDA destination

Values

slot/mda	slot: 1 to 10
	mda: 1, 2
slot/xiom/mda	slot: 1 to 10
	xiom: “x1” or “x2”
	mda: 1, 2

Platforms All

mda

Syntax [**no**] **mda** *mda-id*

Context **[Tree]** (config>isa>tunnel-grp mda)

Full Context configure isa tunnel-group mda

Description This command specifies the MDA ID of the MS-ISA as the member of tunnel-group with multi-active enabled. Up to 16 MDA could be configured under the same tunnel-group.

Parameters *mda-id* — Specifies the id of MS-ISA.

Values iom-slot-id/mda-slot-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mda

Syntax **mda** *mda-id* [**drain**]
no mda *mda-id*

Context **[Tree]** (config>isa>lns-group mda)

Full Context configure isa lns-group mda

Description This command configures an ISA LNS group MDA.

The **no** form of the command removes the MDA ID from the LNS group configuration.

Parameters *mda-id* — Specifies the MDA identifier.

Values

mda-id:	*slot*/*mda*
	slot: 1 to 10
	mda: 1, 2

drain — Prevents new L2TP sessions being associated with the ISA. If an ISA is removed from the lns-group or if the lns-group be shutdown all associated L2TP sessions will be immediately terminated (and L2TP CDN messages sent to the L2TP peer). View show commands to determine which ISA is terminating which session (**show router l2tp session**).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mda

Syntax [**no**] **mda** *mda-id*

Context **[Tree]** (config>isa>nat-group mda)

Full Context configure isa nat-group mda

Description This command configures an ISA NAT group MDA.

Parameters *mda-id* — Specifies the MDA ID in the *slot/mda* format.

Values slot: 1 to 10
mda: 1 to 16

Note: Available parameter values may differ by platform.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mda

Syntax [**no**] **mda** *mda-id*

Context **[Tree]** (config>service>pw-template>egress>mfib-mda mda)

Full Context configure service pw-template egress mfib-allowed-mda-destinations mda

Description This command specifies an MFIB-allowed media adapter destination for an SDP binding configured in the system.

Parameters *mda-id* — Specifies an MFIB-allowed media adapters destination.

Values 1, 2

Platforms All

17.204 mda-type

mda-type

Syntax **mda-type** *mda-type* [**level** *mda-level*]
no mda-type

Context **[Tree]** (config>card>mda mda-type)

Full Context configure card mda mda-type

Description This mandatory command provisions a specific MDA type to the device configuration for the slot. The MDA can be preprovisioned but an MDA must be provisioned before ports can be configured. Ports can be configured once the MDA is properly provisioned.

A maximum of two MDAs can be provisioned on an IOM or XCM. To modify an MDA slot, shut down all port associations.

XMAs are provisioned using MDA commands. A medium severity alarm is generated if an MDA is inserted that does not match the MDA type configured for the slot. This alarm is cleared when the correct MDA is inserted or the configuration is modified. A high severity alarm is raised when an administratively enabled MDA is removed from the chassis. This alarm is cleared if the either the correct MDA type is inserted or the configuration is modified. A low severity trap is issued if an MDA is removed that is administratively disabled.

An MDA can only be provisioned in a slot if the MDA type is allowed in the MDA slot. An error message is generated when an MDA is provisioned in a slot where it is not allowed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Some MDA hardware can support two different firmware loads. One load includes the base Ethernet functionality, including 10G WAN mode, but does not include 1588 port-based timestamping. The second load includes the base Ethernet functionality and 1588 port-based timestamping, but does not include 10G WAN mode. These are identified as two MDA types that are the same, except for a “-ptp” suffix to indicate the second loadset; for example, *x40-10gb-sfp* and *x40-10gb-sfp-ptp*. A hard reset of the MDA occurs when switching between the two provisioned types.

A medium severity alarm is generated if an MDA is inserted that does not match the MDA type configured for the slot. This alarm is cleared when the correct MDA is inserted or the configuration is modified.

A high severity alarm is raised when an administratively enabled MDA is removed from the chassis. This alarm is cleared if the either the correct MDA type is inserted or the configuration is modified. A low severity trap is issued if an MDA is removed that is administratively disabled.

An alarm is raised if partial or complete MDA failure is detected. The alarm is cleared when the error condition ceases.

All parameters in the MDA context remain and if non-default values are required then their configuration remains as it is on all existing MDAs.

New generations of XMAs include variants controlled through hardware and software licensing. For these XMAs, the license level must be provisioned in addition to the MDA type. An XMA cannot become operational unless the provisioned license level matches the license level of the XMA installed into the slot. The set of license levels varies by MDA type.

The provisioned level controls aspects related to connector provisioning and the consumption of hardware egress queues and egress policers. Changes to the provisioned license level may be blocked if configuration that would not be permitted with the new target license level exists.

If the license level is not specified, the level is set to the highest license level for that XMA.

The **no** form of this command deletes the MDA from the configuration. The MDA must be administratively shut down before it can be deleted from the configuration.

Parameters *mda-type* — Specifies the type of MDA selected for the slot position. Values for this attribute vary by platform and release. The release notes include a listing of all supported mda-types and their CLI strings. In addition, the command can be queried to check which mda-types are relevant for the active platform type. Some examples include me6-10gb-spf+ and x4-100g-cfp2.

mda-level — Specifies the MDA level. Possible values vary by MDA type.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mda-type

Syntax **mda-type** *mda-type*
no mda-type

Context **[Tree]** (config>card>xiom>mda mda-type)

Full Context configure card xiom mda mda-type

Description This command adds an MDA-s to the device configuration for the slot. The MDA-s type can be preprovisioned, which means that the MDA-s does not have to be installed in the chassis.

An MDA-s must be provisioned before a connector or a port can be configured.

An MDA-s can only be provisioned in a slot that is vacant. No other MDA-s can be provisioned (configured) for that particular slot. To reconfigure a slot position, use the **no** form of this command to remove the current information.

An MDA-s can only be provisioned in a slot if the MDA-s type is allowed in the slot. An error message is generated if an attempt is made to provision an MDA-s type that is not allowed.

If an MDA-s is inserted that does not match the configured MDA-s type for the slot, then a log event and a facility alarm are raised. The alarm is cleared when the correct MDA-s type is installed or the configuration is modified.

A log event and a facility alarm are raised if an administratively enabled MDA-s is removed from the chassis. The alarm is cleared when the correct MDA-s type is installed or the configuration is modified. A log event is issued when a MDA-s is removed that is administratively disabled.

The **no** form of this command removes the MDA-s from the configuration.

Parameters *mda-type* — Specifies the type of MDA-s to be configured and installed in the slot. Values for this attribute vary by platform and release. The release notes include a listing of all supported mda-types and their CLI strings. In addition, the command can be queried to check which mda-types are relevant for the active platform type.

Platforms 7750 SR-s

17.205 mdl

mdl

Syntax **mdl** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **gen**} *mdl-string*
no mdl [**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **gen**]

Context **[Tree]** (config>port>tdm>ds3 mdl)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port tdm ds3 mdl

Description This command configures the maintenance data link (MDL) message for a DS-3/E-3.

This command is only applicable if the DS-3/E-3 is using C-bit framing (see the **config>port>tdm>ds3 framing** command).

The **no** form of this command removes the MDL string association and stops the transmission of any IDs.

Default no mdl

Parameters *mdl-string* — Specifies an MDL message up to 38 characters long on a DS-3.

eic — Specifies the equipment ID code up to 10 characters long.

lic — Specifies the equipment ID code up to 11 characters long.

fic — Specifies the ID code up to 10 characters long.

unit — Specifies the unit ID code up to 6 characters long.

pfi — Specifies the facility ID code up to 38 characters long.

port — Specifies the port ID code up to 38 characters long.

gen — Specifies the generator number to send in the MDL test signal message up to 38 characters long.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

17.206 mdl-transmit

mdl-transmit

Syntax **mdl-transmit** {**path** | **idle-signal** | **test-signal**}
no mdl-transmit [**path** | **idle-signal** | **test-signal**]

Context **[Tree]** (config>port>tdm>ds3 mdl-transmit)

Full Context configure port tdm ds3 mdl-transmit

Description This command enables the transmission of an MDL message on a DS-3/E-3 over channelized interface.

The **no** form of this command disables transmission of the specified message or all messages.

Default no mdl-transmit

Parameters **path** — Specifies the MDL path message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

idle-signal — Specifies the MDL idle signal message.

test-signal — Specifies the MDL test signal message.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

17.207 mdt-pim

mdt-pim

Syntax **mdt-pim mode** {**asm** | **ssm**} **group-address** *group-ip-address*
no mdt-pim

Context **[Tree]** (config>service>vprn>mvpn>pt>selective>multistream-spmsi mdt-pim)

Full Context configure service vprn mvpn provider-tunnel selective multistream-spmsi mdt-pim

Description This command creates a multi-stream MDT that could match many (C-S,C-G)s into a single data MDT.

Parameters *group-ip-address* — Specifies the group address of this data MDT, that is the provider group address.

Platforms All

17.208 mdt-type

mdt-type

Syntax **mdt-type** {**sender-receiver** | **sender-only** | **receiver-only**}
no mdt-type

Context **[Tree]** (config>service>vprn>mvpn mdt-type)

Full Context configure service vprn mvpn mdt-type

Description This command allows restricting MVPN instance per PE node to a specific role. By default, MVPN instance on a given PE node assumes the role of being a sender as well as receiver. This creates a mesh of MDT/PMSI across all PE nodes from this PE.

This command provides an option to configure either a sender-only or receiver-only mode per PE node. Restricting the role of a PE node prevents creating full mesh of MDT/PMSI across all PE nodes that are participating in MVPN instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

auto-rp-discovery cannot be enabled together with **mdt-type sender-only** or **mdt-type receiver-only**, or **wildcard-spmsi** configurations.

The **no** version of this command restores the default (sender-receiver).

Default mdt-type sender-receiver

Parameters **sender-receiver** — MVPN has both sender and receivers connected to PE node.

sender-only — MVPN has only senders connected to PE node.

receiver-only — MVPN has only receivers connected to PE node.

Platforms All

17.209 meas-interval

meas-interval

Syntax **meas-interval** {**5-mins** | **15-mins** | **1-hour** | **1-day**} [**create**]
no meas-interval {**5-mins** | **15-mins** | **1-hour** | **1-day**}

Context **[Tree]** (config>oam-pm>session meas-interval)

Full Context configure oam-pm session meas-interval

Description This command establishes the parameters of the individual measurement intervals utilized by the session. Multiple measurement intervals may be specified within the session. A maximum of three different measurement intervals may be configured under each session.

The **no** form of this command deletes the specified measurement interval.

Parameters **meas-interval** — Specifies the duration of the measurement interval.

Values 5-mins, 15-mins, 1-hour, 1-day

create — Creates the measurement interval.

Platforms All

17.210 measurement-template

measurement-template

Syntax **measurement-template** *template-name* [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no measurement-template *template-name*

Context **[Tree]** (config>test-oam>link-meas measurement-template)

Full Context configure test-oam link-measurement measurement-template

Description This command configures a measurement template identifier that can be assigned to the IP interface by name.

Configuration modifications can be made to the measurement template without disabling the template and while IP interfaces are actively referencing the **measurement-template**. Refer to the *7250 IXR OAM and Diagnostics Guide* for more information about which modifications will cause the test on associated IP interfaces to “Terminate” and restart.

The **no** form of this command removes the template name. A measurement template can be removed if no interfaces are referencing the template.

Parameters *template-name* — Specifies the measurement template name, up to 64 characters.

create — Keyword used to create the measurement template. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

measurement-template

Syntax **measurement-template** [*64 chars max*]
no measurement-template

Context **[Tree]** (config>router>if>if-attr>delay>dyn measurement-template)

Full Context configure router interface if-attribute delay dynamic measurement-template

Description This command specifies the measurement template name used on the interface. The **measurement-template** associated with the interface can be changed without disabling the test protocol used to carry the test packet. Changing or removing the **measurement-template** associated with the IP interface stops the test and removes all test results for the IP interface.

The **no** form of this command removes the **measurement-template**, which stops the test and removes all test results for the interface.

Default no measurement-template

Parameters *64 chars max* — Specifies the measurement template name, up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.211 med-out

med-out

Syntax **med-out** {*number* | **igp-cost**}
no med-out

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy med-out)

Full Context configure subscriber-mgmt bgp-peering-policy med-out

Description This command enables advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set with a route policy.

The **no** form of this command used at the global level reverts to default where the MED is not advertised.

Parameters *number* — Specifies the MED path attribute value, expressed as a decimal integer.

Values 0 to 4294967295

igp-cost — Specifies that the MED is set to the IGP cost of the given IP prefix.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

med-out

Syntax **med-out** {*number* | **igp-cost**}
no med-out

Context **[Tree]** (config>service>vprn>bgp med-out)
[Tree] (config>service>vprn>bgp>group med-out)
[Tree] (config>service>vprn>bgp>group>neighbor med-out)

Full Context configure service vprn bgp group med-out
configure service vprn bgp group neighbor med-out
configure service vprn bgp med-out

Description This command enables advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set via a route policy.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command used at the global level reverts to default where the MED is not advertised.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no med-out

Parameters *number* — Specifies the MED path attribute value, expressed as a decimal integer.

Values 0 to 4294967295

igp-cost — Specifies the MED is set to the IGP cost of the given IP prefix.

Platforms All

med-out

Syntax **med-out** {*number* | **igp-cost**}
no med-out

Context **[Tree]** (config>router>bgp med-out)
[Tree] (config>router>bgp>group med-out)
[Tree] (config>router>bgp>group>neighbor med-out)

Full Context configure router bgp group med-out
configure router bgp group neighbor med-out
configure router bgp med-out

Description This command enables advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set via a route policy.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to default where the MED is not advertised.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no med-out

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the MED path attribute value, expressed as a decimal integer.

Values 0 to 4294967295

igp-cost — Sets MED to the IGP cost of the given IP prefix.

Platforms All

17.212 medium-duration-flow-count

medium-duration-flow-count

Syntax [**no**] **medium-duration-flow-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-cntr medium-duration-flow-count)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-counters medium-duration-flow-count

Description This command includes the medium duration flow count in the AA subscriber's custom record. This command only applies to the 7750 SR.

The **no** form of this command excludes the medium duration flow count.

Default no medium-duration-flow-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.213 member

member

Syntax [**no**] **member** *port-id*

Context **[Tree]** (config>interface-group-handler member)

Full Context configure interface-group-handler member

Description This command binds the specified port with the associate Interface Group Handler. Up to eight **member** commands can be issued to add multiple ports to the associated IGH. The **member** must be a port or channel on a SONET or POS MDA. It must be a physical port or channel in network mode, and not bound to any router interfaces. A port or channel cannot be a member of more than one IGH at the same time. MLPPP bundles and their members cannot be IGH members.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the specified port ID from the associated IGH.

Parameters *port-id* — Identifies the port to be associated with the interface group handler.

Platforms All

member

Syntax [**no**] **member** *port-id*

Context **[Tree]** (config>port>multilink-bundle member)

Full Context configure port multilink-bundle member

Description This command binds a channel group to a multilink bundle. For IMA and MLFR groups, this command binds a channel group filling up the entire DS-1 or E-1. For MLPPP groups, fractional (n x ds0) DS1 or E1 links are also allowed. However, fractional DS1 links and fractional E1 links may not be combined in the same multilink bundle. If a channel with a different number of timeslots than the primary-link member is added to the bundle, a warning will be provided.

The **no** form of this command removes the specified channel group from the multilink bundle.

Parameters *port-id* — Specifies the physical port ID in the following format:

port-id	*slot*/*mda*/*port*.*channel*		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

Platforms 7450 ESS, 7750 SR-7/12/12e

member

Syntax **member** *port-id*
no member

Context **[Tree]** (config>eth-tunnel>path member)

Full Context configure eth-tunnel path member

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates a port with the path defined under the Ethernet tunnel. If the operator wants to replace an existing member port or control tag, the whole path needs to be shutdown first. The alternate path will be activated as a result keeping traffic interruption to a minimum. Then the whole path must be deleted, the alternate path precedence modified to primary before re-creating the new path.

The following port-level configuration needs to be the same across the two member ports of an Ethernet tunnel:

- port>ethernet>access>{ingress|egress}>queue-group
- port>ethernet>egress-scheduler-policy
- port>access>egress>pool
- port>ethernet>dot1q-etype
- port>ethernet>qinq-etype
- port>ethernet>pbb-etype
- port>ethernet>mtu

The Ethernet tunnel will inherit the configuration from the first member port for these parameters. Additional member port that is added must have the same configuration.

The operator is allowed to update these port parameters only if the port is the sole member of an Ethernet tunnel. This means that in the example below, the operator needs to remove port 1/1/4 and port 1/1/5 before being allowed to modify 1/1/1 for the above parameters.

```
eth-tunnel 1
  path 1
    member 1/1/1
  path 2
    member 1/1/4
eth-tunnel 2
  path 1
    member 1/1/1
  path 2
    member 1/1/5
```

The **no** form of this command is used just to indicate that a member is not configured. The procedure described above, based on the **no path** command must be used to un-configure/change the member port assigned to the path.

Default no member

Parameters *port-id* — Specifies the port-id associated with the path in the format x/y/z where x represents the IOM, y the MDA and z the port numbers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

member

Syntax **member** *encap-value* [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no member *encap-value*

Context **[Tree]** (config>connection-profile member)

Full Context configure connection-profile member

Description This command allows the adding of discrete VPI/VCI values to an ATM connection profile for assignment to an ATM SAP of an Apipe VLL of vc-type atm-cell.

Up to a maximum of 16 discrete VPI/VCI values can be configured in a connection profile. The user can modify the content of a profile which triggers a re-evaluation of all the ATM SAPs which are currently using the profile.

The **no** form of this command deletes the member from the configuration.

Parameters *encap-value* — Specifies the VPI and VCI values of this connection profile member.

Values vpi: NNI: 0 to 4095
UNI: 0 to 255
vci: 1, 2, 5 to 65535

Platforms 7450 ESS, 7750 SR-7/12/12e

member

Syntax [**no**] **member** *encap-id* [**to** *encap-id*]

Context **[Tree]** (config>service>vpls>sap>egress>encap-defined-qos>encap-group member)

Full Context configure service vpls sap egress encap-defined-qos encap-group member

Description This command adds or removes a member ISID or a range of contiguous ISID members to an encap-group. The user can add or remove members to the encap-group one at a time or as a range of contiguous values using the member command. However, when the **qos-per-member** option is enabled, members must be added or removed one at a time.

The **no** form of this command removes the single or range of ISID values from the encap-group.

Parameters *encap-id* — The value of the single encap-id or the start encap-id of the range. ISID is the only encap-id supported.

to *encap-id* — The value of the end encap-id of the range. ISID is the only encap-id supported.

Platforms All

member

Syntax [**no**] **member** *interface-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>isis>link-group>level member)

Full Context configure service vprn isis link-group level member

Description This command adds or removes a links to the associated link-group. The interface name should already exist before it is added to a link-group.

The **no** form of this command removes the specified interface from the associated link-group.

Parameters *interface-name* — Specifies the name of the interface to be added or removed from the associated link-group.

Platforms All

member

Syntax [**no**] **member** *member-id*

Context [Tree] (config>gmpls-tun-grp member)

Full Context configure gmpls-tun-grp member

Description This command configures a member of a GMPLS tunnel group. A member of a GMPLS tunnel group is a GMPLS LSP. All members of a tunnel group must have the same bandwidth. Up to 16 members may be configured for each GMPLS tunnel group.

The **no** form of this command removes the member.

Default no member

Parameters *member-id* — Specifies the identifier of the GMPLS tunnel group member.

Values 1 to 16

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

member

Syntax **member** *user-profile-name* [*user-profile-name*]
no member *user-profile-name*

Context [Tree] (config>system>security>user>console member)

Full Context configure system security user console member

Description This command is used to associate the user with a local command authorization profile.

A user can be associated with up to eight profiles.

The **no** form of this command removes the association between the user and the profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default member default

Parameters *user-profile-name* — Specifies up to eight user profile names, up to 32 characters.

Platforms All

member

Syntax [**no**] **member** *interface-name*

Context **[Tree]** (config>router>isis>link-group>level member)

Full Context configure router isis link-group level member

Description This command adds or removes a link to the associated link-group. The interface name should already exist before it is added to a link-group.

The **no** form of this command removes the specified interface from the associated link-group.

Parameters *interface-name* — Specifies the name of the interface to be added or removed from the associated link-group.

Platforms All

17.214 member-threshold

member-threshold

Syntax [**no**] **member-threshold** *threshold*

Context **[Tree]** (config>gmpls-tun-grp member-threshold)

Full Context configure gmpls-tun-grp member-threshold

Description The **member-threshold** is the number of member GMPLS LSPs that must be operationally up before the GMPLS tunnel group is considered operationally up. If that number is not reached, then the GMPLS tunnel group is taken operationally down.

A member of a GMPLS tunnel group may be treated as down for one of the following reasons. These reason codes are recorded in the tmnxGmplsTunGrpMemberTable in the MIB:

- adminDn — The member or the related tunnel group is admin down.
- wpLspDn — The associated GMPLS LSP working path is down.
- wpPortDn — The data-bearer port associated with the GMPLS LSP working path is down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- wpPortNoRsrc — The data bearer port associated with the LSP working path has no resource to support the services over the GMPLS tunnel group logical port.
- ppLspDn — The associated GMPLS LSP protect path is down.
- ppPortDn — The data-bearer port associated with the GMPLS LSP protect path is down.
- ppPortNoRsrc — The data bearer port associated with the GMPLS LSP protect path has no resource to support the services over the GMPLS tunnel group logical port.

The **no** form of this command resets the member threshold to 0.

Default member-threshold 0

Parameters *threshold* — Specifies the minimum number of GMPLS LSPs that must be operationally up before the GMPLS tunnel group is considered operationally up.

Values 0 to 15

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.215 members

members

Syntax [**no**] **members** *comm-id* [*comm-id*]

Context **[Tree]** (config>router>policy-options>community members)

Full Context configure router policy-options community members

Description This command adds members to a route policy community list to use in route policy entries.

The **no** version of this command deletes route policy community members.

Parameters *comm-id* — Specifies a BGP community value, up to 72 characters. A community ID can be specified in different forms.

Values [*as-num:comm-val* | *reg-ex* | *ext-comm* | *well-known-comm* | *large-comm*]

where:

- *as-num* — 0 to 65535
- *comm-val* — 0 to 65535
- *reg-ex* — A regular expression string. Allowed values are any string up to 72 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (such as “#”, “$”, or spaces), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *ext-comm* — The extended community, defined as one of the following:
  - {*target* | *origin*}:*ip-address*:*comm-val*
  - {*target* | *origin*}:*reg-ex1*&*reg-ex2*
  - {*target* | *origin*}:*ip-address*:*reg-ex2*
  - {*target* | *origin*}:*asnum*:*ext-comm-val*
  - {*target* | *origin*}:*ext-asnum*:*comm-val*
  - **bandwidth**:*asnum*:*val-in-mbps*
  - **ext:4300**:*ovstate*
  - **ext**:*value1*:*value2*
  - **flowspec-set**:*ext-asnum*:*group-id*
  - **flowspec-set-trans**:*ext-asnum*:*group-id*
  - **ipv6-redirect**: *ipv6-addr*
  - **color**:*co-bits*:*color-value*

  where:
  - *target* — route target
  - *origin* — route origin
  - *ip-address* — a.b.c.d
  - *ext-comm-val* — 0 to 4294967295
  - *ext-asnum* — 0 to 4294967295
  - *reg-ex1*, *reg-ex2* — A regular expression string. Allowed values are any string up to 63 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.
  - **bandwidth** — bandwidth
  - *val-in-mbps* — 0 to 16777215
  - **ext:4300** — origin verification
  - *ovstate* — 0, 1, or 2 (0 for valid, 1 for not found, 2 for invalid)
  - **ext** — extended
  - *value1* — 0000 to FFFF
  - *value2* — 0 to FFFFFFFFFFFF
  - **flowspec-set —** FlowSpec set
  - **flowspec-set-trans —** FlowSpec set transitive
  - *ipv6-addr* — x:x:x:x:x:x:x:x (eight 16-bit pieces)
  - *group-id* — 0 to 16383
  - *co-bits* — 00, 01, 10 or 11
  - *color-value* — 0 to 4294967295
- *well-known-comm* — **null**, **no-export**, **no-export-subconfed**, **no-advertise**, **llgr-stale**, **no-llgr**, **blackhole**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- *large-comm* — large community, defined as one of the following:
  - *ext-asnum*:*ext-comm-val*:*ext-comm-val*
  - *reg-ex3*&*reg-ex3*&*reg-ex3*

  where:
  - *reg-ex3* — A regular expression string. Allowed values are any string up to 68 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

17.216 memory

memory

Syntax **memory** *memory-size*
no memory

Context **[Tree]** (config>esa>vm memory)

Full Context configure esa vm memory

Description This command configures the amount of memory (in gigabytes) that is allocated to the ESA-VM instance.

The **no** form of this command removes the memory allocation. To modify the memory allocation, first invoke the **no memory** command.

Parameters *memory-size* — Specifies the amount of memory in GB.

Values 0 to 256

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

17.217 memory-alarm

memory-alarm

Syntax **memory-alarm high-threshold** *high-percentage* **low-threshold** *low-percentage*
no memory-alarm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>li>x-interfaces>x3>alarms memory-alarm)

Full Context configure li x-interfaces x3 alarms memory-alarm

Description This command configures the thresholds for raising the memory alarm. The low threshold value must be configured with a smaller value than the high threshold.

The **no** form of this command reverts to the default values.

Parameters *high-percentage* — Specifies the high threshold value, as a percentage.

Values 1 to 100

Default 100

low-percentage — Specifies the low threshold value, as a percentage.

Values 0 to 99

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.218 memory-use-alarm

memory-use-alarm

Syntax **memory-use-alarm rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no memory-use-alarm

Context [Tree] (config>system>thresholds memory-use-alarm)

Full Context configure system thresholds memory-use-alarm

Description The memory thresholds are based on monitoring the TIMETRA-SYSTEM-MIB sgiMemoryUsed object. This object contains the amount of memory currently used by the system. The severity level is Alarm. The absolute sample type method is used.

The **no** form of this command removes the configured memory threshold warning.

Parameters **rising-threshold** *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The threshold value represents units in bytes.

Values -2147483648 to 2147483647

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

The threshold value represents units in bytes.

Values -2147483648 to 2147483647

Default 0

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

The threshold value represents units in bytes.

Values 1 to 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create an OS logger entry. The RMON-MIB log table entries can be viewed using the CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

alarm-type — Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Configuration example

```
memory-use-alarm rising-threshold 50000000 falling-threshold 45999999
interval 500 rmon-event-type both start-alarm either
```

Platforms All

17.219 memory-use-warn

memory-use-warn

Syntax **memory-use-warn rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no memory-use-warn

Context **[Tree]** (config>system>thresholds memory-use-warn)

Full Context configure system thresholds memory-use-warn

Description The memory thresholds are based on monitoring MemoryUsed object. This object contains the amount of memory currently used by the system. The severity level is Alarm.

The absolute sample type method is used.

The **no** form of this command removes the configured compact flash threshold warning.

Parameters **rising-threshold** *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

The threshold value represents units in bytes.

Values -2147483648 to 2147483647

Default 0

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

The threshold value represents units in bytes.

Values -2147483648 to 2147483647

Default 0

seconds — Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 to 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence.

This does not create an SR OS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — An SR OS logger event is generated. The SR OS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session, memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both an entry in the RMON-MIB logTable and an SR OS logger event are generated.

none — No action is taken.

Default both

startup-alarm *alarm-type* — Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Default either

Values rising, falling, either

Configuration example

```
memory-use-warn rising-threshold 500000 falling-threshold 400000 interval 800 rmon-
event-type log start-alarm falling
```

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.220 mep

mep

Syntax [**no**] **mep** *mep-id* **domain** *md-index* **association** *ma-index*

Context **[Tree]** (config>eth-tunnel>path>eth-cfm mep)

Full Context configure eth-tunnel path eth-cfm mep

Description This command provisions an 802.1ag maintenance endpoint (MEP).

The **no** form of this command reverts to the default values.

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index — Specifies the MA index value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mep

Syntax [**no**] **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**vlan** *vlan-id*]

Context **[Tree]** (config>port>ethernet>eth-cfm mep)
[Tree] (config>lag>eth-cfm mep)
[Tree] (config>router>if>eth-cfm mep)

Full Context configure lag eth-cfm mep
configure port ethernet eth-cfm mep
configure router interface eth-cfm mep

Description This command provisions the maintenance endpoint (MEP).

The **no** form of this command reverts to the default values.

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ma-index — Specifies the MA index value.

Values 1 to 4294967295

vlan-id — Specific to tunnel facility MEPs which means this option is only applicable to the lag>eth-cfm> context. Used to specify the outer vlan id of the tunnel.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}] [**primary-vlan-enable**]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context **[Tree]** (config>service>epipe>sap>eth-cfm mep)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm mep)
[Tree] (config>service>ipipe>sap>eth-cfm mep)

Full Context configure service epipe sap eth-cfm mep
configure service epipe spoke-sdp eth-cfm mep
configure service ipipe sap eth-cfm mep

Description This command provisions the maintenance endpoint (MEP).

The **no** form of this command reverts to the default values.

Parameters *mep-id* — Specifies the maintenance endpoint identifier.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index — Specifies the maintenance association (MA) index value.

Values 1 to 4294967295

direction {up | **down}** — Indicates the direction in which the MEP faces on the bridge port. The UP direction is not supported for all Fpipe services. For example, Ipipe does not support the direction of UP for MEPs.

up — Sends ETH-CFM messages toward the MAC relay entity.

down — Sends ETH-CFM messages away from the MAC relay entity.

primary-vlan-enable — Provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA. This must be configured as part of the creation step and can only be changed by deleting the MEP and re-creating it. Primary VLANs are only supported under Layer 2 Epipe and VPLS services.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}] [**primary-vlan-enable**]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context **[Tree]** (config>service>vpls>mesh-sdp>eth-cfm mep)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm mep)
[Tree] (config>service>vpls>eth-cfm mep)
[Tree] (config>service>vpls>sap>eth-cfm mep)

Full Context configure service vpls eth-cfm mep
configure service vpls mesh-sdp eth-cfm mep
configure service vpls sap eth-cfm mep
configure service vpls spoke-sdp eth-cfm mep

Description This command configures the ETH-CFM maintenance endpoint (MEP). A MEP created at the VPLS service level **vpls>eth-cfm** creates a virtual MEP.

The **no** version of the command will remove the MEP.

Parameters *mep-id* — Specifies the MEP identifier.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index — Specifies the maintenance association (MA) index value.

Values 1 to 4294967295

direction up | down — Indicates the direction in which the MEP faces on the bridge port. Direction is not supported when a MEP is created directly under the vpls>eth-cfm construct (vMEP).

down — Sends ETH-CFM messages away from the MAC relay entity

up — Sends ETH-CFM messages toward the MAC relay entity

primary-vlan-enable — Provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA. MEPs cannot be changed from or to primary VLAN functions. This must be configured as part of the creation step and can only be changed by deleting the MEP and re-creating it. Primary VLANs are only supported under Layer 2 Epipe and VPLS services.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>eth-cfm mep)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm mep)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm mep)

Full Context configure service ies interface sap eth-cfm mep
configure service ies interface spoke-sdp eth-cfm mep
configure service ies subscriber-interface group-interface sap eth-cfm mep

Description This command configures the ETH-CFM maintenance endpoint (MEP).

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index — Specifies the MA index value.

Values 1 to 4294967295

direction up | down — The direction in which the maintenance association (MEP) faces on the bridge port. Direction UP is not applicable to IES MEPs.

down — Sends ETH-CFM messages away from the MAC relay entity.

up — Sends ETH-CFM messages towards the MAC relay entity.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep
- configure service ies interface sap eth-cfm mep

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context [Tree] (config>service>vprn>if>sap>eth-cfm mep)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm mep)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm mep)

Full Context configure service vprn interface sap eth-cfm mep
configure service vprn interface spoke-sdp eth-cfm mep
configure service vprn subscriber-interface group-interface sap eth-cfm mep

Description This command configures the ETH-CFM maintenance endpoint (MEP).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index — Specifies the MA index value.

Values 1 to 4294967295

direction up | down — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction UP is not supported on VPRN MEPs.

Values down — Sends continuity check messages away from the MAC relay entity.
up — Sends continuity check messages towards the MAC relay entity.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm mep
- configure service vprn interface sap eth-cfm mep

mep

Syntax [**no**] **mep**

Context **[Tree]** (config>router>mpls>lsp>working-tp-path mep)
[Tree] (config>router>mpls>lsp>protect-tp-path mep)

Full Context configure router mpls lsp protect-tp-path mep
configure router mpls lsp working-tp-path mep

Description This command creates or edits an MPLS-TP maintenance entity group (MEG) endpoint (MEP) on and MPLS-TP path. MEPs represent the termination point for OAM flowing on the path, as well as linear protection for the LSP. Only one MEP can be configured at each end of the path.

The following commands are applicable to a MEP on an MPLS-TP working or protect path: oam-template, bfd-enable, and shutdown. In addition, a protection-template may be configured on a protect path.

The **no** form of this command removes a MEP from an MPLS-TP path.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mep

Syntax [**no**] **mep** *mep-id* **domain** *md-index* **association** *ma-index*

Context **[Tree]** (debug>eth-cfm mep)

Full Context debug eth-cfm mep

Description This command specifies the MEP from which to debug the CFM PDUs.

The **no** form of this command removes the MEP parameters.

Parameters *mep-id* — Specifies the maintenance association endpoint identifier of the launch point.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value of the launch point.

Values 1 to 4294967295

ma-index — Specifies the maintenance association (MA) index value of the launch point.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mep

Syntax [**no**] **mep** ***mep-id*** **domain** *md-index* **association** *ma-index*

Context **[Tree]** (config>eth-ring>path>eth-cfm mep)

Full Context configure eth-ring path eth-cfm mep

Description This command provisions an 802.1ag maintenance endpoint (MEP).

The **no** form of the command deletes the MEP.

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 to 81921

md-index — Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index — Specifies the MA index value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.221 mesh-group

mesh-group

Syntax **mesh-group** {**value** | **blocked**}
no mesh-group

Context **[Tree]** (config>service>vprn>isis>if mesh-group)

Full Context configure service vprn isis interface mesh-group

Description This command assigns an interface to a mesh group. Mesh groups limit the amount of flooding that occurs when a new or changed LSP is advertised throughout an area.

All routers in a mesh group should be fully meshed. When LSPs need to be flooded, only a single copy is received rather than a copy per neighbor.

To create a mesh group, configure the same mesh group value for each interface that is part of the mesh group. All routers must have the same mesh group value configured for all interfaces that are part of the mesh group.

To prevent an interface from flooding LSPs, the optional **blocked** parameter can be specified. Configure mesh groups carefully. It is easy to create isolated islands that do not receive updates as (other) links fail.

The **no** form of this command removes the interface from the mesh group.

Default no mesh-group — The interface does not belong to a mesh group.

Parameters *value* — Specifies a unique decimal integer value distinguishes this mesh group from other mesh groups on this or any other router that is part of this mesh group.

Values 1 to 2000000000

blocked — Prevents an interface from flooding LSPs.

Platforms All

mesh-group

Syntax **mesh-group** {**value** | **blocked**}
no mesh-group

Context **[Tree]** (config>router>isis>interface mesh-group)

Full Context configure router isis interface mesh-group

Description This command assigns an interface to a mesh group. Mesh groups limit the amount of flooding that occurs when a new or changed LSP is advertised throughout an area.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All routers in a mesh group should be fully meshed. When LSPs need to be flooded, only a single copy is received rather than a copy per neighbor.

To create a mesh group, configure the same mesh group value for each interface that is part of the mesh group. All routers must have the same mesh group value configured for all interfaces that are part of the mesh group.

To prevent an interface from flooding LSPs, the optional **blocked** parameter can be specified. Configure mesh groups carefully to avoid creating isolated islands that do not receive updates as (other) links fail.

The **no** form of this command removes the interface from the mesh group.

Parameters *value* — Specifies the unique decimal integer value that distinguishes this mesh group from other mesh groups on this or any other router that is part of this mesh group.

Values 1 to 2000000000

blocked — Prevents an interface from flooding LSPs.

Platforms All

17.222 mesh-sdp

mesh-sdp

Syntax **mesh-sdp** *sdp-id*[*:vc-id*] [**vc-type** {**ether** | **vlan**}] [**create**]
mesh-sdp *sdp-id*[*:vc-id*] [**vc-type** {**ether** | **vlan**}] [**create**] **leaf-ac**
mesh-sdp *sdp-id*[*:vc-id*] [**vc-type** {**ether** | **vlan**}] [**create**] **root-leaf-tag**
no mesh-sdp *sdp-id*[*:vc-id*]

Context **[Tree]** (config>service>vpls mesh-sdp)

Full Context configure service vpls mesh-sdp

Description This command binds a VPLS service to an existing Service Distribution Point (SDP).

Mesh SDPs bound to a service are logically treated like a single bridge “port” for flooded traffic where flooded traffic received on any mesh SDP on the service is replicated to other “ports” (spoke SDPs and SAPs) and not transmitted on any mesh SDPs.

Note: This command creates a binding between a service and an SDP. The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SDP must already be defined in the **config>service>sdp** context in order to associate the SDP with an Epipe or VPLS service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end router devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No *sdp-id* is bound to a service.

Special Cases **VPLS —** Several SDPs can be bound to a VPLS. Each SDP must be destined to a different router. If two *sdp-id* bindings terminate on the same router, an error occurs and the second SDP binding is rejected.

Parameters *sdp-id* — Specifies an SDP identifier.

Values 1 to 17407

vc-id — Specifies a virtual circuit identifier. This value is used to validate the VC ID portion of each mesh SDP binding defined in the service. The default value of this object is equal to the service ID. Any value may be used for the *vc-id* when there is no existing mesh SDP within the service; if a mesh SDP exists then all other mesh SDPs in the service must be configured with the same *vc-id*.

Values 1 to 4294967295

vc-type — Specifies to override the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the binding's VC type causes the binding to signal the new VC type to the far end when signaling is enabled.

VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

The VC type value for Ethernet is 0x0005.

The VC type value for an Ethernet VLAN is 0x0004.

ether — Defines the VC type as Ethernet. The **vlan** keyword is mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke SDP binding (hex 5).

vlan — Defines the VC type as VLAN. The top VLAN tag, if a VLAN tag is present, is stripped from traffic received on the pseudowire, and a vlan-tag is inserted when forwarding into the pseudowire. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for mesh SDP bindings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The system expects a symmetrical configuration with its peer, specifically it expects to remove the same number of VLAN tags from received traffic as it adds to transmitted traffic. As some of the related configuration parameters are local and not communicated in the signaling plane, an asymmetrical behavior cannot always be detected and so cannot be blocked. Consequently, protocol extractions will not necessarily function for asymmetrical configurations as they would with a symmetrical configurations resulting in an unexpected operation.

root-leaf-tag — Specifies a tagging mesh SDP under an E-Tree VPLS. When a tag SDP binding is required, it is created with a root-leaf-tag flag. Only VLAN tag SDP bindings are supported. The VLAN type must be set to VC VLAN type. The root-leaf-tag parameter indicates this SDP binding is a tag SDP that uses a default VID 1 for root and 2 for leaf. The SDP binding tags egress E-Tree traffic with root and leaf VIDs as appropriate. Root and leaf VIDs are only significant between peering VPLS but the values must be consistent on each end. On ingress a tag SDP binding removes the VID tag on the interface between VPLS in the same E-Tree service. The tag SDP receives root tagged traffic and marks the traffic with a root indication internally. This option is not available on BGP EVPN-enabled E-Tree services.

leaf-ac — Specifies an access (AC) mesh SDP binding under a E-Tree VPLS as a leaf access (AC) SDP. The default E-Tree SDP type is a root AC if *leaf-ac* or *root-leaf-tag* is not specified at SDP binding creation. This option is only available when the VPLS is designated as an E-Tree VPLS. BGP EVPN-enabled E-Tree VPLS services support the **leaf-ac** option.

create — Keyword used to create the mesh SDP. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

17.223 mesh-sdp-binding

mesh-sdp-binding

Syntax [**no**] **mesh-sdp-binding**

Context **[Tree]** (config>service>vpls>site mesh-sdp-binding)

Full Context configure service vpls site mesh-sdp-binding

Description This command enables applications to all mesh SDPs.

The **no** form of reverts the default.

Default no mesh-sdp-binding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.224 message

message

Syntax **message** {**eq** | **neq**} **pattern** *pattern* [**regexp**]
no message

Context **[Tree]** (config>service>vprn>log>filter>entry>match message)

Full Context configure service vprn log filter entry match message

Description This command adds system messages as a match criterion.

The **no** form of this command removes messages as a match criterion.

Parameters **eq** — Determines if the matching criteria should be equal to the specified value.

neq — Determines if the matching criteria should not be equal to the specified value.

pattern — Specifies a message, up to 400 characters, to be used in the match criteria.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **message** command parameters. When the **regexp** keyword is not specified, the default matching algorithm used is a basic substring match.

Platforms All

message

Syntax **message** {**eq** | **neq**} **pattern** *pattern* [**regexp**]
no message

Context **[Tree]** (config>log>filter>entry>match message)

Full Context configure log filter entry match message

Description This command adds system messages as a match criterion.

The **no** form of this command removes messages as a match criterion.

Parameters **eq** — Determines if the matching criteria should be equal to the specified value.

neq — Determines if the matching criteria should not be equal to the specified value.

pattern — Specifies a message up to 400 characters in length to be used in the match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **message** command parameters. When the **regexp** keyword is not specified, the default matching algorithm used is a basic substring match.

Platforms All

17.225 message-count

message-count

Syntax **message-count** *count*

Context **[Tree]** (config>ipsec>tnl-temp>icmp6-gen>pkt-too-big message-count)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>icmp6-gen>pkt-too-big message-count)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>icmp6-gen>pkt-too-big message-count)
[Tree] (config>service>vprn>if>sap>ipsec-tun>icmp6-gen>pkt-too-big message-count)
[Tree] (config>router>if>ipsec-tunnel>icmp-gen>pkt-too-big message-count)

Full Context configure ipsec tunnel-template icmp6-generation pkt-too-big message-count
configure router interface ipsec-tunnel icmp-gen pkt-too-big message-count
configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big message-count
configure service vprn interface ipsec ipsec-tunnel icmp6-generation pkt-too-big message-count
configure service vprn interface sap ipsec-tunnel icmp6-generation pkt-too-big message-count

Description This command configures the maximum number of ICMPv6 messages that can be sent during the configured interval.

Parameters *count* — Specifies the maximum number of ICMPv6 messages that can be sent during the configured interval

Values 10 to 1000

Default 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel icmp6-generation pkt-too-big message-count
- configure ipsec tunnel-template icmp6-generation pkt-too-big message-count

VSR

- configure service vprn interface ipsec ipsec-tunnel icmp6-generation pkt-too-big message-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big message-count

message-count

Syntax **message-count** *number*

Context **[Tree]** (config>ipsec>tnl-temp>icmp-gen>frag-required message-count)
[Tree] (config>router>if>ipsec>ipsec-tunnel>icmp-gen>frag-required message-count)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>icmp-gen>frag-required message-count)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>icmp-gen>frag-required message-count)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel>icmp-gen>frag-required message-count)
[Tree] (config>service>vprn>if>sap>ip-tunnel>icmp-gen>frag-required message-count)

Full Context configure ipsec tunnel-template icmp-generation frag-required message-count
configure router interface ipsec ipsec-tunnel icmp-generation frag-required message-count
configure service ies interface ipsec ipsec-tunnel icmp-generation frag-required message-count
configure service vprn interface ipsec ipsec-tunnel icmp-generation frag-required message-count
configure service vprn interface sap ip-tunnel icmp-generation frag-required message-count
configure service vprn interface sap ipsec-tunnel icmp-generation frag-required message-count

Description This command configures the maximum number of ICMP Destination Unreachable "fragmentation needed and DF set" messages (type 3, code 4) that can be sent during the period specified by the **interval** *seconds* command.

Default message-count 100

Parameters *number* — Specifies the number of ICMP Destination Unreachable "fragmentation needed and DF set" messages that are transmitted within the **interval** *seconds* command time.

Values 10 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec tunnel-template icmp-generation frag-required message-count
- configure service vprn interface sap ip-tunnel icmp-generation frag-required message-count
- configure service vprn interface sap ipsec-tunnel icmp-generation frag-required message-count

VSR

- configure service vprn interface ipsec ipsec-tunnel icmp-generation frag-required message-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router interface ipsec ipsec-tunnel icmp-generation frag-required message-count
- configure service ies interface ipsec ipsec-tunnel icmp-generation frag-required message-count

17.226 message-digest-key

message-digest-key

Syntax **message-digest-key** *keyid* **md5** [*key* | *hash-key*] [**hash** | **hash2** | **custom**]
no message-digest-key *keyid*

Context **[Tree]** (config>service>vprn>ospf>area>if message-digest-key)
[Tree] (config>service>vprn>ospf>area>virtual-link message-digest-key)
[Tree] (config>service>vprn>ospf>area>sham-link message-digest-key)

Full Context configure service vprn ospf area interface message-digest-key
configure service vprn ospf area sham-link message-digest-key
configure service vprn ospf area virtual-link message-digest-key

Description This command configures a message digest key when MD5 authentication is enabled on the interface, virtual-link or sham-link. Multiple message digest keys can be configured.

This command is not valid in the OSPF3 context.

The **no** form of this command removes the message digest key identified by the *key-id*.

Default No message digest keys are defined.

Parameters **keyid** — The *keyid* is expressed as a decimal integer.

Values 1 to 255

md5 *key* — The MD5 key. The *key* can be any alphanumeric string up to 16 characters in length.

md5 *hash-key* — The MD5 hash key. The key can be any combination of ASCII characters up to 32 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms All

message-digest-key

Syntax **message-digest-key** *key-id* **md5** [*key* | *hash-key* | *hash2-key*] [**hash** | **hash2** | **custom**]
no message-digest-key *key-id*

Context **[Tree]** (config>router>ospf>area>interface message-digest-key)
[Tree] (config>router>ospf>area>virtual-link message-digest-key)

Full Context configure router ospf area interface message-digest-key
configure router ospf area virtual-link message-digest-key

Description This command configures a message digest key when MD5 authentication is enabled on the interface. Multiple message digest keys can be configured.

The **no** form of this command removes the message digest key identified by the *key-id*.

By default, no message keys are defined.

Parameters *key-id* — The *keyid* is expressed as a decimal integer.

Values 1 to 255

key — Specifies the MD5 key. The *key* can be any alphanumeric string up to 16 characters in length.

hash-key | *hash2-key* — Specifies the MD5 hash or hash2 key. the hash key. The key can be any combination of ASCII characters up to 32 (hash1-key) or 55 (hash2-key) characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

custom — Specifies the custom encryption to management interface.

Platforms All

17.227 message-fast-tx

message-fast-tx

Syntax **message-fast-tx** *time*
no message-fast-tx

Context **[Tree]** (config>system>lldp message-fast-tx)

Full Context configure system lldp message-fast-tx

Description This command configures the duration of the fast transmission period.

Default no message-fast-tx

Parameters *time* — Specifies the fast transmission period in seconds.

Values 1 to 3600

Default 1

Platforms All

17.228 message-fast-tx-init

message-fast-tx-init

Syntax **message-fast-tx-init** *count*
no message-fast-tx-init

Context **[Tree]** (config>system>lldp message-fast-tx-init)

Full Context configure system lldp message-fast-tx-init

Description This command configures the number of LLDPDUs to send during the fast transmission period.

Default no message-fast-tx-init

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the number of LLDPDUs to send during the fast transmission period.

Values 1 to 8

Default 4

Platforms All

17.229 message-interval

message-interval

Syntax **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
no message-interval

Context **[Tree]** (config>service>ies>if>ipv6>vrrp message-interval)

Full Context configure service ies interface ipv6 vrrp message-interval

Description This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner **vrrp** *virtual-router-id* nodal contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The **no** form of this command restores the default message interval value of 1 second to the virtual router instance.

Default message-interval 1

Parameters *seconds* — The number of seconds that will transpire before the advertisement timer expires.

Values 1 to 255

Default 1

milliseconds *milliseconds* — Specifies the time interval, in milliseconds, between sending advertisement messages.

Values 100 to 900

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

message-interval

Syntax **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
no message-interval

Context **[Tree]** (config>service>ies>if>vrrp message-interval)

Full Context configure service ies interface vrrp message-interval

Description This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner **vrrp** *virtual-router-id* nodal contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The **no** form of this command restores the default message interval value of 1 second to the virtual router instance.

Parameters *seconds* — The number of seconds that will transpire before the advertisement timer expires.

Values 1 to 255

Default 1

milliseconds *milliseconds* — Specifies the time interval, in milliseconds, between sending advertisement messages. This parameter is not supported on non-redundant chassis.

Values 100 to 900

Platforms All

message-interval

Syntax **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
no message-interval

Context **[Tree]** (config>service>vprn>if message-interval)
[Tree] (config>service>vprn>if>ipv6>vrrp message-interval)

Full Context configure service vprn interface ipv6 vrrp message-interval
configure service vprn interface message-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner **vrrp** *virtual-router-id* nodal contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The **no** form of this command restores the default message interval value of 1 second to the virtual router instance.

Parameters *seconds* — The number of seconds that will transpire before the advertisement timer expires.

Values 1 to 255

Default 1

milliseconds *milliseconds* — Specifies the time interval, in milliseconds, between sending advertisement messages. This parameter is not supported on single-slot chassis.

Values 100 to 900

Platforms All

message-interval

Syntax **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
no message-interval

Context **[Tree]** (config>router>if>vrrp message-interval)
[Tree] (config>router>if>ipv6>vrrp message-interval)

Full Context configure router interface ipv6 vrrp message-interval
configure router interface vrrp message-interval

Description This command configures the administrative advertisement message timer used by the master virtual router instance to send VRRP advertisement messages and to derive the master down timer as backup.

For an owner virtual router instance, the administrative advertisement timer directly sets the operational advertisement timer and indirectly sets the master down timer for the virtual router instance.

Non-owner virtual router instances usage of the **message-interval** setting is dependent on the state of the virtual router (master or backup) and the state of the **master-int-inherit** parameter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- When a non-owner is operating as master for the virtual router, the configured **message-interval** is used as the operational advertisement timer similar to an owner virtual router instance. The **master-int-inherit** command has no effect when operating as master.
- When a non-owner is in the backup state with **master-int-inherit** disabled, the configured **message-interval** value is used to match the incoming VRRP advertisement message advertisement interval field. If the locally configured message interval does not match the advertisement interval field, the VRRP advertisement is discarded.
- When a non-owner is in the backup state with **master-int-inherit** enabled, the configured **message-interval** is ignored. The master down timer is indirectly derived from the incoming VRRP advertisement message advertisement interval field value.

VRRP advertisements messages that are fragmented, or contain IP options (IPv4), or contain extension headers (IPv6) require a longer message interval to be configured.

The in-use value of the message interval is used to derive the master down timer to be used when the virtual router is operating in backup mode based on the following formula:

(3x (in-use message interval) + skew time)

The skew time portion is used to slow down virtual routers with relatively low priority values when competing in the master election process.

The command is available in both non-owner and owner **vrrp** nodal contexts.

By default, a **message-interval** of 1 second is used.

The **no** form of the command reverts to the default value.

Default message-interval 1 — Advertisement timer set to 1 second.

Parameters *seconds* — The number of seconds that will transpire before the advertisement timer expires expressed as a decimal integer.

Values IPv4: 1 to 255 IPv6: 1 to 40

milliseconds — Specifies the time interval, in milliseconds, between sending advertisement messages.

Values 100 to 900 IPv6: 10 to 990

Platforms All

17.230 message-length

message-length

Syntax **message-length** *message-length*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no message-length

Context [Tree] (config>service>sdp>keep-alive message-length)

Full Context configure service sdp keep-alive message-length

Description This command configures the SDP monitoring keepalive request message length transmitted.

The **no** form of this command reverts the **message-length** *octets* value to the default setting.

Default no message-length — The message length should be equal to the SDP's operating path MTU as configured in the **config>service>sdp path-mtu** command. If the default size is overridden, the actual size used will be the smaller of the operational SDP ID Path MTU and the size specified.

Parameters *message-length* — Specifies the size of the keepalive request messages in octets, expressed as a decimal integer. The **size** keyword overrides the default keepalive message size.

Values 40 to 9198

Platforms All

17.231 message-path

message-path

Syntax **message-path** *sap-id*
no message-path

Context [Tree] (config>service>ies>sub-if>grp-if>srrp message-path)
[Tree] (config>service>vprn>sub-if>grp-if>srrp message-path)

Full Context configure service ies subscriber-interface group-interface srrp message-path
configure service vprn subscriber-interface group-interface srrp message-path

Description This command defines a specific SAP for SRRP in-band messaging. A message-path SAP must be defined prior to activating the SRRP instance. The defined SAP must exist on the SRRP instances group IP interface for the command to succeed and cannot currently be associated with any dynamic or static subscriber hosts. Once a group IP interface SAP has been defined as the transmission path for SRRP Advertisement messages, it cannot be administratively shutdown, will not support static or dynamic subscriber hosts and cannot be removed from the group IP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SRRP instance message-path command may be executed at any time on the SRRP instance. Changing the message SAP fails if a dynamic or static subscriber host is associated with the new SAP. Once successfully changed, the SRRP instance immediately disables anti-spoof on the SAP and starts sending SRRP Advertisement messages, if the SRRP instance is activated.

Changing the current SRRP message SAP on an active pair of routers should be done in the following manner:

1. Shutdown the backup SRRP instance.
2. Change the message SAP on the shutdown node.
3. Change the message SAP on the active master node.
4. Re-activate the shutdown SRRP instance.

Shutting down the backup SRRP instance prevents the SRRP instances from becoming master due to temporarily using differing message path SAPs.

If an MCS peering is operational between the redundant nodes and the SRRP instance has been associated with the peering, the designated message path SAP is sent from each member.

The **no** form of this command can only be executed when the SRRP instance is shutdown. Executing no message-path allows the existing SAP to be used for subscriber management functions. A new message-path SAP must be defined prior to activating the SRRP instance.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.232 message-retransmit

message-retransmit

Syntax **message-retransmit** [**timeout** *timeout*] [**retry-count** *value*]
no message-retransmit

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile message-retransmit)

Full Context configure subscriber-mgmt gtp peer-profile message-retransmit

Description This command configures the retry-count and response-timeout for GTP messages.

The **no** form of this command reverts to the default values.

Default message-retransmit timeout 5 retry-count 3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *timeout* — Specifies the interval, in seconds, between retransmission of signaling request messages towards the same peer Mobile Gateway.

Values 1 to 30

Default 5

value — Specifies the number of times a signaling request message is transmitted towards the same peer Mobile Gateway.

Values 1 to 8

Default 3

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.233 message-severity-level

message-severity-level

Syntax **message-severity-level**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment message-severity-level)

Full Context configure system management-interface cli md-cli environment message-severity-level

Description This command configures the message severity level.

Platforms All

17.234 message-size

message-size

Syntax **message-size** *max-num-of-routes*
no message-size

Context **[Tree]** (config>service>vprn>rip message-size)
[Tree] (config>service>vprn>rip>group message-size)
[Tree] (config>service>vprn>rip>group>neighbor message-size)
[Tree] (config>service>vprn>ripng message-size)
[Tree] (config>service>vprn>ripng>group message-size)
[Tree] (config>service>vprn>ripng>group>neighbor message-size)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn rip group message-size
configure service vprn rip group neighbor message-size
configure service vprn rip message-size
configure service vprn ripng group message-size
configure service vprn ripng group neighbor message-size
configure service vprn ripng message-size

Description This command sets the maximum number of routes per RIP update message.

The **no** form of this command resets the maximum number of routes back to the default of 25.

Default no message-size

Parameters *size* — An Integer.

Values 25 to 255

Default 25

Platforms All

message-size

Syntax **message-size** *max-num-of-routes*
no message-size

Context **[Tree]** (config>router>rip message-size)
[Tree] (config>router>rip>group message-size)
[Tree] (config>router>rip>group>neighbor message-size)
[Tree] (config>router>ripng message-size)
[Tree] (config>router>ripng>group message-size)
[Tree] (config>router>ripng>group>neighbor message-size)

Full Context configure router rip group message-size
configure router rip group neighbor message-size
configure router rip message-size
configure router ripng group message-size
configure router ripng group neighbor message-size
configure router ripng message-size

Description This command configures the maximum number of routes per RIP update message.

The **no** form of the command reverts to the default value.

Default message-size 25

Parameters *max-num-of-routes* — The maximum number of RIP routes per RIP update message expressed as a decimal integer.

Values 25 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.235 message-timeout

message-timeout

Syntax **message-timeout** *seconds*

Context **[Tree]** (config>li>x-interfaces>x1>timeouts message-timeout)

Full Context configure li x-interfaces x1 timeouts message-timeout

Description This command configures the maximum time that the LIC must reply to an X1 message. If the timer expires, the session is released.

Parameters *seconds* — Specifies the maximum timeout value, in seconds.

Values 180 to 300

Default 180

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.236 message-type

message-type

Syntax **message-type** [**ccr**] [**cca**] [**rar**] [**raa**] [**asr**] [**asa**] [**aar**] [**aaa**]
message-type all
no message-type

Context **[Tree]** (debug>diam>diam-peer-plcy>avp-match message-type)

Full Context debug diameter diameter-peer-policy avp-match message-type

Description This command specifies the message type match criteria for AVP value matching. Only specified diameter application messages are used for AVP value matching. This is a mandatory criteria in an **avp-match** *id* command.

This command does not restrict the debug output to the specified messages.

Parameters **ccr** — credit control request

cca — credit control answer

rar — re-authentication request

raa — re-authentication answer

asr — abort session request

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

asa — abort session answer

aar — aa request

aaa — aa answer

all — all message types

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

message-type

Syntax **message-type** [**ccr**] [**cca**] [**cer**] [**cea**] [**dwr**] [**dwa**] [**dpr**] [**dpa**] [**rar**] [**raa**] [**asr**] [**asa**] [**aar**] [**aaa**]
message-type all
no message-type

Context **[Tree]** (debug>diam>diam-peer-plcy message-type)
[Tree] (debug>diam message-type)

Full Context debug diameter diameter-peer-policy message-type
debug diameter message-type

Description This command restricts the debug output to the specified message types.

When specified within a diameter peer policy, it overrides the message type configuration at the **debug>diam** level for messages received and sent on that diameter peer policy.

The **no** form of this command removes the message type from the debug configuration.

Parameters **ccr** — credit control request

cca — credit control answer

cer — capabilities exchange request

cea — capabilities exchange answer

dwr — device watchdog request

dwa — device watchdog answer

dpr — disconnect peer request

dpa — disconnect peer answer

rar — re-authentication request

raa — re-authentication answer

asr — abort session request

asa — abort session answer

aar — aa request

aaa — aa answer

all — all message types

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

message-type

Syntax **message-type**

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter message-type)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type

Description This command configures a TCA for the counter capturing hits due to the GTP filter message type.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

message-type

Syntax **message-type**

Context **[Tree]** (config>app-assure>group>gtp>gtp-filter message-type)

Full Context configure application-assurance group gtp gtp-filter message-type

Description This command specifies the context for configuration of GTP message-type filtering. If no **message-type** is specified within a filter, then all GTP message types are allowed.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.237 message-type-gtpv2

message-type-gtpv2

Syntax **message-type-gtpv2**

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter message-type-gtpv2)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter message-type-gtpv2

Description This command configures a TCA for the counter capturing hits due to the GTPv2 message type filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

message-type-gtpv2

Syntax **message-type-gtpv2**

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr message-type-gtpv2)

Full Context configure application-assurance group gtp gtp-filter message-type-gtpv2

Description This command specifies the context for the configuration of GTP-v2 message-type filtering. If no **message-type-gtpv2** is specified within a filter, then all GTP message types are allowed, except for the messages that are dropped by GTP-C inspection because they violate the expected GTP protocol for the deployment interface (for example, roaming deployment).

The **gtpc-inspection** command must be enabled before configuring **message-type-gtpv2** filtering.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.238 messages

messages

Syntax [**no**] **messages**

Context **[Tree]** (debug>router>ldp>if>event messages)
[Tree] (debug>router>ldp>peer>event messages)

Full Context debug router ldp interface event messages
debug router ldp peer event messages

Description This command displays specific information (for example, message type, source, and destination) regarding LDP messages sent to and received from LDP peers.

The **no** form of the command disables debugging output for LDP messages.

Platforms All

17.239 meta-data

meta-data

Syntax **meta-data**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action>insert-nsh meta-data)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action insert-nsh meta-data

Description Commands in this context configure opaque metadata to be inserted in NSH in the steered traffic if the forward action indicates NSH insertion.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.240 metering-process

metering-process

Syntax **metering-process** {**standard** | **fp-accelerated**}

Context [Tree] (config>cflowd>sample-profile metering-process)

Full Context configure cflowd sample-profile metering-process

Description This command specifies the method used to process cflowd samples.

Default metering-process standard

Parameters **standard** — Specifies that the samples are extracted at the CPM and are processed there.

fp-accelerated — Specifies to use FP acceleration for cflowd processing, in which flow processing and reporting is performed by the FP complex on the CPM.

Platforms 7750 SR-7s

17.241 metric

metric

Syntax **metric** *value*
no metric

Context [Tree] (config>service>vpls>sap>spb>level metric)
[Tree] (config>service>vpls>spoke-sdp>spb>level metric)

Full Context configure service vpls sap spb level metric
configure service vpls spoke-sdp spb level metric

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This configures metric for this SPB interface SAP/spoke-sdp. This command is valid only for interfaces on control B-VPLS.

Parameters *value* — The configuration metric value.

Values 1 to 16777215

Default 1000

Platforms All

metric

Syntax **metric** *metric-value*
no metric [*metric-value*]

Context **[Tree]** (config>service>vprn>static-route-entry>black-hole metric)
[Tree] (config>service>vprn>static-route-entry>next-hop metric)
[Tree] (config>service>vprn>static-route-entry>grt metric)
[Tree] (config>service>vprn>static-route-entry>indirect metric)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel metric)

Full Context configure service vprn static-route-entry black-hole metric
configure service vprn static-route-entry grt metric
configure service vprn static-route-entry indirect metric
configure service vprn static-route-entry ipsec-tunnel metric
configure service vprn static-route-entry next-hop metric

Description This command specifies the cost metric for the static route, expressed as a decimal integer. This value is used when importing the static route into other protocols such as OSPF. When the metric is configured as 0 then the metric configured in OSPF, default-import-metric, applies. When modifying the metric of an existing static route, the preference will not change unless specified. This value is also used to determine which static route to install in the forwarding table.

If there are multiple static routes with the same preference but different metrics then the lower cost (metric) route will be installed.

The **no** form of this command returns the metric to the default value

Default metric 1

Parameters *metric-value* — Specifies the cost metric value.

Values 0 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>service>vprn>isis>if>level metric)

Full Context configure service vprn isis interface level metric

Description This command configures the metric used for the level on the interface.

In order to calculate the lowest cost to reach a given destination, each configured level on each interface must have a cost. The costs for each level on an interface may be different.

If the metric is not configured, the default of 10 is used unless reference bandwidth is configured.

The **no** form of this command reverts to the default value.

Default no metric

Parameters *metric* — The metric assigned for this level on this interface.

Values 1 to 16777215

Default 10

Platforms All

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>service>vprn>ospf>area>if metric)
[Tree] (config>service>vprn>ospf3>area>if metric)
[Tree] (config>service>vprn>ospf>area>sham-link metric)

Full Context configure service vprn ospf area interface metric
configure service vprn ospf area sham-link metric
configure service vprn ospf3 area interface metric

Description This command configures an explicit route cost metric for the OSPF interface that overrides the metrics calculated based on the speed of the underlying link.

The **no** form of this command deletes the manually configured interface metric, so the interface uses the computed metric based on the **reference-bandwidth** command setting and the speed of the underlying link.

Default no metric

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — The metric to be applied to the interface expressed as a decimal integer.

Values 1 to 65535

Platforms All

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>router>mpls>lsp metric)
[Tree] (config>router>mpls>lsp-template metric)
[Tree] (config>router>mpls>static-lsp metric)

Full Context configure router mpls lsp metric
configure router mpls lsp-template metric
configure router mpls static-lsp metric

Description This command allows the user to override the LSP operational metric with a constant administrative value that will not change regardless of the actual path the LSP is using over its lifetime.

The LSP operational metric will match the metric the active path of this LSP is using at any given time. For a CSPF LSP, this metric represents the cumulative IGP metric of all the links the active path is using. If CSPF for this LSP is configured to use the TE metric, the LSP operational metric is set to the maximum value. For a non-CSPF LSP, the operational metric is the shortest IGP cost to the destination of the LSP.

The LSP operational metric is used by some applications to select an LSP among a set of LSPs that are destined to the same egress router. The LSP with the lowest operational metric will be selected. If more than one LSP with the same lowest LSP metric exists, the LSP with the lowest tunnel index will be selected. The configuration of a constant metric by the user will make sure the LSP always maintains its preference in this selection regardless of the path it is using at any given time. Applications that use the LSP operational metric include LDP-over-RSVP, VPRN auto-bind, and IGP, BGP and static route shortcuts.

The **no** form of this command disables the administrative LSP metric and reverts to the default setting in which the metric value will represent the LSP metric returned by MPLS. The same behavior is obtained if the user entered a metric of value zero (0).

Default no metric. The LSP operational metric defaults to the metric returned by MPLS.

Parameters *metric* — Specifies the integer value which specifies the value of the LSP administrative metric. A value of zero command reverts to the default setting and disables the administrative LSP metric.

Values 0 to 16777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy metric)

Full Context configure router mpls forwarding-policies forwarding-policy metric

Description This command configures the metric of an MPLS forwarding policy.

The *metric* parameter is supported with the endpoint policy only and is inherited by the routes which resolve their next hop to this policy.

The **no** form of this command removes the *metric* parameter from the MPLS forwarding policy.

Parameters *metric* — Specifies the metric value.

Values 1 to 16777215

Platforms All

metric

Syntax **metric** *metric*
no metric [*metric*]

Context **[Tree]** (config>router>static-route-entry>black-hole metric)
[Tree] (config>router>static-route-entry>indirect metric)
[Tree] (config>router>static-route-entry>next-hop metric)

Full Context configure router static-route-entry black-hole metric
configure router static-route-entry indirect metric
configure router static-route-entry next-hop metric

Description This command specifies the cost metric for the static route, expressed as a decimal integer. This value is used when importing the static route into other protocols such as OSPF. When the metric is configured as 0 then the metric configured in OSPF, default-import-metric, applies. When modifying the metric of an existing static route, the preference will not change unless specified. This value is also used to determine which static route to install in the forwarding table.

If there are multiple static routes with the same preference but different metrics then the lower cost (metric) route will be installed.

The **no** form of this command returns the metric to the default value

Default metric 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — Specifies the cost metric value.

Values 0 to 65535

Platforms All

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>service>sdp metric)

Full Context configure service sdp metric

Description This command specifies the metric to be used within the tunnel table manager for decision making purposes. When multiple SDPs going to the same destination exist, this value is used as a tie-breaker by tunnel table manager users such as MP-BGP to select the route with the lower value.

Parameters *metric* — Specifies the SDP metric.

Values 0 to 65535

Platforms All

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>router>isis>if>level metric)

Full Context configure router isis interface level metric

Description This command configures the metric used for the level on the interface.

In order to calculate the lowest cost to reach a given destination, each configured level on each interface must have a cost. The costs for each level on an interface may be different.

If the metric is not configured, the default of 10 is used unless reference bandwidth is configured.

The **no** form of this command reverts to the default value.

Default metric 10

Parameters *metric* — Specifies the metric assigned for this level on this interface.

Values 1 to 16777215

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>router>ospf>area>interface metric)
[Tree] (config>router>ospf3>area>interface metric)

Full Context configure router ospf area interface metric
configure router ospf3 area interface metric

Description This command configures an explicit route cost metric for the OSPF interface that overrides the metrics calculated based on the speed of the underlying link.

The **no** form of this command deletes the manually configured interface metric, so the interface uses the computed metric based on the **reference-bandwidth** command setting and the speed of the underlying link.

Default no metric

Parameters *metric* — Specifies the metric to be applied to the interface expressed as a decimal integer.

Values 1 to 65535

Platforms All

metric

Syntax **metric** *metric* [**equal** | **or-higher** | **or-lower**]
no metric

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from metric)

Full Context configure router policy-options policy-statement entry from metric

Description This command matches BGP routes based on local preference (the value in the MULTI_EXIT_DISC attribute).

If no comparison qualifiers are present (**equal**, **or-higher**, **or-lower**), then **equal** is the implied default.

A non-BGP route does not match a policy entry if it contains the **metric** command. In addition, a BGP route without a MED attribute also does not match a policy entry if it contains a **metric** command.

Default no metric

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — Specifies the MED value.

Values 0 to 4294967295, or a parameter name delimited by starting and ending at-sign (@) characters

equal — Specifies that matched routes should have the same MED as the value specified.

or-higher — Specifies that matched routes should have the same or a greater MED as the value specified.

or-lower — Specifies that matched routes should have the same or a lower MED as the value specified.

Platforms All

metric

Syntax **metric** {**add** | **subtract**} *metric*
metric set [**igp** | *metric-value*]
no metric

Context **[Tree]** (config>router>policy-options>policy-statement>default-action metric)
[Tree] (config>router>policy-options>policy-statement>entry>action metric)

Full Context configure router policy-options policy-statement default-action metric
configure router policy-options policy-statement entry action metric

Description In a BGP import or export policy, this command assigns a MED value to routes matched by the policy statement entry. The MED value may be set to a fixed value (overriding the received value), set to the routing table cost of the route used to resolve the next hop of the BGP route, or modified by adding or subtracting a fixed value offset.

The **no** form of this command removes the MED attribute from the matched routes.

Default no metric

Parameters **add** — Specifies that an integer is added to any existing metric. If the result of the addition results in a number greater than 4294967295, the value 4294967295 is used.

subtract — Specified *integer* is subtracted from any existing metric. If the result of the subtraction results in a number less than 0, the value of 0 is used.

set — Specifies that *integer* replaces any existing metric.

igp — Sets the MED value to the routing table cost of the route used to resolve the next hop of the BGP route.

metric — Specifies the metric modifier expressed as a decimal integer.

Values 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

param-name —Specifies the metric parameter variable name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”

Platforms All

metric

Syntax **metric** *metric*
no metric

Context **[Tree]** (config>router>isis>srv6>locator>level metric)

Full Context configure router isis segment-routing-v6 locator level metric

Description This command configures the Level 1 or Level 2 metric to advertise in the locator TLV.

The **no** form of this command takes the value from the configuration of the Level 1 or Level 2 MT0 default metric parameter **config**>**router**>**isis**>**level**>**default-metric** which has a default value of 10.

Default no metric

Parameters *metric* — Specifies the configuration metric value.

Values 1 to 16777215

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

17.242 metric-in

metric-in

Syntax **metric-in** *metric*
no metric-in

Context **[Tree]** (config>service>vprn>rip metric-in)
[Tree] (config>service>vprn>rip>group metric-in)
[Tree] (config>service>vprn>rip>group>neighbor metric-in)
[Tree] (config>service>vprn>ripng metric-in)
[Tree] (config>service>vprn>ripng>group metric-in)
[Tree] (config>service>vprn>ripng>group>neighbor metric-in)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn rip group metric-in
configure service vprn rip group neighbor metric-in
configure service vprn rip metric-in
configure service vprn ripng group metric-in
configure service vprn ripng group neighbor metric-in
configure service vprn ripng metric-in

Description This command sets the metric added to routes received from a RIP neighbor.

The **no** form of this command reverts the *metric* value back to the default.

Default no metric-in

Parameters *metric* — The value added to the metric of routes received from a RIP neighbor, expressed as a decimal integer.

Values 1 to 16

Platforms All

metric-in

Syntax **metric-in** *metric*
no metric-in

Context **[Tree]** (config>router>rip metric-in)
[Tree] (config>router>rip>group metric-in)
[Tree] (config>router>rip>group>neighbor metric-in)
[Tree] (config>router>ripng metric-in)
[Tree] (config>router>ripng>group metric-in)
[Tree] (config>router>ripng>group>neighbor metric-in)

Full Context configure router rip group metric-in
configure router rip group neighbor metric-in
configure router rip metric-in
configure router ripng group metric-in
configure router ripng group neighbor metric-in
configure router ripng metric-in

Description This command configures the metric added to routes received from a RIP neighbor.

When applying an export policy to a RIP configuration, the policy overrides the metric values determined through calculations involving the **metric-in** and **metric-out** values.

The **no** form of the command reverts to the default value.

Default metric-in 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *metric* — Specifies the value added to the metric of routes received from a RIP neighbor expressed as a decimal integer.

Values 1 to 16

Platforms All

17.243 metric-out

metric-out

Syntax **metric-out** *metric*
no metric-out

Context **[Tree]** (config>service>vprn>rip metric-out)
[Tree] (config>service>vprn>rip>group metric-out)
[Tree] (config>service>vprn>rip>group>neighbor metric-out)
[Tree] (config>service>vprn>ripng metric-out)
[Tree] (config>service>vprn>ripng>group metric-out)
[Tree] (config>service>vprn>ripng>group>neighbor metric-out)

Full Context configure service vprn rip group metric-out
configure service vprn rip group neighbor metric-out
configure service vprn rip metric-out
configure service vprn ripng group metric-out
configure service vprn ripng group neighbor metric-out
configure service vprn ripng metric-out

Description This command sets the metric added to routes exported into RIP and advertised to RIP neighbors.

The **no** form of this command removes the command from the config and resets the metric-in value back to the default.

Default no metric-out

Parameters *metric* — The value added to the metric for routes exported into RIP and advertised to RIP neighbors, expressed as a decimal integer.

Values 1 to 16

Platforms All

metric-out

Syntax **metric-out** *metric*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no metric-out

Context [Tree] (config>router>rip metric-out)
[Tree] (config>router>rip>group metric-out)
[Tree] (config>router>rip>group>neighbor metric-out)
[Tree] (config>router>ripng metric-out)
[Tree] (config>router>ripng>group metric-out)
[Tree] (config>router>ripng>group>neighbor metric-out)

Full Context configure router rip group metric-out
configure router rip group neighbor metric-out
configure router rip metric-out
configure router ripng group metric-out
configure router ripng group neighbor metric-out
configure router ripng metric-out

Description This command configures the metric assigned to routes exported into RIP and advertised to RIP neighbors.

When applying an export policy to a RIP configuration, the policy overrides the metric values determined through calculations involving the **metric-in** and **metric-out** values.

The **no** form of the command reverts to the default value.

Default metric-out 1

Parameters *metric* — Specifies the value added to the metric for routes exported into RIP and advertised to RIP neighbors expressed as a decimal integer.

Values 1 to 16

Platforms All

17.244 metric-type

metric-type

Syntax **metric-type** *metric-type*
no metric-type

Context [Tree] (config>router>mpls>lsp metric-type)
[Tree] (config>router>mpls>lsp-template metric-type)

Full Context configure router mpls lsp metric-type
configure router mpls lsp-template metric-type

Description This command specifies the link metric type to use in the RSVP-TE LSP or SR-TE LSP path computation by either the local CSPF or the PCE.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the metric to its default value.

Default metric-type igp

Parameters *metric-type* — Specifies the metric type for the LSP.

Values igp, te

Platforms All

metric-type

Syntax **metric-type** {**igp** | **te-metric** | **delay**}
no metric-type

Context **[Tree]** (config>router>fad>flex-algo metric-type)

Full Context configure router flexible-algorithm-definitions flex-algo metric-type

Description This command configures the type of metric for the flexible algorithm. The topology graph assumes that all links are configured with the correct metric type.

For example, if the flexible algorithm definition instructs the use of **te-metric** keyword, it is assumed that all links have *te-metric* configured. Links without the *te-metric* configuration are excluded from the flexible algorithm topology graph.

The **no** form of this command removes the configured metric type and sets it to its default value.

Default metric-type igp

Parameters **igp** — Keyword to use the IGP metric for the flexible algorithm topology graph.

te-metric — Keyword to use the TE metric for the flexible algorithm topology graph.

delay — Keyword to use the delay metric for the flexible algorithm topology graph.

Platforms All

17.245 mfib-allowed-mda-destinations

mfib-allowed-mda-destinations

Syntax **mfib-allowed-mda-destinations**

Context **[Tree]** (config>service>vpls>mesh-sdp>egress mfib-allowed-mda-destinations)
[Tree] (config>service>vpls>spoke-sdp>egress mfib-allowed-mda-destinations)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls mesh-sdp egress mfib-allowed-mda-destinations
configure service vpls spoke-sdp egress mfib-allowed-mda-destinations

Description Commands in this context configure MFIB-allowed MDA destinations.

The allowed-mda-destinations node and the corresponding **mda** command are used on spoke and mesh SDP bindings to provide a list of MDA destinations in the chassis that are allowed as destinations for multicast streams represented by [*,g] and [s,g] multicast flooding records on the VPLS service. The MDA list only applies to IP multicast forwarding when IGMP snooping is enabled on the VPLS service. The MDA list has no effect on normal VPLS flooding such as broadcast, L2 multicast, unknown destinations or non-snooped IP multicast.

At the IGMP snooping level, a spoke or mesh SDP binding is included in the flooding domain for an IP multicast stream when it has either been defined as a multicast router port, received a IGMP query through the binding or has been associated with the multicast stream through an IGMP request by a host over the binding. Due to the dynamic nature of the way that a spoke or mesh SDP binding is associated with one or more egress network IP interfaces, the system treats the binding as appearing on all network ports. This causes all possible network destinations in the switch fabric to be included in the multicast streams flooding domain. The MDA destination list provides a simple mechanism that narrows the IP multicast switch fabric destinations for the spoke or mesh SDP binding.

If no MDAs are defined within the allowed-mda-destinations node, the system operates normally and will forward IP multicast flooded packets associated with the spoke or mesh SDP binding to all switch fabric taps containing network IP interfaces.

The MDA inclusion list should include all MDAs that the SDP binding may attempt to forward through. A simple way to ensure that an MDA that is not included in the list is not being used by the binding is to define the SDP the binding is associated with as MPLS and use an RSVP-TE LSP with a strict egress hop. The MDA associated with the IP interface defined as the strict egress hop should be present in the inclusion list. If the inclusion list does not currently contain the MDA that the binding is forwarding through, the multicast packets will not reach the destination represented by the binding.

By default, the MDA inclusion list is empty.

If an MDA is removed from the list, the MDA is automatically removed from the flooding domain of any snooped IP multicast streams associated with a destination on the MDA unless the MDA was the last MDA on the inclusion list. Once the inclusion list is empty, all MDAs are eligible for snooped IP multicast flooding for streams associated with the SDP binding.

Platforms All

mfib-allowed-mda-destinations

Syntax **mfib-allowed-mda-destinations**

Context **[Tree]** (config>service>pw-template>egress mfib-allowed-mda-destinations)

Full Context configure service pw-template egress mfib-allowed-mda-destinations

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure MFIB-allowed XMA or MDA destinations.

The allowed-mda-destinations node and the corresponding **mda** command are used on spoke and mesh SDP bindings to provide a list of XMA or MDA destinations in the chassis that are allowed as destinations for multicast streams represented by [*,g] and [s,g] multicast flooding records on the VPLS service. The XMA or MDA list only applies to IP multicast forwarding when IGMP snooping is enabled on the VPLS service. The XMA or MDA list has no effect on normal VPLS flooding such as broadcast, Layer 2 multicast, unknown destinations or non-snooped IP multicast.

At the IGMP snooping level, a spoke or mesh SDP binding is included in the flooding domain for an IP multicast stream when it has either been defined as a multicast router port, received a IGMP query through the binding or has been associated with the multicast stream through an IGMP request by a host over the binding. Due to the dynamic nature of the way that a spoke or mesh SDP binding is associated with one or more egress network IP interfaces, the system treats the binding as appearing on all network ports. This causes all possible network destinations in the switch fabric to be included in the multicast streams flooding domain. The XMA or MDA destination list provides a simple mechanism that narrows the IP multicast switch fabric destinations for the spoke or mesh SDP binding.

If no XMAs or MDAs are defined within the allowed-mda-destinations node, the system operates normally and will forward IP multicast flooded packets associated with the spoke or mesh SDP binding to all switch fabric taps containing network IP interfaces.

The XMA or MDA inclusion list should include all XMAs or MDAs that the SDP binding may attempt to forward through. A simple way to ensure that an XMA or MDA that is not included in the list is not being used by the binding is to define the SDP the binding is associated with as MPLS and use an RSVP-TE LSP with a strict egress hop. The XMA or MDA associated with the IP interface defined as the strict egress hop should be present in the inclusion list.

If the inclusion list does not currently contain the XMA or MDA that the binding is forwarding through, the multicast packets will not reach the destination represented by the binding. By default, the XMA or MDA inclusion list is empty.

If an XMA or MDA is removed from the list, the XMA or MDA is automatically removed from the flooding domain of any snooped IP multicast streams associated with a destination on the XMA or MDA unless the XMA or MDA was the last XMA or MDA on the inclusion list. Once the inclusion list is empty, all XMAs or MDAs are eligible for snooped IP multicast flooding for streams associated with the SDP binding.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.246 mfib-ping

mfib-ping

Syntax **mfib-ping service** *service-id* **source** *src-ip* **destination** *mcast-address* [**size** *size*] [**ttl** *vc-label-ttl*] [**count** *send-count*] [**return-control**] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam mfib-ping)

Full Context oam mfib-ping

Description This command determines the list of SAPs which egress a certain IP multicast stream (identified by source unicast and destination multicast IP addresses) within a VPLS service. An MFIB ping packet is always sent via the data plane.

An MFIB ping is forwarded across the VPLS following the MFIB. If an entry for the specified source unicast and destination multicast IP addresses exist in the MFIB for that VPLS, then the packet is forwarded along those paths, provided they are active. A response is generated only when there is an egress SAP binding for the specified IP multicast stream.

An MFIB ping reply can be sent using the data plane or the control plane. The **return-control** option configures the reply to be sent using the control plane. If **return-control** is not specified, the reply is sent using the data plane.

Special Cases **MFIB 224.0.0.X pings —** MFIB ping requests directed to a destination address in the special 224.0.0.X range are flooded throughout the service flooding domain and receives a response from all operational SAPs. Note that SAPs that are operationally down do not reply.

Parameters *service-id* — Specifies the service ID of the VPLS to diagnose or manage.

Values 1 to 2147483647, *service-name*, up to 64 characters

src-ip — Specifies the source IP address for the OAM request.

Values ipv4-address - a.b.c.dipv6-address - xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
xx [0..FF]H

mcast-address — Specifies the destination multicast address for the OAM request.

Values ipv4-address - a.b.c.dipv6-address - xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
xx [0..FF]H

size — Specifies the multicast OAM request packet size, in octets, expressed as a decimal integer. The request payload is padded to the specified size with a 6-byte PAD header and a byte payload of 0xAA as necessary.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the octet size specified is less than the minimum packet, the minimum sized packet necessary to send the request is used.

Values 1 to 9786

Default No OAM packet padding

vc-label-ttl — Specifies the TTL value in the VC label for the OAM request, expressed as a decimal integer.

Values 1 to 255

Default 255

send-count — Specifies the number of messages to send, expressed as a decimal integer. The **count** parameter override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent.

The message interval value must be expired before the next message request is sent.

Values 1 to 100

Default 1

return-control — Specifies that the OAM reply must be sent using the control plane instead of the data plane.

timeout — Specifies the value used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the next message request.

Upon the expiration of the message time out, the requesting router assumes that the message response is not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

Values 1 to 100

Default 5

interval — Specifies the value used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the interval is set to 1 second where the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

Output The following output displays multicast FIB connectivity test information

Sample Output

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
A:ALA-A# oam mfib-ping service 10 source 10.10.10.1 destination 225.0.0.1 count 2
Seq Node-id                                                  Path     Size  RTT
-------------------------------------------------------------------------------
[Send request Seq. 1.]
1   51.51.51.51:sap1/1/1                                   Self     100   0ms
1   54.54.54.54:sap1/1/2                                   In-Band  100   20ms
1   54.54.54.54:sap1/1/3                                   In-Band  100   10ms
1   52.52.52.52:sap1/1/3                                   In-Band  100   20ms
[Send request Seq. 2.]
2   51.51.51.51:sap1/1/1                                   Self     100   0ms
2   52.52.52.52:sap1/1/2                                   In-Band  100   10ms
2   54.54.54.54:sap1/1/2                                   In-Band  100   10ms
2   52.52.52.52:sap1/1/3                                   In-Band  100   20ms
2   54.54.54.54:sap1/1/3                                   In-Band  100   30ms
-------------------------------------------------------------------------------
A:ALA-AIM# oam mfib-ping service 1 source 11.11.0.0 destination 224.0.0.1
Seq Node-id                                                  Path     Size  RTT
-------------------------------------------------------------------------------
[Send request Seq. 1.]
1   10.20.1.3:sap1/1/5:1                       Not in MFIB Self     40    0ms
1   10.20.1.3:sap1/1/2:1                                   Self     40    10ms
[Echo replies received: 2]
-------------------------------------------------------------------------------
A:ALA-AIM#
```

Platforms All

17.247 mfib-table-high-wmark

mfib-table-high-wmark

Syntax [**no**] **mfib-table-high-wmark** *high-water-mark*

Context **[Tree]** (config>service>vpls mfib-table-high-wmark)

Full Context configure service vpls mfib-table-high-wmark

Description This command specifies the multicast FIB high watermark. When the percentage filling level of the multicast FIB exceeds the configured value, a trap is generated and a log entry is added.

The **no** form of this command reverts to the default.

Default mfib-table-high-wmark 95

Parameters *high-water-mark* — Specifies the multicast FIB high watermark as a percentage.

Values 1 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.248 mfib-table-low-wmark

mfib-table-low-wmark

Syntax [**no**] **mfib-table-low-wmark** *low-water-mark*

Context **[Tree]** (config>service>vpls mfib-table-low-wmark)

Full Context configure service vpls mfib-table-low-wmark

Description This command specifies the multicast FIB low watermark. When the percentage filling level of the multicast FIB drops below the configured value, the corresponding trap is cleared and a log entry is added.

The **no** form of this command reverts to the default.

Default mfib-table-low-wmark

Parameters *low-water-mark* — Specifies the multicast FIB low watermark as a percentage.

Values 1 to 100

Default 90

Platforms All

17.249 mfib-table-size

mfib-table-size

Syntax **mfib-table-size** *size*
no mfib-table-size

Context **[Tree]** (config>service>vpls mfib-table-size)

Full Context configure service vpls mfib-table-size

Description This command specifies the maximum number of (s,g) entries in the multicast forwarding database (MFIB) for this VPLS instance.

The *mfib-table-size* parameter specifies the maximum number of multicast database entries for both learned and static multicast addresses for the VPLS instance. When a table-size limit is set on the mfib of a service which is lower than the current number of dynamic entries present in the mfib then the number of entries remains above the limit.

The **no** form of this command removes the configured maximum MFIB table size.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no mfib-table-size

Parameters *size* — Specifies the maximum number of (s,g) entries allowed in the Multicast FIB

Values 1 to 40959

Platforms All

17.250 mgmt-ethernet

mgmt-ethernet

Syntax **mgmt-ethernet** [**revert** *seconds*]
no mgmt-ethernet

Context **[Tree]** (config>redundancy mgmt-ethernet)

Full Context configure redundancy mgmt-ethernet

Description If the management Ethernet port on the active CPM goes down, this command allows the active CPM to be configured to use the management Ethernet port of the standby CPM.

The **revert** option allows the administrator to control when to revert back to the management Ethernet port of the primary CPM once it comes up again.

The **no** form of the command disables redundancy, so that connectivity to the active CPM is lost if its Ethernet port goes down.

This feature is not supported on the 7750 SR-a, 7750 SR-e, 7750 SR-1s, 7750 SR-2s, and the VSR platforms.

Default no mgmt-ethernet

Parameters *seconds* — Specifies the duration to wait (in seconds) before reverting back to the primary CPM's management Ethernet port.

Values 1 to 300

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.251 mh-mode

mh-mode

Syntax **mh-mode** {**access** | **network**}

Context **[Tree]** (config>service>vpls>bgp-evpn>vxlan mh-mode)

Full Context configure service vpls bgp-evpn vxlan mh-mode

Description This command configures multihoming mode.

Default mh-mode access

Parameters **access** — When configured in this mode, the BGP-EVPN instance does not participate in multihoming procedures, such as processing DF election for the service or enabling local bias forwarding mode.

network — When configured in this mode, the BGP-EVPN instance participates in multihoming procedures, such as processing DF election for the service or enable local bias forwarding mode.

In services with two VXLAN instances, only one of the two instances can be configured as **network**.

Platforms All

mh-mode

Syntax **mh-mode** {**access** | **network**}

Context **[Tree]** (config>service>vpls>bgp-evpn>mpls mh-mode)

Full Context configure service vpls bgp-evpn mpls mh-mode

Description This command configures each BGP-EVPN instance in a multi-instance EVPN VPLS service, to behave as network or access.

You can only configure one network instance for the service. If the service has a provider tunnel enabled, it requires a network instance.

Default mh-mode network

Parameters **access** — Specifies that the BGP-EVPN instance does not participate in multihoming procedures, such as DF election processing or local bias forwarding.

network — Specifies that the BGP-EVPN instance participates in multihoming procedures, such as DF election processing or local bias forwarding.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.252 mhf-creation

mhf-creation

Syntax **mhf-creation** {**default** | **none** | **explicit** | **static**}
no mhf-creation

Context **[Tree]** (cfg>eth-cfm>domain>assoc>bridge mhf-creation)

Full Context configure eth-cfm domain association bridge-identifier mhf-creation

Description This command defines the MIP method of creation. MIP creation mode and other factors are part of the MIP creation authority (**association** or **default-domain**) logic. The MIP creation algorithm may result in multiple potential MIPs. Only the lowest-level valid MIP is installed. The **static** creation mode is the exception to the single MIP installation rule.

Under the association context, the **level** *level* parameter is not supported as part of this command. The level is derived from the level configuration of the domain.

The **no** form of this command is only available under the **association** context, and reverts the current mode of creation to the default **none**. In order to transition to and from the **static** mode of operation, the active **mhf-creation** mode must be **none**.

Default mhf-creation none

Parameters **default** — Specifies MHFs (MIPs) can be created for this SAP or spoke SDP without the requirement for a MEP at some lower MA level. If a lower-level MEP exists, the creation method will behave as **explicit**.

none — Specifies that no MHFs (MIPs) can be created for this SAP or spoke SDP.

explicit — Specifies that MHFs (MIPs) can be created for this SAP or spoke SDP only if a MEP is created at some lower MD Level. There must be at least one lower MD Level MEP provisioned on the same SAP or spoke SDP.

static — Specifies the exact level of the MHF (MIP) that will be created for this SAP. Multiple MHFs (MIPs) are allowed as long as the MD Level hierarchy is properly configured for the particular Primary VLAN. Ingress MHFs (MIPs) with primary VLAN are not supported on SDP Bindings.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mhf-creation

Syntax **mhf-creation** {**none** | **default** | **explicit** | **static**} **level** *level*
no mhf-creation

Context **[Tree]** (config>eth-cfm>default-domain>bridge-identifier mhf-creation)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure eth-cfm default-domain bridge-identifier mhf-creation

Description This command defines the MIP method of creation. MIP creation mode and other factors are part of the MIP creation authority (**association** or **default-domain**) logic. The MIP creation algorithm may result in multiple potential MIPs. Only the lowest-level valid MIP is installed. The **static** creation mode is the exception to the single MIP installation rule.

Under the association context, the **level** *level* parameter is not supported as part of this command. The level is derived from the level configuration of the domain.

The **no** form of this command is only available under the **association** context, and reverts the current mode of creation to the default **none**. In order to transition to and from the **static** mode of operation, the active **mhf-creation** mode must be **none**.

Default mhf-creation defer (config>eth-cfm>default-domain>bridge-identifier)

Parameters **none** — Specifies that no MHFs (MIPs) can be created for this SAP or spoke SDP.

default — Specifies MHFs (MIPs) can be created for this SAP or spoke SDP without the requirement for a MEP at some lower MA level. If a lower-level MEP exists, the creation method will behave as **explicit**.

explicit — Specifies that MHFs (MIPs) can be created for this SAP or spoke SDP only if a MEP is created at some lower MD Level. There must be at least one lower MD Level MEP provisioned on the same SAP or spoke SDP.

defer — Defers the MIP creation process to the system-wide read-only values. This parameter is only configurable under the **default-domain** context.

level — Specifies the requested level of the MIP. This is used by the MIP creation algorithm to determine its validity in comparison to other ETH-CFM MIPs in the same service. If *level* is configured as “defer”, the level value will be inherited from the global read-only system values, and “-1” will be stored as a MIB value in the table.

Values 0 to 7, **defer**

Default defer

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.253 micro-loop-avoidance

micro-loop-avoidance

Syntax **micro-loop-avoidance** [**fib-delay** *fib-delay*]
no micro-loop-avoidance

Context **[Tree]** (config>router>isis>segment-routing micro-loop-avoidance)

Full Context configure router isis segment-routing micro-loop-avoidance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables, in the IGP instance, the micro-loop avoidance feature to prevent micro-loops from using Segment Routing (SR) loop-free tunnels for packets that are forwarded over SR IS-IS node SIDs.

When enabled, the behavior of the feature is triggered by the receipt of a single event on a on a P2P link or broadcast link with two neighbors:

- link addition or restoration
- link removal or failure
- link metric change

IGP then performs the following procedures.

1. IGP runs the main SPF and LFA SPFs.
2. For a node or a prefix in which the SPF resulted in no change to its next hop(s) and metric(s), then IGP takes no action.
3. For a node or a prefix in which SPF resulted in a change to its next hop(s) or metric(s), IGP marks the route as eligible for micro-loop avoidance.
   a. Activate, for each node SID that uses a micro-loop avoidance eligible route with ECMP next hops, the common set of next hops between the previous and new SPF.
   b. Compute and activate, for each node SID which uses a micro-loop avoidance eligible route, with a single next hop loop-free SR tunnel that is applicable to the specific link event.

      This tunnel acts the micro-loop avoidance primary path for the route and uses the same outgoing interface as the new computed primary next hop.
   c. Program the TI-LFA, base LFA, or remote LFA backup path that protects the new primary next hop for the node SID.
4. Start the **fib-delay** timer to delay programming of new main and LFA SPF results into the FIB.
5. After the expiry of the **fib-delay** timer, program the new primary next hop(s) for node SIDs routes that were marked eligible for micro-loop avoidance procedures.

The **no** form of this command disables the micro-loop avoidance feature.

Default no micro-loop-avoidance

Parameters *fib-delay* — Specifies the delay, in 100s of milliseconds, before the system programs the new next hops for the SR tunnel.

Values 1 to 300

Default 15

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

micro-loop-avoidance

Syntax **[no] micro-loop-avoidance**

Context **[Tree]** (config>router>isis>flex-algos>flex-algo micro-loop-avoidance)

Full Context configure router isis flexible-algorithms flex-algo micro-loop-avoidance

Description This command enables flexible algorithms-aware micro-loop avoidance. When enabled, the micro-loop configuration parameters are inherited from the base SPF.

The **no** form of this command disables the micro-loop avoidance for flexible algorithms.

Default no micro-loop-avoidance

Platforms All

17.254 mid-pool

mid-pool

Syntax [**no**] **mid-pool** *mid-pool-id*

Context **[Tree]** (config>qos>hs-pool-policy>mid-tier mid-pool)

Full Context configure qos hs-pool-policy mid-tier mid-pool

Description Commands in this context configure mid-pool tier parameters for an HS pool policy. Parameters allow for allocating the percentage of the root pool size, defining a mid-tier pool's root-pool parent, specifying the port bandwidth oversubscription factor, or specifying a slope policy for the specific mid-tier pool.

The **no** form of the command reverts the parent root pool association to root-pool 1, reverts to the default allocation-percentage value, the default **port-bw-oversub-factor**, and default slope-policy to the specified mid-pool.

Parameters *mid-pool-id* — Specifies the mid pool ID. This is a required parameter when this command is executed and specifies which mid-pool context is being entered.

Values 1 to 16

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.255 mid-tier

mid-tier

Syntax **mid-tier**

Context **[Tree]** (config>qos>hs-pool-policy mid-tier)

Full Context configure qos hs-pool-policy mid-tier

Description Commands in this context configure HS pool policy parameters. Within the **mid-tier** context, mid-pools can be associated with a root pool, sized as a percentage of the root pool, have an HS slope policy applied, or be configured with a port bandwidth oversubscription factor parameter used to influence the port-class pool sizes associated with the mid-tier pool.

Platforms 7750 SR-7/12/12e

17.256 migrant

migrant

Syntax [**no**] **migrant**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>ue-state migrant)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ue-state migrant

Description This command enables matching on tunnels with migrant UEs.

The **no** form of this command disables matching on migrant UEs, unless UE state matching is disabled altogether.

Default no migrant

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.257 millisecond-event-timestamp

millisecond-event-timestamp

Syntax **[no] millisecond-event-timestamp**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>aaa>isa-radius-plcy>acct-include-attributes millisecond-event-timestamp)

Full Context configure aaa isa-radius-policy acct-include-attributes millisecond-event-timestamp

Description This command enables the router to include the Alc-Millisecond-Event-Timestamp attribute in the accounting message. This attribute specifies the time the accounting event was logged, in milliseconds since Jan 1, 1970 00:00:00 UTC.

The **no** form of this command disables the router from including the Alc-Millisecond-Event-Timestamp attribute in the accounting message.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.258 min-advertisement

min-advertisement

Syntax **min-advertisement** *seconds*
no min-advertisement

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv min-advertisement)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 min-advertisement)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv min-advertisement)
[Tree] (config>service>vprn>router-advert>if min-advertisement)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 min-advertisement)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv min-advertisement)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv min-advertisement)
[Tree] (config>subscr-mgmt>rtr-adv-plcy min-advertisement)

Full Context configure service ies subscriber-interface group-interface ipv6 min-advertisement
configure service ies subscriber-interface group-interface ipv6 router-advertisements min-advertisement
configure service ies subscriber-interface ipv6 router-advertisements min-advertisement
configure service vprn router-advert interface min-advertisement
configure service vprn subscriber-interface group-interface ipv6 min-advertisement
configure service vprn subscriber-interface group-interface ipv6 router-advertisements min-advertisement
configure service vprn subscriber-interface ipv6 router-advertisements min-advertisement
configure subscriber-mgmt router-advertisement-policy min-advertisement

Description This command specifies the minimum time allowed between sending unsolicited router advertisements.

The **no** form of this command reverts to the default.

Default min-advertisement 900

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the minimum advertisement interval, in seconds.

Values 900 to 1350

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.259 min-advertisement-interval

min-advertisement-interval

Syntax [**no**] **min-advertisement-interval** *seconds*

Context **[Tree]** (config>service>vprn>router-advert>if min-advertisement-interval)
[Tree] (config>router>router-advert>if min-advertisement-interval)

Full Context configure router router-advertisement interface min-advertisement-interval
configure service vprn router-advertisement interface min-advertisement-interval

Description This command configures the minimum interval between sending ICMPv6 neighbor discovery router advertisement messages.

Default min-advertisement-interval 200

Parameters *seconds* — Specifies the minimum interval in seconds between sending ICMPv6 neighbor discovery router advertisement messages.

Values 3 to 1350

Platforms All

17.260 min-auth-interval

min-auth-interval

Syntax **min-auth-interval** *min-auth-interval*
no min-auth-interval

Context **[Tree]** (config>service>ies>sub-if>grp-if min-auth-interval)
[Tree] (config>service>vpls>sap>arp-host min-auth-interval)
[Tree] (config>service>vprn>sub-if>grp-if>arp-host min-auth-interval)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>arp-host min-auth-interval)

Full Context configure service ies subscriber-interface group-interface min-auth-interval
configure service vpls sap arp-host min-auth-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface arp-host min-auth-interval
configure subscriber-mgmt msap-policy vpls-only-sap-parameters arp-host min-auth-interval

Description This command configures the minimum authentication interval.

The **no** form of this command reverts to the default.

Default min-auth-interval 15

Parameters *min-auth-interval* — Specifies the minimum authentication interval, in minutes.

Values 1 to 6000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

min-auth-interval

Syntax **min-auth-interval** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no min-auth-interval

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>rtr-sol min-auth-interval)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-sol min-auth-interval)

Full Context configure service ies subscriber-interface group-interface ipv6 router-solicit min-auth-interval

Description This command specify the minimum interval between two consecutive authentication attempts from the same host.

The **no** form of this command reverts to the default.

Parameters *days* — Specifies the number of days that a user must wait for the next authentication attempt.

hours — Specifies the number of hours that a user must wait for the next authentication attempt.

minutes — Specifies the number of minutes that a user must wait for the next authentication attempt.

seconds — Specifies the number of seconds that a user must wait for the next authentication attempt.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

min-auth-interval

Syntax **min-auth-interval** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
min-auth-interval infinite
no min-auth-interval

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipoe-session min-auth-interval)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session min-auth-interval)

Full Context configure service ies subscriber-interface group-interface ipoe-session min-auth-interval
configure service vprn subscriber-interface group-interface ipoe-session min-auth-interval

Description Re-authentication for IPoE sessions enable dynamic policy changes.

This command configures the maximum frequency of re-authentications by specifying a minimum interval between two non-forced authentications for the same IPoE session.

A forced authentication is by default triggered by a circuit-id, interface-id or remote-id change (see the **force-auth** [**config>service>ies>sub-if>grp-if>ipoe-session force-auth**, **config>service>vprn>sub-if>grp-if>ipoe-session force-auth**] command).

Re-authentications are, by default, disabled and can be enabled by configuring a **min-auth-interval**.

Setting the **min-auth-interval** to zero seconds always re-authenticates on each trigger packet.

The **no** form of this command reverts to the default behavior.

Default min-auth-interval infinite

Parameters *days* — Specifies the min number of days between two non-forced authentications for IPoE sessions.

Values 0 to 365

hours — Specifies the min number of hours between two non-forced authentications for IPoE sessions.

Values 0 to 23

minutes — Specifies the min number of minutes between two non-forced authentications for IPoE sessions.

Values 0 to 59

seconds — Specifies the min number of seconds between two non-forced authentications for IPoE sessions.

Values 0 to 59

infinite — Specifies that non-forced re-authentications for IPoE sessions is not performed.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.261 min-bandwidth

min-bandwidth

Syntax **min-bandwidth** *bandwidth-in-mbps*
no min-bandwidth

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth min-bandwidth)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth min-bandwidth)

Full Context configure router mpls lsp auto-bandwidth min-bandwidth
configure router mpls lsp-template auto-bandwidth min-bandwidth

Description This command configures the minimum bandwidth that auto-bandwidth allocation is allowed to request for an LSP.

The LSP minimum applies whether the bandwidth adjustment is triggered by normal adjust-timer expiry or manual request.

The **no** form of this command reverts to the default value.

Default min-bandwidth 0

Parameters *bandwidth-in-mbps* — Specifies the minimum bandwidth in Mb/s.

Values 0 to 6400000

Platforms All

17.262 min-delay

min-delay

Syntax **min-delay** [*delay*]
no min-delay

Context **[Tree]** (config>log>event-handling>handler>action-list>entry min-delay)

Full Context configure log event-handling handler action-list entry min-delay

Description This command specifies the minimum delay in seconds between subsequent executions of the action specified in this entry. This is useful, for example, to ensure that a script does not get triggered to execute too often.

Default no min-delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *delay* — Specifies the unit in seconds.

Values 1 to 604800

Platforms All

17.263 min-first-fragment-size-rx

min-first-fragment-size-rx

Syntax **min-first-fragment-size-rx** *mtu-bytes*
no min-first-fragment-size-rx

Context **[Tree]** (config>router>nat>inside>dslite>address min-first-fragment-size-rx)
[Tree] (config>service>vprn>nat>inside>dslite>address min-first-fragment-size-rx)

Full Context configure router nat inside dual-stack-lite address min-first-fragment-size-rx
configure service vprn nat inside dual-stack-lite address min-first-fragment-size-rx

Description This command configures the minimum MTU size for the first fragment in the upstream direction. This command can be used to enable processing of first IPv6 fragments smaller than 1280 bytes. RFC 8200 recommends the minimum MTU in IPv6 be 1280 bytes which allows fragmentation only for packets that are larger than 1280 bytes. If a first fragment is smaller than 1280 bytes, DS-lite implementation in the SR OS, by default, drops the first fragment.

The **no** form of the command reverts to the default value.

Default min-first-fragment-size-rx 1280

Parameters *mtu-bytes* — Specifies the minimum MTU size for the first fragment in the upstream direction

Values 512 to 1280

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.264 min-frame-length

min-frame-length

Syntax **min-frame-length** *byte-length*

Context **[Tree]** (config>port>ethernet min-frame-length)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet min-frame-length

Description This command configures the minimum transmitted frame length.

Parameters *byte-length* — Specifies the number of bytes for the minimum frame length.

Values 64, 68

Default 64

Platforms All

17.265 min-lease-time

min-lease-time

Syntax **min-lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no min-lease-time

Context **[Tree]** (config>router>dhcp>server>pool min-lease-time)
[Tree] (config>service>vprn>dhcp>server>pool min-lease-time)

Full Context configure router dhcp local-dhcp-server pool min-lease-time
configure service vprn dhcp local-dhcp-server pool min-lease-time

Description This command configures the minimum lease time.

The **no** form of this command reverts to the default.

Default min-lease-time min 10

Parameters *min-lease-time* — Specifies the minimum lease time.

Values

days	0 to 3650
hours	0 to 23
minutes	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.266 min-num-ue

min-num-ue

Syntax **min-num-ue** *minimum*
no min-num-ue

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query min-num-ue)

Full Context configure subscriber-mgmt wlan-gw tunnel-query min-num-ue

Description This command enables matching only on tunnels that have at least the specified number of UEs connected.

The **no** form of this command disables matching on a minimum number of UEs.

Default no min-num-ue

Parameters *minimum* — Specifies the minimum number of UEs.

Values 1 to 4294967295

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.267 min-route-advertisement

min-route-advertisement

Syntax **min-route-advertisement** *seconds*
no min-route-advertisement

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy min-route-advertisement)

Full Context configure subscriber-mgmt bgp-peering-policy min-route-advertisement

Description This command configures the minimum interval, in seconds, at which a prefix can be advertised to a peer.

The **no** form of this command reverts to default values.

Default min-route-advertisement 30

Parameters *seconds* — Specifies the minimum route advertising interval, in seconds, expressed as a decimal integer.

Values 1 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

min-route-advertisement

Syntax **min-route-advertisement** *seconds*
no min-route-advertisement

Context **[Tree]** (config>service>vprn>bgp min-route-advertisement)
[Tree] (config>service>vprn>bgp>group min-route-advertisement)
[Tree] (config>service>vprn>bgp>group>neighbor min-route-advertisement)

Full Context configure service vprn bgp group min-route-advertisement
configure service vprn bgp group neighbor min-route-advertisement
configure service vprn bgp min-route-advertisement

Description This command configures the minimum interval, in seconds, at which a prefix can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command reverts to default values.

Default min-route-advertisement 30

Parameters *seconds* — Specifies the minimum route advertising interval, in seconds, expressed as a decimal integer.

Values 1 to 255

Platforms All

min-route-advertisement

Syntax **min-route-advertisement** *seconds*
no min-route-advertisement

Context **[Tree]** (config>router>bgp min-route-advertisement)
[Tree] (config>router>bgp>group min-route-advertisement)
[Tree] (config>router>bgp>group>neighbor min-route-advertisement)

Full Context configure router bgp group min-route-advertisement
configure router bgp group neighbor min-route-advertisement
configure router bgp min-route-advertisement

Description This command configures the minimum interval, in seconds, between successive updates of a prefix towards a peer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to default.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

The **rapid-update** command can be used to override the peer-level **min-route-advertisement** time and applies the minimum setting (0 seconds) to routes belonging to address families specified by the **rapid-update** command; routes of other address families continue to be advertised according to the session-level MRAI setting.

The **rapid-update** and **rapid-withdrawal** commands may result in the routes being sent before the peer-level MRAI timer expires.

Default min-route-advertisement 30

Parameters *seconds* — Specifies the minimum route advertising interval, in seconds, expressed as a decimal integer.

Values 1 to 255

Platforms All

17.268 min-thresh-separation

min-thresh-separation

Syntax **min-thresh-separation** *size* [**bytes** | **kilobytes**]
no min-thresh-separation

Context **[Tree]**
(config>subscr-mgmt>sub-prof>ingress>policer-control-policy>priority-mbs-thresholds min-thresh-separation)
[Tree]
(config>subscr-mgmt>sub-prof>egress>policer-control-policy>priority-mbs-thresholds min-thresh-separation)

Full Context configure subscriber-mgmt sub-profile egress policer-control-policy priority-mbs-thresholds min-thresh-separation
configure subscriber-mgmt sub-profile ingress policer-control-policy priority-mbs-thresholds min-thresh-separation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **min-thresh-separation** command defines the minimum required separation between each in-use discard threshold maintained for each parent policer context associated with the policer-control-policy. The min-thresh-separation value may be overridden on each SAP or sub-profile to which the policy is applied.

The system uses the default or specified min-thresh-separation value in order to determine the minimum separation required between each of the of the parent policer discard thresholds. The system enforces the minimum separation based on the following behavior in two ways. The first is determining the size of the shared-portion for each priority level (when the **mbs-contribution** command's optional fixed keyword is not specified):

- When a parent policer instance's priority level has less than two child policers associated, the shared-portion for the level is zero.
- When a parent policer instance's priority level has two or more child policers associated, the shared-portion for the level is equal to the current value of **min-thresh-separation**.

The second function the system uses the **min-thresh-separation** value for is determining the value per priority level for the fair-portion:

- When a parent policer instance's priority level has no child policers associated, the fair-portion for the level is zero.
- When a parent policer instance's priority level has one child policer associated, the fair-portion is equal to the maximum of the min-thresh-separation value and the priority level's mbs-contribution value.
- When a parent policer instance's priority level has two or more child policers associated, the fair-portion is equal to the maximum of the following:
  - **min-thresh-separation** value
  - The priority level's **mbs-contribution** value less **min-thresh-separation** value

When the **mbs-contribution** command's optional fixed keyword is defined for a priority level within the policy, the system will treat the defined **mbs-contribution** value as an explicit definition of the priority level's MBS. While the system will continue to track child policer associations with the parent policer priority levels, the association counters will have no effect. Instead the following rules is used to determine a fixed priority level's shared-portion and fair-portion:

- If a fixed priority level's **mbs-contribution** value is set to zero, both the shared-portion and fair-portion is set to zero
- If the **mbs-contribution** value is not set to zero:
  - The shared-portion is set to the current **min-thresh-separation** value
  - The fair-portion is set to the maximum of the following:

min-thresh-separation value

mbs-contribution value less **min-thresh-separation value**

Each time the **min-thresh-separation** value is modified, the thresholds for all instances of the parent policer created through association with this **policer-control-policy** are reevaluated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Determining the Correct Value for the Minimum Threshold Separation Value

The minimum value for **min-thresh-separation** should be set equal to the maximum size packet that is handled by the parent policer. This ensures that when a lower priority packet is incrementing the bucket, the size of the increment will not cause the bucket's depth to equal or exceed a higher priority threshold. It also ensures that an unfair packet within a priority level cannot cause the PIR bucket to increment to the discard-all threshold within the priority.

When evaluating maximum packet size, each child policer's per-packet-offset setting should be taken into consideration. If the maximum size packet is 1518 bytes and a per-packet-offset parameter is configured to add 20 bytes per packet, min-thresh-separation should be set to 1538 due to the fact that the parent policer will increment its PIR bucket using the extra 20 bytes.

In most circumstances, a value larger than the maximum packet size is not necessary. Management of priority level aggregate burst tolerance is intended to be implemented using the priority level **mbs-contribution** command. Setting a value larger than the maximum packet size will not adversely affect the policer performance, but it may increase the aggregate burst tolerance for each priority level.

Note: A priority level's shared-portion of the parent policer's PIR bucket depth is only necessary to provide some separation between a lower priority's discard-all threshold and this priority's discard-unfair threshold. It is expected that the burst tolerance for the unfair packets is relatively minimal since the child policers feeding the parent policer priority level all have some amount of fair burst before entering into an FIR exceed or unfair state. The fair burst amount for a priority level is defined using the mbs-contribution command.

The **no** form of this command returns the policy's **min-thresh-separation** value to the default value.

Parameters *size* — The size parameter is required when executing the **min-thresh-separation** command. It is expressed as an integer and specifies the shared portion in bytes or kilobytes that is selected by the trailing bytes or kilobytes keywords. If both bytes and kilobytes are missing, kilobytes is the assumed value. Setting this value has no effect on parent policer instances where the **min-thresh-separation** value has been overridden.

Values 0 to 16777216

[**bytes** | **kilobytes**] — The **bytes** keyword is optional and is mutually exclusive with the **kilobytes** keyword. When specified, size is interpreted as specifying the size of **min-thresh-separation** in bytes.

The **kilobytes** keyword is optional and is mutually exclusive with the **bytes** keyword. When specified, size is interpreted as specifying the size of **min-thresh-separation** in kilobytes.

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

min-thresh-separation

Syntax **min-thresh-separation** *size* [**bytes** | **kilobytes**]
no min-thresh-separation

Context **[Tree]**
(config>card>fp>ingress>access>queue-group>policer-control-override>priority-mbs-thresholds min-thresh-separation)
[Tree]
(config>card>fp>ingress>network>queue-group>policer-control-override>priority-mbs-thresholds min-thresh-separation)

Full Context configure card fp ingress access queue-group policer-control-override priority-mbs-thresholds min-thresh-separation
configure card fp ingress network queue-group policer-control-override priority-mbs-thresholds min-thresh-separation

Description This command defines the minimum required separation between each in-use discard threshold maintained for each parent policer context associated with the policer-control-policy. The min-thresh-separation value may be overridden on each SAP or sub-profile to which the policy is applied.

The system uses the default or specified min-thresh-separation value in order to determine the minimum separation required between each of the of the parent policer discard thresholds. The system enforces the minimum separation based on the following behavior in two ways. The first is determining the size of the shared-portion for each priority level (when the **mbs-contribution** command's optional fixed keyword is not specified):

- When a parent policer instance's priority level has less than two child policers associated, the shared-portion for the level will be zero.
- When a parent policer instance's priority level has two or more child policers associated, the shared-portion for the level will be equal to the current value of **min-thresh-separation**.

The second function the system uses the **min-thresh-separation** value for is determining the value per priority level for the fair-portion:

- When a parent policer instance's priority level has no child policers associated, the fair-portion for the level will be zero.
- When a parent policer instance's priority level has one child policer associated, the fair-portion will be equal to the maximum of the min-thresh-separation value and the priority level's mbs-contribution value.
- When a parent policer instance's priority level has two or more child policers associated, the fair-portion will be equal to the maximum of the following:
  - **min-thresh-separation** value
  - The priority level's **mbs-contribution** value less **min-thresh-separation** value

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **mbs-contribution** command's optional fixed keyword is defined for a priority level within the policy, the system will treat the defined **mbs-contribution** value as an explicit definition of the priority level's MBS. While the system will continue to track child policer associations with the parent policer priority levels, the association counters will have no effect. Instead the following rules will be used to determine a fixed priority level's shared-portion and fair-portion:

- If a fixed priority level's **mbs-contribution** value is set to zero, both the shared-portion and fair-portion will be set to zero
- If the **mbs-contribution** value is not set to zero:
  - The shared-portion will be set to the current **min-thresh-separation** value
  - The fair-portion will be set to the maximum of the following:
    - **min-thresh-separation** value
    - **mbs-contribution** value less **min-thresh-separation value**

Each time the **min-thresh-separation** value is modified, the thresholds for all instances of the parent policer created through association with this **policer-control-policy** are reevaluated except for parent policer instances that currently have a min-thresh-separation override.

Determining the Correct Value for the Minimum Threshold Separation Value

The minimum value for **min-thresh-separation** should be set equal to the maximum size packet that will be handled by the parent policer. This ensures that when a lower priority packet is incrementing the bucket, the size of the increment will not cause the bucket's depth to equal or exceed a higher priority threshold. It also ensures that an unfair packet within a priority level cannot cause the PIR bucket to increment to the discard-all threshold within the priority.

When evaluating maximum packet size, each child policer's per-packet-offset setting should be taken into consideration. If the maximum size packet is 1518 bytes and a per-packet-offset parameter is configured to add 20 bytes per packet, min-thresh-separation should be set to 1538 due to the fact that the parent policer will increment its PIR bucket using the extra 20 bytes.

In most circumstances, a value larger than the maximum packet size is not necessary. Management of priority level aggregate burst tolerance is intended to be implemented using the priority level **mbs-contribution** command. Setting a value larger than the maximum packet size will not adversely affect the policer performance, but it may increase the aggregate burst tolerance for each priority level.

One thing to note is that a priority level's shared-portion of the parent policer's PIR bucket depth is only necessary to provide some separation between a lower priority's discard-all threshold and this priority's discard-unfair threshold. It is expected that the burst tolerance for the unfair packets is relatively minimal since the child policers feeding the parent policer priority level all have some amount of fair burst before entering into an FIR exceed or unfair state. The fair burst amount for a priority level is defined using the mbs-contribution command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the policy's **min-thresh-separation** value to the default value. This has no effect on instances of the parent policer where **min-thresh-separation** is overridden unless the override is removed.

Default no min-thresh-separation

Parameters *size* — Specifies that the size parameter is required when executing the **min-thresh-separation** command. It is expressed as an integer and specifies the shared portion in bytes or kilobytes that is selected by the trailing bytes or kilobytes keywords. If both bytes and kilobytes are missing, kilobytes is the assumed value. Setting this value has no effect on parent policer instances where the **min-thresh-separation** value has been overridden. Clearing an override on parent policer instance causes this value to be enforced.

Values 0 to 16777216

bytes | **kilobytes** — Specifies that the **bytes** keyword is optional and is mutually exclusive with the **kilobytes** keyword. When specified, size is interpreted as specifying the size of **min-thresh-separation** in bytes.

The **kilobytes** keyword is optional and is mutually exclusive with the **bytes** keyword. When specified, size is interpreted as specifying the size of **min-thresh-separation** in kilobytes.

Values bytes or kilobytes

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

min-thresh-separation

Syntax **min-thresh-separation** *size* [**bytes** | **kilobytes**]

Context **[Tree]** (config>service>apipe>sap>egress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>apipe>sap>ingress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>cpipe>sap>egress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>cpipe>sap>ingress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>epipe>sap>egress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>epipe>sap>ingress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>fpipe>sap>egress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>fpipe>sap>ingress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ipipe>sap>egress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>ipipe>sap>ingress>policy-ctrl-over>mbs-thrshlds min-thresh-separation)

Full Context
configure service apipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service apipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service cpipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service cpipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service epipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service epipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service fpipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service fpipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service ipipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service ipipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation

Description
This command, within the SAP ingress and egress contexts, is used to override the root arbiter's parent policer min-thresh-separation parameter that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy min-thresh-separation parameter have no effect on the SAP's parent policer until the override is removed using the no min-thresh-separation command within the SAP.

The no form of this command removes the override and allows the min-thresh-separation setting from the policer-control-policy to control the root arbiter's parent policer's minimum discard threshold separation size.

Default
no min-thresh-separation

Parameters
size — The minimum discard threshold separation override value.

Values 1 to 16777216 | default

bytes — Signifies that *size* is expressed in bytes. The bytes and kilobytes keywords are mutually exclusive and optional. The default is kilobytes.

kilobytes — Signifies that *size* is expressed in kilobytes. The bytes and kilobytes keywords are mutually exclusive and optional. The default is kilobytes.

Platforms
7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service cpipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service cpipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service fpipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service epipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service ipipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service epipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service ipipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation
- configure service apipe sap egress policer-control-override priority-mbs-thresholds min-thresh-separation

min-thresh-separation

Syntax **min-thresh-separation** *size* [{**bytes** | **kilobytes**}]

Context **[Tree]** (config>service>vpls>sap>egress>policer-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>vpls>sap>ingress>policer-ctrl-over>mbs-thrshlds min-thresh-separation)

Full Context configure service vpls sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service vpls sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation

Description This command within the SAP ingress and egress contexts is used to override the root arbiter's parent policer min-thresh-separation parameter that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy min-thresh-separation parameter have no effect on the SAP's parent policer until the override is removed using the **no min-thresh-separation** command within the SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the override and allows the min-thresh-separation setting from the policer-control-policy to control the root arbiter's parent policer's minimum discard threshold separation size.

Default no min-thresh-separation

Parameters *size* — This parameter is required when specifying min-thresh-separation override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 16777216 or default

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

min-thresh-separation

Syntax **min-thresh-separation** *size* [{**bytes** | **kilobytes**}]

Context **[Tree]** (config>service>ies>if>sap>egress>policer-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>ies>if>sap>ingress>policer-ctrl-over>mbs-thrshlds min-thresh-separation)

Full Context configure service ies interface sap egress policer-control-override priority-mbs-thresholds min-thresh-separation
configure service ies interface sap ingress policer-control-override priority-mbs-thresholds min-thresh-separation

Description This command within the SAP ingress and egress contexts is used to override the root arbiter's parent policer min-thresh-separation parameter that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy min-thresh-separation parameter have no effect on the SAP's parent policer until the override is removed using the no min-thresh-separation command within the SAP.

The **no** form of this command removes the override and allows the min-thresh-separation setting from the policer-control-policy to control the root arbiter's parent policer's minimum discard threshold separation size.

Default no min-thresh-separation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *size* — This parameter is required when specifying min-thresh-separation override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 16777216 or default

Default kilobytes

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

min-thresh-separation

Syntax **min-thresh-separation** *size* [{**bytes** | **kilobytes**}]

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-ctrl-over>mbs-thrshlds min-thresh-separation)
[Tree] (config>service>vprn>if>sap>ingress>policer-ctrl-over>mbs-thrshlds min-thresh-separation)

Full Context configure service vprn interface sap egress policer-ctrl-over priority-mbs-thresholds min-thresh-separation
configure service vprn interface sap ingress policer-ctrl-over priority-mbs-thresholds min-thresh-separation

Description This command within the SAP ingress and egress contexts is used to override the root arbiter's parent policer min-thresh-separation parameter that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy min-thresh-separation parameter have no effect on the SAP's parent policer until the override is removed using the no min-thresh-separation command within the SAP.

The **no** form of this command removes the override and allows the min-thresh-separation setting from the policer-control-policy to control the root arbiter's parent policer's minimum discard threshold separation size.

Default no min-thresh-separation

Parameters *size* — This parameter is required when specifying min-thresh-separation override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional **byte** and **kilobyte** keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 to 16777216 or default

Default kilobytes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

min-thresh-separation

Syntax **min-thresh-separation** *size* [**bytes** | **kilobytes**]
no min-thresh-separation

Context **[Tree]** (config>qos>plcr-ctrl-plcy>root>priority-mbs-thresholds min-thresh-separation)

Full Context configure qos policer-control-policy root priority-mbs-thresholds min-thresh-separation

Description The **min-thresh-separation** command defines the minimum required separation between each in-use discard threshold maintained for each parent policer context associated with the policer-control-policy. The min-thresh-separation value may be overridden on each SAP or sub-profile to which the policy is applied.

The system uses the default or specified **min-thresh-separation** value in order to determine the minimum separation required between each of the of the parent policer discard thresholds. The system enforces the minimum separation based on the following behavior in two ways. The first is determining the size of the shared-portion for each priority level (when the **mbs-contribution** command's optional fixed keyword is not specified):

- When a parent policer instance's priority level has less than two child policers associated, the shared-portion for the level will be zero.
- When a parent policer instance's priority level has two or more child policers associated, the shared-portion for the level will be equal to the current value of **min-thresh-separation**.

The second function the system uses the **min-thresh-separation** value for is determining the value per priority level for the fair-portion:

- When a parent policer instance's priority level has no child policers associated, the fair-portion for the level will be zero.
- When a parent policer instance's priority level has one child policer associated, the fair-portion will be equal to the maximum of the min-thresh-separation value and the priority level's mbs-contribution value.
- When a parent policer instance's priority level has two or more child policers associated, the fair-portion will be equal to the maximum of the following:
  - **min-thresh-separation** value
  - **mbs-contribution** value less **min-thresh-separation** value

When the **mbs-contribution** command's optional fixed keyword is defined for a priority level within the policy, the system will treat the defined **mbs-contribution** value as an explicit definition of the priority level's MBS. While the system will continue to track child policer associations with the parent policer priority levels, the association counters will have no effect. Instead, the following rules will be used to determine a fixed priority level's shared-portion and fair-portion:

- If a fixed priority level's **mbs-contribution** value is set to zero, both the shared-portion and fair-portion will be set to zero
- If the **mbs-contribution** value is not set to zero:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The shared-portion will be set to the current **min-thresh-separation** value
- The fair-portion will be set to the maximum of the following:
  min-thresh-separation value
  mbs-contribution value less **min-thresh-separation value**

Each time the **min-thresh-separation** value is modified, the thresholds for all instances of the parent policer created through association with this **policer-control-policy** are reevaluated.

Determining the Correct Value for the Minimum Threshold Separation Value

The minimum value for **min-thresh-separation** should be set equal to the maximum size packet that will be handled by the parent policer. This ensures that when a lower priority packet is incrementing the bucket, the size of the increment will not cause the bucket's depth to equal or exceed a higher priority threshold. It also ensures that an unfair packet within a priority level cannot cause the PIR bucket to increment to the discard-all threshold within the priority.

When evaluating maximum packet size, each child policer's per-packet-offset setting should be taken into consideration. If the maximum size packet is 1518 bytes and a per-packet-offset parameter is configured to add 20 bytes per packet, min-thresh-separation should be set to 1538 due to the fact that the parent policer will increment its PIR bucket using the extra 20 bytes.

In most circumstances, a value larger than the maximum packet size is not necessary. Management of priority level aggregate burst tolerance is intended to be implemented using the priority level **mbs-contribution** command. Setting a value larger than the maximum packet size will not adversely affect the policer performance, but it may increase the aggregate burst tolerance for each priority level.

Note: A priority level's shared-portion of the parent policer's PIR bucket depth is only necessary to provide some separation between a lower priority's discard-all threshold and this priority's discard-unfair threshold. It is expected that the burst tolerance for the unfair packets is relatively minimal since the child policers feeding the parent policer priority level all have some amount of fair burst before entering into an FIR exceed or unfair state. The fair burst amount for a priority level is defined using the mbs-contribution command.

The **no** form of this command returns the policy's **min-thresh-separation** value to the default value.

Parameters *size* — The *size* parameter is required when executing the **min-thresh-separation** command. It is expressed as an integer. Setting this value has no effect on parent policer instances where the **min-thresh-separation** value has been overridden.

Values 0 to 4194304 or **default** (applies to the 7450 ESS)
0 to 16777216 or **default** (applies to the 7750 SR or 7950 XRS)

Default 1536

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bytes | kilobytes — This parameter indicates whether the size is expressed in bytes or kilobytes.

Default **kilobytes**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

17.269 min-vp-vpi

min-vp-vpi

Syntax **min-vp-vpi** *value*

Context **[Tree]** (config>port>sonet-sdh>path>atm min-vp-vpi)
[Tree] (config>port>ml-bundle>ima>atm min-vp-vpi)
[Tree] (config>port>tdm>ds1>channel-group>atm min-vp-vpi)
[Tree] (config>port>tdm>ds3>atm min-vp-vpi)
[Tree] (config>port>tdm>e1>channel-group>atm min-vp-vpi)
[Tree] (config>port>tdm>e3>atm min-vp-vpi)

Full Context configure port multilink-bundle ima atm min-vp-vpi
configure port sonet-sdh path atm min-vp-vpi
configure port tdm ds1 channel-group atm min-vp-vpi
configure port tdm ds3 atm min-vp-vpi
configure port tdm e1 channel-group atm min-vp-vpi
configure port tdm e3 atm min-vp-vpi

Description This command sets the minimum allowable virtual path identifier (VPI) value that can be used on the ATM interface for a VPC.

Parameters *value* — Specifies the minimum allowable VPI value that can be used on the ATM interface for a VPC.

Values 0 to 4095 (NNI) 0 to 255 (UNI)

Default 0

Platforms 7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle ima atm min-vp-vpi

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group atm min-vp-vpi
- configure port tdm e3 atm min-vp-vpi
- configure port tdm ds1 channel-group atm min-vp-vpi
- configure port tdm ds3 atm min-vp-vpi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure port sonet-sdh path atm min-vp-vpi

17.270 min-wait-to-advertise

min-wait-to-advertise

Syntax **min-wait-to-advertise** *seconds*
no min-wait-to-advertise

Context **[Tree]** (config>service>vprn>bgp>convergence min-wait-to-advertise)

Full Context configure service vprn bgp convergence min-wait-to-advertise

Description This command configures the minimum amount of time that BGP waits, after the first session establishment following a restart of the BGP instance, until it can start advertising IPv4-unicast and IPv6-unicast routes to its BGP peers, to allow time for re-convergence.

The time limit configured by this command should allow sufficient time for all important peers to re-establish their sessions with the restarting router.

The **no** form of this command implements the default time limit of 0 seconds, which disables all forms of delayed route advertisement. In other words, it causes IPv4-unicast and IPv6-unicast routes to be re-advertised as soon as possible after BGP instance restart.

Default no min-wait-to-advertise

Parameters *seconds* — Specifies the minimum amount of time, in seconds, that BGP waits until IPv4-unicast and IPv6-unicast routes can be advertised to peers.

Values 0 to 3600

Platforms All

min-wait-to-advertise

Syntax **min-wait-to-advertise** *seconds*
no min-wait-to-advertise

Context **[Tree]** (config>router>bgp>convergence min-wait-to-advertise)

Full Context configure router bgp convergence min-wait-to-advertise

Description This command configures the minimum amount of time that BGP waits, after the first session establishment following a restart of the BGP instance, until it can start advertising IPv4-unicast and IPv6-unicast routes to its BGP peers, to allow time for re-convergence.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The time limit configured by this command should allow sufficient time for all important peers to re-establish their sessions with the restarting router.

The **no** form of this command implements the default time limit of 0 seconds, which disables all forms of delayed route advertisement. In other words, it causes IPv4-unicast and IPv6-unicast routes to be re-advertised as soon as possible after BGP instance restart.

Default no min-wait-to-advertise

Parameters *seconds* — Specifies the minimum amount of time, in seconds, that BGP waits until IPv4-unicast and IPv6-unicast routes can be advertised to peers.

Values 0 to 3600

Platforms All

17.271 minimum

minimum

Syntax **minimum** [**percent** [*percent*]] [**number** [*number*]]
no minimum

Context **[Tree]** (config>service>vprn>dhcp6>server>pool>prefix>thresholds>minimum-free minimum)
[Tree] (config>router>dhcp6>server>pool>prefix>thresholds>minimum-free minimum)

Full Context configure router dhcp6 local-dhcp-server pool prefix thresholds minimum-free minimum
configure service vprn dhcp6 local-dhcp-server pool prefix thresholds minimum-free minimum

Description This command configures a percentage-based or number-based threshold which represents the minimal available percentage or number of the prefix with a configured length in the provisioned prefix. The system sends out a warning if the actual percentage or number is lower than the configured threshold.

For example:

```
prefix 2001:0:0:ffe0::/50 pd wan-host create
   thresholds
       minimum-free prefix-length 64
           minimum number 3
```

With the above configuration, the system sends a warning when the number of available /64 in prefix 2001:0:0:ffe0::/50 is less than 3.

The **no** form of this command removes the command parameters from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent* — Specifies the percentage of used prefixes with the minimum free threshold length in the pool compared to the number of provisioned prefixes.

Values 0 to 100

number — Specifies the number of prefixes.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.272 minimum-age

minimum-age

Syntax **minimum-age** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no minimum-age

Context **[Tree]** (config>system>security>password minimum-age)

Full Context configure system security password minimum-age

Description Configure the minimum required age of a password before it can be changed again.

Default minimum-age min 10

Parameters *days* — Specifies the minimum required days of a password before it can be changed again.

Values 0 to 1

hours — Specifies the minimum required hours of a password before it can be changed again.

Values 0 to 23

minutes — Specifies the minimum required minutes of a password before it can be changed again.

Values 0 to 59

seconds — Specifies the minimum required seconds of a password before it can be changed again.

Values 0 to 59

Note: This command applies to local users.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.273 minimum-change

minimum-change

Syntax **minimum-change** *distance*
no minimum-change

Context **[Tree]** (config>system>security>password minimum-change)

Full Context configure system security password minimum-change

Description This command configures the minimum number of characters required to be different in the new password from a previous password.

The **no** form of this command reverts to default value.

Default minimum-change 5

Parameters *distance* — Specifies how many characters must be different in the new password from the old password.

Values 1 to 20

Note: This command applies to local users.

Platforms All

17.274 minimum-classes

minimum-classes

Syntax **minimum-classes** *minimum*
no minimum-classes

Context **[Tree]** (config>system>security>password>complexity-rules minimum-classes)

Full Context configure system security password complexity-rules minimum-classes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Force the use of at least this many different character classes

The **no** form of this command resets to default.

Default no minimum-classes

Parameters *minimum* — Specifies the minimum number of classes to be configured.

Values 2 to 4

Platforms All

17.275 minimum-free

minimum-free

Syntax **minimum-free** *minimum-free* [**percent**] [**event-when-depleted**]
no minimum-free

Context **[Tree]** (config>router>dhcp>server>pool minimum-free)
[Tree] (config>service>vprn>dhcp>server>pool minimum-free)

Full Context configure router dhcp local-dhcp-server pool minimum-free
configure service vprn dhcp local-dhcp-server pool minimum-free

Description This command specifies the desired minimum number of free addresses in this pool.

The **no** form of this command reverts to the default.

Default minimum-free 1

Parameters *minimum-free* — Specifies the minimum number of free addresses.

Values 0 to 255

percent — Specifies that the value indicates a percentage.

event-when-depleted — This parameter enables a system-generate event when all available addresses in the pool/subnet of local DHCP server are depleted.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

minimum-free

Syntax **minimum-free** *minimum-free* [**percent**] [**event-when-depleted**]
no minimum-free

Context **[Tree]** (config>router>dhcp>server>pool>subnet minimum-free)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>dhcp>server>pool>subnet minimum-free)

Full Context configure router dhcp local-dhcp-server pool subnet minimum-free
configure service vprn dhcp local-dhcp-server pool subnet minimum-free

Description This command configures the minimum number of free addresses in this subnet. If the actual number of free addresses in this subnet falls below this configured minimum, a notification is generated.

The **no** form of the reverts to the default.

Default minimum-free 1

Parameters *minimum-free* — Specifies the minimum number of free addresses in this subnet.

Values 0 to 255

percent — Specifies that the value indicates a percentage.

event-when-depleted — Enables a system-generate event when all available addresses in the pool or subnet of local DHCP server are depleted.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

minimum-free

Syntax [**no**] **minimum-free prefix-length** [*prefix-length*]

Context [Tree] (config>service>vprn>dhcp6>server>pool>thresholds minimum-free)
[Tree] (config>router>dhcp6>server>pool>thresholds minimum-free)

Full Context configure router dhcp6 local-dhcp-server pool thresholds minimum-free
configure service vprn dhcp6 local-dhcp-server pool thresholds minimum-free

Description This command creates a threshold for a given prefix length on the pool level. Up to 128 thresholds could be created. For example, with **minimum-free prefix-length 64**, then the usage of /64 prefix in the pool is counted.

There are two types of thresholds that could be defined at the pool level:

- Depleted — The system sends out a warning when the prefix with the configured length is no long available in the pool.
- Minimum free — A percentage-based threshold which represents the minimal available percentage of prefix with the configured length in the pool. The system will send out warning if the actual percentage is lower than the configured percentage.

Configuring this command also enables the system stats collection for **configure prefix length**, which could be displayed with the **show router** *router-id* **dhcp6 local-dhcp-server** *dhcp6-server-name* **pool-threshold-stats** command.

The **no** form of this command removes the prefix-length from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *prefix-length* — Specifies the IPv6 prefix length.

Values 1 to 128

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.276 minimum-isa-generation

minimum-isa-generation

Syntax **minimum-isa-generation** *min-isa-generation*

Context **[Tree]** (config>isa>aa-grp minimum-isa-generation)

Full Context configure isa application-assurance-group minimum-isa-generation

Description This command configures the scale parameters for the ISA group. When *min-isa-generation* is configured as 1, the group and per-ISA limits are the MS-ISA scale.

If there is a mix of ISA 1s and 2s, the *min-isa-generation* must be left as 1.

When min-isa-gen is configured as 2, the per-isa resource limits shown in the **show isa application-assurance-group 1 load-balance** output will increase to show ISA2 limits.

Default minimum-isa-generation 1

Parameters *min-isa-generation* — Specifies the minimum ISA Generation allowed in this group.

Values 1 – ISA (ISA1)
2 – ISA2

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

17.277 minimum-length

minimum-length

Syntax **minimum-length** *length*
no minimum-length

Context **[Tree]** (config>system>security>password>complexity-rules minimum-length)

Full Context configure system security password complexity-rules minimum-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and des-keys configured in the system security section.

If multiple minimum-length commands are entered each command overwrites the previous entered command.

The **no** form of this command reverts to default value.

Default minimum-length 6

Parameters *value* — Specifies the minimum number of characters required for a password.

Values 6 to 50

Platforms All

17.278 minimum-lifetimes

minimum-lifetimes

Syntax **minimum-lifetimes**

Context **[Tree]** (config>python>py-pol>cache minimum-lifetimes)

Full Context configure python python-policy cache minimum-lifetimes

Description Commands in this context configure minimum-lifetime of Python cache information.

Platforms All

17.279 minimum-links

minimum-links

Syntax **minimum-links** *minimum-links*
no minimum-links

Context **[Tree]** (config>port>multilink-bundle minimum-links)

Full Context configure port multilink-bundle minimum-links

Description This command sets the minimum number of links that must be active for the bundle to be active.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the number of active links drops below the configured minimum then the multilink bundle will transition to an operationally down state.

The **no** form of this command removes the minimum link limit.

Default minimum-links 1

Parameters *minimum-link* — Specifies the minimum link limit, expressed as an integer.

Values 1 to 8

Platforms 7450 ESS, 7750 SR-7/12/12e

17.280 minute

minute

Syntax **minute** {*minute-number* [*..minute-number*] | **all**}
no minute

Context **[Tree]** (config>system>cron>sched minute)

Full Context configure system cron schedule minute

Description This command specifies the minute to schedule a command. Multiple minutes of the hour can be specified. When multiple minutes are configured, each of them will cause the schedule to occur. If a minute is configured, but no **hour** or day is configured, the event will not execute. If a minute is configured without configuring the month, weekday, day-of-month, and minute, the event will not execute.

The **no** form of this command removes the specified minute from the configuration.

Default no minute

Parameters *minute-number* — Specifies the minute to schedule a command.

Values 0 to 59 (maximum 60 minute-numbers)

all — Specifies all minutes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.281 minutes

minutes

Syntax **minutes** {*minutes* | **disable**}
no minutes

Context **[Tree]** (config>system>security>ssh>key-re-exchange>client minutes)
[Tree] (config>system>security>ssh>key-re-exchange>server minutes)

Full Context configure system security ssh key-re-exchange client minutes
configure system security ssh key-re-exchange server minutes

Description This command configures the maximum time, in minutes, before a key re-exchange is initiated by the server.

The **no** form of this command reverts to the default value.

Default minutes 60

Parameters *minutes* — Specifies the time interval, in minutes, after which the SSH client will initiate the key-re-exchange.

Values 1 to 1440

Default 60

disable — Specifies that a session will never timeout. To re-enable **minutes**, enter the command without the **disable** option.

Platforms All

17.282 mip

mip

Syntax **mip** [**mac** *mac-address*] [**primary-vlan-enable** *vlan-id*] [**cfm-vlan-tag** *qtag1*[.*qtag2*]]
mip default-mac [**primary-vlan-enable** *vlan-id*] [**cfm-vlan-tag** *qtag1*[.*qtag2*]]
no mip [**primary-vlan-enable** *vlan-id*]

Context **[Tree]** (config>service>epipe>sap>eth-cfm mip)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm mip)
[Tree] (config>service>vpls>sap>eth-cfm mip)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm mip)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm mip)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service epipe sap eth-cfm mip
configure service epipe spoke-sdp eth-cfm mip
configure service vpls mesh-sdp eth-cfm mip
configure service vpls sap eth-cfm mip
configure service vpls spoke-sdp eth-cfm mip

Description This command configures Maintenance Intermediate Points (MIPs). The creation rules of the MIP are dependent on the **mhf-creation** configuration for the MA.

The MIP can be created with a primary VLAN using the **primary-vlan-enable** *vlan-id* parameter matching the VLAN configured under the applicable association. Optional VLANs can be added the to the locally-generated CFM frames for egress processing using the **cfm-vlan-tag** option.

The **no** form of this command removes the MIP creation request.

Default no mip

Parameters *qtag1* — Specifies the outer VLAN ID.

Values 1 to 4094

qtag2 — Specifies the inner VLAN ID and can only be specified if *qtag1* is configured.

Values 1 to 4094

mac — Provides a method for manually configuring the MIP MAC address.

mac-address — Specifies the MAC address of the MIP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MIP. The MAC address must be unicast. Using the all-zeros address is equivalent to the **no** form of this command.

default-mac — Specifies to change the MAC address back to the default MAC without having to delete and reconfigure the MIP.

primary-vlan-enable — Provides a method for linking the MIP with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs cannot be changed from or to primary VLAN functions without first being deleted. This must be configured as part of the creation step and can only be changed by deleting the MIP and re-creating it. Primary VLANs are only supported under Layer 2 Epipe and VPLS services.

vlan-id — Specifies the VLAN ID. This parameter must match the VLAN ID under the bridge-identifier for the MA that is appropriate for this service.

Values 0 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mip

Syntax **mip primary-vlan-enable** [**vlan** *vlan-id*]
no mip

Context **[Tree]** (config>service>template>vpls-sap-template>eth-cfm mip)

Full Context configure service template vpls-sap-template eth-cfm mip

Description This command allows Maintenance Intermediate Points (MIPs). The creation rules of the MIP are dependent on the mhf-creation configuration for the MA. This MIP option is only available for default and static mhf-creation methods.

Parameters **primary-vlan-enable** — Provides a method for linking the MIP with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs cannot be changed from or to primary VLAN functions without first being deleted. This must be configured as part of the creation step and can only be changed by deleting the MEP and re-creating it. Primary VLANs are only supported under Ethernet SAPs.

vlan — A required parameter when including primary-vlan-enable. Provides a method for associating the VLAN under the bride-identifier under the MA with the MIP.

vlan-id — Must match the vlan-id under the bridge-identifier for the MA that is appropriate for this service.

Values 0 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mip

Syntax [**no**] **mip**

Context **[Tree]** (config>router>mpls>mpls-tp>transit-path>forward-path mip)
[Tree] (config>router>mpls>mpls-tp>transit-path>reverse-path mip)

Full Context configure router mpls mpls-tp transit-path forward-path mip
configure router mpls mpls-tp transit-path reverse-path mip

Description This command creates a context for maintenance entity group intermediate point (MIP) parameters for the forward path and the reverse path of an MPLS-TP LSP at an LSR.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mip

Syntax [**no**] **mip domain** *md-index* **association** *ma-index*

Context **[Tree]** (debug>eth-cfm mip)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug eth-cfm mip

Description This command specifies the MIP from which to debug the CFM PDUs.

The **no** form of this command removes the MIP parameters.

Parameters *md-index* — Specifies the maintenance domain (MD) index value of the launch point.

Values 1 to 4294967295

ma-index — Specifies the maintenance association (MA) index value of the launch point.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.283 mip-ltr-priority

mip-ltr-priority

Syntax **mip-ltr-priority** *priority*

Context **[Tree]** (cfg>eth-cfm>domain>assoc>bridge mip-ltr-priority)

Full Context configure eth-cfm domain association bridge-identifier mip-ltr-priority

Description This command allows the operator to set the priority of the Linktrace Response Message (ETH-LTR) from a MIP for this association.

Default 7

Parameters *priority* — Specifies the priority of the Linktrace Response Message (ETH-LTR) from a MIP.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mip-ltr-priority

Syntax **mip-ltr-priority** *priority*

Context **[Tree]** (config>eth-cfm>default-domain>bridge-identifier mip-ltr-priority)

Full Context configure eth-cfm default-domain bridge-identifier mip-ltr-priority

Description This command allows the operator to set the priority of the Linktrace Response Message (ETH-LTR) from a MIP for this association.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default defer

Parameters *priority* — Specifies the priority of the Linktrace Response Message (ETH-LTR) from a MIP. The “defer” value is only supported under the default-domain context and causes **mip-ltr-priority** to inherit values from the global read-only-system values.

Values 0 to 7, **defer**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.284 mir

mir

Syntax **mir** *mir-value*
no mir

Context **[Tree]** (config>qos>mlppp-profile-egress>class mir)

Full Context configure qos mlppp-profile-egress class mir

Description This command configures the minimum information rate (MIR) scheduling parameter for each MLPPP class queue for this profile.

Parameters *mir-value* — Specifies the MIR scheduling parameter.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mir

Syntax **mir** *mir*
no mir

Context **[Tree]** (config>qos>mc-fr-profile-egress>class mir)

Full Context configure qos mc-fr-profile-egress class mir

Description This command configures the minimum information rate scheduling parameter for each Frame Relay scheduling class queue for this profile.

Default 90% for all classes

Parameters *mir* — Specifies the percentage of the available link or bundle rate.

Values 1 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.285 mirror-dest

mirror-dest

Syntax **mirror-dest** *service-id* [**create**] [**type** *mirror-type*] [**name** *name*]
no mirror-dest *service-id*

Context **[Tree]** (config>mirror mirror-dest)

Full Context configure mirror mirror-dest

Description This command creates a context to set up a service that is intended for packet mirroring. It is configured as a service to allow mirrored packets to be directed locally (within the same router) or remotely, over the core of the network and have a far-end decode mirror encapsulation.

The mirror destination service is comprised of destination parameters that define where the mirrored packets are to be sent. It also specifies whether the defined *service-id* will receive mirrored packets from far-end router over the network core.

The mirror destination service IDs are persistent between boots of the router and are included in the configuration saves. The local sources of mirrored packets for the service ID are defined within the **debug mirror mirror-source** command that references the same *service-id*. Up to 255 mirror destination service IDs can be created within a single system.

The **mirror-dest** command creates or edits a service ID for mirroring purposes. If the *service-id* does not exist within the context of all defined services, the mirror destination service is created and the context of the CLI is changed to that service ID. If the *service-id* exists within the context of defined mirror destination services, the CLI context is changed for editing parameters on that service ID. If the *service-id* exists within the context of another service type, an error message is returned and CLI context is not changed from the current context.

LI source configuration is saved using the **li>save** command.

The **no** form of this command removes a mirror destination from the system. The mirror source or **li-source** associations with the mirror destination *service-id* do not need to be removed or shutdown first. The mirror destination *service-id* must be shutdown before the service ID can be removed. When the service ID is removed, all **mirror-source** or **li-source** commands that have the service ID defined will also be removed from the system.

Parameters *service-id* — The service identification identifies the service in the service domain. This ID is unique to this service and cannot be used by any other service, regardless of service type. The same service ID must be configured on every router that this particular service is defined on.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If particular a service ID already exists for a service, then the same value cannot be used to create a mirror destination service ID with the same value. For example:

If an Epipe service ID **11** exists, then a mirror destination service ID **11** cannot be created. If a VPLS service ID **12** exists, then a mirror destination service ID **12** cannot be created.

If an IES service ID **13** exists, then a mirror destination service ID **13** cannot be created.

Values

service-id:	1 to 2147483647
svc-name:	64 characters maximum

create — Keyword used to create a mirror destination service.

mirror-type — The type describes the encapsulation supported by the mirror service.

Values The following values apply to the 7750 SR:

ether, frame-relay, ppp, ip-only, atm-sdu, satop-e1, satop-e3, satop-t1, cesopsn, cesopsn-cas

Values The following values apply to the 7950 XRS:

ether, ip-only

Values The following values apply to the 7450 ESS:

ether, frame-relay, ppp

name — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Service names may not begin with an integer (0 to 9).

Platforms All

17.286 mirror-dest-reservation

mirror-dest-reservation

Syntax **mirror-dest-reservation** *service-id* **to** *service-id*
no mirror-dest-reservation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>li mirror-dest-reservation)

Full Context configure li mirror-dest-reservation

Description This command configures a range of service IDs reserved for RADIUS-triggered mirror destination. The range can be expanded or reduced in real time. The range cannot conflict with other service IDs.

The **no** form of this command removes the service IDs reserved for LI mirror destination services.

Parameters *service-id* — Specifies the starting or ending service ID in the range for the mirror destination.

Values 1 to 2147483647

Platforms All

17.287 mirror-dest-template

mirror-dest-template

Syntax **mirror-dest-template** *name* [**type** *mirror-type*] [**create**]
no mirror-dest-template *name*

Context [Tree] (config>li mirror-dest-template)

Full Context configure li mirror-dest-template

Description This command creates a template used by RADIUS-triggered mirror destinations. RADIUS provides the IP destination (and other optional attributes) for the mirror destination and the mirror template provides the remaining mirror destination attributes for mirroring packets remotely over the core of an IP network.

The system supports up to eight mirror destination templates and allows a mirror destination to be swapped in real time. Only new LI sources will use the new attribute of the mirror destination template. Existing LI sources remain unchanged and continue to use the attribute of the previous mirror destination template.

The **no** form of this command removes a mirror destination template from the system.

Parameters *name* — Specifies the template name, up to 32 characters.

mirror-type — Specifies the type of encapsulation supported by the mirror service.

Values ether, frame-relay, ppp, ip-only, atm-sdu, satop-e1, satop-t1, cesopsn, cesopsn-cas

create — Keyword required to create a template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

mirror-dest-template

Syntax **mirror-dest-template** *template-name*
no mirror-dest-template

Context **[Tree]** (config>li>radius mirror-dest-template)

Full Context configure li radius mirror-dest-template

Description This command enables or disables the use of a RADIUS triggered mirror destination template to be used by new LI sources.

Parameters *template-name* — Specifies the template name, up to 32 characters. The template must already exist.

Platforms All

17.288 mirror-source

mirror-source

Syntax **mirror-source** [**all-inclusive**] *mirror-service-id*
no mirror-source

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action mirror-source)

Full Context configure application-assurance group policy app-qos-policy entry action mirror-source

Description This command configures an application-based policy mirroring service that uses this AA ISA group's AQP entry as a mirror source. When configured, AQP entry becomes a mirror source for IP packets seen by the AA (the mirrored packet is an IP packet analyzed by AA and does not include encapsulations present on the incoming interfaces).

Default no mirror-source

Parameters **all-inclusive** — Specifies that all packets during identification phase that could match a given AQP rule are mirrored in addition to packets after an application identification completes that match the AQP rule. This ensures all packets of a given flow are mirrored at a cost of sending unidentified packets that once the application is identified will no longer match this AQP entry.

mirror-service-id — Specifies the mirror source service ID to use for flows that match this policy.

Values 1 to 2147483647

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

svc-name: 64 characters maximum

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mirror-source

Syntax [**no**] **mirror-source** *service-id*

Context **[Tree]** (debug>app-assure>group>traffic-capture>match mirror-source)

Full Context debug app-assure group traffic-capture match mirror-source

Description This command configures debugging on a mirror source.

mirror-source

Syntax [**no**] **mirror-source** *service-id*

Context **[Tree]** (config>mirror mirror-source)

Full Context configure mirror mirror-source

Description This command configures mirror source parameters for a mirrored service.

The **mirror-source** command is used to enable mirroring of packets specified by the association of the **mirror-source** to sources of packets defined within the context of the *mirror-dest-service-id*. The mirror destination service must already exist within the system.

A mirrored packet cannot be mirrored to multiple destinations. If a packet matches multiple mirror source entries (for example, a SAP on one **mirror-source** and a port on another **mirror-source**), then the packet is mirrored to a single *mirror-dest-service-id* based on the following precedence:

1. Filter entry
2. Subscriber (applies to the 7750 SR and 7450 ESS)
3. SAP
4. Physical port

The precedence is structured so the most specific match criteria has precedence over a less specific match. For example, if a **mirror-source** defines a port and a SAP on that port, then a packet arriving on the SAP will be mirrored using the SAP mirror (and not mirrored using the Port mirror) because the SAP is more specific than the port.

The **no** form of this command deletes all related source commands within the context of the **mirror-source** *service-id*. The command does not remove the service ID from the system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — Specifies the service identification identifies the service in the service domain. This ID is unique to this service and cannot be used by any other service, regardless of service type. The same service ID must be configured on every router that this particular service is defined on.

Values

service-id:	1 to 2147483647
svc-name:	64 characters maximum

Platforms All

mirror-source

Syntax [**no**] **mirror-source** *service-id*

Context **[Tree]** (debug mirror-source)

Full Context debug mirror-source

Description This command configures mirror source parameters for a mirrored service.

The **mirror-source** command is used to enable mirroring of packets specified by the association of the **mirror-source** to sources of packets defined within the context of the *mirror-dest-service-id*. The mirror destination service must already exist within the system.

A mirrored packet cannot be mirrored to multiple destinations. If a packet matches multiple mirror source entries (for example, a SAP on one **mirror-source** and a port on another **mirror-source**), then the packet is mirrored to a single *mirror-dest-service-id* based on the following precedence:

1. Filter entry
2. Subscriber (applies to the 7750 SR and 7450 ESS)
3. SAP
4. Physical port

The precedence is structured so the most specific match criteria has precedence over a less specific match. For example, if a **mirror-source** defines a port and a SAP on that port, then a packet arriving on the SAP will be mirrored using the SAP mirror (and not mirrored using the Port mirror) because the SAP is more specific than the port.

The **mirror-source** configuration is not saved when a configuration is saved. A **mirror-source** manually configured within an ASCII configuration file will not be preserved if that file is overwritten by a **save** command. Define the **mirror-source** within a file associated with a **config exec** command to make a **mirror-source** persistent between system reboots.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, all mirror destination service IDs have a **mirror-source** associated with them. The **mirror-source** is not technically created with this command. Instead the service ID provides a contextual node for storing the current mirroring sources for the associated mirror destination service ID. The **mirror-source** is created for the mirror service when the operator enters the **debug>mirror-source** *svcId* for the first time. If the operator enters **li>li-source** *svcId* for the first time, an LI source is created for the mirror service. The **mirror-source** is also automatically removed when the mirror destination service ID is deleted from the system.

The **no** form of this command deletes all related source commands within the context of the **mirror-source** *service-id*. The command does not remove the service ID from the system.

Parameters *service-id* — Specifies the mirror destination service ID for which match criteria will be defined. The *service-id* must already exist within the system.

Values *service-id*: 1 to 2147483647
svc-name: 64 characters maximum

Platforms All

17.289 misc

misc

Syntax [**no**] **misc**

Context **[Tree]** (debug>router>igmp misc)

Full Context debug router igmp misc

Description This command enables debugging for IGMP miscellaneous information.

The **no** form of the command disables the debugging.

Output The following is shows debugged IGMP miscellaneous information

Sample Output

```
A:ALA-CA# debug router 100 igmp misc
*A:ALA-CA# show debug
debug
    router "100"
        igmp
            misc
        exit
    exit
exit
*A:ALA-CA#
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

misc

Syntax [**no**] **misc**

Context **[Tree]** (debug>router>gmpls>event misc)

Full Context debug router gmpls event misc

Description This command enables and disables debugging for GMPLS Misc events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

misc

Syntax **misc** [**detail**]
no misc

Context **[Tree]** (debug>router>mpls>event misc)
[Tree] (debug>router>rsvp>event misc)

Full Context debug router mpls event misc
debug router rsvp event misc

Description This command debugs miscellaneous events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about miscellaneous events.

Platforms All

misc

Syntax [**no**] **misc**

Context **[Tree]** (debug>router>mtrace misc)
[Tree] (debug>router>mtrace2 misc)

Full Context debug router mtrace misc
debug router mtrace2 misc

Description This command enables debugging for mtrace and mtrace2 miscellaneous.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

misc

Syntax [**no**] **misc**

Context **[Tree]** (debug>router>isis misc)

Full Context debug router isis misc

Description This command enables debugging for IS-IS misc.

The **no** form of the command disables debugging.

Platforms All

misc

Syntax [**no**] **misc**

Context **[Tree]** (debug>router>ospf misc)
[Tree] (debug>router>ospf3 misc)

Full Context debug router ospf misc
debug router ospf3 misc

Description This command enables debugging for miscellaneous OSPF events.

Platforms All

17.290 mismatch-reaction

mismatch-reaction

Syntax **mismatch-reaction** {**squelch-rx**}
no mismatch-reaction

Context **[Tree]** (config>port>otu>pm-tti mismatch-reaction)

Full Context configure port otu pm-tti mismatch-reaction

Description This command allows the user to configure the consequent action to a pm-tti mismatch.

The **no** form of this command reverts to the default value.

Default n/a, the received traffic is passed through.

Parameters **squelch-rx** — Specifies that the received traffic is blocked.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mismatch-reaction

Syntax **mismatch-reaction** {**none** | **squelch-rx**}

Context **[Tree]** (config>port>otu>psi-payload mismatch-reaction)

Full Context configure port otu psi-payload mismatch-reaction

Description This command allows the user to configure the consequent action to a psi-payload type mismatch.

Parameters **none** — Specifies the received traffic is passed through.

squelch-rx — Specifies the received traffic is blocked.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mismatch-reaction

Syntax **mismatch-reaction** {**none** | **squelch-rx**}

Context **[Tree]** (config>port>otu>sm-tti mismatch-reaction)

Full Context configure port otu sm-tti mismatch-reaction

Description This command allows the user to configure the consequent action to a sm-tti mismatch.

Default n/a

Parameters **none** — Specifies that the received traffic is passed through.

squelch-rx — Specifies that the received traffic is blocked.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.291 missing-mandatory-ie

missing-mandatory-ie

Syntax **missing-mandatory-ie direction** *direction* [**create**]
no missing-mandatory-ie direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter missing-mandatory-ie)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter missing-mandatory-ie

Description This command configures a TCA for the counter capturing drops due to the GTP filter missing mandatory IE check. A missing-mandatory-ie drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a missing-mandatory-ie TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.292 mixed-lsp-mode

mixed-lsp-mode

Syntax [**no**] **mixed-lsp-mode**

Context **[Tree]** (config>service>sdp mixed-lsp-mode)

Full Context configure service sdp mixed-lsp-mode

Description This command enables the use by an SDP of the mixed-LSP mode of operation. This command indicates to the service manager that it must allow a primary LSP type and a backup LSP type in the same SDP configuration. For example, the **lsp** and **ldp** commands are allowed concurrently in the SDP configuration. The user can configure one or two types of LSPs under the same SDP. Without this command, these commands are mutually exclusive.

The user can configure an RSVP LSP as a primary LSP type with an LDP LSP as a backup type. The user can also configure a BGP RFC 3107 BGP LSP as a backup LSP type.

If the user configures an LDP LSP as a primary LSP type, then the backup LSP type must be an RFC 3107 BGP labeled route.

At any given time, the service manager programs only one type of LSP in the linecard that will activate it to forward service packets according to the following priority order:

- RSVP LSP type. Up to 16 RSVP LSPs can be entered by the user and programmed by the service manager in ingress linecard to load balance service packets. This is the highest priority LSP type.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- LDP LSP type. One LDP FEC programmed by the service manager but the ingress card can use up to 16 LDP ECMP paths for the FEC to load balance service packets when ECMP is enabled on the node.
- BGP LSP type. One RFC 3107-labeled BGP prefix programmed by the service manager. The ingress card can use more than one next-hop for the prefix.

In the case of the RSVP/LDP SDP, the service manager will program the NHLFE(s) for the active LSP type preferring the RSVP LSP type over the LDP LSP type. If no RSVP LSP is configured or all configured RSVP LSPs go down, the service manager will re-program the card with the LDP LSP if available. If not, the SDP goes operationally down.

When a higher priority type LSP becomes available, the service manager reverts back to this LSP at the expiry of the sdp-revert-time timer or the failure of the currently active LSP, whichever comes first. The service manager then re-programs the card accordingly. If the infinite value is configured, then the SDP reverts to the highest priority type LSP only if the currently active LSP failed.

Note: LDP uses a tunnel down damp timer which is set to three seconds by default. When the LDP LSP fails, the SDP will revert to the RSVP LSP type after the expiry of this timer. For an immediate switchover, this timer must be set to zero. Use the **config>router>ldp>tunnel-down-damp-time** command.

If the user changes the value of the sdp-revert-time timer, it will take effect only at the next use of the timer. Any timer which is outstanding at the time of the change will be restarted with the new value.

If class based forwarding is enabled for this SDP, the forwarding of the packets over the RSVP LSPs will be based on the FC of the packet as in current implementation. When the SDP activates the LDP LSP type, then packets are forwarded over the LDP ECMP paths using the regular hash routine.

In the case of the LDP/BGP SDP, the service manager will prefer the LDP LSP type over the BGP LSP type. The service manager will re-program the card with the BGP LSP if available otherwise it brings down the SDP operationally.

Also note the following difference in behavior of the LDP/BGP SDP compared to that of an RSVP/LDP SDP. For a given /32 prefix, only a single route will exist in the routing table: the IGP route or the BGP route. Thus, either the LDP FEC or the BGP label route is active at any given time. The impact of this is that the tunnel table needs to be re-programmed each time a route is deactivated and the other is activated. Furthermore, the SDP revert-time cannot be used since there is no situation where both LSP types are active for the same /32 prefix.

The **no** form of this command disables the mixed-LSP mode of operation. The user first has to remove one of the LSP types from the SDP configuration or the command will fail.

Default no mixed-lsp-mode

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.293 mka-hello-interval

mka-hello-interval

Syntax **mka-hello-interval** *interval*
no mka-hello-interval

Context **[Tree]** (config>macsec>conn-assoc>static-cak mka-hello-interval)

Full Context configure macsec connectivity-association static-cak mka-hello-interval

Description This command specifies the MKA hello interval.

The **no** form of this command disables the MKA hello interval.

Default mka-hello-interval 2

Parameters *interval* — Specifies the MKA hello interval, in seconds.

Values 1 to 6 s in 1-s increments, 500ms

Platforms All

17.294 mka-key-server-priority

mka-key-server-priority

Syntax **mka-key-server-priority** *priority*
no mka-key-server-priority

Context **[Tree]** (config>macsec>conn-assoc>static-cak mka-key-server-priority)

Full Context configure macsec connectivity-association static-cak mka-key-server-priority

Description This command specifies the key server priority used by the MACsec Key Agreement (MKA) protocol to select the key server when MACsec is enabled using static connectivity association key (CAK) security mode.

The **no** form of this command disables the **mka-key-server-priority**.

Default mka-key-server-priority 16

Parameters *priority* — Specifies the priority of the server.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.295 mld

mld

Syntax [**no**] **mld**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync mld)

Full Context configure redundancy multi-chassis peer sync mld

Description This command specifies whether MLD protocol information should be synchronized with the multi-chassis peer.

Default no mld

Platforms All

mld

Syntax [**no**] **mld**

Context **[Tree]** (config>service>vprn mld)

Full Context configure service vprn mld

Description Commands in this context configure Multicast Listener Discovery (MLD) parameters.

The **no** form of this command disables MLD.

Default no mld

Platforms All

mld

Syntax [**no**] **mld**

Context **[Tree]** (config>router mld)

Full Context configure router mld

Description Commands in this context configure Multicast Listener Discovery (MLD) parameters.

The **no** form of the command disables MLD.

Default no mld

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.296 mld-parameters

mld-parameters

Syntax **mld-parameters**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host mld-parameters)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host mld-parameters)

Full Context configure subscriber-mgmt local-user-db ipoe host mld-parameters
configure subscriber-mgmt local-user-db ppp host mld-parameters

Description Commands in this context configure an MLD import policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.297 mld-policy

mld-policy

Syntax **mld-policy** *mld-policy-name* [**create**]
no mld-policy *mld-policy-name*

Context **[Tree]** (config>subscr-mgmt mld-policy)

Full Context configure subscriber-mgmt mld-policy

Description Commands in this context create an MLD policy.

The **no** form of this command reverts to the default.

Parameters *mld-policy-name* — Specifies the MLD policy name up to 32 characters.

create — Keyword required to create the configuration context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mld-policy

Syntax **mld-policy** *policy name*
no mld-policy

Context **[Tree]** (config>subscr-mgmt>sub-prof mld-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt sub-profile mld-policy

Description This command enables Multicast Listener Discovery (MLD) processing per subscriber host.

The **no** form of this command reverts to the default.

Default no mld-policy

Parameters *policy-name* — Specifies the name of the MLD policy, up to 32 characters. The MLD policy must be defined in the config>subscr-mgmt context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.298 mld-snooping

mld-snooping

Syntax **mld-snooping**

Context **[Tree]** (config>service>vpls mld-snooping)
[Tree] (config>service>vpls>sap mld-snooping)
[Tree] (config>service>vpls>spoke-sdp mld-snooping)
[Tree] (config>service>vpls>mesh-sdp mld-snooping)
[Tree] (config>service>vpls>allow-ip-int-bind mld-snooping)

Full Context configure service vpls allow-ip-int-bind mld-snooping
configure service vpls mesh-sdp mld-snooping
configure service vpls mld-snooping
configure service vpls sap mld-snooping
configure service vpls spoke-sdp mld-snooping

Description Commands in this context configure MLD snooping parameters.

Platforms All

mld-snooping

Syntax [**no**] **mld-snooping**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync mld-snooping)

Full Context configure redundancy multi-chassis peer sync mld-snooping

Description This command is not supported. It is not blocked for backwards-compatibility reasons but has no effect on the system if configured.

Default no mld-snooping

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

mld-snooping

Syntax [**no**] **mld-snooping**

Context **[Tree]** (debug>service>id mld-snooping)

Full Context debug service id mld-snooping

Description This command enables and configures MLD-snooping debugging.

The **no** form of this command disables MLD-snooping debugging.

Platforms All

mld-snooping

Syntax **mld-snooping**

Context **[Tree]** (config>service>vpls>vxlan mld-snooping)

Full Context configure service vpls vxlan mld-snooping

Description This command enables the MLD snooping context.

Platforms All

mld-snooping

Syntax **mld-snooping**

Context **[Tree]** (config>service>vpls>pbb>bvpls mld-snooping)
[Tree] (config>service>vpls>pbb>bvpls>sap mld-snooping)
[Tree] (config>service>vpls>pbb>bvpls>sdp mld-snooping)

Full Context configure service vpls pbb backbone-vpls mld-snooping
configure service vpls pbb backbone-vpls sap mld-snooping
configure service vpls pbb backbone-vpls sdp mld-snooping

Description This command configures MLD snooping attributes for I-VPLS.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.299 mldp

mldp

Syntax [**no**] **mldp**

Context **[Tree]** (config>service>vpls>provider-tunnel>inclusive mldp)

Full Context configure service vpls provider-tunnel inclusive mldp

Description Commands in this context configure the parameters of an LDP P2MP LSP used for forwarding Broadcast, Unicast unknown and Multicast (BUM) packets of a VPLS or B-VPLS instance.

Platforms All

mldp

Syntax [**no**] **mldp**

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive mldp)
[Tree] (config>service>vprn>mvpn>pt>selective mldp)

Full Context configure service vprn mvpn provider-tunnel inclusive mldp
configure service vprn mvpn provider-tunnel selective mldp

Description This command enables use of P2MP mLDP LSP as inclusive or selective PMSI tunnels.

For multi-stream S-PMSI, either LDP or RSVP-TE must first be configured before multi-stream policy can be configured.

Default no mldp

Platforms All

17.300 mlfr

mlfr

Syntax **mlfr**

Context **[Tree]** (config>port>multilink-bundle mlfr)

Full Context configure port multilink-bundle mlfr

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure a Multi-link Frame Relay (MLFR) bundle.

Platforms 7450 ESS, 7750 SR-7/12/12e

17.301 mlppp

mlppp

Syntax **mlppp**

Context **[Tree]** (config>port>ml-bundle mlppp)
[Tree] (config>subscr-mgmt>ppp-policy mlppp)

Full Context configure port multilink-bundle mlppp
configure subscriber-mgmt ppp-policy mlppp

Description Commands in this context configure multi-link PPP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure subscriber-mgmt ppp-policy mlppp

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlppp

17.302 mlppp-profile-egress

mlppp-profile-egress

Syntax **mlppp-profile-egress** *profile-id* [**create**]
no mlppp-profile-egress *profile-id*

Context **[Tree]** (config>qos mlppp-profile-egress)

Full Context configure qos mlppp-profile-egress

Description This command creates a profile for the user to configure the egress QoS parameters of a multiclass MLPPP bundle.

A maximum of 128 egress QoS profiles can be created on the system.

The **no** form of this command deletes the profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *profile-id* — Specifies an ingress mlppp-profile ID.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mlppp-profile-egress

Syntax **mlppp-profile-egress** *src-mlppp-prof dst-mlppp-prof* [**overwrite**]

Context **[Tree]** (config>qos>copy mlppp-profile-egress)

Full Context configure qos copy mlppp-profile-egress

Description This command copies an existing ingress **mlppp-profile-egress** profile ID to another egress **mlppp-profile-egress** profile ID. The **copy** command is a configuration level maintenance tool used to create new entries using an existing profile ID. If **overwrite** is not specified, an error occurs if the destination profile ID exists.

Parameters *src-mlppp-prof* — Specifies the existing source egress **mlppp-profile-egress** profile ID from which the **copy** command attempts to copy.

Values 1 to 65535

dst-mlppp-prof — Specifies the destination egress **mlppp-profile-egress** profile ID to which the copy command attempts to copy.

Values 1 to 65535

overwrite — Use this parameter when the **mlppp-profile-egress** *dst-mlppp-prof* already exists. If it does, everything in the existing destination **mlppp-profile-egress** *dst-mlppp-prof* is completely overwritten with the contents of the **mlppp-profile-egress** *src-mlppp-prof*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI use {overwrite}; destination mlppp-egress-profile
"1010" exists
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.303 mlppp-profile-ingress

mlppp-profile-ingress

Syntax [**no**] **mlppp-profile-ingress** *profile-id* [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos mlppp-profile-ingress)

Full Context configure qos mlppp-profile-ingress

Description This command creates a profile for the user to configure the ingress QoS parameters of a multiclass MLPPP bundle.

A maximum of 128 ingress QoS profiles can be created on the system.

The **no** form of this command deletes the profile.

Parameters *profile-id* — Specifies a specific multi-class ingress profile.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mlppp-profile-ingress

Syntax **mlppp-profile-ingress** *src-mlppp-prof dst-mlppp-prof* [**overwrite**]

Context [Tree] (config>qos>copy mlppp-profile-ingress)

Full Context configure qos copy mlppp-profile-ingress

Description This command copies an existing ingress **mlppp-profile-ingress** profile ID to another ingress **mlppp-profile-ingress** profile ID. The **copy** command is a configuration level maintenance tool used to create new entries using an existing profile ID. If **overwrite** is not specified, an error occurs if the destination profile ID exists.

Parameters *src-mlppp-prof* — Specifies the existing source MLPPP profile ID from which the **copy** command attempts to copy.

Values 1 to 65535

dst-mlppp-prof — Specifies the destination MLPPP profile ID to which the copy command attempts to copy.

Values 1 to 65535

overwrite — Use this parameter when the **mlppp-profile-ingress** *dst-mlppp-prof* already exists. If it does, everything in the existing destination **mlppp-profile-ingress** *dst-mlppp-prof* is completely overwritten with the contents of the **mlppp-profile-ingress** *src-mlppp-prof*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI use {overwrite}; destination mlppp-ingress-profile
"100" exists
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.304 mme

mme

Syntax **mme**

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile mme)

Full Context configure subscriber-mgmt gtp peer-profile mme

Description This command configures parameters specific to a Mobility Management Entity (MME) peer.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.305 mmrp

mmrp

Syntax **mmrp**

Context **[Tree]** (config>service>vpls>mrp mmrp)

Full Context configure service vpls mrp mmrp

Description This command configures MMRP parameters.

Platforms All

17.306 mmrp-impm-override

mmrp-impm-override

Syntax [**no**] **mmrp-impm-override**

Context **[Tree]** (config>mcast-mgmt>chassis-level mmrp-impm-override)

Full Context configure mcast-management chassis-level mmrp-impm-override

Description This command enables ingress Multicast Path Management (IMPM) from monitoring PIM and IGMP.

The **no** form of this command disables the IMPM monitoring.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

17.307 mmrp-mac

mmrp-mac

Syntax [**no**] **mmrp-mac** *ieee-address*

Context **[Tree]** (debug>service>id>mrp mmrp-mac)

Full Context debug service id mrp mmrp-mac

Description This command filters debug events and only shows events related to the MAC address specified.

The **no** form of this command removes the debug filter.

Parameters *ieee-address* — xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx (cannot be all zeros)

Platforms All

17.308 mobility

mobility

Syntax **mobility**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw mobility)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw mobility)

Full Context configure service ies subscriber-interface group-interface wlan-gw mobility
configure service vprn subscriber-interface group-interface wlan-gw mobility

Description Commands in this context configure mobility parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.309 mobility-acct-updates

mobility-acct-updates

Syntax [**no**] **mobility-acct-updates**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range>xconnect mobility-acct-updates)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range>xconnect mobility-acct-updates)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect mobility-acct-updates
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect mobility-acct-updates

Description This command enables the administrative state to send mobility-triggered accounting interim updates.

The **no** form of this command disables sending the mobility-triggered accounting updates.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.310 mobility-triggered-acct

mobility-triggered-acct

Syntax **mobility-triggered-acct**

Context **[Tree]** (config>router>wlan-gw mobility-triggered-acct)
[Tree] (config>service>vprn>wlan-gw mobility-triggered-acct)

Full Context configure router wlan-gw mobility-triggered-acct
configure service vprn wlan-gw mobility-triggered-acct

Description Commands in this context configure the mobility-triggered-accounting in wlan-gw context under router or VPRN service.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.311 mode

mode

Syntax **mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}
no mode

Context **[Tree]** (debug>router>ip>dhcp mode)
[Tree] (debug>router>ip>dhcp6 mode)
[Tree] (debug>router>local-dhcp-server mode)

Full Context debug router ip dhcp mode
debug router ip dhcp6 mode
debug router local-dhcp-server mode

Description This command debugs the DHCP tracing detail level.

Parameters **dropped-only** — Displays only dropped packets.

ingr-and-dropped — Displays only ingress packet and dropped packets.

egr-ingr-and-dropped — Displays ingress, egress and dropped packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- debug router local-dhcp-server mode

All

- debug router ip dhcp mode
- debug router ip dhcp6 mode

mode

Syntax **mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}
no mode

Context **[Tree]** (debug>service>id>ppp>packet mode)

Full Context debug service id ppp packet mode

Description This command specifies PPP packet debug mode.

The **no** form of this command disables debugging.

Parameters **dropped-only** — Displays only dropped packets.

ingr-and-dropped — Displays only ingress packet and dropped packets.

egr-ingr-and-dropped — Displays ingress, egress and dropped packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mode

Syntax **mode** *mode*

Context **[Tree]** (config>card>mda>atm mode)

Full Context configure card mda atm mode

Description This command configures the ATM MDA into a mode with the increased VC scale (16k VCs, as opposed to 8K VCs). ESM is supported only in 16K VCs mode. In 16K VCs mode, there is only one queue allocated to each VC in the ATM MDA. In 8K VCs mode, there are two queues allocated per VC.

The 16K VC mode is supported only on the 4-port oc-3/12c/STM-1/4c ATM MDA.

Changing the ATM MDA mode requires a reset of the MDA. A warning is issued asking for the confirmation before the command is executed.

Default mode max8k-vc

Parameters *mode* — Specifies the VC scale.

Values max8k-vc, max16k-vc

Platforms All

mode

Syntax **mode** {**strict** | **loose** | **strict-no-ecmp**}
no mode

Context **[Tree]** (config>service>ies>if>ipv6>urpf-check mode)
[Tree] (config>service>ies>if>urpf-check mode)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>urpf-check mode)
[Tree] (config>service>vprn>if>ipv6>urpf-check mode)
[Tree] (config>service>vprn>if>urpf-check mode)
[Tree] (config>service>vprn>nw-if>urpf-check mode)
[Tree] (config>service>vprn>sub-if>grp-if>urpf-check mode)

Full Context configure service ies interface ipv6 urpf-check mode
configure service ies interface urpf-check mode
configure service ies subscriber-interface group-interface ipv6 urpf-check mode
configure service vprn interface ipv6 urpf-check mode
configure service vprn interface urpf-check mode
configure service vprn network-interface urpf-check mode
configure service vprn subscriber-interface group-interface urpf-check mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the mode of unicast RPF check.

The **no** form of this command reverts to the default (strict) mode.

Default mode strict

Parameters **strict** — When specified, uRPF checks whether incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

loose — In **loose** mode, uRPF checks whether incoming packet has source address with a corresponding prefix in the routing table. However, the loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. This object is valid only when **urpf-check** is enabled.

strict-no-ecmp — When a packet is received on an interface in this mode and the SA matches an ECMP route the packet is dropped by uRPF.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface urpf-check mode
- configure service ies subscriber-interface group-interface ipv6 urpf-check mode

All

- configure service ies interface ipv6 urpf-check mode
- configure service vprn network-interface urpf-check mode
- configure service vprn interface ipv6 urpf-check mode
- configure service vprn interface urpf-check mode
- configure service ies interface urpf-check mode

mode

Syntax **mode** {**strict** | **loose** | **strict-no-ecmp**}
no mode

Context **[Tree]** (config>subscr-mgmt>git>ipv4>urpf-check mode)

Full Context configure subscriber-mgmt group-interface-template ipv4 urpf-check mode

Description This command configures the mode of Unicast RPF (uRPF) check.

The **no** form of this command reverts to the default.

Default mode strict

Parameters **strict** — Specifies that the uRPF checks whether the incoming packet has a source IP address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source IP address prefix.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

loose — Specifies that the uRPF checks whether the incoming packet has a source IP address with a corresponding prefix in the routing table. However, the **loose** mode does not check whether the interface expects to receive a packet with a specific source IP address prefix. This object is valid only when the **urpf-check** command is enabled.

strict-no-ecmp — Specifies that when a packet is received on an interface in this mode and the SA matches an ECMP route, the packet is dropped by uRPF.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mode

Syntax **mode** {**none** | **basic** | **advanced**}

Context **[Tree]** (config>system>power-management mode)

Full Context configure system power-management mode

Description This command sets the power mode. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Default mode basic

Parameters **none** — Specifies that there is no management of power to modules. In this mode, no gradual shutdown of active XCMs and XMAs is enforced. No spare capacity is reserved and any APEQ failure may result in brownouts or card failures.

basic — Specifies that the node will bring up as many provisioned modules (in order of priority) as possible using the N+1 algorithm. In **basic** mode the system shuts down IO cards when power capacity drops below the Power Safety Level.

advanced — Specifies that the operator can maintain a spare APEQ as long as possible to make it immune to the possibility of power brown-outs. In **advanced** mode, the system starts shutting down IO cards when the power capacity drops below the Power Safety Level + Max rated APEQ.

Platforms 7750 SR-s, 7950 XRS

mode

Syntax **mode** {**automatic** | **manual**}

Context **[Tree]** (config>port>dwdm>coherent mode)

Full Context configure port dwdm coherent mode

Description This command configures the mode used to compensate for chromatic dispersion.

Parameters **automatic** — Sets to automatic mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

manual — Sets to manual mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mode

Syntax **mode** {**none** | **uni-n**}

Context **[Tree]** (config>port>ethernet>elmi mode)

Full Context configure port ethernet elmi mode

Description This command configures the Ethernet LMI mode.

Parameters **none** — Specifies that the E LMI mode is set to none.

uni-n — Specifies that the E LMI mode is set to UNI-N.

Platforms All

mode

Syntax **mode** {**access** | **network** | **hybrid**}
no mode

Context **[Tree]** (config>lag mode)
[Tree] (config>port>ethernet mode)
[Tree] (config>port>sonet-sdh>path mode)
[Tree] (config>port>tdm>ds1>channel-group mode)
[Tree] (config>port>tdm>ds3 mode)
[Tree] (config>port>tdm>e1>channel-group mode)
[Tree] (config>port>tdm>e3 mode)

Full Context configure lag mode
configure port ethernet mode
configure port sonet-sdh path mode
configure port tdm ds1 channel-group mode
configure port tdm ds3 mode
configure port tdm e1 channel-group mode
configure port tdm e3 mode

Description This command configures an Ethernet port, TDM channel, or SONET/SDH path (sub-port) for **access, network or hybrid** mode operation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An **access** port or channel is used for customer facing traffic on which services are configured. A Service Access Point (SAP) can only be configured on an access port or channel. When a port is configured for access mode, the appropriate **encap-type** must be specified to distinguish the services on the port or SONET path. Once an Ethernet port, a TDM channel or a SONET path has been configured for access mode, multiple services can be configured on the Ethernet port, a TDM channel or SONET path.

A network port or channel participates in the service provider transport or infrastructure network when a network mode is selected. When the network option is configured, the encap-type cannot be configured for the port/channel.

When network mode is selected on a SONET/SDH path, the appropriate control protocols are activated when the need arises. For example, configuring an IP interface on the SONET path activates IPCP while the removal of the IP interface causes the IPCP to be removed. The same applies for MPLS, MPLSCP, and OSICP. When configuring a SONET/SDH port, the mode command must be entered in the channel context or an error message is generated.

A hybrid Ethernet port allows the combination of network and access modes of operation on a per-VLAN basis and must be configured as either dot1q or QinQ encapsulation.

When the hybrid port is configured to the dot1q encapsulation, the user configures a SAP inside a service simply by providing the SAP ID which must include the port-id value of the hybrid mode port and an unused VLAN tag value. The format is <*port-id*>:*qtag1*. A SAP of format <*port-id*>:* also supported.

The user configures a network IP interface under **config>router>if>port** by providing the port name which consists of the port-id of the hybrid mode port and an unused VLAN tag value. The format is <*port-id*>:*qtag1*. The user must explicitly enter a valid value for qtag1. The <*port-id*>:* value is not supported on a network IP interface. The 4096 VLAN tag space on the port is shared among VLAN SAPs and VLAN network IP interfaces.

When the hybrid port is configured to QinQ encapsulation, the user configures a SAP inside a service simply by providing the SAP ID which must include the port-id value of the hybrid mode port and the outer and inner VLAN tag values. The format is <port-id>:qtag1.qtag2. A SAP of format <*port-id*>: *qtag1*.* is also supported. The outer VLAN tag value must not have been used to create an IP network interface on this port. In addition, the qtag1.qtag2 value combination must not have been used by another SAP on this port.

The user configures a network IP interface under **config>router>if>port** by providing the port name which consists of the port-id of the hybrid mode port and a VLAN tag value. The format is <*port-id*>:*qtag1*.*. An outer VLAN tag qtag2 of * creates an IP network interface. In addition, the qtag1.qtag2 value combination must not have been used on another SAP or IP network interface on this port.

The **no** form of this command restores the default.

Default mode network — For Ethernet ports

mode access — For TDM channel or SONET paths

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Special Cases **SONET/SDH Path —** When network mode is selected, the appropriate control protocols are activated when the need arises. For example, configuring an IP interface on the SONET path activates IPCP while the removal of the IP interface causes the IPCP to be removed. The same applies for MPLS, MPLSCP, and OSICP. When configuring a SONET/SDH port, the **mode** command must be entered in the channel context or an error message is generated.

Parameters **access** — Configures the Ethernet port, TDM channel or SONET path as service access.

network — Configures the Ethernet port, TDM channel or SONET path for transport network use.

hybrid — Configures the Ethernet port for hybrid use.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path mode

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group mode
- configure port tdm e3 mode
- configure port tdm ds1 channel-group mode
- configure port tdm ds3 mode

All

- configure port ethernet mode
- configure lag mode

mode

Syntax **mode** {**active** | **passive**}

Context **[Tree]** (config>port>ethernet>efm-oam mode)

Full Context configure port ethernet efm-oam mode

Description This command configures the mode of OAM operation for this Ethernet port. These two modes differ in that active mode causes the port to continually send out efm-oam info PDUs while passive mode waits for the peer to initiate the negotiation process. A passive mode port cannot initiate monitoring activities (such as loopback) with the peer.

Default mode active

Parameters **active** — Provides capability to initiate negotiation and monitoring activities.

passive — Relies on peer to initiate negotiation and monitoring activities.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mode

Syntax **mode** {**dce** | **dte** | **bidir**}

Context **[Tree]** (config>port>ml-bundle>mlfr>frame-relay mode)

Full Context configure port multilink-bundle mlfr frame-relay mode

Description This command configures the DCE/DTE mode of the Frame Relay interface.

Parameters **dce** — Enables the DCE mode.

dte — Enables the DTE mode.

bidir — Enables the bidirectional mode for LMI types ANSI and ITU.

Platforms 7450 ESS, 7750 SR-7/12/12e

mode

Syntax **mode** {**dce** | **dte** | **bidir**}

Context **[Tree]** (config>port>multi-link-bundle>mlfr>frame-relay mode)
[Tree] (config>port>sonet-sdh>path>frame-relay mode)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay mode)
[Tree] (config>port>tdm>ds3>frame-relay mode)
[Tree] (config>port>tdm>e1>channel-group>frame-relay mode)
[Tree] (config>port>tdm>e3>frame-relay mode)

Full Context configure port multilink-bundle mlfr frame-relay mode
configure port sonet-sdh path frame-relay mode
configure port tdm ds1 channel-group frame-relay mode
configure port tdm ds3 frame-relay mode
configure port tdm e1 channel-group frame-relay mode
configure port tdm e3 frame-relay mode

Description This command sets the Frame Relay interface into the DCE, DTE, or Bidirectional mode of LMI operation. The DTE mode causes the router to send status inquiries over the interface. The DCE mode causes the router to respond to status inquiries. In bidirectional mode, the router performs both DTE and DCE operation over the FR interface. The bidirectional mode applies to the ANSI and ITU LMI types only.

This feature is used when two routers are connected back-to-back, running frame relay encapsulation.

Default mode dte

Parameters **dce** — Enables the DCE mode.

dte — Enables the DTE mode.

bidir — Enables the bidirectional mode for LMI types ANSI and ITU.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay mode

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlfr frame-relay mode

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group frame-relay mode
- configure port tdm e1 channel-group frame-relay mode
- configure port tdm e3 frame-relay mode
- configure port tdm ds3 frame-relay mode

mode

Syntax **mode** {**manual** | **auto** | **off**}

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>service-carving mode)

Full Context configure service system bgp-evpn ethernet-segment service-carving mode

Description This command configures the service-carving mode. This determines how the DF is elected for a specified Ethernet-Segment and service.

Default mode auto

Parameters **auto** — This mode is the service-carving algorithm defined in RFC 7432. The DF for the service is calculated based on the modulo function of the service (identified by either the evi or the isid) and the number of PEs.

manual — In this mode the DF is elected based on the manual configuration added in the **service-carving>manual** context.

off — In this mode all the services elect the same DF PE (assuming the same PEs are active for all the configured services). The PE with the lowest IP is elected as DF for the Ethernet-Segment.

Platforms All

mode

Syntax **mode** *mode*

Context **[Tree]** (config>service>vpls>pim-snooping mode)

Full Context configure service vpls pim-snooping mode

Description This command sets the PIM snooping mode to proxy or plain snooping.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mode* — Specifies PIM snooping mode

Values snoop, proxy

Default proxy

Platforms All

mode

Syntax **mode** {*rstp* | *comp-dot1w* | *dot1w* | *mstp* | *pmstp*}
no mode

Context **[Tree]** (config>service>vpls>stp mode)
[Tree] (config>service>template>vpls-template>stp mode)

Full Context configure service template vpls-template stp mode
configure service vpls stp mode

Description This command specifies the version of Spanning Tree Protocol the bridge is currently running.

See section Spanning Tree Operating Modes for more information about these modes.

The **no** form of this command returns the STP variant to the default.

Default mode rstp

Parameters **rstp** — Corresponds to the Rapid Spanning Tree Protocol specified in IEEE 802.1D/D4-2003

dot1w — Corresponds to the mode where the Rapid Spanning Tree is backward compatible with IEEE 802.1w

compdot1w — Corresponds to the Rapid Spanning Tree Protocol in conformance with IEEE 802.1w

mstp — Sets MSTP as the STP mode of operation. Corresponds to the Multiple Spanning Tree Protocol specified in 802.1Q REV/D5.0-09/200

pmstp — The PMSTP mode is only supported in VPLS services where the M-VPLS flag is configured

Platforms All

mode

Syntax **mode** {**all** | **dropped-only**}
no mode

Context **[Tree]** (debug>service>id>arp-host mode)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug service id arp-host mode

Description This command configures the ARP host tracing mode.

Parameters **all** — Debugs all dropped packets.

dropped-only — Only displays dropped packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mode

Syntax **mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}
no mode

Context **[Tree]** (debug>service>id>igmp-snooping mode)

Full Context debug service id igmp-snooping mode

Description This command enables and configures the IGMP tracing mode.

The **no** form of this command disables the configures the IGMP tracing mode.

Platforms All

mode

Syntax **mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}
no mode

Context **[Tree]** (debug>service>id>mld mode)

Full Context debug service id mld-snooping mode

Description This command enables and configures the MLD tracing mode.

The **no** form of this command disables the configures the MLD tracing mode.

Platforms All

mode

Syntax **mode** {**mesh-group** | **standard**}

Context **[Tree]** (config>service>vprn>msdp>group mode)

Full Context configure service vprn msdp group mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers.

Multicast Source Discovery Protocol (MSDP) peers can be configured grouped in a full-mesh topology that prevents excessive flooding of source-active messages to neighboring peers.

In a meshed configuration, all members of the group must have a peer connection with every other mesh group member. If this rule is not adhered to, then unpredictable results may occur.

Default mode standard

Parameters **mesh-group** — Specifies that source-active message received from a mesh group member are always accepted but are not flooded to other members of the same mesh group. These source-active messages are only flooded to non-mesh group peers or members of other mesh groups.

standard — Specifies a non-meshed mode.

Platforms All

mode

Syntax **mode** {**auto** | **napt** | **one-to-one**}
no mode

Context **[Tree]** (config>service>vprn>nat>outside>pool mode)

Full Context configure service vprn nat outside pool mode

Description This command configures the mode of operation of this NAT address pool.

The mode value is only relevant while the value of pool type is equal to largeScale; while the value of pool type is equal to l2Aware, the mode of operation is always NAPT.

Default mode auto

Parameters **napt** — Specifies NAPT (Network Address Port Translation)

auto — The system selects the actual mode based upon other configuration parameters; the actual mode can be NAPT or 1:1 NAT (also known as 'Basic NAT').

one-to-one — Indicates 1:1 NAT (also known as 'Basic NAT')

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mode

Syntax **mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}
no mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>service>id>dhcp mode)

Full Context debug service id dhcp mode

Description This command configures the DHCP tracing mode.

The **no** form of the command disables debugging.

Parameters **dropped-only** — Only displays dropped packets.

ingr-and-dropped — Only displays ingress packet and dropped packets.

egr-ingr-and-dropped — Displays ingress, egress and dropped packets.

Platforms All

mode

Syntax **mode** *mode*

Context [Tree] (config>gmpls-tun-grp mode)

Full Context configure gmpls-tun-grp mode

Description This command sets the operating mode of the GMPLS tunnel group.

In **load-sharing** mode, traffic is load-shared across the member GMPLS LSPs of the tunnel group. The same hashing algorithm is used as for LAG (see the "LAG and ECMP hashing" chapter of the 7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide). If load-sharing is configured, then all of the GMPLS LSPs must terminate on the same far-end node. All of the ports used by GMPLS LSPs must be equivalent in that they must have the same named QoS policy, bandwidth, and so on Once more than one gLSP is associated with a tunnel group, the QoS policy / scheduler policy cannot be changed for any of the ports. All GMPLS LSPs must be unprotected end-to-end. Segment protection is allowed for GMPLS LSPs associated in a load sharing mode tunnel group.

In **active-standby** mode, only one member gLSP can be associated with the tunnel group.

The **no** form of this command removes the member.

Default mode load-sharing

Parameters *mode* — Specifies the operating mode of the GMPLS tunnel group.

Values **active-standby** — Sets the operating mode to active-standby.**load-sharing** — Sets the operating mode to load-sharing.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mode

Syntax **mode** *mode*

Context **[Tree]** (config>app-assure>group>gtp mode)

Full Context configure application-assurance group gtp mode

Description This command is used to either untunnel GTP-U traffic received on UDP port number 2152, or apply GTP filtering/firewall rules as specified under this GTP CLI context.

Default mode filtering

Parameters *mode* — Specifies the operational mode of the command.

Values **filtering** — AA applies GTP filtering rules to GTP-U traffic, without further analysis of IP traffic tunneled within GTP.

untunneling — AA untunnels GTP traffic and provides analytical reporting of the applications running within the GTP tunnels. The rest of the commands under GTP CLI context (such as GTP-filter and event-log) are not applicable in this mode.

For AA to untunnel GTP traffic, the operator must configure “gtp” under the partition by using the **config**>**app-assure**>**group**>**gtp** command.

The following caveats apply:

- Only GTP-U traffic with TID <> 0 is untunneled.
- Any UDP but non-GTP traffic that uses port 2152 will be identified as UDP traffic.
- Only GTP-U packets with message type: G-PDU (0xFF) is untunneled. Other GTP-U packets with different message types are reported as GTP Protocol.
- Only GTP-u packets with non-fragmented outer IP and no IPv4 options or IPv6 extension headers are untunneled. Otherwise, no inner GTP tunnel classification is performed and the traffic is identified and reported as GTP protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mode

Syntax **mode** {**auto** | **napt** | **one-to-one**}
no mode

Context **[Tree]** (config>router>nat>outside>pool mode)

Full Context configure router nat outside pool mode

Description This command specifies the mode of operation of this NAT address pool.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command reverts to the default.

Default auto

Parameters **{auto | napt | one-to-one}** — Specifies the mode of operation of this NAT pool.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mode

Syntax **mode** {**mesh-group** | **standard**}

Context **[Tree]** (config>router>msdp>group mode)

Full Context configure router msdp group mode

Description This command configures groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers.

Multicast Source Discovery Protocol (MSDP) peers can be configured grouped in a full-mesh topology that prevents excessive flooding of source-active messages to neighboring peers.

In a meshed configuration, all members of the group must have a peer connection with every other mesh group member. If this rule is not adhered to, then unpredictable results may occur.

Default mode standard

Parameters **mesh-group** — Specifies that source-active message received from a mesh group member are always accepted but are not flooded to other members of the same mesh group. These source-active messages are only flooded to non-mesh group peers or members of other mesh groups.

standard — Specifies a non-meshed mode.

Platforms All

mode

Syntax **mode** {**strict** | **loose** | **strict-no-ecmp**}

Context **[Tree]** (config>router>if>urpf-check mode)
[Tree] (config>router>if>ipv6>urpf-check mode)

Full Context configure router interface ipv6 urpf-check mode
configure router interface urpf-check mode

Description This command specifies the mode of unicast RPF check.

The **no** form of this command reverts to the default (strict) mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default mode strict

Parameters **strict** — When specified, uRPF checks whether incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

loose — In **loose** mode, uRPF checks whether incoming packet has source address with a corresponding prefix in the routing table. However, the loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. This object is valid only when **urpf-check** is enabled.

strict-no-ecmp — When a packet is received on an interface in this mode and the SA matches an ECMP route the packet is dropped by uRPF.

Platforms All

mode

Syntax **mode** {**ecmp-protected** | **linear**}
no mode

Context **[Tree]** (config>router>segment-routing>maintenance-policy mode)

Full Context configure router segment-routing maintenance-policy mode

Description This command specifies the data path programming and protection mechanism for SR policy candidate paths to which the maintenance policy is applied.

In both the **linear** mode and **ecmp-protected** modes, if two or more candidate paths of the same {headend, color, endpoint} and also have the same mode, then the best preference path is treated as the primary while the next best preference path is the standby. If a third path is present in the linear mode, then this is treated as a tertiary and also programmed in the IOM.

If the currently active path goes unavailable due to S-BFD, the system failovers to the next best preference available candidate path. If S-BFD is down on all segment lists of all programmed candidate paths of an SR Policy, then the SR Policy is marked as down in TTM.

If the default mode is specified, the router only programs the segment lists of the best preference paths in the IOM.

The **no** form of this command removes the configured mode.

Default no mode

Parameters **ecmp-protected** — Specifies only the top two routes (paths) are programmed in the IOM. Up to 32 segment lists can be programmed for each path.

linear — Specifies the top three routes are programmed in the IOM. Only one segment list is allowed per path.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mode

Syntax **mode** {**target-defined** | **on-change** | **sample**}

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription mode)

Full Context configure system telemetry persistent-subscriptions subscription mode

Description This command configures the subscription path mode for telemetry notifications that are sent for the persistent subscription.

Default mode target-defined

Parameters **target-defined** — Keyword specifying that target defined mode is used.

on-change — Keyword specifying that on change mode is used.

sample — Keyword specifying that sample mode is used.

Platforms All

17.312 mode-annexb

mode-annexb

Syntax [**no**] **mode-annexb**

Context **[Tree]** (config>port>aps mode-annexb)

Full Context configure port aps mode-annexb

Description This command configures the APS group for 1+1 Optimized operation as described in Annex B of ITU.T G.841. Note that Annex B operates in non-revertive bi-directional switching mode only as defined in G.841.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

17.313 modify-buffer-allocation-rate

modify-buffer-allocation-rate

Syntax **modify-buffer-allocation-rate**

Context **[Tree]** (config>port modify-buffer-allocation-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port modify-buffer-allocation-rate

Description Commands in this context configure ingress and egress percentage of rate parameters. This command only applies to physical ports (for example, it will not work on APS or similar logical ports). The percentage of rate commands are used to define a percentage value that affects the amount of buffers used by ingress and egress port managed buffer space. Enter the modify-buffer-allocation-rate context when editing the port's percentage of rate commands.

Platforms All

17.314 module

module

Syntax **module** *cpm-slot*

Context **[Tree]** (config>system>bluetooth module)

Full Context configure system bluetooth module

Description Commands in this context define Bluetooth parameters for the specific CPM slot.

Parameters *cpm-slot* — Specifies the CPM slot.

Values {A | B | C | D}

Platforms 7750 SR-1, 7750 SR-s

17.315 mofrr

mofrr

Syntax [**no**] **mofrr**

Context **[Tree]** (debug>router>pim mofrr)

Full Context debug router pim mofrr

Description This command enables debugging for PIM multicast fast failover (MoFRR).

The **no** form of this command disables MoFRR debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.316 mon-hw-agg-shaper-sch

mon-hw-agg-shaper-sch

Syntax [**no**] **mon-hw-agg-shaper-sch**

Context **[Tree]** (config>port>ethernet>access>egress>vport mon-hw-agg-shaper-sch)

Full Context configure port ethernet access egress vport mon-hw-agg-shaper-sch

Description This command enables congestion monitoring of the hardware aggregate shaper scheduler on the specified vport.

The **no** form of this command disables congestion monitoring.

Default no mon-hw-agg-shaper-sch

Platforms 7750 SR-1, 7750 SR-s

17.317 mon-port-sch

mon-port-sch

Syntax [**no**] **mon-port-sch**

Context **[Tree]** (config>port>ethernet mon-port-sch)
[Tree] (config>port>ethernet>access>egress>vport mon-port-sch)
[Tree] (config>port>sonet-sdh>path>access>egress>vport mon-port-sch)

Full Context configure port ethernet access egress vport mon-port-sch
configure port ethernet mon-port-sch
configure port sonet-sdh path access egress vport mon-port-sch

Description This command enables congestion monitoring on an Egress Port Scheduler (EPS) that is applied to a physical port or to a Vport.

Congestion monitoring must be further configured under the port-scheduler CLI hierarchy. Once the congestion monitoring is in effect, the offered rate (incoming traffic) is compared to the configured port-scheduler congestion threshold. The results of these measurements are stored as the number of samples representing the number of times the offered rates exceeded the configured congestion threshold since the last clearing of the stats. Therefore, the results represent the number of times that the port-scheduler that is applied to a port/Vport was congested since the last reset of the stats (via a **clear** command).

The **no** form of this command disables congestion monitoring.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no mon-port-sch

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path access egress vport mon-port-sch

All

- configure port ethernet access egress vport mon-port-sch
- configure port ethernet mon-port-sch

17.318 monitor

monitor

Syntax **monitor** *ip-prefix/length*
no monitor

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>redundancy monitor)

Full Context configure service ies subscriber-interface wlan-gw redundancy monitor

Description This command specifies an IPv4 route (prefix/length) per subscriber-interface to be monitored in the FDB to determine liveness of the subscriber-interface (and consequently all associated group-interfaces of type **wlangw**) on a peer WLAN-GW. This route is the one that is advertised in routing by the peer WLAN-GW when the subscriber-interface and WLAN-GW group are operationally up.

Parameters *ip-prefix/length* — Specifies the IP prefix and length.

Values ip-prefix:a.b.c.d
ip-prefix-length: 0 to 32

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

monitor

Syntax **monitor** *ip-prefix/length*
no monitor

Context **[Tree]** (config>service>vprn>nat>outside>pool>redundancy monitor)
[Tree] (config>router>nat>outside>pool>redundancy monitor)

Full Context configure router nat outside pool redundancy monitor
configure service vprn nat outside pool redundancy monitor

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the monitoring route based on which the NAT multi-chassis switchover is triggered. Monitoring route of a NAT pool on the local node must match the export route of a corresponding NAT pool on the peering node. Presence of the monitoring route in the routing table is an indication that the peering NAT pool is active (since it is advertising its export route). The disappearance of the monitoring route from the routing table is an indication that the peering pool has failed and consequently the nodal switchover is triggered, the local pool becomes active and its export route is consequently advertised. The export route can be advertised only from:

- The active lead pool.
- Active pool for which fate-sharing is disabled.

Default no monitor

Parameters *ip-prefix/length* — Specifies the IP prefix and length.

Syntax:

ip-prefix/length:	ip-prefix	a.b.c.d
	ip-prefix-length	0 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

monitor

Syntax [**no**] **monitor**

Context **[Tree]** (config>router>bgp monitor)
[Tree] (config>router>bgp>group monitor)
[Tree] (config>router>bgp>group>neighbor monitor)
[Tree] (config>service>vprn>bgp>group monitor)
[Tree] (config>service>vprn>bgp>group>neighbor monitor)

Full Context configure router bgp group monitor
configure router bgp group neighbor monitor
configure router bgp monitor
configure service vprn bgp group monitor
configure service vprn bgp group neighbor monitor

Description Commands in this context configure monitor parameters.

The **no** form of this command disables BGP BMP monitoring.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.319 monitor-agg-egress-queue-stats

monitor-agg-egress-queue-stats

Syntax [**no**] **monitor-agg-egress-queue-stats**

Context **[Tree]** (config>port monitor-agg-egress-queue-stats)

Full Context configure port monitor-agg-egress-queue-stats

Description This command enables the monitoring of aggregate egress queue statistics on the port. All queues on the port are monitored, including SAP egress, network egress, subscriber egress, and egress queue group queues, as well as system queues that can be used, for example, to send port-related protocol packets (LACP, EFM, and so on). The aggregate in-profile, out-of-profile, and total statistics are provided for both forwarded and dropped packets and octets.

Monitoring of aggregate statistics is supported on **PXC** sub-ports but not on a **PXC** physical port. It is also not supported on satellite ports.

The **no** form of this command disables aggregate egress queue statistics monitoring on the specified port.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.320 monitor-bandwidth

monitor-bandwidth

Syntax [**no**] **monitor-bandwidth**

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth monitor-bandwidth)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth monitor-bandwidth)

Full Context configure router mpls lsp auto-bandwidth monitor-bandwidth
configure router mpls lsp-template auto-bandwidth monitor-bandwidth

Description This command enables the collection and display of auto-bandwidth measurements, but prevents any automatic bandwidth adjustments from taking place.

The **no** form of this command disables the collection and display of auto-bandwidth measurements.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.321 monitor-oper-group

monitor-oper-group

Syntax **monitor-oper-group** *name* **priority-step** *step*
no monitor-oper-group

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp monitor-oper-group)
[Tree] (config>service>vprn>sub-if>grp-if>srrp monitor-oper-group)

Full Context configure service ies subscriber-interface group-interface srrp monitor-oper-group
configure service vprn subscriber-interface group-interface srrp monitor-oper-group

Description This command will configure the association between the SRRP instance in a Fate Sharing Group and the operational-group that contains messaging SAPs. A state transition of a messaging SAP within an operational-group will trigger calculation of the priority for all SRRP instances that are associated with that operational-group.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies the name of the operational-group, up to 32 characters, that is tracking operational state of SRRP messaging SAPs

priority-step — Specifies the priority step for which the priority of an SRRP instance is changed. If a messaging SAP within an operational-group transition to a non-UP state, the priority is decreased by the step value. If the messaging SAP within the operational-group transition into the UP state, the priority of the SRRP instance is increased by the step value.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

monitor-oper-group

Syntax **monitor-oper-group** *name*
no monitor-oper-group

Context **[Tree]** (config>lag monitor-oper-group)

Full Context configure lag monitor-oper-group

Description This command, supported on access LAG only, specifies the operational group to monitor. The state of the operational group affects the state of this LAG. When the operational group is inactive, the state of the LAG goes down and the LAG uses the configured **lag**>**standby-signaling** mechanism (**lacp** or **power-off**) to signal the CE that the LAG is not available.

Default no monitor-oper-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the name of the **oper-group**, up to 32 characters.

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *name*
no monitor-oper-group

Context **[Tree]** (config>service>vpls>site monitor-oper-group)
[Tree] (config>service>vpls>spoke-sdp monitor-oper-group)
[Tree] (config>service>vpls>sap monitor-oper-group)
[Tree] (config>service>vpls>bgp>pw-template-binding monitor-oper-group)

Full Context configure service vpls bgp pw-template-binding monitor-oper-group
configure service vpls sap monitor-oper-group
configure service vpls site monitor-oper-group
configure service vpls spoke-sdp monitor-oper-group

Description This command specifies the operational group to be monitored by the object under which it is configured. The **oper-group** *name* must be already configured under the **config>service** context before its name is referenced in this command.

The **no** form of this command removes the association.

Default no monitor-oper-group

Parameters *group-name* — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *group-name*
no monitor-oper-group

Context **[Tree]** (config>service>epipe>spoke-sdp monitor-oper-group)
[Tree] (config>service>epipe>sap monitor-oper-group)

Full Context configure service epipe sap monitor-oper-group
configure service epipe spoke-sdp monitor-oper-group

Description This command specifies the operational group to be monitored by the object under which it is configured. The **oper-group** *name* must be already configured under the **config>service** context before its name is referenced in this command.

The **no** form of this command removes the association.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-name* — Specifies an oper group name.

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *group-name*
no monitor-oper-group

Context **[Tree]** (config>service>epipe>pw-port monitor-oper-group)

Full Context configure service epipe pw-port monitor-oper-group

Description This command configures the monitoring operational group name, up to 32 characters in length, associated with this PW-port entry.

Parameters *group-name* — Specifies an operational group to monitor.

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *name*
no monitor-oper-group

Context **[Tree]** (config>service>ies>if monitor-oper-group)

Full Context configure service ies interface monitor-oper-group

Description This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The **no** form of this command removes the association from the configuration.

Default no monitor-oper-group

Parameters *name* — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *name*
no monitor-oper-group

Context **[Tree]** (config>service>vprn>if monitor-oper-group)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface monitor-oper-group

Description This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The **no** form of this command removes the association from the configuration.

Default no monitor-oper-group

Parameters *name* — Specifies a character string, up to 32 ASCII characters, identifying the group instance.

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *group-name* **family** {**ipv4** | **ipv6**} **add** [*1..4294967295*]
monitor-oper-group *group-name* **family** {**ipv4** | **ipv6**} **set** [*1..4294967295*]
monitor-oper-group *group-name* **family** {**ipv4** | **ipv6**} **subtract** [*1..4294967295*]
no monitor-oper-group [**family** {**ipv4** | **ipv6**}]

Context **[Tree]** (config>service>vprn>pim>if monitor-oper-group)

Full Context configure service vprn pim interface monitor-oper-group

Description This command configures PIM to monitor the state of an operational group to provide a redundancy mechanism. PIM monitors the operational group and changes its DR priority to the specified value when the status of the operational group is up. This enables the router to become the PIM DR only when the operational group is up. If the operational group status changes to down, PIM changes its DR priority to the default or the value configured with **priority** under **config**>**service**>**vprn**>**pim**>**if**. The **oper-group** *group-name* must already be configured under the **config**>**service** context before its name is referenced in this command. Two operational groups are supported per PIM interface.

The **no** form of this command removes the operational group from the configuration.

Parameters *group-name* — Specifies the operational group identifier up to 32 characters in length.

family — Specifies the address family.

ipv4 — Specifies the IPv4 designated router priority.

ipv6 — Specifies the IPv6 designated router priority.

add — Specifies that the value is to be added to the existing priority to become the designated router.

subtract — Specifies that the value is to be subtracted from the existing priority to become the designated router.

set — Specifies the priority to become the designated router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

value — Specifies the priority modifier expressed as a decimal integer.

Values 1 to 4294967295

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *name* **health-drop** *drop*
no monitor-oper-group *name*

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy monitor-oper-group)

Full Context configure isa nat-group inter-chassis-redundancy monitor-oper-group

Description This command enables monitoring of the objects, such as SAPs, BFD sessions, or VRRP sessions for the purpose of adjusting the overall health of the node in a redundant inter-chassis NAT system. A state change of the objects in the oper-group influences the health of a NAT node in a redundant configuration.

The **no** form of this command reverts to the default.

Default no monitor-oper-group

Parameters *name* — Specifies the name of the operational group that is being monitored, up to 32 characters.

drop — A state change of an object in the oper-group influences the overall health of the system in the context of NAT inter-chassis redundancy. For example, a transition into a non-operational (down) state of an object within the monitored oper-group triggers a decrease of the overall health of the node for the amount specified by the health-drop value.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

monitor-oper-group

Syntax **monitor-oper-group** *name* **health-drop** *drop*
no monitor-oper-group *name*

Context **[Tree]** (config>service>ies>subscriber-mgmt>up-resiliency monitor-oper-group)
[Tree] (config>service>vprn>subscriber-mgmt>up-resiliency monitor-oper-group)

Full Context configure service ies subscriber-mgmt up-resiliency monitor-oper-group
configure service vprn subscriber-mgmt up-resiliency monitor-oper-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines parameters to derive the service health based on monitored operational groups. The BNG UPF sends the health value to the BNG CPF. The BNG CPF uses the value to determine the need for a BNG UPF status change (active or standby).

The **no** form of the command removes the configuration.

Parameters *name* — Specifies the operational group name, up to 32 characters.

drop — Specifies how the failure of an operational group member affects the health value. The base health value is 255; the value decreases with the defined *drop* per member failure to a minimum of 0.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

monitor-oper-group

Syntax **monitor-oper-group** *name* **health-drop** *drop*
no monitor-oper-group *name*

Context **[Tree]** (config>service>vpls>sap>pfcp>up-resiliency monitor-oper-group)

Full Context configure service vpls sap pfcp up-resiliency monitor-oper-group

Description This command defines parameters to derive the service health based on monitored operational groups. The BNG UPF sends the health value to the BNG CPF. The BNG CPF uses the value to determine the need for a BNG UPF status change (active or standby).

If the configured groups are not the same for all capture SAPs sharing the same underlying port or LAG, the configuration of a Layer 2 access ID alias is required, or else the system chooses arbitrarily one set of configured groups.

The **no** form of the command removes the configuration.

Parameters *name* — Specifies the operational group name, up to 32 characters.

drop — Specifies how the failure of an operational group member affects the health value. The base health value is 255; the value decreases with the defined *drop* per member failure to a minimum of 0.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

monitor-oper-group

Syntax **monitor-oper-group** *group-name* **family** {**ipv4** | **ipv6**} **add** [*value*]
monitor-oper-group *group-name* **family** {**ipv4** | **ipv6**} **set** [*value*]
monitor-oper-group *group-name* **family** {**ipv4** | **ipv6**} **subtract** [*value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no monitor-oper-group [**family** {**ipv4** | **ipv6**}]

Context [Tree] (config>router>pim>if monitor-oper-group)

Full Context configure router pim interface monitor-oper-group

Description This command configures PIM to monitor the state of an operational group to provide a redundancy mechanism. PIM monitors the operational group and changes its DR priority to the specified value when the status of the operational group is up. This enables the router to become the PIM DR only when the operational group is up. If the operational group status changes to down, PIM changes its DR priority to the default or the value configured with **priority** under **config**>**router**>**pim**>**if**. The **oper-group** *group-name* must already be configured under the **config**>**service** context before its name is referenced in this command. Two operational groups are supported per PIM interface.

The **no** form of this command removes the operational group from the configuration.

Parameters *group-name* — Specifies the operational group identifier, up to 32 characters.

family — Specifies the address family.

ipv4 — Specifies the IPv4 designated router priority.

ipv6 — Specifies the IPv6 designated router priority.

add — Specifies that the value is to be added to the existing priority to become the designated router.

subtract — Specifies that the value is to be subtracted from the existing priority to become the designated router.

set — Specifies the priority to become the designated router.

value — Specifies the priority modifier expressed as a decimal integer.

Values 1 to 4294967295

Platforms All

monitor-oper-group

Syntax **monitor-oper-group** *group name*
no monitor-oper-group

Context [Tree] (config>service>sdp>binding>pw-port monitor-oper-group)

Full Context configure service sdp binding pw-port monitor-oper-group

Description This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The **no** form of the command removes the association from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no monitor-oper-group

Parameters *name* — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

Platforms All

17.322 monitor-port

monitor-port

Syntax **monitor-port** *port-id* **health-drop** *drop*
no monitor-port *port-id*

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy monitor-port)

Full Context configure isa nat-group inter-chassis-redundancy monitor-port

Description This command enables monitoring of the ports to adjust the overall health of the node in a redundant inter-chassis NAT system. A state change of a monitored port influences the health of a NAT node in a redundant configuration.

The **no** form of this command reverts to the default.

Default no monitor-port

Parameters *port-id* — Specifies the port being monitored.

Values slot/mda/port

drop — A state change of an object in the oper-group influences the overall health of the system in the context of NAT inter-chassis redundancy. For example, a transition into a non-operational (down) state of an object within the monitored oper-group triggers a decrease of the overall health of the node for the amount specified by the health-drop value.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.323 monitor-ptsf-unusable

monitor-ptsf-unusable

Syntax **monitor-ptsf-unusable**

Context **[Tree]** (config>system>ptp>ptsf monitor-ptsf-unusable)

Full Context configure system ptp ptsf monitor-ptsf-unusable

Description Commands in this context configure the monitoring of neighbor clocks for the Packet Timing Signal Fail (PTSF) unusable state (condition) when the profile is set to g8275dot1-2014.

When enabled, the local clock monitors the noise level of PTP event messages exchanged between external neighbor PTP ports and the local clock. If there is too much noise and the expectation is these event message would not allow the clock to meet its output performance requirements, that neighbor port is considered unusable. This relates to declaring the PTSF-unusable state as defined in the profile.

Once a neighbor port is declared unusable, its Announce messages are excluded from the BMCA and the port cannot be selected as the parent clock.

The unusable condition can be cleared using the following command:

clear system ptp port *port-id* **neighbor** *mac-address* **ptsf-unusable**

When disabled, PTP clears the PTSF-unusable state from all neighbor PTP ports.

Deleting or disabling the local PTP port clears the PTSF-unusable state from all neighbor PTP ports that are accessed through the local PTP port.

Disabling the **monitor-ptsf-unusable** function of the PTP clock clears the PTSF-unusable state from all neighbor PTP ports.

In addition, if no PTP messages have been received from a neighbor for 15 minutes, the neighbor information is purged, which also clears the PTSF-unusable state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.324 monitor-queue-depth

monitor-queue-depth

Syntax **monitor-queue-depth** [**fast-polling**] [**violation-threshold** *percentage*]
no monitor-queue-depth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>port>eth>access>egr>qgrp>qover>q monitor-queue-depth)
[Tree] (config>port>ethernet>network>egr>qgrp>qover>q monitor-queue-depth)
[Tree] (config>port>ethernet>network>egress-port-queue-overrides>queue monitor-queue-depth)
[Tree] (config>service>apipe>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>epipe>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>ies>if>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>vpls>sap>egress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>vprn>if>sap>egress>queue-override>queue monitor-queue-depth)

Full Context
configure port ethernet access egress queue-group queue-overrides queue monitor-queue-depth
configure port ethernet network egress queue-group queue-overrides queue monitor-queue-depth
configure port ethernet network egress-port-queue-overrides queue monitor-queue-depth
configure service apipe sap egress queue-override queue monitor-queue-depth
configure service cpipe sap egress queue-override queue monitor-queue-depth
configure service epipe sap egress queue-override queue monitor-queue-depth
configure service fpipe sap egress queue-override queue monitor-queue-depth
configure service ies interface sap egress queue-override queue monitor-queue-depth
configure service ipipe sap egress queue-override queue monitor-queue-depth
configure service vpls sap egress queue-override queue monitor-queue-depth
configure service vprn interface sap egress queue-override queue monitor-queue-depth

Description
This command configures queue depth monitoring for the specified queue.

The **no** form of this command disables queue depth monitoring for the specified queue.

Parameters
fast-polling — Keyword used to specify that fast queue polling is enabled. Fast queue polling is only supported on FP3- and FP4-based hardware.

percentage — Specifies a percentage, up to two decimal places, of the queue MBS. When the depth of the queue exceeds this percentage, a violation is registered.

Values 00.01 to 99.99

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress queue-override queue monitor-queue-depth
- configure service fpipe sap egress queue-override queue monitor-queue-depth

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue monitor-queue-depth

All

- configure port ethernet network egress-port-queue-overrides queue monitor-queue-depth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port ethernet access egress queue-group queue-overrides queue monitor-queue-depth
- configure port ethernet network egress queue-group queue-overrides queue monitor-queue-depth
- configure service ies interface sap egress queue-override queue monitor-queue-depth
- configure service vpls sap egress queue-override queue monitor-queue-depth
- configure service epipe sap egress queue-override queue monitor-queue-depth
- configure service ipipe sap egress queue-override queue monitor-queue-depth
- configure service vprn interface sap egress queue-override queue monitor-queue-depth

monitor-queue-depth

Syntax **monitor-queue-depth** [**fast-polling**]
no monitor-queue-depth

Context **[Tree]** (config>port>eth>access>ingress>qgrp>qover>q monitor-queue-depth)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue monitor-queue-depth)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue monitor-queue-depth)

Full Context configure port ethernet access ingress queue-group queue-overrides queue monitor-queue-depth
configure service apipe sap ingress queue-override queue monitor-queue-depth
configure service cpipe sap ingress queue-override queue monitor-queue-depth
configure service epipe sap ingress queue-override queue monitor-queue-depth
configure service fpipe sap ingress queue-override queue monitor-queue-depth
configure service ies interface sap ingress queue-override queue monitor-queue-depth
configure service ipipe sap ingress queue-override queue monitor-queue-depth
configure service vpls sap ingress queue-override queue monitor-queue-depth
configure service vprn interface sap ingress queue-override queue monitor-queue-depth

Description This command enters the context for queue depth monitoring for the specified queue. The **fast-polling** option is not supported at ingress.

The **no** form of this command disables queue depth monitoring.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress queue-override queue monitor-queue-depth
- configure service fpipe sap ingress queue-override queue monitor-queue-depth

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe sap ingress queue-override queue monitor-queue-depth

All

- configure service ies interface sap ingress queue-override queue monitor-queue-depth
- configure service vprn interface sap ingress queue-override queue monitor-queue-depth
- configure service ipipe sap ingress queue-override queue monitor-queue-depth
- configure port ethernet access ingress queue-group queue-overrides queue monitor-queue-depth
- configure service epipe sap ingress queue-override queue monitor-queue-depth
- configure service vpls sap ingress queue-override queue monitor-queue-depth

17.325 monitor-threshold

monitor-threshold

Syntax **monitor-threshold** *percent*
no monitor-threshold

Context **[Tree]** (config>qos>port-scheduler-policy monitor-threshold)
[Tree] (config>qos>port-scheduler-policy>group monitor-threshold)

Full Context configure qos port-scheduler-policy group monitor-threshold
configure qos port-scheduler-policy monitor-threshold

Description This command defines the congestion monitoring threshold for the desired monitoring entity under the port-scheduler for per aggregate port-scheduler rate, per individual level, and per group that is aggregating multiple levels.

The congestion threshold is specified in percentages of the configured PIR rate for the entity for which congestion monitoring is desired. For example, if the configured PIR rate for level 1 is 100,000 kb/s, and the monitoring threshold is set to 90%, then an event where the offered rate is >90,000 kb/s will be recorded. This event is shown as part of the cumulative count of congestion threshold exceeds since the last clearing of the counters.

The **no** form of this command removes the congestion monitoring threshold.

Default no monitor-threshold

Parameters *percent* — Specifies the percent of the configured rate. If the offered rate exceeds the configured threshold, a counter monitoring the threshold will be increased.

Values 0 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

monitor-threshold

Syntax **monitor-threshold** *percent*
no monitor-threshold

Context **[Tree]** (config>qos>hw-agg-shap-sched-plcy monitor-threshold)

Full Context configure qos hw-agg-shaper-scheduler-policy monitor-threshold

Description This command configures the egress scheduler monitor threshold for the hardware aggregate shaper scheduler policy. The value is expressed as a percentage of the scheduler rate, which is considered as a limit for determining congestion.

The **no** form of this command removes the congestion monitoring threshold.

Default no monitor-threshold

Parameters *percent* — Specifies the percent of the configured rate.

Values 0 to 100

Platforms 7750 SR-1, 7750 SR-s

17.326 month

month

Syntax **month** {*month-number* [*..month-number*] | *month-name* [*..month-name*] | **all**}
no month

Context **[Tree]** (config>system>cron>sched month)

Full Context configure system cron schedule month

Description This command specifies the month when the event should be executed. Multiple months can be specified. When multiple months are configured, each of them will cause the schedule to trigger. If a month is configured without configuring the month, weekday, day-of-month, and minute, the event will not execute.

The **no** form of this command removes the specified month from the configuration.

Default no month

Parameters **month-number** — Specifies a month number.

Values 1 to 12 (maximum 12 month-numbers)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

month-name — Specifies a month by name.

Values january, february, march, april, may, june, july, august, september, october, november, december (maximum 12 month names)

all — Specifies all months.

Platforms All

17.327 more

more

Syntax [**no**] **more**

Context **[Tree]** (environment more)

Full Context environment more

Description This command enables per-screen CLI output, meaning that the output is displayed on a screen-by- screen basis. The terminal screen length can be modified with the **terminal** command.

The following prompt appears at the end of each screen of paginated output:

```
Press any key to continue (Q to quit)
```

The **no** form of the command displays the output all at once. If the output length is longer than one screen, the entire output will be displayed, which may scroll the screen.

Default more

Platforms All

more

Syntax [**no**] **more**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment more)

Full Context configure system management-interface cli md-cli environment more

Description This command configures pagination of the output text.

The **no** form of this command reverts to the default value.

Default more

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.328 more-fragments

more-fragments

Syntax **more-fragments** *more-fragments*
no more-fragments

Context **[Tree]** (config>test-oam>build-packet>header>ipv4 more-fragments)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv4 more-fragments)

Full Context configure test-oam build-packet header ipv4 more-fragments
debug oam build-packet packet field-override header ipv4 more-fragments

Description This command defines if the MF flag should be set in the associated IPv4 header.

The **no** form of this command reverts to the default value.

Default more-fragments 0

Parameters *more-fragments* — Specifies an MF flag for an IPv4 packet header to be launched by the OAM **find-egress** tool. A value of 1 means there are more fragments to be sent.

Values 0, 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.329 motd

motd

Syntax **motd** {**url** *url-prefix*: *source-url* | **text** *motd-text-string*}
no motd

Context **[Tree]** (config>system>login-control motd)

Full Context configure system login-control motd

Description This command creates the message of the day displayed after a successful console login. Only one message can be configured.

The **no** form of this command removes the message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no motd

Parameters **url** *url-prefix*: *source-url* — When the message of the day is present as a text file, provide both url-prefix and the source-url of the file containing the message of the day. The URL prefix can be local or remote.

text *motd-text-string* — Specifies the text of the message of the day. The *motd-text-string* must be enclosed in double quotes. Multiple text strings are not appended to one another.

Some special characters can be used to format the message text. The \n character can be used to create multi-line messages. A \n in the message moves to the beginning of the next line by sending ASCII/UTF-8 chars 0xA (LF) and 0xD (CR) to the client terminal. An \r in the message sends the ASCII/UTF-8 char 0xD (CR) to the client terminal.

Platforms All

17.330 move

move

Syntax **move** *old-file-url new-file-url* [**force**] [**no-redirect**] [**client-tls-profile** *profile*] [**proxy** *proxy-url*]

Context **[Tree]** (file move)

Full Context file move

Description This command moves a local file, system file, or a directory. If the target already exists, the command fails and an error message displays.

The following prompt appears if the destination file already exists:

“Overwrite destination file (y/n)?”

Parameters *old-file-url* — Specifies the file or directory to be moved.

Values

local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp:// | http:// | https://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
	x:x:x:x:x:x:d.d.d.d[-*interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

new-file-url — Specifies the new destination to place the old-file-url.

Values

local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*]
	up to 247 characters
	directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
	x:x:x:x:x:x:d.d.d.d[-*interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

force — Forces an immediate move of the specified file(s).

The **file move force** command moves the specified file(s) without displaying a user prompt message. This command also automatically accepts HTTP redirects unless overridden by the **no-redirect** parameter.

profile — Specifies the TLS client profile configured under **config**>**system**>**security**>**tls**>**client-tls-profile** to use.

proxy-url — Specifies the URL of an HTTP proxy. For example, http://proxy.mydomain.com:8000. This URL must be an HTTP URL and not an HTTPS URL.

no-redirect — Specifies to automatically refuse any HTTP redirects without prompting the user.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.331 move-frequency

move-frequency

Syntax **move-frequency** *frequency*
no move-frequency

Context **[Tree]** (config>service>vpls>mac-move move-frequency)
[Tree] (config>service>template>vpls-template>mac-move move-frequency)

Full Context configure service template vpls-template mac-move move-frequency
configure service vpls mac-move move-frequency

Description This command indicates the maximum rate at which MACs can be re-learned in the VPLS service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MACs.

The **no** form of this command reverts to the default value.

Default move-frequency 2 (when mac-move is enabled). For example, 10 relearns in a 5 second period.

Parameters *frequency* — Specifies the rate, in 5-second intervals for the maximum number of relearns

Values 1 to 10

Platforms All

17.332 mp-bgp-keep

mp-bgp-keep

Syntax [**no**] **mp-bgp-keep**

Context **[Tree]** (config>router>bgp mp-bgp-keep)

Full Context configure router bgp mp-bgp-keep

Description As a result of enabling this command, route refresh messages are no longer needed, or issued when VPN route policy changes are made; RIB-IN will retain all MP-BGP routes.

The **no** form of this command is used to disable this feature.

Default no mp-bgp-keep

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.333 mp-mbb-time

mp-mbb-time

Syntax **mp-mbb-time** *interval*
no interval

Context **[Tree]** (config>router>ldp mp-mbb-time)

Full Context configure router ldp mp-mbb-time

Description This command configures the maximum time a P2MP transit/bud node must wait before switching over to the new path if the new node does not send MBB TLV to inform of the availability of data plane.

The **no** form of this command reverts to the default value.

Default no mp-mbb-time (which equals a value of 3 seconds)

Parameters *interval* — Specifies the MP MBB time, in seconds.

Values 1 to 10

Platforms All

17.334 mpls

mpls

Syntax **mpls** [**bgp** *bgp*] [**endpoint** *endpoint-name*]
no mpls [**bgp** *bgp*]

Context **[Tree]** (config>service>epipe>bgp-evpn mpls)
[Tree] (config>service>vpls>bgp-evpn mpls)
[Tree] (config>service>vprn>bgp-evpn mpls)

Full Context configure service epipe bgp-evpn mpls
configure service vpls bgp-evpn mpls
configure service vprn bgp-evpn mpls

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the BGP EVPN MPLS parameters. In VPLS, either instance BGP 1 or BGP 2 can be configured, but not both simultaneously in the same service. Epipe and VPRN services only support instance 1. If the **bgp** *bgp* parameter is not specified, the instance is set to 1.

The **endpoint** option is only supported for Epipe services. When configured, the same endpoint name can be configured for the **bgp-evpn>mpls** context and an additional spoke SDP. An EVPN MPLS destination always has higher preference than a spoke SDP.

The **no** form of this command removes the MPLS instance from the service.

Parameters *bgp* — Indicates the BGP instance identifier.

Values 1, 2

endpoint-name — Specifies the endpoint name for Epipe services, up to 32 characters.

Platforms All

mpls

Syntax **mpls**

Context **[Tree]** (config>service>vprn>bgp-ipvpn mpls)

Full Context configure service vprn bgp-ipvpn mpls

Description Commands in this context configure the BGP IPVPN parameters.

Platforms All

mpls

Syntax [**no**] **mpls**

Context **[Tree]** (config>router mpls)

Full Context configure router mpls

Description Commands in this context configure MPLS parameters. MPLS is not enabled by default and must be explicitly enabled (**no shutdown**).

The **no** form of this command deletes this MPLS protocol instance and removes all configuration parameters for this MPLS instance.

You must remove all SDP bindings and use the **shutdown** command to administratively disable the MPLS instance before deleting it.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mpls

Syntax **mpls**

Context **[Tree]** (config>router>rib-api mpls)

Full Context configure router rib-api mpls

Description Commands in this context configure MPLS parameters related to the RIB-API gRPC service.

Platforms All

mpls

Syntax **mpls** [**lsp** *lsp-name*] [**sender** *source-address*] [**endpoint** *endpoint-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*]
no mpls

Context **[Tree]** (debug>router mpls)

Full Context debug router mpls

Description This command enables and configures debugging for MPLS.

Parameters **lsp** *lsp-name* — Specifies the LSP name up to 64 characters in length.

sender *source-address* — Specifies the IP address of the sender.

endpoint *endpoint-address* — Specifies the far-end IP address.

tunnel-id *tunnel-id* — Specifies the MPLS SDP ID.

Values 0 to 4294967295

lsp-id *lsp-id* — Specifies the LSP ID.

Values 1 to 65535

Platforms All

mpls

Syntax **mpls**

Context **[Tree]** (config>test-oam>build-packet>header mpls)
[Tree] (debug>oam>build-packet>packet>field-override>header mpls)

Full Context configure test-oam build-packet header mpls
debug oam build-packet packet field-override header mpls

Description This command causes the associated header to be defined as an MPLS label header template and enables the context to define the MPLS parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mpls

Syntax **mpls**

Context **[Tree]** (config>oam-pm>session mpls)

Full Context configure oam-pm session mpls

Description Commands in this context configure MPLS-specific source and destination, LSP type and tunnel information, the priority, and the MPLS DM test configuration on the launch point.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

mpls

Syntax [**no**] **mpls**

Context **[Tree]** (config>cflowd>collector>export-filter>family mpls)

Full Context configure cflowd collector export-filter family mpls

Description This command filters MPLS flow data from being sent to the associated collector.

The **no** form of this command removes the filter, allowing MPLS flow data to be sent to the associated collector.

Default no mpls

Platforms All

mpls

Syntax **mpls**

Context **[Tree]** (config>system>ip mpls)

Full Context configure system ip mpls

Description Commands in this context configure system-wide MPLS parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.335 mpls-dm

mpls-dm

Syntax **mpls-dm**

Context **[Tree]** (config>test-oam mpls-dm)

Full Context configure test-oam mpls-dm

Description Commands in this context configure global MPLS delay measurement parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.336 mpls-echo-request-downstream-map

mpls-echo-request-downstream-map

Syntax **mpls-echo-request-downstream-map** {**dsmap** | **ddmap**}

Context **[Tree]** (config>test-oam mpls-echo-request-downstream-map)

Full Context configure test-oam mpls-echo-request-downstream-map

Description This command specifies which format of the downstream mapping TLV to use in all LSP trace packets and LDP tree trace packets originated on this node. The Downstream Mapping (DSMAP) TLV is the original format in RFC 4379 (obsoleted by RFC 8029) and is the default value. The new Downstream Detailed Mapping (DDMAP) TLV is the new enhanced format specified in RFC 6424 and RFC 8029.

This command applies to LSP trace of an RSVP P2P LSP, a MPLS-TP LSP, or LDP unicast FEC, and to LDP tree trace of a unicast LDP FEC. It does not apply to LSP trace of an RSVP P2MP LSP which always uses the DDMAP TLV.

The global DSMAP/DDMAP setting impacts the behavior of both OAM LSP trace packets and SAA test packets of type **lsp-trace** and is used by the sender node when one of the following events occurs:

1. An SAA test of type **lsp-trace** is created (not modified) and no value is specified for the per-test **downstream-map-tlv** {**dsmap** | **ddmap** | **none**} option. In this case, the SAA test **downstream-map-tlv** value defaults to the global **mpls-echo-request-downstream-map** value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

2. An OAM test of type **lsp-trace** test is executed and no value is specified for the per-test **downstream-map-tlv** {**dsmap** | **ddmap** | **none**} option. In this case, the OAM test **downstream-map-tlv** value defaults to the global **mpls-echo-request-downstream-map** value.

A consequence of the rules above is that a change to the value of **mpls-echo-request-downstream-map** option does not affect the value inserted in the downstream mapping TLV of existing tests.

Following are the details of the processing of the new DDMAP TLV:

1. When either the DSMAP TLV or the DDMAP TLV is received in an echo request message, the responder node includes the same type of TLV in the echo reply message with the proper downstream interface information and label stack information.
2. If an echo request message without a Downstream Mapping TLV (DSMAP or DDMAP) expires at a node which is not the egress for the target FEC stack, the responder node always includes the DSMAP TLV in the echo reply message. This can occur in the following cases:
   a. The user issues a LSP trace from a sender node with a **min-ttl** value higher than 1 and a **max-ttl** value lower than the number of hops to reach the egress of the target FEC stack. This is the sender node behavior when the global configuration or the per-test setting of the DSMAP/DDMAP is set to DSMAP.
   b. The user issues a LSP ping from a sender node with a **ttl** value lower than the number of hops to reach the egress of the target FEC stack. This is the sender node behavior when the global configuration of the DSMAP/DDMAP is set to DSMAP.
   c. The behavior in (a) is changed when the global configuration or the per-test setting of the Downstream Mapping TLV is set to DDMAP. The sender node includes in this case the DDMAP TLV with the Downstream IP address field set to the all-routers multicast address as per Section 3.4 of RFC 8029. The responder node then bypasses the interface and label stack validation and replies with a DDMAP TLV with the correct downstream information for the target FEC stack.
3. A sender node never includes the DSMAP or DDMAP TLV in an lsp-ping message.

In addition to performing the same features as the DSMAP TLV, the new DDMAP TLV addresses the following scenarios:

1. Full validation of an LDP FEC stitched to a BGP IPv4 label route. In this case, the LSP trace message is inserted from the LDP LSP segment or from the stitching point.
2. Full validation of a BGP IPv4 label route stitched to an LDP FEC. This includes the case of explicit configuration of the LDP-BGP stitching in which the BGP label route is active in Route Table Manager (RTM) and the case of a BGP IPv4 label route resolved to the LDP FEC due to the IGP route of the same prefix active in RTM. In this case, the LSP trace message is inserted from the BGP LSP segment or from the stitching point.
3. Full validation of an LDP FEC which is stitched to a BGP LSP and stitched back into an LDP FEC. In this case, the LSP trace message is inserted from the LDP segments or the or from the stitching points.
4. Full validation of an LDP FEC tunneled over an RSVP LSP using LSP trace.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To properly check a target FEC which is stitched to another FEC (stitching FEC) of the same or a different type, or which is tunneled over another FEC (tunneling FEC), it is necessary for the responding nodes to provide details about the FEC manipulation back to the sender node. This is achieved via the use of the new FEC stack change sub-TLV in the Downstream Detailed Mapping TLV (DDMAP) defined in RFC 6424.

When the user configures the use of the DDMAP TLV on a trace for an LSP that does not undergo stitching or tunneling operation in the network, the procedures at the sender and responder nodes are the same as in the case of the DSMAP TLV.

This feature however introduces changes to the target FEC stack validation procedures at the sender and responder nodes in the case of LSP stitching and LSP hierarchy. These changes pertain to the processing of the new FEC stack change sub-TLV in the new DDMAP TLV and the new return code of value `15 Label switched with FEC change`.

The **no** form of this command reverts to the default behavior of using the DSMAP TLV in a LSP trace packet and LDP tree trace packet.

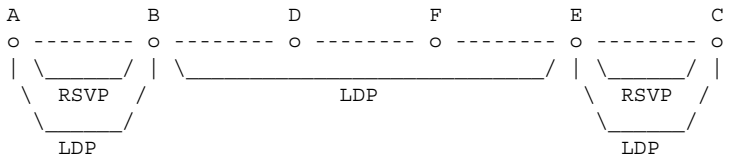
Default mpls-echo-request-downstream-map dsmap

Parameters **dsmap** — Specifies that the DSMAP TLV should be used in all LSP trace packets and LDP tree trace packets originating on the node.

ddmap — Specifies that the DDMAP TLV should be used in all LSP trace packets and LDP tree trace packets originating on the node.

Output The following output is an example of mpls-echo-request-downstream-map information.

Sample Output for LDP-over-RSVP

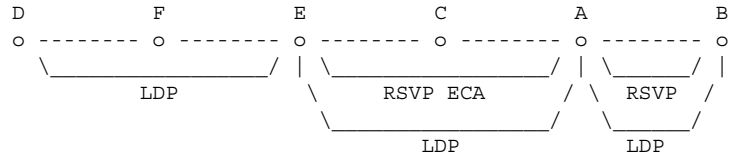



```
Testing LDP FEC of Node C with DSMAP TLV
----------------------------------------
*A:Dut-A#
*A:Dut-A# oam lsp-trace prefix 10.20.1.3/32 downstream-map-tlv dsmap detail
lsp-trace to 10.20.1.3/32: 0 hops min, 0 hops max, 104 byte packets
1  10.20.1.2  rtt=3.90ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.4.4 ifaddr=10.10.4.4 iftype=ipv4Numbered MRU=1500
           label[1]=131068 protocol=3(LDP)
2  10.20.1.4  rtt=5.69ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.9.6 ifaddr=10.10.9.6 iftype=ipv4Numbered MRU=1500
           label[1]=131066 protocol=3(LDP)
3  10.20.1.6  rtt=7.88ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.10.5 ifaddr=10.10.10.5 iftype=ipv4Numbered MRU=1500
           label[1]=131060 protocol=3(LDP)
4  10.20.1.5  rtt=23.2ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.5.3 ifaddr=10.10.5.3 iftype=ipv4Numbered MRU=1496
           label[1]=131071 protocol=3(LDP)
5  10.20.1.3  rtt=12.0ms rc=3(EgressRtr) rsc=1
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
*A:Dut-A#


Testing LDP FEC of Node C with DDMAP TLV
----------------------------------------
*A:Dut-A# oam lsp-trace prefix 10.20.1.3/32 downstream-map-tlv ddmap detail
lsp-trace to 10.20.1.3/32: 0 hops min, 0 hops max, 136 byte packets
1  10.20.1.2  rtt=4.00ms rc=3(EgressRtr) rsc=2
1  10.20.1.2  rtt=3.48ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.4.4 ifaddr=10.10.4.4 iftype=ipv4Numbered MRU=1500
           label[1]=131068 protocol=3(LDP)
2  10.20.1.4  rtt=5.34ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.9.6 ifaddr=10.10.9.6 iftype=ipv4Numbered MRU=1500
           label[1]=131066 protocol=3(LDP)
3  10.20.1.6  rtt=7.78ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.10.5 ifaddr=10.10.10.5 iftype=ipv4Numbered MRU=1500
           label[1]=131060 protocol=3(LDP)
4  10.20.1.5  rtt=12.8ms rc=15(LabelSwitchedWithFecChange) rsc=1
     DS 1: ipaddr=10.10.5.3 ifaddr=10.10.5.3 iftype=ipv4Numbered MRU=1496
           label[1]=131054 protocol=4(RSVP-TE)
           label[2]=131071 protocol=3(LDP)
           fecchange[1]=PUSH fectype=RSVP IPv4 prefix=10.20.1.3 remotepeer=10.10.5.3
5  10.20.1.3  rtt=12.8ms rc=3(EgressRtr) rsc=2
5  10.20.1.3  rtt=13.4ms rc=3(EgressRtr) rsc=1
*A:Dut-A#
```

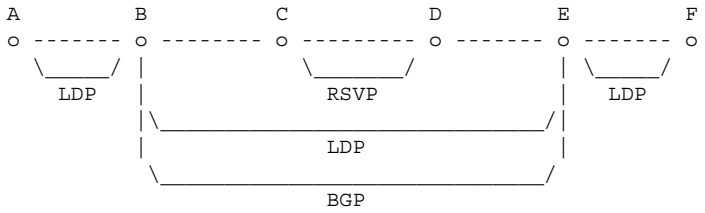



```
Testing LDP FEC of Node B with DDMAP TLV
----------------------------------------
*A:Dut-D#
*A:Dut-D# oam lsp-trace prefix 10.20.1.2/32 downstream-map-tlv ddmap detail
lsp-trace to 10.20.1.2/32: 0 hops min, 0 hops max, 108 byte packets
1  10.20.1.6  rtt=3.17ms rc=8(DSRtrMatchLabel) rsc=1
     DS 1: ipaddr=10.10.10.5 ifaddr=10.10.10.5 iftype=ipv4Numbered MRU=1500
           label[1]=131065 protocol=3(LDP)
2  10.20.1.5  rtt=8.27ms rc=15(LabelSwitchedWithFecChange) rsc=1
     DS 1: ipaddr=10.10.5.3 ifaddr=10.10.5.3 iftype=ipv4Numbered MRU=1496
           label[1]=131068 protocol=4(RSVP-TE)
           label[2]=131065 protocol=3(LDP)
           fecchange[1]=PUSH fectype=RSVP IPv4 prefix=10.20.1.1 remotepeer=10.10.5.3
3  10.20.1.3  rtt=9.50ms rc=8(DSRtrMatchLabel) rsc=2
     DS 1: ipaddr=10.10.2.1 ifaddr=10.10.2.1 iftype=ipv4Numbered MRU=1500
           label[1]=131068 protocol=4(RSVP-TE)
4  10.20.1.1  rtt=10.4ms rc=3(EgressRtr) rsc=2
4  10.20.1.1  rtt=10.2ms rc=15(LabelSwitchedWithFecChange) rsc=1
     DS 1: ipaddr=10.10.1.2 ifaddr=10.10.1.2 iftype=ipv4Numbered MRU=1496
           label[1]=131066 protocol=4(RSVP-TE)
           label[2]=131071 protocol=3(LDP)
           fecchange[1]=PUSH fectype=RSVP IPv4 prefix=10.20.1.2 remotepeer=10.10.1.2
5  10.20.1.2  rtt=13.7ms rc=3(EgressRtr) rsc=2
5  10.20.1.2  rtt=13.6ms rc=3(EgressRtr) rsc=1
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

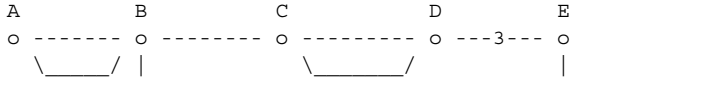
```
*A:Dut-D#
```

Sample Output for LDP-BGP Stitching




```
Testing LDP FEC of Node F with DSMAP TLV
----------------------------------------
*A:Dut-A# *A:Dut-A# oam lsp-trace prefix 10.20.1.6/32 downstream-map-
tlv dsmap detail lsp-trace to 10.20.1.6/32: 0 hops min, 0 hops max, 104 byte packets
1  10.20.1.2  rtt=2.65ms rc=8(DSRtrMatchLabel) rsc=1
2  10.20.1.3  rtt=4.89ms rc=8(DSRtrMatchLabel) rsc=1
3  10.20.1.4  rtt=6.49ms rc=5(DSMappingMismatched) rsc=1
*A:Dut-A#

Testing LDP FEC of Node F with DDMAP TLV
----------------------------------------
*A:Dut-A# oam lsp-trace prefix 10.20.1.6/32 downstream-map-tlv ddmap detail lsp-
trace to 10.20.1.6/32: 0 hops min, 0 hops max, 108 byte packets
1  10.20.1.2  rtt=3.50ms rc=15(LabelSwitchedWithFecChange) rsc=1
      DS 1: ipaddr=10.10.3.3 ifaddr=10.10.3.3 iftype=ipv4Numbered MRU=1496
            label[1]=131068 protocol=3(LDP)
            label[2]=131060 protocol=2(BGP)
            fecchange[1]=POP  fectype=LDP IPv4 prefix=10.20.1.6 remotepeer=0.0.0.0
(Unknown)
            fecchange[2]=PUSH fectype=BGP IPv4 prefix=10.20.1.6 remotepeer=10.20.1.5
            fecchange[3]=PUSH fectype=LDP IPv4 prefix=10.20.1.5 remotepeer=10.10.3.3
2  10.20.1.3  rtt=6.53ms rc=15(LabelSwitchedWithFecChange) rsc=2
      DS 1: ipaddr=10.10.11.4 ifaddr=10.10.11.4 iftype=ipv4Numbered MRU=1496
          label[1]=131060 protocol=4(RSVP-TE)
          label[2]=131070 protocol=3(LDP)
          label[3]=131060 protocol=2(BGP)
          fecchange[1]=PUSH fectype=RSVP IPv4 prefix=10.20.1.4 remotepeer=10.10.11.4
3  10.20.1.4  rtt=7.94ms rc=3(EgressRtr) rsc=3
3  10.20.1.4  rtt=6.69ms rc=8(DSRtrMatchLabel) rsc=2
      DS 1: ipaddr=10.10.6.5 ifaddr=10.10.6.5 iftype=ipv4Numbered MRU=1500
            label[1]=131071 protocol=3(LDP)
            label[2]=131060 protocol=2(BGP)
4  10.20.1.5  rtt=10.1ms rc=3(EgressRtr) rsc=2
4  10.20.1.5  rtt=8.97ms rc=15(LabelSwitchedWithFecChange) rsc=1
      DS 1: ipaddr=10.10.10.6 ifaddr=10.10.10.6 iftype=ipv4Numbered MRU=1500
           label[1]=131071 protocol=3(LDP)
           fecchange[1]=POP  fectype=BGP IPv4 prefix=10.20.1.6 remotepeer=0.0.0.0
(Unknown)
           fecchange[2]=PUSH fectype=LDP IPv4 prefix=10.20.1.6 remotepeer=10.10.10.6
5  10.20.1.6  rtt=11.8ms rc=3(EgressRtr) rsc=1 *A:Dut-A#
```



© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
    LDP   |              RSVP              |
          |\_______________________________/|
          |              LDP               |
           \_______________________________/
                         BGP
Testing BGP Label Route of Node E with DDMAP TLV
------------------------------------------------
*A:Dut-B# oam lsp-trace prefix 11.20.1.5/32 bgp-label downstream-map-
tlv ddmap detail lsp-trace to 11.20.1.5/32: 0 hops min, 0 hops max, 124 byte packets
1  10.20.1.3  rtt=2.35ms rc=15(LabelSwitchedWithFecChange) rsc=2
      DS 1: ipaddr=10.10.11.4 ifaddr=10.10.11.4 iftype=ipv4Numbered MRU=1496
          label[1]=131060 protocol=4(RSVP-TE)
          label[2]=131070 protocol=3(LDP)
          label[3]=131070 protocol=2(BGP)
          fecchange[1]=PUSH fectype=RSVP IPv4 prefix=10.20.1.4 remotepeer=10.10.11.4
2  10.20.1.4  rtt=4.17ms rc=3(EgressRtr) rsc=3
2  10.20.1.4  rtt=4.50ms rc=8(DSRtrMatchLabel) rsc=2
      DS 1: ipaddr=10.10.6.5 ifaddr=10.10.6.5 iftype=ipv4Numbered MRU=1500
            label[1]=131071 protocol=3(LDP)
            label[2]=131070 protocol=2(BGP)
3  10.20.1.5  rtt=7.78ms rc=3(EgressRtr) rsc=2
3  10.20.1.5  rtt=6.80ms rc=3(EgressRtr) rsc=1 *A:Dut-B#

B          C           D         E         F
o -------- o --------- o ---3--- o ---3--- o
|            \_______/           | \_____/
|              RSVP              |
|\_______________________________/|
|              LDP               |
 \_______________________________/
              BGP

Testing with DDMAP TLV LDP FEC of Node F when stitched to a BGP Label Route
---------------------------------------------------------------------------

*A:Dut-B# oam lsp-trace prefix 10.20.1.6/32 bgp-label downstream-map-
tlv ddmap detail lsp-trace to 10.20.1.6/32: 0 hops min, 0 hops max, 124 byte packets
1  10.20.1.3  rtt=3.21ms rc=15(LabelSwitchedWithFecChange) rsc=2
      DS 1: ipaddr=10.10.11.4 ifaddr=10.10.11.4 iftype=ipv4Numbered MRU=1496
          label[1]=131060 protocol=4(RSVP-TE)
          label[2]=131070 protocol=3(LDP)
          label[3]=131060 protocol=2(BGP)
          fecchange[1]=PUSH fectype=RSVP IPv4 prefix=10.20.1.4 remotepeer=10.10.11.4
2  10.20.1.4  rtt=5.50ms rc=3(EgressRtr) rsc=3
2  10.20.1.4  rtt=5.37ms rc=8(DSRtrMatchLabel) rsc=2
      DS 1: ipaddr=10.10.6.5 ifaddr=10.10.6.5 iftype=ipv4Numbered MRU=1500
          label[1]=131071 protocol=3(LDP)
          label[2]=131060 protocol=2(BGP)
3  10.20.1.5  rtt=7.82ms rc=3(EgressRtr) rsc=2
3  10.20.1.5  rtt=6.11ms rc=15(LabelSwitchedWithFecChange) rsc=1
      DS 1: ipaddr=10.10.10.6 ifaddr=10.10.10.6 iftype=ipv4Numbered MRU=1500
          label[1]=131071 protocol=3(LDP)
          fecchange[1]=POP  fectype=BGP IPv4 prefix=10.20.1.6 remotepeer=0.0.0.0
(Unknown)
          fecchange[2]=PUSH fectype=LDP IPv4 prefix=10.20.1.6 remotepeer=10.10.10.6
4  10.20.1.6  rtt=10.2ms rc=3(EgressRtr) rsc=1 *A:Dut-B#
```

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.337 mpls-fwd-policy

mpls-fwd-policy

Syntax [**no**] **mpls-fwd-policy**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter mpls-fwd-policy)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter mpls-fwd-policy)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter mpls-fwd-policy)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter mpls-fwd-policy)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter mpls-fwd-policy
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter mpls-fwd-policy
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter mpls-fwd-policy
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter mpls-fwd-policy

Description This command selects the MPLS forwarding policy type.

The **mpls-fwd-policy** value instructs BGP to use the MPLS forwarding policy to determine the address of the BGP next hop.

The **no** form of this command removes the selected the MPLS forwarding policy type.

Default no mpls-fwd-policy

Platforms All

mpls-fwd-policy

Syntax [**no**] **mpls-fwd-policy**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter mpls-fwd-policy)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter mpls-fwd-policy

Description This command enables the use of the MPLS forwarding policy to resolve the indirect next hops of statically-configured routes.

Default no mpls-fwd-policy

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mpls-fwd-policy

Syntax [**no**] **mpls-fwd-policy**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter mpls-fwd-policy)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter mpls-fwd-policy)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter mpls-fwd-policy
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter mpls-fwd-policy

Description This command selects MPLS forwarding policy to be used for next-hop resolution.

Platforms All

17.338 mpls-label

mpls-label

Syntax **mpls-label** *value*
no mpls-label

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy>segment-list>segment mpls-label)

Full Context configure router segment-routing sr-policies static-policy segment-list segment mpls-label

Description This command configures the MPLS label value this is associated with a segment.

The **no** form of this command removes the label value.

Default no mpls-label

Parameters *value* — Specifies the MPLS label value.

Values 0 to 1048575

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.339 mpls-labels

mpls-labels

Syntax **mpls-labels**

Context **[Tree]** (config>router mpls-labels)

Full Context configure router mpls-labels

Description This command creates a context for the configuration of global parameters related to MPLS labels.

Platforms All

17.340 mpls-time-stamp-format

mpls-time-stamp-format

Syntax **mpls-time-stamp-format** {**rfc4379** | **unix**}

Context **[Tree]** (config>test-oam mpls-time-stamp-format)

Full Context configure test-oam mpls-time-stamp-format

Description This command configures the format of the timestamp used by for lsp-ping, lsp-trace, p2mp-lsp-ping and p2mp-lsp-trace, vccv-ping, vccv-trace, and lsp-trace.

If **rfc4379** is selected, then the timestamp is in seconds and microseconds since 1900, otherwise it is in seconds and microseconds since 1970.

Changing this system-wide setting does not affect tests that are currently in progress, but SAAs starts to use the new timestamp when they are restarted. When an SR OS receives an echo request, it replies with the locally configured timestamp format, and does not try to match the timestamp format of the incoming echo request message.

Default mpls-time-stamp-format unix

Parameters **rfc4379** — Specifies the RFC 4379 (obsoleted by RFC 8029) time stamp format. The timestamp's **seconds** field holds the integral number of seconds since 1-Jan-1900 00:00:00 UTC. The timestamp's **microseconds** field contains a microseconds value in the range 0 to 999999. This setting is used to inter-operate with network elements which are fully compliant with RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*, (such as an SR OS system with the same setting, or any other RFC 4379 compliant router).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

unix — Specifies the Unix time stamp format. The time stamps **seconds** field holds a Unix time, the integral number of seconds since 1-Jan-1970 00:00:00 UTC. The time stamps **microseconds** field contains a microseconds value in the range 0 to 999999. This setting is used to inter-operate with network elements which send and expect a 1970-based timestamp in MPLS Echo Request/Reply PDUs (such as an SR OS system with the same setting, or an SR OS system running software earlier than R8.0 R4).

Platforms All

17.341 mpls-tp

mpls-tp

Syntax [**no**] **mpls-tp**

Context **[Tree]** (config>router>mpls mpls-tp)

Full Context configure router mpls mpls-tp

Description Generic MPLS-TP parameters and MPLS-TP transit paths are configured under this context. If a user configures **no mpls**, normally the entire mpls configuration is deleted. However, in the case of mpls-tp, a check is made that there is no other mpls-tp configuration (e.g., services or LSPs using mpls-tp on the node). The mpls-tp context cannot be deleted if MPLS-TP LSPs or SDPs exist on the system.

A **shutdown** of mpls-tp will bring down all MPLS-TP LSPs on the system.

Default no mpls-tp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.342 mpls-tp-mep

mpls-tp-mep

Syntax [**no**] **mpls-tp-mep**

Context **[Tree]** (config>router>mpls>interface mpls-tp-mep)

Full Context configure router mpls interface mpls-tp-mep

Description Commands in this context configure a section layer MEP for MPLS-TP on an MPLS interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.343 mpls-tp-static

mpls-tp-static

Syntax **mpls-tp-static**

Context **[Tree]** (config>oam-pm>session>mpls>lsp mpls-tp-static)

Full Context configure oam-pm session mpls lsp mpls-tp-static

Description Commands in this context configure an MPLS TP LSP and its attributes to be tested.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.344 mrib

mrib

Syntax **mrib** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no mrib

Context **[Tree]** (debug>router>pim mrib)

Full Context debug router pim mrib

Description This command enables debugging for PIM MRIB.

The **no** form of this command disables debugging for PIM MRIB.

Parameters *grp-ip-address* — Debugs information associated with the specified PIM MRIB.

Values multicast group address (ipv4, ipv6)

ip-address — Debugs information associated with the specified PIM MRIB.

Values source address (ipv4, ipv6)

detail — Debugs detailed MRIB information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.345 mrinfo

mrinfo

Syntax **mrinfo** {*ip-address* | *dns-name*} [**router** *router-instance* | **service-name** *service-name*]

Context **[Tree]** (global mrinfo)

Full Context global mrinfo

Description This command is used to print relevant multicast information from the target multicast router. Information displayed includes adjacency information, protocol, metrics, thresholds, and flags from the target multicast route.

Parameters *ip-address* — Specifies the IP address of the multicast-capable target router.

Values ipv4 unicast address (a.b.c.d)

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

router-instance — Specifies the router name or service ID for the router instance.

Values *router-name*: Base
vprn-service-id: 1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

Output The following output displays mrinfo information. The output fields are described in the following table.

Output Sample

```
A:dut-f# mrinfo 10.1.1.2

10.1.1.2  [version 3.0,prune,genid,mtrace]:
  10.1.1.2 -> 10.1.1.1 [1/0/pim]
  10.1.1.3 -> 0.0.0.0 [1/0/pim/down/disabled]
  10.1.1.4 -> 0.0.0.0 [1/0/pim/querier/leaf]
  239.200.200.3 -> 239.200.200.5 [1/0/tunnel/pim]...
```

Table 97 **Mrinfo Output Fields**

Label	Description
General flags	
version	Indicates software version on queried router
prune	Indicates that router understands pruning

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 97 **Mrinfo Output Fields**

Label	Description
genid	Indicates that router sends generation IDs
mtrace	Indicates that the router handles mtrace requests
Neighbors flags	
1	Metric
0	Threshold (multicast time-to-live)
pim	PIM enabled on interface
down	Operational status of interface
disabled	Administrative status of interface
leaf	No downstream neighbors on interface
querier	Interface is IGMP querier
tunnel	Neighbor reached via tunnel

17.346 mrouter-dest

mrouter-dest

Syntax [**no**] **mrouter-dest** *mac-name*

Context **[Tree]** (config>service>vpls>pbb>bvpls>igmp-snooping mrouter-dest)
[Tree] (config>service>vpls>pbb>bvpls>mld-snooping mrouter-dest)

Full Context configure service vpls pbb backbone-vpls igmp-snooping mrouter-dest
configure service vpls pbb backbone-vpls mld-snooping mrouter-dest

Description This command configures the destination B-MAC address name to be used in the related backbone VPLS to reach a specific IGMP or MLD snooping MRouter. The name is associated at system level with the MAC address, using the command **config>service>pbb mac-name**.

Parameters *mac-name* — Specifies the MAC name.

Values 32 chars max

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.347 mrouter-port

mrouter-port

Syntax [**no**] **mrouter-port**

Context **[Tree]** (config>service>vpls>bind>igmp-snooping mrouter-port)
[Tree] (config>service>vpls>bind>mld-snooping mrouter-port)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping mrouter-port)
[Tree] (config>service>vpls>sap>igmp-snooping mrouter-port)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping mrouter-port)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping mrouter-port)

Full Context configure service vpls allow-ip-int-bind igmp-snooping mrouter-port
configure service vpls allow-ip-int-bind mld-snooping mrouter-port
configure service vpls mesh-sdp igmp-snooping mrouter-port
configure service vpls sap igmp-snooping mrouter-port
configure service vpls spoke-sdp igmp-snooping mrouter-port
configure service vpls spoke-sdp mld-snooping mrouter-port

Description This command specifies whether a multicast router is attached behind this SAP, SDP, or routed VPLS IP interface.

Configuring these objects as an mrouter-port will have a double effect. Firstly, all multicast traffic received on another SAP, SDP, or routed VPLS IP interface will be copied to this SAP, SDP, or routed VPLS IP interface. Secondly, IGMP/MLD reports generated by the system as a result of a router joining or leaving a multicast group, will be sent to this SAP, SDP, or routed VPLS IP interface.

If two multicast routers exist in the network, one of them will become the active querier. While the other multicast router (non-querier) stops sending IGMP queries, it should still receive reports to keep its multicast trees up-to-date. To support this, the mrouter-port should be enabled on all SAPs, SDPs, or routed VPLS IP interfaces connecting to a multicast router.

Note: The IGMP version to be used for the reports (v1, v2, or v3) can only be determined after an initial query has been received. Until such time, no reports are sent on the SAP, spoke-SDP, or routed VPLS IP interface, even if **mrouter-port** is enabled.

If the **send-queries** command is enabled on this SAP or spoke-SDP, the **mrouter-port** parameter cannot be set.

When PIM-snooping is enabled within a VPLS service, all IP multicast traffic and PIM messages will be sent to any SAP or SDP binding configured with an IGMP-snooping mrouter port. This occurs even without IGMP-snooping enabled, but is not supported in a BGP-VPLS or M-VPLS service.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no mrouter-port

Platforms All

mrouter-port

Syntax [**no**] **mrouter-port**

Context **[Tree]** (config>service>vpls>vxlan>igmp-snooping mrouter-port)

Full Context configure service vpls vxlan igmp-snooping mrouter-port

Description This command enables all VXLAN binds to be mrouter ports, indicating that a multicast router is attached behind each VXLAN binding. Configuring these objects as an **mrouter-port** has two effects. Firstly, all multicast traffic received on another object is copied to each VXLAN binding. Secondly, IGMP reports generated by the system as a result of a router joining or leaving a multicast group is sent to all VXLAN bindings. When PIM snooping for IPv4 is enabled within a VPLS service, all IP multicast traffic and PIM for IPv4 messages are sent to all VXLAN bindings configured with an **igmp-snooping mrouter-port**. This occurs even without **igmp-snooping** enabled.

Default no mrouter-port

Platforms All

mrouter-port

Syntax [**no**] **mrouter-port**

Context **[Tree]** (config>service>vpls>vxlan>mld-snooping mrouter-port)

Full Context configure service vpls vxlan mld-snooping mrouter-port

Description This command enables all VXLAN binds to be mrouter ports, indicating that a multicast router is attached behind each VXLAN binding. Configuring these objects as an **mrouter-port** has two effects. Firstly, all multicast traffic received on another object is copied to each VXLAN binding. Secondly, MLD reports generated by the system as a result of a router joining or leaving a multicast group is sent to all VXLAN bindings.

Default no mrouter-port

Platforms All

mrouter-port

Syntax [**no**] **mrouter-port**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>pbb>bvpls>sap>igmp-snooping mrouter-port)
[Tree] (config>service>vpls>pbb>bvpls>sdp>igmp-snooping mrouter-port)
[Tree] (config>service>vpls>pbb>bvpls>sap>mld-snooping mrouter-port)
[Tree] (config>service>vpls>pbb>bvpls>sdp>mld-snooping mrouter-port)

Full Context configure service vpls pbb backbone-vpls sap igmp-snooping mrouter-port
configure service vpls pbb backbone-vpls sap mld-snooping mrouter-port
configure service vpls pbb backbone-vpls sdp igmp-snooping mrouter-port
configure service vpls pbb backbone-vpls sdp mld-snooping mrouter-port

Description This command specifies whether a multicast router is attached behind this SAP or spoke-SDP.

Configuring a SAP or spoke-SDP as an mrouter-port will have a double effect. Firstly, all multicast traffic received on another SAP or spoke-SDP will be copied to this SAP or spoke-SDP. Secondly, IGMP or MLD reports generated by the system as a result of someone joining or leaving a multicast group, will be sent to this SAP or SDP.

If two multicast routers exist in the local area network, one of them will become the active querier. The other multicast router (non-querier) stops sending IGMP or MLD queries, but it should still receive reports to keep its multicast trees up to date. To support this, the mrouter-port should be enabled on all SAPs or spoke-SDPs connecting to a multicast router.

The IGMP version to be used for the reports (v1, v2 or v3) or MLD version (v1 or v2) can only be determined after an initial query has been received. Until such time no reports are sent on the SAP, even if mrouter-port is enabled.

If the **send-queries** command is enabled on this SAP or spoke-SDP, the **mrouter-port** parameter cannot be set.

Default no mrouter-port

Platforms All

17.348 mrp

mrp

Syntax **mrp**

Context [Tree] (config>service>vpls mrp)
[Tree] (config>service>vpls>sap mrp)
[Tree] (config>service>vpls>mesh-sdp mrp)
[Tree] (config>service>vpls>spoke-sdp mrp)

Full Context configure service vpls mesh-sdp mrp
configure service vpls mrp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap mrp
configure service vpls spoke-sdp mrp

Description This command configures Multiple Registration Protocol (MRP) parameters. MRP is valid only under B-VPLS.

Platforms All

mrp

Syntax **mrp**

Context **[Tree]** (config>service mrp)

Full Context configure service mrp

Description This command configures a Multi-service Route Processor (MRP).

Platforms All

mrp

Syntax [**no**] **mrp**

Context **[Tree]** (debug>service>id mrp)

Full Context debug service id mrp

Description This command enables and configures MRP debugging.

Platforms All

17.349 mrp-policy

mrp-policy

Syntax **mrp-policy** *policy-name* [**create**]
no mrp-policy *policy-name*

Context **[Tree]** (config>service>mrp mrp-policy)

Full Context configure service mrp mrp-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure an MRP policy. The mrp-policy specifies either a forward or a drop action for the Group B-MAC attributes associated with the ISIDs specified in the match criteria. The mrp-policy can be applied to multiple BVPLS services as long as the scope of the policy is template.

Any changes made to the existing policy, using any of the sub-commands, will be applied immediately to all services where this policy is applied. For this reason, when many changes are required on a mrp-policy, Nokia recommends that the policy be copied to a work area. That work-in-progress policy can be modified until complete and then written over the original mrp-policy. Use the **config mrp-policy copy** command to maintain policies in this manner.

The **no** form of this command deletes the mrp-policy. An MRP policy cannot be deleted until it is removed from all the SAPs or SDPs where it is applied.

Default no mrp-policy

Parameters *policy-name* — Specifies the redirect policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

create — This keyword is required when first creating the configuration context. When the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms All

mrp-policy

Syntax **mrp-policy** *policy-name*
no mrp-policy

Context **[Tree]** (config>service>vpls>sap>mrp mrp-policy)
[Tree] (config>service>vpls>spoke-sdp>mrp mrp-policy)
[Tree] (config>service>vpls>mesh-sdp>mrp mrp-policy)

Full Context configure service vpls mesh-sdp mrp mrp-policy
configure service vpls sap mrp mrp-policy
configure service vpls spoke-sdp mrp mrp-policy

Description This command instructs MMRP to use the mrp-policy specified in the command to control which Group B-MAC attributes will be declared and registered on the egress SAP/Mesh-SDP/Spoke-SDP. The Group B-MACs will be derived from the ISIDs using the procedure used in the PBB solution. The Group MAC is standard OUI with the last 24 bits being the ISID value. If the policy-name refers to a non-existing mrp-policy the command should return error. Changes to a mrp-policy are allowed and applied to the SAP/SDPs under which the policy is referenced.

Default no mrp-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the redirect policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

17.350 mrpdu

mrpdu

Syntax [**no**] **mrpdu**

Context **[Tree]** (debug>service>id>mrp mrpdu)

Full Context debug service id mrp mrpdu

Description This command enables debugging of the MRP PDUs that are received or transmitted.

The **no** form of this command disables debugging of MRP PDUs.

Platforms All

17.351 mrru

mrru

Syntax **mrru** *mrru*
no mrru

Context **[Tree]** (config>port>multilink-bundle mrru)

Full Context configure port multilink-bundle mrru

Description This command specifies the maximum received reconstructed unit (MRRU), similar to a maximum transmission unit (MTU), but applies only to MLPPP multilink bundles. The MRRU is the maximum frame size that can be reconstructed from multilink fragments. This command is only valid for MLPPP bundles.

The **no** form of this command resets the MRRU to the default.

Default mrru 1524

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mrru* — Specifies the maximum received reconstructed unit size, in bytes.

Values 1500 to 9206

Platforms 7450 ESS, 7750 SR-7/12/12e

17.352 mru

mru

Syntax **mru** *mru-bytes*
no mru

Context **[Tree]** (config>subscr-mgmt>pppoe-client-policy mru)

Full Context configure subscriber-mgmt pppoe-client-policy mru

Description This command defines which Maximum Receive Unit (MRU) value is signaled by the PPPoE client.

The **no** form of this command reverts to the default.

Default mru 1492

Parameters *mru-bytes* — Specifies the MRU value in octets.

Values 512 to 9154

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.353 mru-mismatch-detection

mru-mismatch-detection

Syntax **mru-mismatch-detection**
no mru-mismatch-detection

Context **[Tree]** (config>router>isis mru-mismatch-detection)
[Tree] (config>service>vprn>isis mru-mismatch-detection)

Full Context configure router isis mru-mismatch-detection
configure service vprn isis mru-mismatch-detection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command verifies that the received IS-IS Hello (IIH) packet size does not exceed the maximum configured port MTU size. The received IIH packet is dropped when its size exceeds the maximum port MTU size.

By default, FP-based hardware does not send IS-IS packets larger than the configured port MTU size, but can accept IS-IS packets larger than the configured port MTU size.

The **no** form of this command allows the IS-IS router instance not to drop oversized received IIH packets.

Default no mru-mismatch-detection

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.354 msap

msap

Syntax [**no**] **msap** *msap-id*

Context **[Tree]** (debug>service>id>ppp msap)

Full Context debug service id ppp msap

Description This command enable PPP debug for the specified managed SAP.

Multiple msap filters could be specified in the same debug command.

The **no** form of this command disables debugging.

Parameters *msap-id* — Specifies the managed SAP ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.355 msap-defaults

msap-defaults

Syntax **msap-default**

Context **[Tree]** (config>service>vpls>sap msap-defaults)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host msap-defaults)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host msap-defaults)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls sap msap-defaults
configure subscriber-mgmt local-user-db ipoe host msap-defaults
configure subscriber-mgmt local-user-db ppp host msap-defaults

Description This command configures MSAP authentication defaults.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt local-user-db ppp host msap-defaults
- configure subscriber-mgmt local-user-db ipoe host msap-defaults

All

- configure service vpls sap msap-defaults

17.356 msap-policy

msap-policy

Syntax **msap-policy** *msap-policy-name* [**create**]
no msap-policy *msap-policy-name*

Context **[Tree]** (config>subscr-mgmt msap-policy)

Full Context configure subscriber-mgmt msap-policy

Description This command configures a managed SAP policy. Managed SAPs allow the use of policies and a SAP template for the creation of a SAP.

The **no** form of this command removes the MSAP policy from the configuration.

Parameters *msap-policy-name* — Specifies the managed SAP policy name, up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — Keyword used to create the managed SAP policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.357 msdp

msdp

Syntax [**no**] **msdp**

Context **[Tree]** (config>service>vprn msdp)

Full Context configure service vprn msdp

Description This command enables a Multicast Source Discovery Protocol (MSDP) instance. When an MSDP instance is created, the protocol is enabled. To start or suspend execution of the MSDP protocol without affecting the configuration, use the [**no**] **shutdown** command.

For the MSDP protocol to function, at least one peer must be configured.

When MSDP is configured and started, an appropriate event message should be generated.

When the **no** form of this command is executed, all sessions must be terminated and an appropriate event message should be generated.

When all peering sessions are terminated, an event message per peer is not required.

The **no** form of this command deletes the MSDP protocol instance, removing all associated configuration parameters.

Default no msdp

Platforms All

msdp

Syntax [**no**] **msdp**

Context **[Tree]** (debug>router msdp)

Full Context debug router msdp

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP).

The **no** form of the command disables MSDP debugging.

Platforms All

msdp

Syntax [**no**] **msdp**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router msdp)

Full Context configure router msdp

Description This command enables a Multicast Source Discovery Protocol (MSDP) instance. When an MSDP instance is created, the protocol is enabled. To start or suspend execution of the MSDP protocol without affecting the configuration, use the [**no**] **shutdown** command.

For the MSDP protocol to function, at least one peer must be configured.

When MSDP is configured and started an appropriate event message should be generated.

When **the** no form of the command is executed, all sessions must be terminated and an appropriate event message should be generated.

When all peering sessions are terminated, an event message per peer is not required.

The **no** form of the command deletes the MSDP protocol instance, removing all associated configuration parameters.

Default no msdp

Platforms All

17.358 msg

msg

Syntax [**no**] **msg**

Context [Tree] (debug>router>pim msg)

Full Context debug router pim msg

Description This command enables debugging for PIM messaging.

The **no** form of this command disables debugging for PIM messaging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.359 msg-pacing

msg-pacing

Syntax [**no**] **msg-pacing**

Context **[Tree]** (config>router>rsvp msg-pacing)

Full Context configure router rsvp msg-pacing

Description This command enables RSVP message pacing in which the specified number of RSVP messages, specified in the **max-burst** command, are sent in a configured interval, specified in the **period** command. A count is kept of the messages that were dropped because the output queue for the interface used for message pacing was full.

Default no msg-pacing

Platforms All

17.360 msisdn

msisdn

Syntax [**no**] **msisdn**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute msisdn)
[Tree] (config>subscr-mgmt>auth-plcy>include-radius-attribute msisdn)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute msisdn
configure subscriber-mgmt authentication-policy include-radius-attribute msisdn

Description This command enables the inclusion of the MSISDN in AAA protocols as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.361 mss-adjust-group

mss-adjust-group

Syntax **mss-adjust-group** *bb-group-id* **segment-size** *segment-size*
no mss-adjust-group

Context **[Tree]** (config>router mss-adjust-group)
[Tree] (config>service>vprn mss-adjust-group)

Full Context configure router mss-adjust-group
configure service vprn mss-adjust-group

Description This command associates the MSS adjust group consisting of multiple ISAs with the routing context in which the application requiring TCP MSS adjust resides.

Parameters *bb-group-id* — Specifies the group used for TCP MSS adjust

segment-size — Specifies the value to put into the TCP Maximum Segment Size (MSS) option if it is not already present, or if the present value is higher

Values 160 to 10240

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.362 mst-instance

mst-instance

Syntax **mst-instance** *mst-inst-number*

Context **[Tree]** (config>service>vpls>sap>stp mst-instance)

Full Context configure service vpls sap stp mst-instance

Description Commands in this context configure MSTI related parameters at SAP level. This context can be open only for existing mst-instances defined at the service level (see **config**>**service**>**vpls**>**stp mst-instance**).

Parameters *mst-inst-number* — Specifies an existing Multiple Spanning Tree Instance number

Values 1 to 4094

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mst-instance

Syntax **mst-instance** *mst-inst-number* [**create**]
no mst-instance [*mst-inst-number*]

Context **[Tree]** (config>service>vpls>stp mst-instance)

Full Context configure service vpls stp mst-instance

Description This command creates the context to configure MST instance (MSTI) related parameters. Up to 16 instances will be supported by MSTP. The instance 0 is mandatory by protocol and therefore, it cannot be created by the CLI. The software will maintain this instance automatically.

Parameters *mst-inst-number* — Specifies the Multiple Spanning Tree instance

Values 1 to 4094

Platforms All

17.363 mst-max-hops

mst-max-hops

Syntax **mst-max-hops** *hops-count*
no mst-max-hops

Context **[Tree]** (config>service>vpls>stp mst-max-hops)

Full Context configure service vpls stp mst-max-hops

Description This command specifies the number of hops in the region before BPDU is discarded and the information held for the port is aged out. The root bridge of the instance sends a BPDU (or M-record) with remaining-hop-count set to configured <*max-hops*>. When a bridge receives the BPDU (or M-record), it decrements the received remaining-hop-count by 1 and propagates it in BPDU (or M-record) it generates.

The **no** form of this command sets the *hops-count* to its default value.

Default mst-max-hops 20

Parameters *hops-count* — Specifies the maximum number of hops

Values 1 to 40

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.364 mst-name

mst-name

Syntax **mst-name** *region-name*
no mst-name

Context **[Tree]** (config>service>vpls>stp mst-name)

Full Context configure service vpls stp mst-name

Description This command defines an MST region name. Two bridges are considered as a part of the same MST region as soon as their configuration of the MST region name, the MST-revision and VLAN-to-instance assignment is identical.

The **no** form of this command removes *region-name* from the configuration.

Default no mst-name

Parameters *region-name* — Specifies an MST-region name up to 32 characters in length

Platforms All

17.365 mst-path-cost

mst-path-cost

Syntax **mst-path-cost** *inst-path-cost*
no mst-path-cost

Context **[Tree]** (config>service>vpls>sap>stp>mst-instance mst-path-cost)

Full Context configure service vpls sap stp mst-instance mst-path-cost

Description This commands specifies path-cost within a specified instance, expressing probability that a specified port will be put into the forwarding state in case a loop occurs (the highest value expresses lowest priority).

The **no** form of this command sets port-priority to its default value.

Default The path-cost is proportional to link speed.

Parameters *inst-path-cost* — Specifies the contribution of this port to the MSTI path cost of paths toward the spanning tree regional root which include this port

Values 1 to 200000000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.366 mst-port-priority

mst-port-priority

Syntax **mst-port-priority** *stp-priority*
no mst-port-priority

Context **[Tree]** (config>service>vpls>sap>stp>mst-instance mst-port-priority)

Full Context configure service vpls sap stp mst-instance mst-port-priority

Description This commands specifies the port priority within a specified instance, expressing probability that a specified port will be put into the forwarding state if a loop occurs.

The **no** form of this command sets port-priority to its default value.

Default mst-port-priority 128

Parameters *stp-priority* — Specifies the value of the port priority field.

Platforms All

17.367 mst-priority

mst-priority

Syntax **mst-priority** *bridge-priority*
no mst-priority

Context **[Tree]** (config>service>vpls>stp>mst-instance mst-priority)

Full Context configure service vpls stp mst-instance mst-priority

Description This command specifies the bridge priority for this specific Multiple Spanning Tree Instance for this service. The *bridge-priority* value reflects likelihood that the switch will be chosen as the regional root switch (65535 represents the least likely). It is used as the highest 4 bits of the Bridge ID included in the MSTP BPDUs generated by this bridge.

The priority can only take on values that are multiples of 4096 (4k). If a value is specified that is not a multiple of 4K, then the value will be replaced by the closest multiple of 4K, which is lower than the value entered.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command sets the bridge-priority to its default value.

Default mst-priority 32768 — All instances created by the **config>service>vpls>stp>mst-instance vlan-range** command and not having explicit definition of bridge-priority will inherit default value

Parameters *bridge-priority* — Specifies the priority of this specific Multiple Spanning Tree Instance for this service

Values 0 to 65535

Platforms All

17.368 mst-revision

mst-revision

Syntax **mst-revision** *revision-number*
no mst-revision

Context **[Tree]** (config>service>vpls>stp mst-revision)

Full Context configure service vpls stp mst-revision

Description This command defines the MST configuration revision number. Two bridges are considered as a part of the same MST region as soon as their configuration of MST-region name, MST-revision and VLAN-to-instance assignment is identical.

The **no** form of this command returns MST configuration revision to its default value.

Default mst-revision 0

Parameters *revision-number* — Specifies the MSTP region revision number to define the MSTP region

Values 0 to 65535

Platforms All

17.369 mstat

mstat

Syntax **mstat source** [*ip-address* | *dns-name*] **group** {*ip-address* | *dns-name*} [**destination**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]

Context [Tree] (global mstat)

Full Context global mstat

Description This command traces a multicast path from a source to a receiver and displays multicast packet rate and loss information.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4 address (a.b.c.d)

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) is used. This will suffice if packet loss statistics for a particular multicast group are not needed.

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response is also returned to the address specified as the receiver.

hop — Specifies the maximum number of hops that will be traced from the receiver back toward the source.

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — Specifies the router name or service ID used to identify the router instance.

Values

router-name:	Base
service-id:	1 to 2147483647

Default Base

service-name — Specifies the service name up to 64 characters in length.

wait-time — Specifies the number of seconds to wait for the response.

Values 1 to 60

Output The following output is an example of mstat information. The output fields are described in the following table.

Output Sample

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
  Source          Response Dest     Overall       Packet Statistics for Traffic From
10.10.16.9        10.20.1.6        Mcast Pkt       10.10.16.9 to 239.5.6.7
     |          __/  rtt   29 ms      Rate          Lost/Sent = Pct Rate
     v        /                     ---------       --------------------
10.10.16.3
10.10.2.3         ?
     |       ^      ttl   2          1pps             0/0   = --     0 pps
     v       |
10.10.2.1
10.10.1.1         ?
     |       ^      ttl   3          1pps             0/0   = --     0 pps
     v       |
10.10.1.2
10.10.4.2         ?             Reached RP/Core
     |       ^      ttl   4          1pps             0/0   = --     0 pps
     v       |
10.10.4.4
10.10.6.4         ?
     |       ^      ttl   5          1pps             0/0   = --     0 pps
     v       |
10.10.6.5
10.10.10.5        ?
     |       \__    ttl   6          1pps             0/0   = --     0 pps
     v          \
10.10.10.6       10.20.1.6
Receiver         Query Source
```

Table 98 **Mstat Output Fields**

Label	Description
hop	The number of hops from the source to the listed router
router name	The number of the router for this hop or “?” when not reverse DNS translated
address	The address of the router for this hop
protocol	The protocol used
ttl	The forward TTL threshold. TTL that a packet is required to have before it is forwarded over the outgoing interface.
forwarding code	Forwarding information/error code for this hop

For each interface between two nodes a line is printed, following the same layout as other routers with an implementation derived from mrouted. Consider the following:

- The forwarding information/error code is only displayed when different from “No Error”.
- “?” means there is no reverse DNS translation.
- There is no “Overall Mcast Pkt Rate” available in the PE for the VPRN case.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.370 mstat2

mstat2

Syntax **mstat2 source** [*ip-address* | *dns-name* | *starg*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *vprn-service-name*] [**wait-time** *seconds*]

Context **[Tree]** (global mstat2)

Full Context global mstat2

Description This command traces a multicast path from a source to a receiver and displays multicast packet rate and loss information.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4-prefix:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

starg — Specifies a static (*,G) entry. This command can only be enabled if no existing source addresses for this source is specified.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) is used. This will suffice if packet loss statistics for a particular multicast group are not needed.

Values ipv4-prefix:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response is also returned to the address specified as the receiver.

Values ipv4-prefix:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

hop — Specifies the maximum number of hops that are traced from the receiver back toward the source.

Values 1 to 255

Default 32

router-instance — Specifies the router name or service ID used to identify the router instance.

Values

router-name:	Base
service-id:	1 to 2147483647

Default Base

vprn-service-name — Specifies the service name, up to 64 characters.

seconds — Specifies the number of seconds to wait for the response.

Values 1 to 60

Default 3

Output

Table 99 **Mstat2 Output Fields**

Label	Description
hop	Number of hops from the source to the listed router.
router name	Name of the router for this hop or “?” when not reverse DNS translated.
address	Address of the router for this hop.
protocol	Protocol used.
ttl	Forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 99 **Mstat2 Output Fields**

Label	Description
forwarding code	Forwarding information/error code for this hop.

For each interface between two nodes a line is printed, following the same layout as other routers with an implementation derived from mrouted. Consider the following:

- The forwarding information/error code is only displayed when different from “No Error”.
- “?” means there is no reverse DNS translation.
- There is no “Overall Mcast Pkt Rate” available in the PE for the VPRN case.

Output Sample

```
*A:Dut-A# mstat2 group 239.225.6.1 source 10.0.1.66
Mtrace2 from 150.0.1.66 via group 225.6.6.1 Querying full reverse path...
Waiting to accumulate statistics...Results after 10 seconds:
 Source         Response Dest    Overall     Packet Statistics For
Traffic From
10.0.1.66       10.0.0.1         Mcast Pkt    10.10.1.66 To 239.5.6.7
      |        __/  rtt 24.0ms     Rate       Lost/Sent = Pct  Rate
      v      /                     -------     ---------------------
10.0.1.6
10.0.1.6        ?
      |      ^       ttl    2        10 pps        0/100  =  0%   10 pps
      v      |
10.0.1.4
10.10.4.4        usilhc03-hb2.ndc.lucent.com Reached RP/Core
      |      ^       ttl    3        10 pps        0/100  =  0%   10 pps
      v      |
10.10.4.2
10.0.1.2        10.1.0.110.ap.yournet.ne.jp
      |       \__    ttl    4        10 pps        0/100  =  0%   10 pps
      v          \
10.0.1.1        10.0.0.1
   Receiver      Query Source

*A:Dut-A# mstat2  group ff05::225:6:6:1 source 3ffe::150:0:1:66
Mtrace2 from source
<S> = 3ffe::150:0:1:66
via group
<G> = ff05::225:6:6:1
Querying full reverse path...
Waiting to accumulate statistics...Results after 10 seconds:
Destination <D> = 3ffe::120:0:1:1
Response Destination <RD> = 3ffe::1
   Source         Response Dest    Overall     Packet Statistics For
Traffic From
<S>              <RD>             Mcast Pkt    Source <S> To Group <G>
      |        __/  rtt 23.0ms     Rate       Lost/Sent = Pct  Rate
      v      /                     -------     ---------------------
Remote Address ::
Incoming IF 4
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
3ffe::6 ?
Outgoing IF 3
      |     ^      ttl    2        20 pps        0/100  =  0%   10 pps
      v     |
Remote Address fe80::a248:1ff:fe01:2
Incoming IF 2
3ffe::5 ? Reached RP/Core
Outgoing IF 3
      |     ^      ttl    3        20 pps        0/100  =  0%   10 pps
      v     |
Remote Address fe80::a246:1ff:fe01:1
Incoming IF 3
3ffe::3 ?
Outgoing IF 2
      |      \__   ttl    4        30 pps        0/100  =  0%   10 pps
      v         \
<D>             <RD>
   Receiver      Query Source
```

17.371 mt

mt

Syntax **mt** {**ipv4-unicast** | **ipv4-multicast** | **ipv6-unicast** | **ipv6-multicast**}
no mt

Context **[Tree]** (config>router>bier>template>sub-domain mt)

Full Context configure router bier template sub-domain mt

Description This command specifies the multi-topology for this sub-domain.

The **no** form of this command removes the multi-topology from this sub-domain.

Parameters **ipv4-unicast** — Specifies that the sub-domain uses IPv4 unicast topology. IPv4 unicast imports routes into the unicast RTM.

ipv4-multicast — Specifies that the sub-domain uses IPv4 multicast topology. IPv4 multicast imports routes into the multicast RTM.

ipv6-unicast — Specifies that the sub-domain uses IPv6 unicast topology. IPv6 unicast imports routes into the unicast RTM.

ipv6-multicast — Specifies that the sub-domain uses IPv6 multicast topology. IPv6 multicast imports routes into the multicast RTM.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.372 mtrace

mtrace

Syntax **mtrace source** [*ip-address* | *dns-name*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]

Context **[Tree]** (global mtrace)

Full Context global mtrace

Description This command traces a multicast path from a source to a receiver.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4 address (a.b.c.d)

dns-name — Specifies the DNS name (if DNS name resolution is configured). 63 characters maximum.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) will be used. This will suffice if packet loss statistics for a particular multicast group are not needed.

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response will also be returned to the address specified as the receiver.

hop — Specifies the maximum number of hops that will be traced from the receiver back toward the source.

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — Specifies the router name or service ID used the identify the router instance.

Values

router-name:	“Base”
service-id:	1 to 2147483647

Default Base

service-name — Specifies the service name up, to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

wait-time — Specifies the time, in seconds, to wait for the response.

Values 1 to 60

Output The following output is an example of mtrace information.

Output Sample

```
A:Dut-F# mtrace source 10.10.16.9 group 239.5.6.7

Mtrace from 10.10.16.9 via group 239.5.6.7
Querying full reverse path...

 0 ? (10.10.10.6)
-1 ? (10.10.10.5) PIM thresh^ 1 No Error
-2 ? (10.10.6.4) PIM thresh^ 1 No Error
-3 ? (10.10.4.2) PIM thresh^ 1 Reached RP/Core
-4 ? (10.10.1.1) PIM thresh^ 1 No Error
-5 ? (10.10.2.3) PIM thresh^ 1 No Error
-6 ? (10.10.16.9)

Round trip time 29 ms; total ttl of 5 required.
```

Table 100 **Mtrace Output Fields**

Label	Description
hop	The number of hops from the source to the listed router
router name	The name of the router for this hop. If a DNS name query is not successful a “?” displays.
address	The address of the router for this hop
protocol	The protocol used
ttl	The forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.
forwarding code	The forwarding information/error code for this hop

mtrace

Syntax [**no**] **mtrace**

Context **[Tree]** (debug>router mtrace)

Full Context debug router mtrace

Description This command configures debugging for mtrace.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.373 mtrace2

mtrace2

Syntax **mtrace2**

Context **[Tree]** (config>service>vprn mtrace2)
[Tree] (config>router mtrace2)

Full Context configure router mtrace2
configure service vprn mtrace2

Description This command traces a multicast path from a source to a receiver.

Platforms All

mtrace2

Syntax **mtrace2 source** [*ip-address* | *dns-name* | *starg*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop-count*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]

Context **[Tree]** (global mtrace2)

Full Context global mtrace2

Description This command traces a multicast path from a source to a receiver.

Parameters **source** *ip-address* — Specifies the IP address of the multicast capable target router.

Values ipv4-prefix:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

starg — Specifies a static (*,G) entry. This command can only be enabled if no existing source addresses for this source is specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that is used. If the group is not specified, address 224.2.0.1 (the MBone audio) is used. This suffices if packet loss statistics for a particular multicast group are not needed.

Values ipv4-prefix:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted, the IP address of the system where the command is entered is used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response is returned to the address specified as the receiver.

Values ipv4-prefix:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

hop-count — Specifies the maximum number of hops that are traced from the receiver back toward the source.

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — Specifies the router name or service ID used the identify the router instance.

Values

router-name:	“Base”
service-id:	1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

wait-time — Specifies the number of seconds to wait for the response.

Values 1 to 60

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Output

Table 101 **Mtrace2 Output Fields**

Label	Description
hop	The number of hops from the source to the listed router
router name	The name of the router for this hop. If a DNS name query is not successful a “?” displays.
address	The address of the router for this hop
protocol	The protocol used
ttl	The forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.
forwarding code	The forwarding information/error code for this hop

Output Sample

```
*A:Dut-A# mtrace2 group 239.225.6.1 source 192.0.1.66
Mtrace2 from 192.0.1.66 via group 239.225.6.1 Querying full reverse path...
   0  1.1.0.110.ap.yournet.ne.jp (110.0.1.1)
  -1  2.1.0.110.ap.yournet.ne.jp (110.0.1.2)  rtg=ospf mrtg=pimSparseMode  thresh^ 1
  No Error
  -2  usilhc03-hb2.ndc.lucent.com(10.10.4.4)rtg=ospf mrtg=pimSparseMode thresh^ 1 Re
ached RP/ Core
  -3  ? (10.0.1.6)  rtg=local mrtg=pimSparseMode  thresh^ 1  No Error
  -4  ? (10.0.1.66)
Round trip time 23.3 ms; total ttl of 3 required.

*A:Dut-A# mtrace2 group ff05::225:2:6:1 source 3ffe::255:0:1:66
Mtrace2 from source
<S> = 3ffe::255:0:1:66
via group
<G> = ff05::225:6:6:1
Querying full reverse path...
   0  ? (3ffe::120:0:1:1)
  -1  ? (3ffe::3)  IIF=3 OIF=2  rtg=ospf mrtg=pimSparseMode thresh^ N/A No Error
  -2  ? (3ffe::5)  IIF=2 OIF=3  rtg=ospf mrtg=pimSparseMode thresh^ N/A Reached RP/
Core
  -3  ? (3ffe::6)  IIF=4 OIF=3  rtg=local mrtg=pimSparseMode thresh^ N/A  No Error
  -4  ? (3ffe::150:0:1:66)
Round trip time 46.5 ms; total ttl of 3 required.
```

mtrace2

Syntax [**no**] **mtrace2**

Context **[Tree]** (debug>router mtrace2)

Full Context debug router mtrace2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures debugging for mtrace2.

Platforms All

17.374 mtu

mtu

Syntax **mtu** *mtu-bytes*
no mtu

Context **[Tree]** (config>router>l2tp>group>ppp mtu)
[Tree] (config>router>l2tp>group>tunnel>ppp mtu)
[Tree] (config>service>vprn>l2tp>group>ppp mtu)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp mtu)

Full Context configure router l2tp group ppp mtu
configure router l2tp group tunnel ppp mtu
configure service vprn l2tp group ppp mtu
configure service vprn l2tp group tunnel ppp mtu

Description This command configures the maximum PPP MTU size.

Default mtu 1500

Parameters *mtu-bytes* — Specifies, in bytes, the maximum PPP MTU size.

Values 512 to 9212

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mtu

Syntax **mtu** *bytes*
no mtu

Context **[Tree]** (config>router>router-advert>if mtu)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv mtu)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 mtu)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv mtu)
[Tree] (config>service>vprn>router-advert>if mtu)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv mtu)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 mtu)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv mtu)
[Tree] (config>subscr-mgmt>rtr-adv-plcy mtu)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router router-advertisement interface mtu
configure service ies subscriber-interface group-interface ipv6 mtu
configure service ies subscriber-interface group-interface ipv6 router-advertisements mtu
configure service ies subscriber-interface ipv6 router-advertisements mtu
configure service vprn router-advertisement interface mtu
configure service vprn subscriber-interface group-interface ipv6 mtu
configure service vprn subscriber-interface group-interface ipv6 router-advertisements mtu
configure service vprn subscriber-interface ipv6 router-advertisements mtu
configure subscriber-mgmt router-advertisement-policy mtu

Description This command specifies the value to be placed in link MTU options sent by the router on this interface.

The **no** form of this command reverts to the default.

Default no mtu — The MTU option is not sent in the router advertisement messages.

Parameters *bytes* — Specifies the advertised MTU value in bytes for this interface.

Values 1280 to 9800 (for **config**>**router**>**router-advert**>**if** and **config**>**service**>**vprn**>**router-advert**>**if** contexts only)
1280 to 9212 (for subscriber management context, ies and vprn service subscriber-interface contexts)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt router-advertisement-policy mtu
- configure service ies subscriber-interface ipv6 router-advertisements mtu
- configure service vprn subscriber-interface ipv6 router-advertisements mtu
- configure service vprn subscriber-interface group-interface ipv6 router-advertisements mtu
- configure service ies subscriber-interface group-interface ipv6 router-advertisements mtu

All

- configure router router-advertisement interface mtu
- configure service vprn router-advertisement interface mtu

mtu

Syntax **mtu** *mtu-bytes*
no mtu

Context **[Tree]** (config>subscr-mgmt>pppoe-client-policy mtu)

Full Context configure subscriber-mgmt pppoe-client-policy mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines which Maximum Transmission Unit (MTU) is applied, by default, for packets egressing the PPP link. If a lower MRU is sent during PPP link establishment, the MRU value is used.

The **no** form of this command reverts to the default.

Default mtu 1492

Parameters *mtu-bytes* — Specifies the MTU value in octets.

Values 512 to 9154

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

mtu

Syntax **mtu** *mtu-bytes*
no mtu

Context **[Tree]** (config>port>ethernet mtu)
[Tree] (config>port>sonet-sdh>path mtu)
[Tree] (config>port>tdm>ds1>channel-group mtu)
[Tree] (config>port>tdm>ds3 mtu)
[Tree] (config>port>tdm>e1>channel-group mtu)
[Tree] (config>port>tdm>e3 mtu)

Full Context configure port ethernet mtu
configure port sonet-sdh path mtu
configure port tdm ds1 channel-group mtu
configure port tdm ds3 mtu
configure port tdm e1 channel-group mtu
configure port tdm e3 mtu

Description This command configures the maximum payload MTU size for an Ethernet port, PPP-enabled port or sub-port and Frame Relay-enabled port or subport. The Ethernet port level MTU parameter indirectly defines the largest physical packet the port can transmit or the far-end Ethernet port can receive. Packets that cannot be fragmented at egress and exceed the MTU are discarded.

The value specified for the MTU includes the destination MAC address, source MAC address, the Ethertype or Length field and the complete Ethernet payload. The MTU value does not include the preamble, start of frame delimiter or the trailing CRC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

PoS channels use the MTU to define the largest PPP payload a PoS frame may contain. A significant difference between SONET/SDH PoS channel and Ethernet physical MTU values the overhead considered part of the framing method and the overhead considered to be part of the application using the frame. In Ethernet, the preamble, start of frame delimiter and the CRC are considered part of the framing overhead and not part of the frame payload. For a PoS channel, the HDLC framing overhead is not included in the physical MTU; only the PPP and PPP payload are included. If the port mode or encapsulation type is changed, the MTU assumes the default values of the new mode or encapsulation type.

The **no** form of this command restores the default values.

Default The default MTU value depends on the (sub-)port type, mode and encapsulation and are listed in Table 102:

Table 102 **Default MTU Values**

Type	Mode	Encap Type	Default (Bytes)
10/100, Gig, or 10GigE	Access	null	1514
10/100, Gig, or 10GigE	Access	dot1q	1518
10/100, Gig, or 10GigE	Access	q-in-q	1522
SONET/SDH or TDM	Access	mpls	1506
SONET/SDH or TDM	Access	bcp-null	1518
SONET/SDH or TDM	Access	bcp-dot1q	1522
SONET/SDH or TDM	Access	ipcp	1502
SONET/SDH or TDM	Access	frame-relay	1578
ATM, SONET/SDH or TDM	Access	atm	1524
10/100 or 100FX Ethernet	Network	null	1514
10/100 or 100FX Ethernet	Network	dot1q	1518
SONET/SDH	Network	ppp-auto	1524

Parameters *mtu-bytes* — Sets the maximum allowable size of the MTU, expressed as an integer.

Values

512 to 9212	config>port>ethernet
512 to 9800	config>port>ethernet (for FP4-based connector ports)
512 to 9208	config>port>sonet-sdh>path
512 to 9208	config>port>tdm>ds1>channel-group
512 to 9208	config>port>tdm>ds3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

512 to 9208	config>port>tdm>e1>channel-group
512 to 9208	config>port>tdm>e3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path mtu

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 mtu
- configure port tdm ds1 channel-group mtu
- configure port tdm e1 channel-group mtu
- configure port tdm e3 mtu

All

- configure port ethernet mtu

mtu

Syntax **mtu** *mtu-bytes*
no mtu

Context **[Tree]** (config>service>vprn>ospf>area>if mtu)
[Tree] (config>service>vprn>ospf3>area>if mtu)

Full Context configure service vprn ospf area interface mtu
configure service vprn ospf3 area interface mtu

Description This command configures the OSPF packet size used on this interface. If this parameter is not configured, OSPF derives the MTU value from the MTU configured (default or explicitly) in the following contexts:

config>port>ethernet, **config>port>sonet-sdh>path**, **config>port>tdm>t3-e3**, **config>port>tdm>t1-e1>channel-group**

If this parameter is configured, the smaller value between the value configured here and the MTU configured (default or explicitly) in an above-mentioned contexts is used.

To determine the actual packet size, add 14 bytes for an Ethernet packet and 18 bytes for a tagged Ethernet packet to the size of the OSPF (IP) packet MTU configured in this command.

The **no** form of this command reverts to default value derived from the MTU configured in the **config>port** context.

Default no mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mtu-bytes* — Specifies the MTU to be used by OSPF for this logical interface, in bytes.

Values 512 to 9786

Platforms All

mtu

Syntax **mtu** *value*
no mtu

Context **[Tree]** (config>service>vprn>nat>outside mtu)

Full Context configure service vprn nat outside mtu

Description This command configures the Maximum Transmission Unit (MTU) for downstream traffic flowing through this router (as outside NAT router). The system fragments IP datagrams exceeding the MTU.

The **no** form of the command reverts to the default.

Default no mtu

Parameters *value* — Specifies the MTU for downstream traffic.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mtu

Syntax **mtu** *mtu-size*
no mtu

Context **[Tree]** (config>router>nat>outside mtu)

Full Context configure router nat outside mtu

Description This command configures the MTU for downstream traffic flowing through this router (as outside NAT router). The system fragments IP datagrams exceeding the MTU.

Default no mtu

Parameters *mtu-size* — Specifies the MTU for downstream traffic.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mtu

Syntax **mtu** *mtu*
no mtu

Context **[Tree]** (config>service>ipfix>export-policy>collector mtu)

Full Context configure service ipfix ipfix-export-policy collector mtu

Description This command sets the MTU size of the UDP packet containing IPFIX records destined for the collector node. Multiple records will be stuffed into a single IP packet until stuffing an additional data record would exceed MTU or the internal timer of 250 ms expires.

Default mtu 1500

Parameters *mtu* — Specifies the Maximum Transmission Unit range.

Values 512 to 9212

Platforms All

mtu

Syntax **mtu** *mtu-size*

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy mtu)

Full Context configure service nat syslog syslog-export-policy mtu

Description The command defines the MTU, the maximum size of the IP frame that can be transmitted. The size of the frame includes the syslog message and the IP header. This is an IP-MTU value.

When aggregation is enabled (the **max-tx-delay** command), generation of a syslog frame carrying multiple flow logs is triggered by one of the two events (whichever occurs first):

- Expiry of the max-tx-delay timer
- Exceeding MTU size

Default mtu 1500

Parameters *mtu-size* — Specifies the MTU size in bytes.

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

mtu

Syntax **mtu** *mtu-size*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no mtu

Context [Tree] (config>service>nat>map-domain mtu)

Full Context configure service nat map-domain mtu

Description This command configures the IPv6 MTU in a MAP domain. The configured MTU applies to traffic in the downstream direction, towards the CE. The configured MTU value must be lower than the MTU of the outgoing port for the traffic, which includes L2 overhead.

Default mtu 8686

Parameters *mtu-size* — Specifies the IPMTU size of the translated IPv6 packet.

Values 160 to 8686

Platforms VSR

mtu

Syntax **mtu** *bytes*
no mtu

Context [Tree] (config>router>ospf>area>interface mtu)
[Tree] (config>router>ospf3>area>interface mtu)

Full Context configure router ospf area interface mtu
configure router ospf3 area interface mtu

Description This command configures the OSPF packet size used on this interface. If this parameter is not configured OSPF derives the MTU value from the MTU configured (default or explicitly) in the following contexts:

- **config>port>ethernet**
- **config>port>sonet-sdh>path**
- **config>port>tdm>t3-e3**
- **config>port>tdm>t1-e1>channel-group**

If this parameter is configured, the smaller value between the value configured here and the MTU configured (default or explicitly) in an above-mentioned context is used.

To determine the actual packet size, add 14 bytes for an Ethernet packet and 18 bytes for a tagged Ethernet packet to the size of the OSPF (IP) packet MTU configured in this command.

The **no** form of this command reverts to the default derived from the MTU configured in the **config>port** context.

Default no mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *bytes* — Specifies the MTU to be used by OSPF for this logical interface in bytes.

Values 512 to 9786 in the **config**>**router**>**ospf**>**area**>**interface** context.
1280 to 9786 in the **config**>**router**>**ospf3**>**area**>**interface** context.

Platforms All

mtu

Syntax **mtu** *mtu-size*
no mtu

Context **[Tree]** (config>fwd-path-ext>fpe>srv6>interface-b mtu)

Full Context configure fwd-path-ext fpe srv6 interface-b mtu

Description This command configures the Maximum Transfer Unit (MTU) of interface-b of the SRv6 originating FPE.

The MTU is used to check if an IPv4 service packet should be fragmented and if an IPv6 service packet should be dropped when tunneled over SRv6.

The minimum value is the IPv6 minimum MTU value. The maximum value is set to the FP4 maximum Ethernet port MTU of 9800 minus 14 bytes for Null Ethernet encapsulation.

The **no** form of this command reverts to the default value.

Default mtu 9786

Parameters *mtu-size* — Specifies the MTU size, in bytes.

Values 1280 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

17.375 mtu-over-head

mtu-over-head

Syntax **mtu-over-head** *mtu-value*
no mtu-over-head

Context **[Tree]** (config>service>vprn>pim mtu-over-head)

Full Context configure service vprn pim mtu-over-head

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This commands subtracts the specified value from the MVPN MTU to allow a BIER header to be added without exceeding the network MTU.

Default no mtu-over-head

Parameters *mtu-value* — Specifies the value subtracted from the MVPN MTU.

Values 44, 76, 140, 268, 536

Platforms All

17.376 multi-access

multi-access

Syntax [**no**] **multi-access**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>access multi-access)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>access multi-access)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access multi-access
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access multi-access

Description This command enables access from multiple APs into a per-tenant BD and the associated vRGW (BRG) instance.

The **no** form of this command disables access from multiple APs and limits access from a single AP into per tenant bridge domain (BD) and the associated vRGW (BRG) instance.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.377 multi-active

multi-active

Syntax [**no**] **multi-active**

Context **[Tree]** (config>isa>tunnel-grp multi-active)

Full Context configure isa tunnel-group multi-active

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables configuring multiple active MS-ISA in the tunnel-group. IPsec traffic will be load balanced to configured active MS-ISAs.

Operational notes:

- A shutdown of group and removal of all existing configured tunnels of the tunnel-group are needed before provisioning command “multi-active”.
- If the tunnel-group is admin-up with “multi-active” configured then the configuration of “primary” and “backup” are not allowed.
- The active-mda-number must be =< total number of ISA configured.
  - If active-mda-number is less than total number of ISA configured then the delta number of ISA will become backup ISA.

Default no multi-active

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.378 multi-chassis

multi-chassis

Syntax **multi-chassis**

Context **[Tree]** (config>redundancy multi-chassis)

Full Context configure redundancy multi-chassis

Description Commands in this context configure multi-chassis parameters.

Platforms All

17.379 multi-chassis-redundancy

multi-chassis-redundancy

Syntax **multi-chassis-redundancy** *seconds*
no multi-chassis-redundancy

Context **[Tree]** (config>python>py-pol>cache>minimum-lifetimes multi-chassis-redundancy)

Full Context configure python python-policy cache minimum-lifetimes multi-chassis-redundancy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the minimum lifetime for a cache entry to be synchronized with the MCS peer.

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the multi-chassis redundancy time in second.

Values 1 to 600

Platforms All

17.380 multi-chassis-shunt-id

multi-chassis-shunt-id

Syntax **multi-chassis-shunt-id** *id*
no multi-chassis-shunt-id

Context **[Tree]** (config>service>ies>subscriber-mgmt multi-chassis-shunt-id)
[Tree] (config>service>vprn>subscriber-mgmt multi-chassis-shunt-id)

Full Context configure service ies subscriber-mgmt multi-chassis-shunt-id
configure service vprn subscriber-mgmt multi-chassis-shunt-id

Description This command configures the shunt ID that is used to shunt downstream traffic from a standby node to an active node. Because this ID identifies the traffic service on the standby node, the same ID must be configured per service on each node.This configuration is required for BNG CUPS inter-UPF resiliency shunting, not for non-BNG CUPS shunting. However, when configured, it is also used for shunting non-BNG CUPS sessions in the same service.

The **no** form of the command removes the configuration.

Parameters *id* — Specifies the shunt ID.

Values 1 to 8191

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.381 multi-homed-prefix

multi-homed-prefix

Syntax [**no**] **multi-homed-prefix**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ospf>lfa multi-homed-prefix)

Full Context configure router ospf loopfree-alternates multi-homed-prefix

Description This command enables multi-homed prefix LFA for both OSPF routes (IP FRR) and SR-OSPF node SID tunnels.

This feature makes use of the multi-homed prefix model described in RFC 8518 to compute a backup IP next hop using an alternate ABR or ASBR for external prefixes and to an alternate router owner for local anycast prefixes.

This feature further enhances the multi-homed prefix backup path calculation beyond RFC 8518 with the addition of repair tunnels that make use of a PQ node or a P-Q set to reach the alternate exit ABR or ASBR of external prefixes or the alternate owner router of local anycast prefixes.

The computed IP next-hop based backup path is added to OSPF routes of external /32 prefixes (OSPFv2 routes types 3, 4, 5, and 7) and local /32 anycast prefixes in the RTM if the prefix is not protected by base LFA or if the user set leaf preference value to **all**. The user must enable the **ip-fast-reroute** leaf to have these backup paths programmed into the FIB in data path.

The computed IP next hop or repair tunnel based backup path is also programmed for SR-OSPF node SID tunnels of external /32 prefixes and to /32 prefixes in same area as the computing node S and which are advertised by multiple routers (anycast prefix) in both algorithm 0 and flexible-algorithm numbers.

The **no** form of this command disables multi-homed prefix LFA.

Default no multi-homed-prefix

Platforms All

17.382 multi-homing

multi-homing

Syntax **multi-homing single-active** [**no-esi-label**]
multi-homing all-active
no multi-homing

Context [Tree] (config>service>system>bgp-evpn>eth-seg multi-homing)

Full Context configure service system bgp-evpn ethernet-segment multi-homing

Description This command configures the multi-homing mode for the Ethernet-Segment as **single-active** or all-active multi-homing, as defined in RFC7432.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, the use of **esi-label** is enabled for **all-active** and **single-active** as defined in RFC7432 (for **single-active multi-homing,** the esi-label is used to avoid transient loops).

When **single-active no-esi-label** is specified, the system will not allocate a label for the esi and hence advertise esi label 0 to peers. Even if the esi is configured to not send the esi-label, upon reception of an esi-label from a peer, the PE will always send traffic to that peer using the received esi-label.

Default no multi-homing

Parameters **single-active** — Configures single-active mode for the Ethernet-Segment.

all-active — Configures the system to not send an esi-label for **single-active** mode.

no-esi-label — Configures single-active mode for the Ethernet-Segment.

Platforms All

17.383 multi-instance

multi-instance

Syntax [**no**] **multi-instance**

Context **[Tree]** (config>router>ospf multi-instance)

Full Context configure router ospf multi-instance

Description This command enables OSPF multi-instance RFC 6549, *OSPFv2 Multi-Instance Extensions,* support in the BASE router. This support is enabled per instance and allows flexibility when migrating a particular instance from classic OSPFv2 to a multi-instance OSPFv2.

The **no** form of the command reverts to the default.

Default no multi-instance

Platforms All

17.384 multi-path

multi-path

Syntax **multi-path**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>service>vprn>bgp multi-path)

Full Context configure service vprn bgp multi-path

Description This command configures ECMP multipath parameters to apply to address families that support BGP multipath.

Platforms All

multi-path

Syntax **multi-path**

Context **[Tree]** (config>router>bgp multi-path)

Full Context configure router bgp multi-path

Description This command configures ECMP multipath parameters to apply to address families that support BGP multipath.

Platforms All

multi-path

Syntax [**no**] **multi-path**

Context **[Tree]** (config>fwd-path-ext>fpe multi-path)

Full Context configure fwd-path-ext fpe multi-path

Description This command enables configuration of multipath FPEs that can contain multiple port cross-connect (PXC) ports or LAGs of PXC ports.

The **no** form of the command disables multipath FPE.

Default no multi-path

Platforms All

17.385 multi-path-list

multi-path-list

Syntax **multi-path-list**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>fwd-path-ext>fpe multi-path-list)

Full Context configure fwd-path-ext fpe multi-path-list

Description This command enables the context to configure a multipath FPE list instance, which can contain multiple PXC ports or LAGs of PXC ports.

Platforms All

17.386 multi-service-site

multi-service-site

Syntax [**no**] **multi-service-site** *customer-site-name*

Context [Tree] (config>service>ies>if>sap multi-service-site)
[Tree] (config>service>ies>sub-if>grp-if>sap multi-service-site)
[Tree] (config>service>vprn>sub-if>grp-if>sap multi-service-site)

Full Context configure service ies interface sap multi-service-site
configure service ies subscriber-interface group-interface sap multi-service-site
configure service vprn subscriber-interface group-interface sap multi-service-site

Description This command creates a new customer site or edits an existing customer site with the *customer-site-name* parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When a site is created, it must be assigned to a chassis slot or port. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object generates a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

The **no** form of this command removes the value from the configuration.

Default n/a — Each customer site must be explicitly created.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *customer-site-name* — Each customer site must have a unique name within the context of the customer. If *customer-site-name* already exists for the customer ID, the CLI context changes to that site name for the purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site affects all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing policers and queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing policers and queues relying on that scheduler to be orphaned.

If the *customer-site-name* does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

The maximum number of customer sites defined for the chassis slot has not been met.

The *customer-site-name* is valid.

The **create** keyword is included in the command line syntax (if the system requires it).

When the maximum number of customer sites has been exceeded a configuration error occurs, the command will not execute and the CLI context will not change.

If the *customer-site-name* is invalid, a syntax error occurs, the command will not execute and the CLI context will not change.

Values Valid names consist of any string, up to 32 characters, composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface sap multi-service-site
- configure service ies subscriber-interface group-interface sap multi-service-site

All

- configure service ies interface sap multi-service-site

multi-service-site

Syntax **multi-service-site** *customer-site-name*
no multi-service-site

Context **[Tree]** (config>service>ies>sap multi-service-site)
[Tree] (config>service>vpls>sap multi-service-site)
[Tree] (config>service>vprn>if>sap multi-service-site)

Full Context configure service ies sap multi-service-site
configure service vpls sap multi-service-site
configure service vprn interface sap multi-service-site

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates the SAP with a *customer-site-name*. If the specified *customer-site-name* does not exist in the context of the service customer ID an error occurs and the command is not executed. If *customer-site-name* exists, the current and future defined queues on the SAP (ingress and egress) attempts to use the scheduler hierarchies created within *customer-site-name* as parent schedulers.

This command is mutually exclusive with the SAP ingress and egress scheduler policy commands. If a scheduler policy has been applied to either the ingress or egress nodes on the SAP, the **multi-service-site** command fails without executing. The locally applied scheduler policies must be removed prior to executing the **multi-service-site** command.

The **no** form of this command removes the SAP from any multi-service customer site the SAP belongs to. Removing the site can cause existing or future policers and queues to enter an orphaned state.

Parameters *customer-site-name* — Specifies an existing customer site name, up to 32 characters. If the *customer-site-name* exists and local scheduler policies have not been applied to the SAP, the current and future policers queues defined on the SAP looks for their parent schedulers within the scheduler hierarchies defined in the customer-site-name.

Platforms All

multi-service-site

Syntax **multi-service-site** *customer-site-name*
no multi-service-site *customer-site-name*

Context **[Tree]** (config>service>vprn>if>sap multi-service-site)

Full Context configure service vprn interface sap multi-service-site

Description This command creates a new customer site or edits an existing customer site with the *customer-site-name* parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When a site is created, it must be assigned to a chassis slot or port on the 7750 SR. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object will generate a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *customer-site-name* — Each customer site must have a unique name within the context of the customer. If *customer-site-name* already exists for the customer ID, the CLI context changes to that site name for the purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site will affect all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing policers and queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing policers and queues relying on that scheduler to be orphaned.

If the *customer-site-name* does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

- The maximum number of customer sites defined for the chassis slot has not been met.
- The *customer-site-name* is valid.
- The **create** keyword is included in the command line syntax (if the system requires it).

When the maximum number of customer sites has been exceeded a configuration error occurs; the command will not execute and the CLI context will not change.

If the *customer-site-name* is invalid, a syntax error occurs; the command will not execute and the CLI context will not change.

Values Valid names consist of any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms All

multi-service-site

Syntax **multi-service-site** *customer-site-name*
no multi-service-site

Context **[Tree]** (config>service>apipe>sap multi-service-site)
[Tree] (config>service>cpipe>sap multi-service-site)
[Tree] (config>service>epipe>sap multi-service-site)
[Tree] (config>service>fpipe>sap multi-service-site)
[Tree] (config>service>ipipe>sap multi-service-site)

Full Context configure service apipe sap multi-service-site
configure service cpipe sap multi-service-site
configure service epipe sap multi-service-site
configure service fpipe sap multi-service-site
configure service ipipe sap multi-service-site

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates the SAP with a *customer-site-name*. If the specified *customer-site-name* does not exist in the context of the service customer ID an error occurs and the command will not execute. If *customer-site-name* exists, the current and future defined queues on the SAP (ingress and egress) will attempt to use the scheduler hierarchies created within *customer-site-name* as parent schedulers.

The **no** form of this command removes the SAP from any multi-service customer site the SAP belongs to. Removing the site can cause existing or future queues to enter an orphaned state.

Parameters *customer-site-name* — The customer-site-name must exist in the context of the customer-id defined as the service owner. If customer-site-name exists and local scheduler policies have not been applied to the SAP, the current and future queues defined on the SAP will look for their parent schedulers within the scheduler hierarchies defined on customer-site-name.

Values Any valid customer-site-name created within the context of the customer-id.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap multi-service-site
- configure service fpipe sap multi-service-site

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap multi-service-site

All

- configure service epipe sap multi-service-site
- configure service ipipe sap multi-service-site

multi-service-site

Syntax **multi-service-site** *customer-site-name* [**create**]
no multi-service-site *customer-site-name*

Context **[Tree]** (config>service>cust multi-service-site)

Full Context configure service customer multi-service-site

Description This command creates a new customer site or edits an existing customer site with the *customer-site-name* parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When a site is created, it must be assigned to a chassis slot or port. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object will generate a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

Parameters *customer-site-name* — Specifies the customer site name. Each customer site must have a unique name within the context of the customer. If *customer-site-name* already exists for the customer ID, the CLI context changes to that site name for the purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site will affect all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing policers and queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing policers and queues relying on that scheduler to be orphaned.

If the *customer-site-name* does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

- The maximum number of customer sites defined for the chassis has not been met.
- The *customer-site-name* is valid.
- The **create** keyword is included in the command line syntax (if the system requires).

When the maximum number of customer sites has been exceeded a configuration error occurs; the command will not execute and the CLI context will not change.

If the *customer-site-name* is invalid, a syntax error occurs; the command will not execute and the CLI context will not change.

Values Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

17.387 multi-session-id

multi-session-id

Syntax [**no**] **multi-session-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes multi-session-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa isa-radius-policy acct-include-attributes multi-session-id

Description This command enables the inclusion of the multi-session-id attributes.

The **no** form of the command excludes the multi-session-id attributes.

Default no multi-session-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.388 multi-sub-sap

multi-sub-sap

Syntax **multi-sub-sap** [**subscriber** *limit*]
no multi-sub-sap

Context **[Tree]** (config>subscr-mgmt>msap-policy>sub-sla-mgmt multi-sub-sap)

Full Context configure subscriber-mgmt msap-policy sub-sla-mgmt multi-sub-sap

Description This command defines the maximum number of subscribers (dynamic + static) that can be simultaneously active on an MSAP.

If the limit is reached, a new host is denied access and the corresponding DHCP ACK is dropped.

The **no** form of this command reverts back to the default setting.

Default multi-sub-sap 1

Parameters *limit* — Specifies the maximum number of subscribers allowed.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 1 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

multi-sub-sap

Syntax **multi-sub-sap** *subscriber-limit*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no multi-sub-sap

Context [Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt multi-sub-sap)
[Tree] (config>service>vpls>sap>sub-sla-mgmt multi-sub-sap)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt multi-sub-sap)

Full Context configure service ies subscriber-interface group-interface sap sub-sla-mgmt multi-sub-sap
configure service vpls sap sub-sla-mgmt multi-sub-sap
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt multi-sub-sap

Description This command defines the maximum number of subscribers (dynamic and static) that can be simultaneously active on this SAP.

If the limit is reached, a new host is denied access and the corresponding DHCP ACK is dropped.

The **no** form of this command reverts back to the default setting.

Parameters *subscriber-limit* — Specifies the maximum number of subscribers allowed for this SAP. The operational maximum value may be smaller than the configured value due to equipped hardware dependencies.

Values 2 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.389 multi-topology

multi-topology

Syntax [**no**] **multi-topology**

Context [Tree] (config>service>vprn>isis multi-topology)

Full Context configure service vprn isis multi-topology

Description This command enables IS-IS multi-topology support.

The **no** form of this command disables IS-IS multi-topology.

Default no multi-topology

Platforms All

multi-topology

Syntax [**no**] **multi-topology**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis multi-topology)

Full Context configure router isis multi-topology

Description This command enables IS-IS multi-topology support.

Default no multi-topology

Platforms All

17.390 multi-tunnel-type

multi-tunnel-type

Syntax [**no**] **multi-tunnel-type**

Context [Tree] (config>service>ies>sub-if>grp-if>wlan-gw>mobility multi-tunnel-type)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>mobility multi-tunnel-type)

Full Context configure service ies subscriber-interface group-interface wlan-gw mobility multi-tunnel-type
configure service vprn subscriber-interface group-interface wlan-gw mobility multi-tunnel-type

Description This command enables terminating multiple types of tunnels.

The **no** form of this command disables terminating multiple types of tunnels.

Default no multi-tunnel-type

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

17.391 multicast

multicast

Syntax **multicast**

Context [Tree] (config>service>vprn>sub-if>grp-if>bonding-parameters multicast)
[Tree] (config>service>ies>sub-if>grp-if>bonding-parameters multicast)

Full Context configure service ies subscriber-interface group-interface bonding-parameters multicast
configure service vprn subscriber-interface group-interface bonding-parameters multicast

Description Commands in this context configure multicast in a bonding environment.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multicast

Syntax **multicast** [**key-id** *key-id*] [**version** *version*]
no multicast

Context **[Tree]** (config>system>time>ntp multicast)

Full Context configure system time ntp multicast

Description This command configures NTP the node to transmit multicast packets on the CPM/CCM MGMT port. Broadcast and multicast messages can easily be spoofed; authentication is strongly recommended.

The **no** form of this command removes the multicast address from the configuration.

Parameters *key-id* — Specifies the configured authentication key and authentication type used by this version to transmit NTP packets. If this command is omitted from the configuration, packets are sent unencrypted.

Values 1 to 255

Default None

version — Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all three versions are accepted.

Values 2 to 4

Default 4

Platforms All

17.392 multicast-fast-failover

multicast-fast-failover

Syntax [**no**] **multicast-fast-failover**

Context **[Tree]** (config>router>pim multicast-fast-failover)

Full Context configure router pim multicast-fast-failover

Description This command configures the option to enable Multicast-Only Fast Reroute (MoFRR) functionality for IPv4 PIM-SSM interfaces in the global routing table instance.

The **no** form of this command disables MoFRR for IPv4 PIM-SSM interfaces.

Default no multicast-fast-failover

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.393 multicast-import

multicast-import

Syntax [**no**] **multicast-import**

Context **[Tree]** (config>service>vprn>isis multicast-import)

Full Context configure service vprn isis multicast-import

Description This command enables ISIS to submit routes into the multicast Route Table Manager (RTM).

The **no** form of this command disables the submission of routes into the multicast RTM.

Default no multicast-import

Platforms All

multicast-import

Syntax [**no**] **multicast-import**

Context **[Tree]** (config>service>vprn>ospf multicast-import)
[Tree] (config>service>vprn>ospf3 multicast-import)

Full Context configure service vprn ospf multicast-import
configure service vprn ospf3 multicast-import

Description This command enables the submission of routes into the multicast Route Table Manager (RTM) by OSPF.

The **no** form of this command disables the submission of routes into the multicast RTM.

Default no multicast-import

Platforms All

multicast-import

Syntax [**no**] **multicast-import** [{**both** | **ipv4** | **ipv6**}]

Context **[Tree]** (config>router>isis multicast-import)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router isis multicast-import

Description This command enables the submission of routes into the multicast Route Table Manager (RTM) by IS-IS.

The **no** form of this command disables the submission of routes into the multicast RTM.

Default no multicast-import

Parameters **both** — Allows submission of both IPv4 and IPv6 routes.

ipv4 — Allows submission of IPv4 routes only.

ipv6 — Allows submission of IPv6 routes only.

Platforms All

multicast-import

Syntax [**no**] **multicast-import**

Context **[Tree]** (config>router>ospf multicast-import)
[Tree] (config>router>ospf3 multicast-import)

Full Context configure router ospf multicast-import
configure router ospf3 multicast-import

Description This command enables the submission of routes into the multicast Route Table Manager (RTM) by OSPF.

The **no** form of this command disables the submission of routes into the multicast RTM.

Default no multicast-import

Platforms All

17.394 multicast-info-policy

multicast-info-policy

Syntax **multicast-info-policy** *policy-name* [**create**]
no multicast-info-policy

Context **[Tree]** (config>mcast-management multicast-info-policy)

Full Context configure mcast-management multicast-info-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a multicast information policy. Multicast information policies are used to manage parameters associated with Layer 2 and Layer 3 multicast records. Multiple features use the configured information within the policy. The multicast ingress path manager uses the policy to decide the inactive and active state behavior for each multicast record using the ingress paths to the switch fabric. The system's multicast ECMP join decisions are influenced by the channel information contained within the policy.

Multicast Bundles:

A multicast information policy consists of one or multiple named bundles. Multicast streams are mapped to a bundle based on matching the destination address of the multicast stream to configured channel ranges defined within the bundles. Each policy has a bundle named 'default' that is used when a destination address does not fall within any of the configured channel ranges.

Each bundle has a set of default parameters used as the starting point for multicast channels matching the bundle. The default parameters may be overridden by optional exception parameters defined under each channel range. Further optional parameter overrides are possible under explicit source address contexts within each channel range.

Default Multicast Information Policy

A multicast information policy always exists with the name 'default' and cannot be edited or deleted. The following parameters are contained in the default multicast information policy:

Policy Description:	Default policy, cannot be edited or deleted.
Bundle:	default
Bundle Description:	Default Bundle, cannot be edited or deleted.
Congestion-Priority-Threshold:	4
ECMP-Optimization-Limit-Threshold:	7
Bundle Defaults:	
Administrative Bandwidth:	0 (undefined)
Preference:	0
CAC-Type:	Optional
Bandwidth Activity:	Dynamic with no black-hole rate
Explicit Ingress SF Path:	None (undefined)
Configured Channel Ranges:	None

The default multicast information policy is applied to all VPLS and VPRN services and all routing contexts until an explicitly defined multicast information policy has been mapped.

Explicit Multicast Information Policy Associations

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each VPLS service and each routing context (including VPRN routing contexts) supports an explicit association with an pre-existing multicast information policy. The policy may need to be unique per service or routing context since that each context has its own multicast address space. The same multicast channels may be and most likely be used for completely different multicast streams and applications in each forwarding context.

Interaction with Ingress Multicast Path Management

When ingress multicast path management is enabled on an MDA, the system automatically creates a bandwidth manager context that manages the multicast path bandwidth into the switch fabric used by the ingress ports on the MDA. As routing or snooping protocols generate Layer 2 or Layer 3 multicast FIB records that are populated on the MDA's forwarding plane, they are processed though the multicast information policy that is associated with the service or routing context associated with the record. The policy returns the following information for the record to be used by the ingress bandwidth manager:

- The records administrative bandwidth (0 if undefined)
- Preference level (0 to 7 with 7 being highest)
- Bandwidth activity monitoring setting (use admin bw or dynamic monitoring) If admin bw is indicated, also returns active and inactive thresholds
- Initial switch fabric multicast path (primary or secondary)
- Explicit switch fabric multicast path (primary, secondary, or none)

Interaction with Multicast ECMP Optimization

The multicast information policy is used by the multicast ECMP optimization function to derive each channels administrative bandwidth. The ECMP function tallies all bandwidth information for channels joined and attempts to equalize the load between the various paths to the sender. The multicast information policy returns the following information to the ECMP path manager:

- Administrative bandwidth (0 if undefined)
- Preference (0 to 7 with 7 the highest preference value)

Default multicast-info-policy "default"

Parameters *policy-name* — Identifies the name of the policy to be either created or edited. Each multicast information policy must be uniquely named within the system. Names of up to 32 ASCII characters are supported with the normal character restrictions.

create — The create keyword is required if creating a new multicast information policy when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the multicast information policy name already exists.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multicast-info-policy

Syntax **multicast-info-policy** *policy-name*
no multicast-info-policy

Context **[Tree]** (config>service>ies multicast-info-policy)
[Tree] (config>service>vpls multicast-info-policy)
[Tree] (config>service>vprn multicast-info-policy)
[Tree] (config>router multicast-info-policy)

Full Context configure router multicast-info-policy
configure service ies multicast-info-policy
configure service vpls multicast-info-policy
configure service vprn multicast-info-policy

Description This command overrides the default multicast information policy on a service or routing context. When the policy association is changed, all multicast channels in the service or routing context must be reevaluated.

If a multicast information policy is not explicitly associated with the service or routing context, the default multicast information policy is used when ingress multicast path management is enabled.

While a multicast information policy is associated with a service or routing context, the policy cannot be deleted from the system.

The **no** form of the command removes an explicit multicast information policy from the service or routing context and restores the default multicast information policy.

Parameters *policy-name* — Specifies the policy name, up to 32 characters. The *policy-name* parameter is required and specifies an existing multicast information policy that should be associated with the service or routing context.

Platforms All

17.395 multicast-leave-sync-propagation

multicast-leave-sync-propagation

Syntax **multicast-leave-sync-propagation** *time*

Context **[Tree]** (config>service>system>bgp-evpn multicast-leave-sync-propagation)

Full Context configure service system bgp-evpn multicast-leave-sync-propagation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the additional amount of time that the system waits before removing a multicast state that was synchronized in an Ethernet Segment via Multicast Join or Leave Synch routes. This value represents a delta corresponding to the time it takes for a BGP advertisement to propagate to ES peers.

The node triggering the route computes the maximum response time as the product of the locally configured values, Last Member Query Count and Last Member Query Interval (this value is taken from the **config**>**service**>**vpls**>**sap**>**igmp-snooping**>**last-member-query-interval** or **config**>**service**>**vpls**>**spoke-sdp**>**igmp-snooping**>**last-member-query-interval** commands depending on the Ethernet Segment being used), and adds the delta value to the Maximum Response Time. Increasing the Maximum Response Time by this value can help minimize the churn of removing and recreating the state on the node.

The maximum response time value should be configured consistently in all ES peers. For example, in a scenario where a maximum response time of five seconds is advertised by PE-A and there is a delay of four seconds in the BGP propagation to PE-B, the timer could already expire on PE-A while PE-B is still in LMQ time and can still receive joins (which would recreate state in A after a join synch route from B). To minimize this situation, adding an extra delta timer on PE-A, reduces the potential churn of PE-A removing and recreating the state.

Default multicast-leave-sync-propagation 5

Parameters *time* — Specifies the multicast leave sync propagation delay time, in seconds.

Values 0 to 300

Default 5

Platforms All

17.396 multicast-lsp

multicast-lsp

Syntax **multicast-lsp** *lsp-name*
no multicast-lsp

Context **[Tree]** (config>service>sdp>class-forwarding multicast-lsp)

Full Context configure service sdp class-forwarding multicast-lsp

Description This command specifies the RSVP or static LSP in this SDP to use to forward VPLS multicast and broadcast packets. The LSP name must exist and must have been associated with this SDP using the command **config**>**service**>**sdp**>**lsp**. In the absence of an explicit configuration by the user, the default LSP is used.

Default no multicast-lsp — traffic mapped to default-lsp *name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *lsp-name* — Specifies the RSVP or static LSP to use.

Platforms All

17.397 multicast-network-domain

multicast-network-domain

Syntax **multicast-network-domain** *multicast-network-domain*
no multicast-network-domain

Context **[Tree]** (config>service>ies>if multicast-network-domain)

Full Context configure service ies interface multicast-network-domain

Description This command is used to enable efficient multicast replication over a spoke SDP. Multicast traffic is copied to only a subset of network interfaces that may be used as egress for a spoke SDP. A network domain is defined by associating multiple interfaces to a logical group that may participate in multicast replication for a spoke SDP.

The **no** form of command disables efficient multicast replication to a network domain for a spoke SDP and traffic is replicated to all forwarding complexes.

Default no multicast-network-domain

Platforms All

17.398 multicast-policer

multicast-policer

Syntax **multicast-policer** *policer-id* [**fp-redirect-group**]
no multicast-policer

Context **[Tree]** (config>qos>sap-ingress>fc multicast-policer)

Full Context configure qos sap-ingress fc multicast-policer

Description Within a **sap-ingress** QoS policy forwarding class context, the **multicast-policer** command is used to map packets that match the forwarding class and are considered multicast in nature to the specified policer-id. The specified policer-id must already exist within the **sap-ingress** QoS policy. While the system is determining the forwarding class of a packet, it is also looking up its forwarding destination based on the ingress service type and the service

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

instance forwarding records. Two basic types of services support multicast packets: routed services (IES and VPRN) and L2 multipoint services (VPLS, I-VPLS, and B-VPLS). For the routed service types, a multicast packet is destined to an IPv4 or IPv6 multicast address. For the L2 multipoint services, a multicast packet is a packet destined to a multicast MAC address (multicast bit set in the destination MAC address but not the ff:ff:ff:ff:ff:ff broadcast address). The VPLS services also support two other multipoint forwarding types (broadcast and unknown), which are considered separate from the multicast forwarding type.

If ingress forwarding logic has resolved a packet to the multicast forwarding type within the forwarding class, it will be mapped to either an ingress multipoint queue (using the **multicast** *queue-id* or **multicast** *queue-id* **group** *ingress-queue-group* commands) or an ingress policer (**multicast-policer** *policer-id*). The **multicast** and **multicast-policer** commands within the forwarding class context are mutually exclusive. By default, the multicast forwarding type is mapped to the SAP ingress default multipoint queue. If the **multicast-policer** *policer-id* command is executed, any previous policer mapping or queue mapping for the multicast forwarding type within the forwarding class is overridden if the policer mapping is successful.

A policer defined within the **sap-ingress** policy is not actually created on an ingress SAP or a subscriber using an **sla-profile** where the policy is applied until at least one forwarding type (unicast, broadcast, unknown, or multicast) from one of the forwarding classes is mapped to the policer. If insufficient policer resources exist to create the policer for a SAP or subscriber or multiservice site, or ingress policing is not supported on the port associated with the SAP or subscriber or multiservice site, the initial forwarding class forwarding type mapping will fail.

The **multicast-policer** command is ignored for instances of the policer applied to SAPs subscribers or multiservice site where broadcast packets are not supported.

When the multicast forwarding type within a forwarding class is mapped to a policer, the multicast packets classified to the subclasses within the forwarding class are also mapped to the policer.

The **no** form of this command is used to restore the mapping of the multicast forwarding type within the forwarding class to the default multipoint queue. If all forwarding class forwarding types had been removed from the default multipoint queue, the queue will not exist on the SAPs subscribers or multiservice site associated with the QoS policy, and the **no multicast-policer** command will cause the system to attempt to create the default multipoint queue on each object. If the system cannot create the queue on each instance, the **no multicast-policer** command will fail and the multicast forwarding type within the forwarding class will continue its mapping to the existing *policer-id*. If the **no multicast-policer** command results in a policer without any current mappings, the policer will be removed from the SAPs and subscribers associated with the QoS policy. All statistics associated with the policer on each SAP and subscriber will be lost.

Parameters *policer-id* — When the forwarding class **multicast-policer** command is executed, a valid *policer-id* must be specified. The parameter *policer-id* references a *policer-id* that has already been created within the **sap-ingress** QoS policy.

Values 1 to 63

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fp-redirect-group — Redirects a forwarding class to a forwarding plane queue-group as specified in a SAP QoS policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

17.399 multicast-queue

multicast-queue

Syntax **multicast-queue** *queue-id* [**group** *queue-group-name*]
no multicast-queue

Context **[Tree]** (config>qos>sap-ingress>fc multicast-queue)

Full Context configure qos sap-ingress fc multicast-queue

Description This command overrides the default multicast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all multicast traffic on a SAP using this policy is forwarded using the *queue-id*.

The multicast forwarding type includes the **unknown** unicast forwarding type and the **broadcast** forwarding type unless each is explicitly defined to a different multipoint queue. When the unknown and broadcast forwarding types are left as default, they will track the defined queue for the multicast forwarding type.

The **no** form of this command sets the multicast forwarding type *queue-id* back to the default queue for the forwarding class. If the **broadcast** and **unknown** forwarding types were not explicitly defined to a multipoint queue, they will also be set back to the default multipoint queue (queue 11).

Parameters *queue-id* — The *queue-id* parameter specified must be an existing, multipoint queue defined in the config>qos>sap-ingress context.

Values Any valid multipoint queue-ID in the policy including 2 through 32.

Default 11

group *queue-group-name* — This optional parameter is used to redirect the forwarding type within the forwarding class to the specified queue-id within the queue-group-name. When the policy is applied, all packets matching the forwarding class and forwarding type will be redirected to the queue within the specified queue group. The *queue-group-name* are configured in the **config>qos>queue-group-templates** egress and ingress contexts.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multicast-queue

Syntax **multicast-queue** *queue-id*
no multicast-queue

Context **[Tree]** (config>qos>network-queue>fc multicast-queue)

Full Context configure qos network-queue fc multicast-queue

Description This command overrides the default multicast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all multicast traffic using this policy is forwarded using the *queue-id*.

The multicast forwarding type includes the **unknown** unicast forwarding type and the **broadcast** forwarding type, unless each is explicitly defined to a different multipoint queue. When the unknown and broadcast forwarding types are left as default, they will track the defined queue for the multicast forwarding type.

The **no** form of this command sets the multicast forwarding type *queue-id* back to the default queue for the forwarding class. If the **broadcast** and **unknown** forwarding types were not explicitly defined to a multipoint queue, they will also be set back to the default multipoint queue (queue 11).

Resource Utilization

When a multipoint queue is created and at least one forwarding class is mapped to the queue using the **multipoint-queue** command, a single ingress multipoint hardware queue is created per instance of the applied network-queue policy, using the queue-policy command at the ingress network FP level. Multipoint queues are not created at egress and the multipoint queues defined in the network-queue policy are ignored when the policy is applied to an egress port.

Parameters *queue-id* — Specifies any valid multipoint queue-ID in the policy. The *queue-id* parameter specified must be an existing, multipoint queue defined in the **config>qos>network-queue>queue** context.

Values 1 to 16

Default 11

Platforms All

multicast-queue

Syntax **multicast-queue** *queue-id*

Context **[Tree]** (config>qos>shared-queue>fc multicast-queue)

Full Context configure qos shared-queue fc multicast-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the multicast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all multicast traffic on a SAP using this policy is forwarded using the *queue-id*.

The multicast forwarding type includes the **unknown** unicast forwarding type and the **broadcast** forwarding type unless each is explicitly defined to a different multipoint queue. When the unknown and broadcast forwarding types are left as default, they will track the defined queue for the multicast forwarding type.

The **no** form of this command sets the multicast forwarding type *queue-id* back to the default queue for the forwarding class. If the **broadcast** and **unknown** forwarding types were not explicitly defined to a multipoint queue, they will also be set back to the default multipoint queue (queue 11).

Parameters *queue-id* — The *queue-id* parameter specified must be an existing, multipoint queue defined in the **config>qos>sap-ingress** context policer-output-queues profile. For the 7950 XRS, this is not configurable in the policer-output-queues profile.

Values 9 to 16

Default 11

Platforms All

17.400 multicast-redirection

multicast-redirection

Syntax **multicast-redirection** [**fwd-service** *service-id*] *ip-int-name*
no multicast-redirection

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action multicast-redirection)

Full Context configure router policy-options policy-statement entry action multicast-redirection

Description This command configures the interface where to redirect IGMP multicast traffic to.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

multicast-redirection

Syntax **multicast-redirection** [**fwd-service** *service-id*] *ip-int-name*
no multicast-redirection

Context **[Tree]** (config>router>policy-options>policy-statement>default-action multicast-redirection)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router policy-options policy-statement default-action multicast-redirection

Description This command enables a redirection under a filtering policy. The filtering policy in this case becomes a redirection policy and it is defined under the **router>policy-option** hierarchy.

After the redirection policy is applied to the subscriber, all IGMP messages will be processed per subscriber host before they get redirected to the referenced interface (and possibly service). However, multicast traffic will not be replicated directly per subscriber host but instead it will be forwarded on the interface that is referenced in the redirection policy. The redirected interface must have IGMP enabled.

Currently all traffic is redirected and there is no ability to selectively redirect multicast traffic based on match conditions (such as, multicast-groups, source IP address of IGMP messages). Multicast redirection is supported between VPRN services and also between interfaces within the Global Routing Context. Multicast redirection is not supported between the VPRN services and the Global Routing Context. Multicast redirection is supported in the wholesale/retail VPRN context.

Note: Redirecting from a VPRN instance to the GRT is not supported. Redirecting from a VPRN to a different VPRN is supported and redirecting from an IES to another IES is also supported.

Default no multicast-redirection

Parameters **fwd-service** *service-id* — Specifies the service to which traffic should be redirected. This option is applied only in the VPRN context. It is possible to redirect the multicast group into another service instance routing interface.

ip-int-name — specifies the alternate interface to which IGMP messages are redirected.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.401 multicast-senders

multicast-senders

Syntax **multicast-senders** {**auto** | **always** | **never**}
no multicast-senders

Context **[Tree]** (config>service>vprn>pim>if multicast-senders)

Full Context configure service vprn pim interface multicast-senders

Description This command configures the way subnet matching is done for incoming data packets on this interface. An IP multicast sender is an user entity to be authenticated in a receiving host.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **auto** — Subnet matching is automatically performed for incoming data packets on this interface.

always — Subnet matching is always performed for incoming data packets on this interface.

never — Subnet matching is never performed for incoming data packets on this interface.

Platforms All

multicast-senders

Syntax **multicast-senders** {**auto** | **always** | **never**}
no multicast-senders

Context **[Tree]** (config>router>pim>interface multicast-senders)

Full Context configure router pim interface multicast-senders

Description This command configures how traffic from directly-attached multicast sources should be treated on broadcast interfaces. It can also be used to treat all traffic received on an interface as traffic coming from a directly-attached multicast source. This is particularly useful if a multicast source is connected to a point-to-point or unnumbered interface.

The **no** form of this command reverts to the default value.

Default multicast-senders auto

Parameters **auto** — Specifies that, on broadcast interfaces, the forwarding plane performs subnet-match check on multicast packets received on the interface to determine if the packet is from a directly-attached source. On unnumbered/point-to-point interfaces, all traffic is implicitly treated as coming from a remote source.

always — Treats all traffic received on the interface as coming from a directly-attached multicast source.

never — Specifies that, on broadcast interfaces, traffic from directly-attached multicast sources will not be forwarded; however, traffic from a remote source will still be forwarded if there is a multicast state for it. On unnumbered/point-to-point interfaces, it means that all traffic received on that interface must not be forwarded.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.402 multicast-service

multicast-service

Syntax **multicast-service** *service-id*
no multicast-service

Context **[Tree]** (config>service>ies>video-interface multicast-service)
[Tree] (config>service>vpls>video-interface multicast-service)
[Tree] (config>service>vprn>video-interface multicast-service)

Full Context configure service ies video-interface multicast-service
configure service vpls video-interface multicast-service
configure service vprn video-interface multicast-service

Description This command adds a multicast service association to the video interface. This parameter is not required on the video interface when the service carries both unicast and multicast traffic.

When multicast and unicast are carried in separate service instances, the operator can set this parameter on the unicast video interface to form an association with the multicast service when replies need to be sent in the multicast service instance.

When multicast and unicast are carried in separate services when a downstream device (such as a DSLAM) can perform a service cross connect between the services and performs multicast replication.

The **no** form of the command removes the multicast service association.

Default none

Parameters *service-id* — The service ID of the associated multicast service.

Values

service-id:	1 to 2147483647
svc-name:	64 characters maximum

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

17.403 multicast6-fast-failover

multicast6-fast-failover

Syntax [**no**] **multicast6-fast-failover**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>pim multicast6-fast-failover)

Full Context configure router pim multicast6-fast-failover

Description This command enables Multicast-Only Fast Reroute (MoFRR) functionality for IPv6 PIM-SSM interfaces in the global routing table instance.

The **no** form of this command disables MoFRR for IPv6 PIM-SSM interfaces.

Default no multicast6-fast-failover

Platforms All

17.404 multicastclient

multicastclient

Syntax **multicastclient** [**authenticate**]
no multicastclient

Context [Tree] (config>system>time>ntp multicastclient)

Full Context configure system time ntp multicastclient

Description This command configures the node to receive multicast NTP messages on the CPM MGMT port. If **multicastclient** is not configured, received NTP multicast traffic will be ignored. Use the **show** command to view the state of the configuration.

The **no** construct of this message removes the multicast client for the specified interface from the configuration.

Parameters **authenticate** — Specifies to make authentication a requirement (optional). If authentication is required, the authentication key-id received must have been configured in the **authentication-key** command, and that key-id type and key value must also match.

Platforms All

17.405 multiclass

multiclass

Syntax **multiclass** *count*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no multiclass

Context **[Tree]** (config>port>ml-bundle>mlpp multiclass)

Full Context configure port multilink-bundle mlppp multiclass

Description This command enables multi-class MLPPP as defined by RFC 2686*, The Multi-Class Extension to Multi-Link PPP*, on a MLPPP bundle (including MLPPP bundle protection groups) with 2, 3 or 4 classes. For multiclass MLPPP bundles with a non-zero count, the class index takes valid values from 0 to one less than the maximum number of classes inclusive. For example a 4-class MLPPP bundle has 4 classes with indexes 0, 1, 2, and 3. A bundle must be shutdown with no links for this value to be changed.

Entries are created and deleted by the system depending on the number of classes being used by a given MLPPP bundle.

The **no** form of this command disables multi-class MLPPP.

Default multiclass 4

Parameters *count* — Specifies the number of classes in a MLPPP bundle.

Values 2 to 4

Platforms 7450 ESS, 7750 SR-7/12/12e

17.406 multihop

multihop

Syntax **multihop** *ttl-value*
no multihop

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy multihop)

Full Context configure subscriber-mgmt bgp-peering-policy multihop

Description This command configures the time to live (TTL) value entered in the IP header of packets sent to an EBGP peer multiple hops away.

This parameter is meaningful only when configuring EBGP peers. It is ignored if set for an IBGP peer.

The **no** form of this command is used to convey to the BGP instance that the EBGP peers are directly connected.

The **no** form of this command reverts to default values.

Default multihop 1 (EBGP peers are directly connected)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multihop 64 (IBGP)

Parameters *ttl-value* — Specifies the TTL value, expressed as a decimal integer.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

multihop

Syntax **multihop** *ttl-value*
no multihop

Context **[Tree]** (config>service>vprn>bgp multihop)
[Tree] (config>service>vprn>bgp>group multihop)
[Tree] (config>service>vprn>bgp>group>neighbor multihop)

Full Context configure service vprn bgp group multihop
configure service vprn bgp group neighbor multihop
configure service vprn bgp multihop

Description This command configures the time to live (TTL) value entered in the IP header of packets sent to an EBGP peer multiple hops away.

This parameter is meaningful only when configuring EBGP peers. It is ignored if set for an IBGP peer.

The **no** form of this command is used to convey to the BGP instance that the EBGP peers are directly connected.

The **no** form of this command reverts to default values.

Default **multihop** 1 (EBGP peers are directly connected)

multihop 64 (IBGP)

Parameters *ttl-value* — Specifies the TTL value, expressed as a decimal integer.

Values 1 to 255

Platforms All

multihop

Syntax **multihop** *ttl-value*
no multihop

Context **[Tree]** (config>router>bgp multihop)
[Tree] (config>router>bgp>group multihop)
[Tree] (config>router>bgp>group>neighbor multihop)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bgp group multihop
configure router bgp group neighbor multihop
configure router bgp multihop

Description This command configures the time to live (TTL) value entered in the IP header of packets sent to an EBGP peer multiple hops away.

The **no** form of this command is used to convey to the BGP instance that the EBGP peers are directly connected.

The **no** form of this command used at the global level reverts to default.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default multihop 1 — EBGP peers are directly connected.

multihop 64 — IBGP

Parameters *ttl-value* — Specifies the TTL value, expressed as a decimal integer.

Values 1 to 255

Platforms All

17.407 multilink-bundle

multilink-bundle

Syntax [**no**] **multilink-bundle**

Context **[Tree]** (config>port multilink-bundle)

Full Context configure port multilink-bundle

Description This command creates the context to configure bundle properties for this bundle port.

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.408 multipath-eligible

multipath-eligible

Syntax [**no**] **multipath-eligible**

Context **[Tree]** (config>service>vprn>bgp>group multipath-eligible)
[Tree] (config>service>vprn>bgp>neighbor multipath-eligible)

Full Context configure service vprn bgp group multipath-eligible
configure service vprn bgp neighbor multipath-eligible

Description This command specifies that a BGP neighbor or the set of BGP neighbors in a peer group should be part of a selective multipath set. Selective multipaths are only supported by the ipv4, label-ipv4, ipv6, and label-ipv6 address families.

If no candidate multipath route for an IP prefix came from a multipath-eligible peer, multipaths are selected without further constraints.

If the best route for an IP prefix is received from a neighbor marked as multipath-eligible, other routes for the same prefix are not eligible to be used as multipaths unless they also came from peers marked as multipath-eligible.

If the best route for an IP prefix did not come from a multipath-eligible peer but there is at least one candidate multipath route for the same prefix from a multipath-eligible peer, multipath is not used.

The **no** form of this command marks a neighbor or group as non-multipath eligible. The effect of this depends on whether other neighbors and groups are marked as multipath eligible.

Default no multipath-eligible

Platforms All

multipath-eligible

Syntax [**no**] **multipath-eligible**

Context **[Tree]** (config>router>bgp>group multipath-eligible)
[Tree] (config>router>bgp>group>neighbor multipath-eligible)

Full Context configure router bgp group multipath-eligible
configure router bgp group neighbor multipath-eligible

Description This command specifies that a BGP neighbor or the set of BGP neighbors in a peer group should be part of a selective multipath set. Selective multipaths are only supported by the **ipv4**, **label-ipv4**, **ipv6**, and **label-ipv6** address families.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If no candidate multipath route for an IP prefix came from a multipath-eligible peer then multipaths are selected without further constraints.

If the best route for an IP prefix is received from a neighbor marked as multipath-eligible, then other routes for the same prefix are not eligible to be used as multipaths unless they also came from peers marked as multipath-eligible.

If the best route for an IP prefix did not come from a multipath-eligible peer but there is at least one candidate multipath route for the same prefix from a multipath-eligible peer then multipath is not used.

The **no** form of this command marks a neighbor or group as non-multipath eligible. The effect of this depends on whether other neighbors and groups are marked as multipath eligible.

Default no multipath-eligible

Platforms All

17.409 multiple-option

multiple-option

Syntax **multiple-option** {**true** | **false**}

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match multiple-option)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match multiple-option)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match multiple-option
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match multiple-option

Description This command configures the multiple-option match condition.

The **no** form of this command reverts to the default.

Parameters **true** — Enables checking the number of IP options in the IP header.

false — Disables checking the number of IP options in the IP header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multiple-option

Syntax **multiple-option** {**true** | **false**}
no multiple-option

Context **[Tree]** (config>filter>ip-filter>entry>match multiple-option)

Full Context configure filter ip-filter entry match multiple-option

Description This command configures matching packets that contain one or more than one option fields in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the number of option fields in the IP header as a match criterion.

Default no multiple-option

Parameters **true** — Specifies matching on IP packets that contain more than one option field in the header.

false — Specifies matching on IP packets that do not contain multiple option fields present in the header.

Platforms All

multiple-option

Syntax **multiple-option** {**true** | **false**}
no multiple-option

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match multiple-option)

Full Context configure system security cpm-filter ip-filter entry match multiple-option

Description This command configures matching packets that contain more than one option fields in the IP header as an IP filter match criterion.

The **no** form of this command removes the checking of the number of option fields in the IP header as a match criterion.

Default no multiple-option

Parameters **true** — Specifies matching on IP packets that contain more than one option field in the header.

false — Specifies matching on IP packets that do not contain multiple option fields present in the header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.410 multiplier

multiplier

Syntax **multiplier** [*multiplier*]
no multiplier

Context **[Tree]** (config>lag>bfd>family multiplier)

Full Context configure lag bfd family multiplier

Description This command specifies the detect multiplier used for a micro-BFD session over the associated LAG links. If a BFD control packet is not received for a period of multiplier X receive-interval then the session is declared down.

The **no** form of this command removes multiplier from the configuration.

Default multiplier 3

Parameters *multiplier* — Specifies the multiplier value.

Values 3 to 20

Platforms All

multiplier

Syntax **multiplier** *multiplier-value*
no multiplier

Context **[Tree]** (config>port>ethernet>eth-cfm>mep>csf-enable multiplier)
[Tree] (cfg>lag>eth-cfm>mep>csf multiplier)

Full Context configure lag eth-cfm mep csf-enable multiplier
configure port ethernet eth-cfm mep csf-enable multiplier

Description This command configures the multiplier used for timing out the CSF.

Parameters *multiplier-value* — Specifies the multiplier used for timing out CSF.

Values 0.0, 2.0 to 30.0

Default 3.5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multiplier

Syntax **multiplier** *multiplier-value*
no multiplier

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>ies>if>sap>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>csf-enable multiplier)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep multiplier)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>vpls>sap>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>vprn>if>sap>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>csf-enable multiplier)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>csf-enable multiplier)

Full Context configure service epipe sap eth-cfm mep csf-enable multiplier
configure service epipe spoke-sdp eth-cfm mep csf-enable multiplier
configure service ies interface sap eth-cfm mep csf-enable multiplier
configure service ies interface spoke-sdp eth-cfm mep csf-enable multiplier
configure service ies subscriber-interface group-interface sap eth-cfm csf-enable multiplier
configure service ies subscriber-interface group-interface sap eth-cfm mep multiplier
configure service vpls mesh-sdp eth-cfm mep csf-enable multiplier
configure service vpls sap eth-cfm mep csf-enable multiplier
configure service vpls spoke-sdp eth-cfm mep csf-enable multiplier
configure service vprn interface sap eth-cfm mep csf-enable multiplier
configure service vprn interface spoke-sdp eth-cfm mep csf-enable multiplier
configure service vprn subscriber-interface group-interface sap eth-cfm mep csf-enable multiplier

Description This command configures the multiplication factor applied to the receive time that is used to clear the CSF condition.

The **no** form of this command disables the multiplier used for timing out CSF.

Default multiplier 3.5

Parameters *multiplier-value* — Specifies the multiplication factor applied to the receive time that is used to clear the CSF condition. This value can only be configured in increments of 0.5. Configuring a value of 0.0 means that the CSF condition is cleared only when C-DCI is received.

Values 0.0, 2.0 to 30.0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep csf-enable multiplier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls spoke-sdp eth-cfm mep csf-enable multiplier
- configure service vprn interface spoke-sdp eth-cfm mep csf-enable multiplier
- configure service epipe sap eth-cfm mep csf-enable multiplier
- configure service ies interface sap eth-cfm mep csf-enable multiplier
- configure service epipe spoke-sdp eth-cfm mep csf-enable multiplier
- configure service vpls mesh-sdp eth-cfm mep csf-enable multiplier
- configure service ies interface spoke-sdp eth-cfm mep csf-enable multiplier
- configure service vpls sap eth-cfm mep csf-enable multiplier
- configure service vprn interface sap eth-cfm mep csf-enable multiplier

multiplier

Syntax **multiplier** *multiplier*
no multiplier

Context **[Tree]** (config>router>bfd>bfd-template multiplier)

Full Context configure router bfd bfd-template multiplier

Description This command specifies the detect multiplier for a BFD session. If a BFD control packet is not received for a period of *multiplier* x *receive-interval* (the parameter value of the **receive-interval** command), the session is declared down.

The **no** form of this command reverts to the default value.

Default multiplier 3

Parameters *multiplier* — Specifies the multiplier.

Values 3 to 20

Default 3

Platforms All

multiplier

Syntax **multiplier** *sample-window-durations*

Context **[Tree]** (config>test-oam>link-meas>template>asw multiplier)

Full Context configure test-oam link-measurement measurement-template aggregate-sample-window multiplier

Description This command configures the number of sample windows in an aggregate sample window.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default multiplier 12

Parameters *sample-window-durations* — Specifies the number of sample windows

Values 1 to 12

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

multiplier

Syntax **multiplier** *interval-durations*

Context **[Tree]** (config>test-oam>link-meas>template>sw multiplier)

Full Context configure test-oam link-measurement measurement-template sample-window multiplier

Description This command configures the number of probe results that should be in the sample window. For example, a multiplier of 10 and an interval of 5 results in 50 probes being transmitted from an individual sample window. Consequently, 50 probe results are expected within the 50 second duration that the sample window is “In-progress”.

Default multiplier 10

Parameters *interval-durations* — Specifies the number of intervals in a sample window.

Values 1 to 900

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

17.411 multipliers

multipliers

Syntax **multipliers sample-multiplier** *num1* **adjust-multiplier** *num2*
no multipliers

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth multipliers)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth multipliers)

Full Context configure router mpls lsp auto-bandwidth multipliers
configure router mpls lsp-template auto-bandwidth multipliers

Description This command configures the sample-multiplier and adjust-multiplier applicable to one particular LSP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The sample-multiplier configures the number of collection intervals between measurements of the number of bytes that have been transmitted on the LSP. The byte counts include the layer 2 encapsulation of MPLS packets and represent traffic of all forwarding classes and priorities (in-profile vs, out-of-profile) belonging to the LSP. The router calculates the average data rate in each sample interval. The maximum of this average data rate over multiple sample intervals is the measured bandwidth input to the auto-bandwidth adjustment algorithms.

The adjust-multiplier is the number of collection intervals between periodic evaluations by the ingress LER about whether to adjust the LSP bandwidth. The router keeps track of the maximum average data rate of each LSP since the last reset of the adjust-count.

The adjust-multiplier is not allowed to be set to a value less than the sample-multiplier. It is recommended that the adjust-multiplier be a multiple of the sample-multiplier.

The **no** form of this command instructs the system to take the value from the **auto-bandwidth-multipliers** command.

Default no multipliers

Parameters *number1* — Specifies the number of collection intervals in a sample interval.

Values 1 to 511

number2 — Specifies the number of collection intervals in an adjust interval.

Values 1 to 16383

Platforms All

17.412 multistream-spmsi

multistream-spmsi

Syntax **multistream-spmsi** *index* [**create**]
no multistream-spmsi *index*

Context **[Tree]** (config>service>vprn>mvpn>pt>selective multistream-spmsi)

Full Context configure service vprn mvpn provider-tunnel selective multistream-spmsi

Description This command creates a multi-stream S-PMSI policy. Having multiple multi-stream S-PMSIs per MVPN creates a link list, in which the first match (lowest index) will be chosen for a multicast stream. The number of configured multi-stream S-PMSIs cannot exceed the configured maximum S-PMSI for a given MVPN.

Parameters *index* — Specifies the index number.

Values 1 to 1024

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.413 mvpn

mvpn

Syntax **mvpn**

Context **[Tree]** (config>service>vprn mvpn)

Full Context configure service vprn mvpn

Description Commands in this context configure MVPN-related parameters for the IP VPN.

Platforms All

mvpn

Syntax [**no**] **mvpn**

Context **[Tree]** (config>router>ldp>import-pmsi-routes mvpn)

Full Context configure router ldp import-pmsi-routes mvpn

Description This command specifies that the SR OS is to cache inter-as MVPN PMSI AD routes for option B.

The **no** form of this command disables caching of MVPN PMSI AD routes. The default is disabled, however when an upgrade from a software load that does not supports this command is performed, this command will be enabled after the upgrade.

This command is not enabled if the user is using an older config file.

Default no mvpn

Platforms All

mvpn

Syntax [**no**] **mvpn**

Context **[Tree]** (config>router>gtm mvpn)

Full Context configure router gtm mvpn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables and disables the context to configure MVPN-related parameters.

Platforms All

17.414 mvpn-ipv4

mvpn-ipv4

Syntax **mvpn-ipv4 send** *send-limit* **receive** [**none**]
mvpn-ipv4 send *send-limit*
no mvpn-ipv4

Context **[Tree]** (config>router>bgp>add-paths mvpn-ipv4)
[Tree] (config>router>bgp>group>add-paths mvpn-ipv4)
[Tree] (config>router>bgp>group>neighbor>add-paths mvpn-ipv4)

Full Context configure router bgp add-paths mvpn-ipv4
configure router bgp group add-paths mvpn-ipv4
configure router bgp group neighbor add-paths mvpn-ipv4

Description This command configures the add-paths capability for multicast VPN IPv4 routes. By default, add-paths is not enabled for multicast VPN IPv4 routes.

The maximum number of paths per multicast VPN IPv4 NRLI to send is the configured *send-limit*, which is a mandatory parameter. The capability to receive multiple multicast paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command, receive capability is enabled by default. The **none** option disables the receive capability.

The **no** form of this command disables add-paths support for multicast VPN IPv4 routes, causing sessions established using add-paths for multicast VPN IPv4 to go down and come back up without the add-paths capability.

Default no mvpn-ipv4

Parameters *send-limit* — Specifies the maximum number of paths per multicast VPN IPv4 NRLI that are allowed to be advertised to add-paths peers. The actual number of advertised routes may be less. If the value is **none**, the router does not negotiate the send capability with respect to multicast VPN IPv4 AFI/SAFI.

Default 1 to 16, none

receive — Specifies that the router negotiates to receive multiple routes per multicast VPN IPv4 NRLI.

none — Specifies that the router does not negotiate to receive multiple routes per multicast VPN IPv4 NRLI.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

17.415 mvpn-ipv6

mvpn-ipv6

Syntax **mvpn-ipv6 send** *send-limit* **receive** [**none**]
mvpn-ipv6 send *send-limit*
no mvpn-ipv6

Context **[Tree]** (config>router>bgp>add-paths mvpn-ipv6)
[Tree] (config>router>bgp>group>add-paths mvpn-ipv6)
[Tree] (config>router>bgp>group>neighbor>add-paths mvpn-ipv6)

Full Context configure router bgp add-paths mvpn-ipv6
configure router bgp group add-paths mvpn-ipv6
configure router bgp group neighbor add-paths mvpn-ipv6

Description This command configures the add-paths capability for multicast VPN IPv6 routes. By default, add-paths is not enabled for multicast VPN IPv6 routes.

The maximum number of paths per multicast VPN IPv6 NRLI to send is the configured *send-limit*, which is a mandatory parameter. The capability to receive multiple multicast VPN paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command, receive capability is enabled by default. The **none** option disables the receive capability.

The **no** form of this command disables add-paths support for multicast VPN IPv6 routes, causing sessions established using add-paths for multicast VPN IPv6 to go down and come back up without the add-paths capability.

Default no mvpn-ipv6

Parameters *send-limit* — Specifies the maximum number of paths per multicast VPN IPv6 NRLI that are allowed to be advertised to add-paths peers. The actual number of advertised routes may be less. If the value is **none**, the router does not negotiate the send capability with respect to multicast VPN IPv6 AFI/SAFI.

receive — Specifies that the router negotiates to receive multiple routes per multicast VPN IPv6 NRLI.

none — Specifies that the router does not negotiate to receive multiple routes per multicast VPN IPv6 NRLI.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.416 mvpn-no-export

mvpn-no-export

Syntax [**no**] **mvpn-no-export**

Context **[Tree]** (config>router>ldp>import-pmsi-routes mvpn-no-export)

Full Context configure router ldp import-pmsi-routes mvpn-no-export

Description This command specifies that the SR OS is to cache intra-as MVPN PMSI AD routes for option B.

The **no** form of this command disables caching of intra-as MVPN PMSI AD routes. The default is disabled, however when an upgrade from a software load that does not supports this command is performed, this command will be enabled after the upgrade.

This command is enabled if the user is using an older config file.

Default no mvpn-no-export

17.417 mvpn-rtcache

mvpn-rtcache

Syntax **mvpn-rtcache** [**group** *grp-ip-address*] [**peer** *ip-address*]
no mvpn-rtcache

Context **[Tree]** (debug>router>pim mvpn-rtcache)

Full Context debug router pim mvpn-rtcache

Description This command enables debugging for the PIM MVPN route cache.

The **no** form of this command disables debugging for the PIM MVPN route cache.

Parameters *grp-ip-address* — Debugs information associated with the specified group.

Values multicast group address (ipv4, ipv6) or zero

peer-ip-address — Debugs information associated with the specified peer.

Values peer address (ipv4, ipv6)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.418 mvpn-type

mvpn-type

Syntax **mvpn-type** {**1** | **2** | **3** | **4** | **5** | **6** | **7**}
no mvpn-type

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from mvpn-type)

Full Context configure router policy-options policy-statement entry from mvpn-type

Description This command allows match on ng-MVPN BGP route type when the policy is used for VRF-import/VRF-export/BGP global export policy. The policy will only be applied to multicast routes.

The **no** form of this command disables **mvpn-type** in the policy evaluation.

Default no mvpn-type

Parameters *1* | *2* | *3* | *4* | *5* | *6* | *7* — BGP MVPN route-type as per RFC 6514.

Platforms All

17.419 mvpn-vrf-import-subtype-new

mvpn-vrf-import-subtype-new

Syntax [**no**] **mvpn-vrf-import-subtype-new**

Context **[Tree]** (config>router>bgp mvpn-vrf-import-subtype-new)

Full Context configure router bgp mvpn-vrf-import-subtype-new

Description When enabled, the type/subtype in advertised routes is encoded as 0x010b.

The **no** form of this command (the default) encodes the type/subtype as 0x010a (to preserve backwards compatibility).

Default no mvpn-vrf-import-subtype-new

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

17.420 mvr

mvr

Syntax **mvr**

Context **[Tree]** (config>service>vpls>igmp-snooping mvr)
[Tree] (config>service>vpls>mld-snooping mvr)
[Tree] (config>service>vpls>sap>igmp-snooping mvr)
[Tree] (config>service>vpls>sap>mld-snooping mvr)

Full Context configure service vpls igmp-snooping mvr
configure service vpls mld-snooping mvr
configure service vpls sap igmp-snooping mvr
configure service vpls sap mld-snooping mvr

Description Commands in this context configure Multicast VPLS Registration (MVR) parameters.

Platforms All

mvr

Syntax **mvr**

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp mvr)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mvr

Description Commands in this context configure Multicast VPLS Registration (MVR) parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

17.421 mvrp

mvrp

Syntax **mvrp**

Context **[Tree]** (config>service>vpls>mrp mvrp)
[Tree] (config>service>vpls>sap>mrp mvrp)

Full Context configure service vpls mrp mvrp
configure service vpls sap mrp mvrp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This object consolidates the MVRP attributes. MVRP is only supported initially in the management VPLS so the object is not supported under BVPLS, IVPLS or regular VPLS not marked with the m-vpls tag.

Platforms All

17.422 mvrp-control

mvrp-control

Syntax [**no**] **mvrp-control**

Context **[Tree]** (config>service>vpls>vpls-group mvrp-control)

Full Context configure service vpls vpls-group mvrp-control

Description This command enables MVRP control in the VPLS instances instantiated using the templates for the specified vpls-group. That means the flooding FDB will be created empty and will be populated with endpoints whenever MVRP receives a declaration and a registration on a specific endpoint. Also the VLAN ID associated by the control VPLS with the instantiated VPLS will be declared on service activation by MVRP on all virtual MVRP ports in the control VPLS. Service activation takes place when at least one other SAP is provisioned and brought up under the data VPLS. This is usually a customer facing SAP or a SAP leading outside of the MVRP controlled domain.

The **no** form of this command disallows MVRP control over this VPLS. The VPLS will be created with a regular FDB and will become as a result active upon creation time. Command change is allowed only when the related vpls-group is in shutdown state.

Default no mvrp-control

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18 n Commands

18.1 n391dte

n391dte

Syntax **n391dte** *intervals*
no n391dte

Context **[Tree]** (config>port>multi-link-bundle>mlfr>frame-relay n391dte)
[Tree] (config>port>sonet-sdh>path>frame-relay n391dte)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay n391dte)
[Tree] (config>port>tdm>ds3>frame-relay n391dte)
[Tree] (config>port>tdm>e1>channel-group>frame-relay n391dte)
[Tree] (config>port>tdm>e3>frame-relay n391dte)

Full Context configure port multilink-bundle mlfr frame-relay n391dte
configure port sonet-sdh path frame-relay n391dte
configure port tdm ds1 channel-group frame-relay n391dte
configure port tdm ds3 frame-relay n391dte
configure port tdm e1 channel-group frame-relay n391dte
configure port tdm e3 frame-relay n391dte

Description This command sets the DTE full status polling interval for the Frame Relay Local Management Interface (LMI). The number specifies the frequency at which inquiries expect a full status report.

The **no** form of this command returns the **n391dte** counter to the default value.

Default n391dte 6

Parameters *intervals* — The number of exchanges to be done before requesting a full-status report. A value of 1 specifies to receive full-status messages only.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay n391dte

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlfr frame-relay n391dte

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group frame-relay n391dte

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port tdm e3 frame-relay n391dte
- configure port tdm ds3 frame-relay n391dte
- configure port tdm e1 channel-group frame-relay n391dte

18.2 n392dce

n392dce

Syntax **n392dce** *threshold*
no n392dce

Context **[Tree]** (config>port>multi-link-bundle>mlfr>frame-relay n392dce)
[Tree] (config>port>sonet-sdh>path>frame-relay n392dce)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay n392dce)
[Tree] (config>port>tdm>ds3>frame-relay n392dce)
[Tree] (config>port>tdm>e1>channel-group>frame-relay n392dce)
[Tree] (config>port>tdm>e3>frame-relay n392dce)

Full Context configure port multilink-bundle mlfr frame-relay n392dce
configure port sonet-sdh path frame-relay n392dce
configure port tdm ds1 channel-group frame-relay n392dce
configure port tdm ds3 frame-relay n392dce
configure port tdm e1 channel-group frame-relay n392dce
configure port tdm e3 frame-relay n392dce

Description This command sets the DCE error threshold for the Frame Relay Local Management Interface (LMI).

The threshold specifies the number of errors needed to bring down a link.

The **no** form of this command returns the **n392dce** counter to the default value.

Default n392dce 3

Parameters *threshold* — Specifies the number of errors that will place the channel in an operationally down state.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay n392dce

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlfr frame-relay n392dce

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group frame-relay n392dce
- configure port tdm e3 frame-relay n392dce
- configure port tdm ds3 frame-relay n392dce
- configure port tdm e1 channel-group frame-relay n392dce

18.3 n392dte

n392dte

Syntax **n392dte** *threshold*
no n392dte

Context **[Tree]** (config>port>multi-link-bundle>mlfr>frame-relay n392dte)
[Tree] (config>port>sonet-sdh>path>frame-relay n392dte)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay n392dte)
[Tree] (config>port>tdm>ds3>frame-relay n392dte)
[Tree] (config>port>tdm>e1>channel-group>frame-relay n392dte)
[Tree] (config>port>tdm>e3>frame-relay n392dte)

Full Context configure port multilink-bundle mlfr frame-relay n392dte
configure port sonet-sdh path frame-relay n392dte
configure port tdm ds1 channel-group frame-relay n392dte
configure port tdm ds3 frame-relay n392dte
configure port tdm e1 channel-group frame-relay n392dte
configure port tdm e3 frame-relay n392dte

Description This command sets the DTE error threshold for the Frame Relay Local Management Interface (LMI).

The count specifies the number of errors needed to bring down a link.

The **no** form of this command returns the **n392dte** counter to the default value.

Default n392dte 3

Parameters *threshold* — Specifies the number of errors that will place the path or channel in an operationally down state.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay n392dte

7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port multilink-bundle mlfr frame-relay n392dte

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group frame-relay n392dte
- configure port tdm e1 channel-group frame-relay n392dte
- configure port tdm ds3 frame-relay n392dte
- configure port tdm e3 frame-relay n392dte

18.4 n393

n393

Syntax **n393** [*value*]
no n393

Context **[Tree]** (config>port>ethernet>elmi n393)

Full Context configure port ethernet elmi n393

Description This command configures the monitored count of consecutive errors.

Parameters *value* — Specifies the monitored count of consecutive errors.

Values 2 to 10

Platforms All

18.5 n393dce

n393dce

Syntax **n393dce** *count*
no n393dce

Context **[Tree]** (config>port>multi-link-bundle>mlfr>frame-relay n393dce)
[Tree] (config>port>sonet-sdh>path>frame-relay n393dce)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay n393dce)
[Tree] (config>port>tdm>ds3>frame-relay n393dce)
[Tree] (config>port>tdm>e1>channel-group>frame-relay n393dce)
[Tree] (config>port>tdm>e3>frame-relay n393dce)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port multilink-bundle mlfr frame-relay n393dce
configure port sonet-sdh path frame-relay n393dce
configure port tdm ds1 channel-group frame-relay n393dce
configure port tdm ds3 frame-relay n393dce
configure port tdm e1 channel-group frame-relay n393dce
configure port tdm e3 frame-relay n393dce

Description This command sets the DCE monitored event count for the Frame Relay Local Management Interface (LMI).

The **no** form of this command returns the **n393dce** counter to the default value.

Default n393dce 4

Parameters *count* — Specifies the diagnostic window used to verify link integrity on the DCE interface.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay n393dce

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle mlfr frame-relay n393dce

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group frame-relay n393dce
- configure port tdm e3 frame-relay n393dce
- configure port tdm ds3 frame-relay n393dce
- configure port tdm ds1 channel-group frame-relay n393dce

18.6 n393dte

n393dte

Syntax **n393dte** *count*
no n393dte

Context **[Tree]** (config>port>ml-bundle>mlfr>frame-relay n393dte)

Full Context configure port multilink-bundle mlfr frame-relay n393dte

Description This command configures the DTE monitored event count for the LMI.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the diagnostic window used to verify link integrity on the DTE interface.

Values 1 to 10

Platforms 7450 ESS, 7750 SR-7/12/12e

n393dte

Syntax **n393dte** *count*
no n393dte

Context **[Tree]** (config>port>sonet-sdh>path>frame-relay n393dte)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay n393dte)
[Tree] (config>port>tdm>ds3>frame-relay n393dte)
[Tree] (config>port>tdm>e1>channel-group>frame-relay n393dte)
[Tree] (config>port>tdm>e3>frame-relay n393dte)

Full Context configure port sonet-sdh path frame-relay n393dte
configure port tdm ds1 channel-group frame-relay n393dte
configure port tdm ds3 frame-relay n393dte
configure port tdm e1 channel-group frame-relay n393dte
configure port tdm e3 frame-relay n393dte

Description This command sets the DTE monitored event count for the Frame Relay Local Management Interface (LMI).

The **no** form of this command returns the **n393dte** counter to the default value.

Default n393dte 4

Parameters *count* — Specifies the diagnostic window used to verify link integrity on the DTE interface.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay n393dte

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds1 channel-group frame-relay n393dte
- configure port tdm e3 frame-relay n393dte
- configure port tdm e1 channel-group frame-relay n393dte
- configure port tdm ds3 frame-relay n393dte

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.7 nak-non-matching-subnet

nak-non-matching-subnet

Syntax [**no**] **nak-non-matching-subnet**

Context **[Tree]** (config>router>dhcp>server>pool nak-non-matching-subnet)
[Tree] (config>service>vprn>dhcp>server>pool nak-non-matching-subnet)

Full Context configure router dhcp local-dhcp-server pool nak-non-matching-subnet
configure service vprn dhcp local-dhcp-server pool nak-non-matching-subnet

Description When this command is enabled, if the local DHCPv4 server receives a DHCP request with option 50 (client requested a previously allocated message as described in section 3.2 of RFC 2131, *Dynamic Host Configuration Protocol*) and the address allocation algorithm uses a pool that does not have option 50, the system returns a DHCP NAK. Otherwise, the system drops the DHCP packet.

The **no** form of this command reverts to the default.

Default no nak-non-matching-subnet

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.8 name

name

Syntax **name** *header-name*

Context **[Tree]** (config>app-assure>group>http-enrich>field name)

Full Context configure application-assurance group http-enrich field name

Description This command configures an HTTP enrichment template field header name.

The **no** form of this command removes the http enrichment template field header name from the configuration.

Parameters *header-name* — Specifies the name of the http enrichment policy that is inserted before the actual field name (e.g. x-subId = subscriberID).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name

Syntax **name** *system-name*
no name

Context **[Tree]** (config>system name)

Full Context configure system name

Description This command creates a system name string for the device.

For example, system-name parameter ALA-1 for the **name** command configures the device name as ALA-1.

```
ABC>config>system# name "ALA-1"
ALA-1>config>system#
```

Only one system name can be configured. If multiple system names are configured, the last one encountered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default no name

Parameters *system-name* — Specifies the system name as a character string. The string may be up to 64 characters. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

name

Syntax **name** *name-string* **value** *value-string*
name *name-string* **address** *ip-address*
name *name-string* **number** *value-number*
no name *name-string*

Context **[Tree]** (config>router>policy-options>global-variables name)
[Tree] (config>router>policy-options>policy-statement>entry>from>policy-variables name)

Full Context configure router policy-options global-variables name
configure router policy-options policy-statement entry from policy-variables name

Description This command allows operators to configure routing policies that are often reused across BGP peers of a common type (transit, peer, customer, and so on). Using global variables allows an operator to have a single variable that is consistent across all peers of a type, while retaining the flexibility to reference different policy functions (prefixes, prefix-lists, community lists, and so on) with unique names.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Depending on the parameter referenced, the correct type should be specified as follows:

- value-string: **as-path, as-path-group, community, prefix-list, damping**
- ip-address: **next-hop**
- value-number: **aigp-metric, as-path-prepend, local-preference, metric, origin, origin-validation, preference, tag, type**

The **no** form of this command removes the global variable.

Parameters *name-string* — Specifies the name of the global variable, with the variable delimited by at-signs (@) at the beginning and the end of the name. Allowed values are any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

value-string — The value of the policy variable. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

value-number — Specifies the numerical value of the policy variable.

Values 0 to 4294967295

ip-address — Specifies the IP address of the policy variable.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x [-interface]
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

18.9 named-pool-policy

named-pool-policy

Syntax **named-pool-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy named-pool-policy)

Full Context configure qos copy named-pool-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command copies an existing **named-pool-policy** to another **named-pool-policy**. The **copy** command is a configuration level maintenance tool used to create new entries using an existing profile ID. If **overwrite** is not specified, an error occurs if the destination policy exists.

Parameters *src-name* — Specifies the existing source **named-pool-policy**, up to 32 characters, from which the **copy** command attempts to copy.

dst-name — Specifies the destination **named-pool-policy** *dst-name*, up to 32 characters, to which the copy command attempts to copy.

overwrite — Use this parameter when the **named-pool-policy** *dst-name* already exists. If it does, everything in the existing destination **named-pool-policy** *dst-name* is completely overwritten with the contents of the **named-pool-policy** *src-name*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI use {overwrite}; destination named-pool-policy
"test" exists.
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

18.10 nas-identifier

nas-identifier

Syntax [**no**] **nas-identifier**

Context **[Tree]** (config>aaa>l2tp-acct-plcy>include-radius-attribute nas-identifier)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute nas-identifier

Description This command enables the generation of the nas-identifier RADIUS attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-identifier

Syntax [**no**] **nas-identifier**

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute nas-identifier)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute nas-identifier)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute nas-identifier
configure subscriber-mgmt authentication-policy include-radius-attribute nas-identifier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the generation of the **nas-identifier** RADIUS attribute.

The **no** form of this command disables the generation of the **nas-identifier** RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-identifier

Syntax [**no**] **nas-identifier**

Context **[Tree]** (config>ipsec>rad-acct-plcy>include nas-identifier)
[Tree] (config>ipsec>rad-auth-plcy>include nas-identifier)

Full Context configure ipsec radius-accounting-policy include-radius-attribute nas-identifier
configure ipsec radius-authentication-policy include-radius-attribute nas-identifier

Description This command enables the generation of the **nas-identifier** RADIUS attribute.

Default no nas-identifier

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nas-identifier

Syntax [**no**] **nas-identifier**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes nas-identifier)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes nas-identifier)

Full Context configure aaa isa-radius-policy acct-include-attributes nas-identifier
configure aaa isa-radius-policy auth-include-attributes nas-identifier

Description This command enables the inclusion of the NAS-Identifier attributes.

The **no** form of the command excludes NAS-Identifier attributes.

Default no nas-identifier

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.11 nas-ip-addr

nas-ip-addr

Syntax [**no**] **nas-ip-addr**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>rad-acct-plcy>include nas-ip-addr)
[Tree] (config>ipsec>rad-auth-plcy>include nas-ip-addr)

Full Context configure ipsec radius-accounting-policy include-radius-attribute nas-ip-addr
configure ipsec radius-authentication-policy include-radius-attribute nas-ip-addr

Description This command enables the generation of the NAS IP address attribute.

Default no nas-ip-addr

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.12 nas-ip-address

nas-ip-address

Syntax [**no**] **nas-ip-address**

Context [Tree] (config>aaa>isa-radius-plcy>acct-include-attributes nas-ip-address)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes nas-ip-address)

Full Context configure aaa isa-radius-policy acct-include-attributes nas-ip-address
configure aaa isa-radius-policy auth-include-attributes nas-ip-address

Description This command enables the generation of the NAS-IP-Address RADIUS attribute.

Default no nas-ip-address

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.13 nas-ip-address-origin

nas-ip-address-origin

Syntax **nas-ip-address-origin** {**isa-ip** | **system-ip**}
no nas-ip-address-origin

Context [Tree] (config>aaa>isa-radius-plcy nas-ip-address-origin)

Full Context configure aaa isa-radius-policy nas-ip-address-origin

Description This command specifies the RADIUS NAS-IP-Address attribute.

The **no** form of the command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default nas-ip-address-origin system-ip

Parameters **system-ip** — Specifies that the value of the object TIMETRA-VRTR-MIB::vRiaIpAddress.1.1.1 is used.

isa-ip — Specifies that a value in the range specified by tmnxRadIsaPlcySrvSrcAddrStart and tmnxRadIsaPlcySrvSrcAddrEnd is used that corresponds to the ISA card that transmits the Access-Request packet or the Accounting-Request packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.14 nas-port

nas-port

Syntax [**no**] **nas-port** *binary-spec*

Context **[Tree]** (config>aaa>l2tp-acct-plcy>include-radius-attribute nas-port)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute nas-port

Description This command enables the generation of the nas-port RADIUS attribute. Enter decimal representation of a 32-bit string that indicates the port information. This 32-bit string can be compiled based on different information from the port (data types). Using number-of-bits data-type syntax indicates the number of bits from the 32 bits that are used for the specific data type. These data types can be combined up to 32 bits. In between the different data types 0s and 1s as bits can be added.

The **no** form of this command disables the **nas-port** configuration.

Parameters *binary-spec* — Specifies the NAS port attribute.

Values		
binary-spec	<bit-specification> <binary-spec>	
bit-specification	0 | 1 | <bit-origin>	
bit-origin	*<number-of-bits><origin>	
number-of-bits	1 to 32	
origin	s | m | p | o | i | v | c	
	s	slot number
	m	MDA number
	p	port number, lag-id, pw-id or pxc-id
	o	outer VLAN ID
	i	inner VLAN ID
	v	ATM VPI

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	c	ATM VCI or PXC subport (subport a = 0, subport b = 1)

Output The following output shows an example.

Sample

```
*12o*12i00*2s*2m*2p => oooo oooo oooo iiii iiii iiii 00ss mmpp
If outer vlan = 0 & inner vlan = 1 & slot = 3 & mda = 1 & port = 1
=>  0000 0000 0000 0000 0000 0001 0011 0101 => nas-port = 309
```

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port

Syntax **nas-port** *binary-spec*
no nas-port

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute nas-port)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute nas-port)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute nas-port
configure subscriber-mgmt authentication-policy include-radius-attribute nas-port

Description This command enables the generation of the **nas-port** RADIUS attribute. You enter decimal representation of a 32-bit string that indicates your port information. This 32-bit string can be compiled based on different information from the port (data types). By using syntax number-of-bits data-type you indicate how many bits from the 32 bits are used for the specific data type. These data types can be combined up to 32 bits. In between the different data types 0's and/or 1's as bits can be added.

The **no** form of this command disables the **nas-port** configuration.

Parameters *binary-spec* — Specifies the NAS port attribute.

Values		
binary-spec	<bit-specification> <binary-spec>	
bit-specification	0 | 1 | <bit-origin>	
bit-origin	*<number-of-bits><origin>	
number-of-bits	1 to 32	
origin	s | m | p | o | i | v | c	
	s	slot number
	m	MDA number
	p	port number, lag-id, pw-id or pxc-id
	o	outer VLAN ID
	i	inner VLAN ID
	v	ATM VPI

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

c	ATM VCI or PXC subport (subport a = 0, subport b = 1)

Output The following is an example of binary spec information.

Sample

```
*12o*12i00*2s*2m*2p => oooo oooo oooo iiii iiii iiii 00ss mmpp
If outer vlan = 0 & inner vlan = 1 & slot = 3 & mda = 1 & port = 1
=>  0000 0000 0000 0000 0000 0001 0011 0101 => nas-port = 309
```

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port

Syntax **nas-port** *binary-spec*
no nas-port

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp nas-port)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp nas-port)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp nas-port
configure subscriber-mgmt diameter-application-policy nasreq include-avp nas-port

Description This command specifies the format of the 32 bit string used as value for the Nas-Port AVP.

Parameters *binary-spec* — Specifies the NAS-Port AVP format.

Values

binary-spec	<bit-specification> <binary-spec>
bit-specification	0 | 1 | <bit-origin>
bit-origin	*<number-of-bits><origin>
number-of-bits	1 to 32
origin	s | m | p | o | i | v | c
	s — slot number
	m — MDA number
	p — port number, lag-id, pw-id or pxc-id
	o — outer VLAN ID
	i — inner VLAN ID
	v — ATM VPI
	c — ATM VCI or PXC subport (subport a = 0, subport b = 1)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nas-port

Syntax [**no**] **nas-port**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes nas-port)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes nas-port)

Full Context configure aaa isa-radius-policy acct-include-attributes nas-port
configure aaa isa-radius-policy auth-include-attributes nas-port

Description This command enables the generation of the NAS-Port RADIUS attribute.

Default no nas-port

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.15 nas-port-id

nas-port-id

Syntax **nas-port-id**
nas-port-id [**prefix-string** *string*] [**suffix** *suffix-option*]
no nas-port-id

Context **[Tree]** (config>aaa>l2tp-acct-plcy>include-radius-attribute nas-port-id)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute nas-port-id

Description This command enables the generation of the nas-port-id RADIUS attribute. Optionally, the value of this attribute (the SAP ID) can be prefixed by a fixed string and suffixed by the circuit-id or the remote-id of the client connection. If a suffix is configured, but no corresponding data is available, the suffix used is 0/0/0/0/0/0.

The **no** form of this command reverts to the default.

Parameters *string* — Specifies that a user configurable string be added to the RADIUS NAS port attribute, up to 8 characters.

suffix-option — Specifies the suffix type to be added to the RADIUS NAS port attribute.

Values circuit-id, remote-id

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port-id

Syntax [**no**] **nas-port-id** [**prefix-string** *string*] [**suffix** *suffix-option*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>auth-policy>include-radius-attribute nas-port-id)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute nas-port-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute nas-port-id
configure subscriber-mgmt authentication-policy include-radius-attribute nas-port-id

Description This command enables the generation of the **nas-port-id** RADIUS attribute. Optionally, the value of this attribute (the SAP ID) can be prefixed by a fixed string and suffixed by the circuit-id or the remote-id of the client connection. If a suffix is configured, but no corresponding data is available, the suffix used is 0/0/0/0/0/0.

The **no** form of this command disables the generation of the **nas-port-id** RADIUS attribute.

Parameters *string* — Specifies that a user configurable string is added to the RADIUS NAS port attribute, up to 8 characters.

suffix-option — Specifies the suffix type to be added to the RADIUS NAS port attribute.

Values circuit-id, remote-id

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port-id

Syntax **nas-port-id** [**prefix-type** {**none** | **user-string**}] [**prefix-string** *prefix-string*] [**suffix-type** {**circuit-id** | **none** | **remote-id** | **user-string**}] [**suffix-string** *suffix-string*]
no nas-port-id

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gx>include-avp nas-port-id)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp nas-port-id)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp nas-port-id
configure subscriber-mgmt diameter-application-policy nasreq include-avp nas-port-id

Description This command includes the Nas-Port-Id AVP.

Parameters **prefix-type** — Specifies what type of prefix is added to the NAS-Port-Id attribute if included in Nas-Port-Id AVP messages.

Values **none** — No prefix is added

user-string — Specifies the user configurable string to be added as prefix to the NAS-Port-Id attribute if included in DIAMETER Gx messages

prefix-string — Specifies the user configurable string up to 8 characters, to be added as a prefix.

suffix-type} — Specifies the suffix to be added to the NAS-Port attribute NAS-Port AVP.

Values **none** — No suffix is added

circuit-id — Specifies the circuit-id is added as suffix-string

remote-id — Specifies the remote-id is added as suffix-string

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

user-string — Specifies a user configurable suffix-string is added

suffix-string — Specifies the string, up to 64 characters, to be added as suffix.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port-id

Syntax [**no**] **nas-port-id**

Context **[Tree]** (config>ipsec>rad-acct-plcy>include nas-port-id)
[Tree] (config>ipsec>rad-auth-plcy>include nas-port-id)

Full Context configure ipsec radius-accounting-policy include-radius-attribute nas-port-id
configure ipsec radius-authentication-policy include-radius-attribute nas-port-id

Description This command enables the generation of the **nas-port-id** RADIUS attribute. Optionally, the value of this attribute (the SAP-id) can be prefixed by a fixed string and suffixed by the circuit-id or the remote-id of the client connection. If a suffix is configured, but no corresponding data is available, the suffix used will be 0/0/0/0/0/0.

Default no nas-port-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nas-port-id

Syntax [**no**] **nas-port-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes nas-port-id)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes nas-port-id)

Full Context configure aaa isa-radius-policy acct-include-attributes nas-port-id
configure aaa isa-radius-policy auth-include-attributes nas-port-id

Description This command enables the generation of the nas-port-id RADIUS attribute. Optionally, the value of this attribute (the SAP-id) can be prefixed by a fixed string and suffixed by the circuit-id or the remote-id of the client connection. If a suffix is configured, but no corresponding data is available, the suffix used will be 0/0/0/0/0/0.

Default no nas-port-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.16 nas-port-type

nas-port-type

Syntax **nas-port-type**
nas-port-type [*type*]
no nas-port-type

Context **[Tree]** (config>aaa>l2tp-acct-plcy>include-radius-attribute nas-port-type)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute nas-port-type

Description This command enables the generation of the nas-port-type RADIUS attribute. If set to **nas-port-type**, the following values are sent: 32 (null-encap), 33 (dot1q), 34 (qinq), 15 (DHCP hosts). The **nas-port-type** can also be set as a specified value, with an integer from 0 to 255.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies an enumerated integer that specifies the value that is put in the RADIUS nas-port-type attribute.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port-type

Syntax **nas-port-type**
nas-port-type *value*
no nas-port-type

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute nas-port-type)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute nas-port-type)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute nas-port-type
configure subscriber-mgmt authentication-policy include-radius-attribute nas-port-type

Description This command enables the generation of the **nas-port-type** RADIUS attribute. If set to **nas-port-type**, the following values are sent: 32 (null-encap), 33 (dot1q), 34 (qinq), 15 (DHCP hosts). The **nas-port-type** can also be set as a specified value, with an integer from 0 to 255.

The **no** form of this command disables the generation of the **nas-port-type** RADIUS attribute

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies an enumerated integer that specifies the value that is put in the RADIUS nas-port-type attribute.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port-type

Syntax **nas-port-type**
nas-port-type [*type*]
no nas-port-type

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp nas-port-type)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp nas-port-type)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp nas-port-type
configure subscriber-mgmt diameter-application-policy nasreq include-avp nas-port-type

Description This command includes the Nas-Port-Type AVP.

Parameters **none** — Specifies values as defined in RFC 2865, Remote Authentication Dial In User Service (RADIUS), and RFC 4603, Additional Values for the NAS-Port-Type Attribute.

type — Specifies the integer value for the Nas-Port-Type AVP.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nas-port-type

Syntax [**no**] **nas-port-type**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes nas-port-type)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes nas-port-type)

Full Context configure aaa isa-radius-policy acct-include-attributes nas-port-type
configure aaa isa-radius-policy auth-include-attributes nas-port-type

Description This command enables the generation of the NAS-Port-Type RADIUS attribute.

The **no** form of the command disables the generation.

Default no nas-port-type

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.17 nasreq

nasreq

Syntax **nasreq**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy nasreq)

Full Context configure subscriber-mgmt diameter-application-policy nasreq

Description Commands in this context configure NASREQ application-specific attributes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.18 nat

nat

Syntax **nat**

Context **[Tree]** (config>isa>wlan-gw-group nat)

Full Context configure isa wlan-gw-group nat

Description Commands in this context configure NAT parameters under wlan-gw-group.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat

Syntax [**no**] **nat**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync nat)

Full Context configure redundancy multi-chassis peer sync nat

Description Commands in this context synchronize NAT groups.

The **no** form of this command disables the feature.

Default nat

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat

Syntax [**no**] **nat**

Context **[Tree]** (config>service>vprn nat)
[Tree] (config>router nat)

Full Context configure router nat
configure service vprn nat

Description This command enables a NAT instance for the specified router or service.

The **no** form of this command disables the NAT instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat

Syntax **nat**

Context **[Tree]** (config>li>li-source nat)

Full Context configure li li-source nat

Description Commands in this context configure LI NAT parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat

Syntax **nat**

Context **[Tree]** (config>subscriber-mgmt>pfcp-association nat)

Full Context configure subscriber-mgmt pfcp-association nat

Description Commands in this context configure NAT groups for BNG CUPS PFCP association (see the **nat-group** command in the **config**>**subscriber-mgmt**>**pfcp-association**>**nat** context).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat

Syntax **nat** [**nat-policy** *nat-policy-name*]

Context **[Tree]** (config>filter>ip-filter>entry>action nat)

Full Context configure filter ip-filter entry action nat

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables NAT traffic diversion based on IPv4 filters (LSN44) or IPv6 filters (DS-Lite, NAT64). The filter contains a matching condition based on any combination of the 5 tuple. Traffic is diverted to NAT based on such defined matching condition. Filter fields outside of the 5 tuples are not valid and it will be ignored in filter based traffic diversion to NAT.

The pool selection for the outside IP address and port along with other mapping characteristics can be specified by the means on the NAT policy.

Parameters *nat-type* — Specifies the NAT type.

nat-policy-name — Specifies the NAT policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat

Syntax **nat nat-type** *nat-type* [**nat-policy** *nat-policy-name*]

Context **[Tree]** (config>filter>ipv6-filter>entry>action nat)

Full Context configure filter ipv6-filter entry action nat

Description This command enables NAT traffic diversion based on IPv4 filters (LSN44) or IPv6 filters (DS-Lite, NAT64). The filter contains a matching condition based on any combination of the 5 tuple. Traffic is diverted to NAT based on such defined matching condition. Filter fields outside of the 5 tuples are not valid and it will be ignored in filter based traffic diversion to NAT.

The pool selection for the outside IP address and port along with other mapping characteristics can be specified by the means on the NAT policy.

Parameters *nat-type* — Specifies the NAT type.

nat-policy-name — Specifies the NAT policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat

Syntax **nat**

Context **[Tree]** (admin nat)

Full Context admin nat

Description This command performs NAT operations.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.19 nat-access-mode

nat-access-mode

Syntax **nat-access-mode** *access-mode*

Context **[Tree]** (config>subscr-mgmt>sub-profile nat-access-mode)

Full Context configure subscriber-mgmt sub-profile nat-access-mode

Description This command configures the NAT access mode.

Access mode in L2-Aware NAT environment is a reflection of supported home set up (bridged or routed) in relation to the configured anti-spoof setting.

This configuration option is only applicable to L2-Aware NAT subscribers. It determines which home model is supported with L2-Aware NAT:

- Bridged RG with mac-ip anti-spoof
- Bridged RG with nh-mac anti-spoof
- Routed RG with NAT and mac-ip anti-spoof
- Routed RG with NAT and nh-mac anti-spoof
- Routed RG without NAT and nh-mac anti-spoof

Default nat-access-mode auto

Parameters *access-mode* — Specifies the NAT access mode.

Values auto — The supported combinations are:

- Bridged RG with mac-ip anti-spoof
- Routed RG with NAT and mac-ip anti-spoof
- Routed RG with NAT and nh-mac anti-spoof
- Routed RG without NAT and nh-mac anti-spoof

bridged — The supported combinations are:

- Bridged RG with mac-ip anti-spoof
- Bridged RG with nh-mac anti-spoof
- Routed RG with NAT and mac-ip anti-spoof
- Routed RG with NAT and nh-mac anti-spoof
- Routed RG without NAT and nh-mac anti-spoof

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.20 nat-allow-bypass

nat-allow-bypass

Syntax [**no**] **nat-allow-bypass**

Context **[Tree]** (config>subscr-mgmt>sub-prof nat-allow-bypass)

Full Context configure subscriber-mgmt sub-profile nat-allow-bypass

Description This command enables L2-Aware NAT host for selective bypass. L2-aware NAT subscribers eligible for NAT bypass must be explicitly enabled with this command. Once enabled, the ip-filter configuration applied in sub-profile determines whether the traffic is bypassed.

The **no** form of this command causes traffic received from subscribers associated with this profile to not bypass the Layer-2-Aware NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.21 nat-classifier

nat-classifier

Syntax **nat-classifier** *nat-classifier-name*
no nat-classifier

Context **[Tree]** (config>service>nat>nat-policy>dnat nat-classifier)

Full Context configure service nat nat-policy dnat nat-classifier

Description This command when configured within the nat-policy, references a nat-classifier and consequently activates DNAT functionality. Unless this command is provisioned, the destination IP address translation will not take place. The **nat-classifier** identifies the traffic (in a filter-like fashion) that is subjected to DNAT.

The **no** form of this command removes the *nat-classifier-name* from the configuration.

Default none

Parameters *nat-classifier-name* — Specifies the name, up to 32 characters, of the NAT classifier.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat-classifier

Syntax **nat-classifier** *nat-classifier-name* [**create**]
no nat-classifier

Context **[Tree]** (config>service>nat nat-classifier)

Full Context configure service nat nat-classifier

Description This command creates a nat-classifier. Traffic can be identified in nat-classifier based on the protocol type and destination ports. Once the traffic is identified, an action associated with identified traffic, such as destination NAT (DNAT), can be taken.

The **no** form of the command removes the *nat-classifier-name* from the configuration.

Default none

Parameters *nat-classifier-name* — Specifies the name, up to 32 characters, of the referenced NAT classifier.

create — Keyword used to create the NAT classifier.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.22 nat-group

nat-group

Syntax **nat-group** *nat-group-id* [**create**]
no nat-group nat-group-id

Context **[Tree]** (config>router>isa-svc-chain nat-group)

Full Context configure router isa-service-chaining nat-group

Description This command allows service chaining to be enabled for subscribers whose NAT flows are established on the set of ISAs in the specified NAT group.

The **no** form of this command removes the NAT group from the configuration.

Parameters *nat-group-id* — Specifies the NAT group identifier.

Values 1 to 4

create — Keyword used to create the NAT group instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat-group

Syntax **nat-group** *nat-group-id* **sync-tag** *tag*
no nat-group *nat-group-id*

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync>nat nat-group)

Full Context configure redundancy multi-chassis peer sync nat nat-group

Description This command enables MCS for NAT. NAT group health information is exchanged between the pair of redundant NAT nodes. The system elects one of the nodes as the active node for the NAT group, while the other node becomes a standby node.

The **no** form of this command disables multi-chassis synchronization for a NAT group.

Default no nat-group

Parameters *nat-group-id* — Specifies the NAT group that is synchronized.

Values 1 to 4

tag — Specifies the synchronization tag that must be the same on both nodes of the NAT group. It is mandatory and must match its counterpart on the peering node for the NAT group that is being synchronized, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat-group

Syntax **nat-group** *nat-group-id* [**create**]
no nat-group *nat-group-id*

Context **[Tree]** (config>isa nat-group)

Full Context configure isa nat-group

Description This command configures an ISA NAT group.

The **no** form of the command removes the ID from the configuration.

Default none

Parameters *nat-group-id* — Specifies the ISA NAT group ID.

Values 1 to 4

create — Keyword used to create the NAT group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat-group

Syntax **nat-group** *nat-group-id*
no nat-group

Context **[Tree]** (config>subscriber-mgmt>pfcp-association>nat nat-group)

Full Context configure subscriber-mgmt pfcp-association nat nat-group

Description This command configures a NAT group participating in NAT on BNG CUPS. ISAs in the NAT group are enabled for operation in BNG CUPS, but are not limited to BNG CUPS deployment. They can be used simultaneously with other versions of NAT in BNG, outside of the CUPS functionality.

The **no** version of this command deletes the NAT group.

Parameters *nat-group-id* — Specifies the NAT group ID.

Values 1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.23 nat-import

nat-import

Syntax **nat-import** *policy-name* [*policy-name*]
no nat-import

Context **[Tree]** (config>router>nat>inside nat-import)
[Tree] (config>service>vprn>nat>inside nat-import)

Full Context configure router nat inside nat-import
configure service vprn nat inside nat-import

Description This command references an import-policy to determine the routes that should be installed in the routing table as NAT routes, which are used to steer traffic to NAT.

A dynamic route obtained by BGP-VPN can be imported into an inside (private side) routing context in NAT environment. This route is associated with a NAT policy that maps traffic destined into a NAT pool and outside routing context. If the NAT policy is not explicitly configured in the import route policy, the imported NAT route is, by default, associated with the default NAT policy defined in the NAT inside routing context.

All BGP-VPN routes that are destined to be imported into NAT inside routing context must be configured with **action-type accept** in the route policy.

Parameters *policy-name* — Specifies up to five NAT import policy names, up to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat-import

Syntax **nat-import all** [**inside-router** *router-instance*]
nat-import route *ipv4-address* [**inside-router** *router-instance*]
no nat-import all [**inside-router** *router-instance*]
no nat-import route *ipv4-address* [**inside-router** *router-instance*]

Context **[Tree]** (debug>nat nat-import)

Full Context debug nat nat-import

Description This command enables debugging for routes dynamically imported into NAT from BGP.

The events related to dynamic routes in NAT can be filtered by a specific route and inside routing context.

Only events related to dynamic imports are dispayed. Events related to static route configurations are not shown.

Typical debug output displays the following information:

- `18 2021/06/15 09:29:54.436 UTC MINOR: DEBUG #2001 vprn550 NAT_IMPORT`
  This entry represents the debug event, the inside service in which the event occurred, and the process related to the event. For this particular log, the event ID is 2001 which occurred in the inside service vprn 550 and was related to a dynamic route importing into NAT.
- `dest-prefix 10.10.10.0/24 nat-policy ls-outPolicy service 500 : start import : ACCEPT by policy-statement evaluation`
  This entry represents the description of the event. The destination prefix 10.10.10.0/24 is associated with **nat-policy** *ls-outPolicy* and was successfully imported from the outside vprn 500 (into the inside vprn 550 identified by the first entry).

The **no** form of the command disables debugging of the specified parameters.

Parameters **all** — Specifies to debug all routes dynamically imported into NAT from BGP.

router-instance — Specifies filtering based on specific inside routing context.

ipv4-address — Specifies filtering based on the specific route.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.24 nat-outside

nat-outside

Syntax **nat-outside** *nat-group-id* [**create**]
no nat-outside *nat-group-id*

Context **[Tree]** (config>service>epipe nat-outside)

Full Context configure service epipe nat-outside

Description This command binds an Epipe to a NAT context running on an ISA-BB, allowing the Epipe to act as the outside service for the NAT or firewall. When **nat-outside** is enabled, one end of the Epipe is implicitly tied to ISA BB forwarding, leaving one remaining SAP, spoke, or similar available to be configured.

The **no** version of this command removes the Epipe binding to a NAT context.

Parameters *nat-group-id* — The NAT group ID where the PPPoE client is applied.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.25 nat-policy

nat-policy

Syntax **nat-policy** *policy-name*
no nat-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range nat-policy)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range nat-policy)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range nat-policy
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range nat-policy

Description This command specifies the NAT policy for WLAN-GW ISA subscribers.

The **no** form of this command reverts to the default.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat-policy

Syntax **nat-policy** *nat-policy-name*
no nat-policy

Context **[Tree]** (config>router>nat>inside nat-policy)
[Tree] (config>router>policy-options>policy-statement>entry>action nat-policy)
[Tree] (config>service>vprn>nat>inside nat-policy)

Full Context configure router nat inside nat-policy
configure router policy-options policy-statement entry action nat-policy
configure service vprn nat inside nat-policy

Description This command configures the NAT policy that is used for large-scale NAT in this service. If a **nat-policy** is not configured, then the default **nat-policy** is used.

The **no** form of the command removes the policy name from the configuration.

Parameters *nat-policy-name* — Specifies the NAT policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat-policy

Syntax **nat-policy** *nat-policy-name*
no nat-policy

Context **[Tree]** (config>router>policy-options>policy-statement>default-action nat-policy)

Full Context configure router policy-options policy-statement default-action nat-policy

Description This command assigns a NAT policy to the matched routes that do not have a more specific nat-policy configured under action.

A dynamic route obtained by BGP-VPN can be imported into an inside (private side) routing context in NAT environment. This route must be associated with a NAT policy that maps traffic destined to it into a NAT pool and outside routing context. If the NAT policy is not specified within the route policy, the imported NAT route, by default, is associated with the default NAT policy defined in the NAT inside routing context.

All BGP-VPN routes that are destined to be imported into NAT inside routing context must have action-type set to **accept** , regardless of whether the NAT policy is configured in the action.

The **no** form of the command removes the policy name from the configuration.

Parameters *nat-policy-name* — Specifies the NAT policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat-policy

Syntax **nat-policy** *nat-policy-name* [**create**]
no nat-policy *nat-policy-name*

Context **[Tree]** (config>service>nat nat-policy)

Full Context configure service nat nat-policy

Description This command configures a NAT policy.

Parameters *nat-policy-name* — Specifies the NAT policy name, up to 32 characters.

create — Keyword used to create the NAT policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat-policy

Syntax **nat-policy** *policy-name*
no nat-policy

Context **[Tree]** (config>subscr-mgmt>sub-profile nat-policy)

Full Context configure subscriber-mgmt sub-profile nat-policy

Description This command configures the NAT policy to be used for subscribers associated with this subscriber profile.

Parameters *policy-name* — Specifies the policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.26 nat-policy-name

nat-policy-name

Syntax [**no**] **nat-policy-name**

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>include nat-policy-name)

Full Context configure service nat syslog syslog-export-policy include nat-policy-name

Description This command includes the NAT policy name in the flow log.

The **no** form of the command disables the feature.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.27 nat-port-forwarding

nat-port-forwarding

Syntax **nat-port-forwarding**

Context **[Tree]** (config>system>persistence nat-port-forwarding)

Full Context configure system persistence nat-port-forwarding

Description This command configures NAT port forwarding persistence parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.28 nat-port-range

nat-port-range

Syntax [**no**] **nat-port-range**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute nat-port-range)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute nat-port-range

Description This command enables the generation of the of **nat-port-range** attribute.

The **no** form of this command disables the generation of the **nat-port-range** attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.29 nat-prefix-list

nat-prefix-list

Syntax **nat-prefix-list** *name*
no nat-prefix-list *name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>sub-prof nat-prefix-list)

Full Context configure subscriber-mgmt sub-profile nat-prefix-list

Description This command specifies the nat-prefix-list referenced within the subscriber-profile is used to associate L2-aware subscriber traffic with additional nat-policies based on the destination IPv4 address of the traffic.

The **no** form of the command removes the prefix list name from the configuration.

Default none

Parameters *name* — Specifies the nat prefix list name. Allowed values are any string up to 32 characters long composed of printable,7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

nat-prefix-list

Syntax **nat-prefix-list** *name* [**create**] [**application** *application-choice*]
no nat-prefix-list *name*

Context [Tree] (config>service>nat nat-prefix-list)

Full Context configure service nat nat-prefix-list

Description This command is used to create configuration context for:

- IP prefixes that are used select multiple nat-policies per subscriber in L2-aware NAT.
- Inside IP prefixes in DNAT-only scenario. The inside IP prefixes are then setup as downstream routes used to steer the return (downstream) traffic to the proper MS-ISA.

The **no** form of the command removes the prefix list name from the configuration.

Default none

Parameters *name* — Specifies the nat prefix list name. Allowed values are any string up to 32 characters long composed of printable,7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

application *application-choice* — Specifies how this NAT prefix list is to be applied.

Values **l2-aware-dest-to-policy**: Specifies that the nat-prefix-list can be applied only within the sub-profile for l2-aware subscribers. It will contain mapping between the destination prefix and a nat-policy.
dnat-only-subscribers: Specifies that the nat-prefix-list can be applied only to dnat-only-subscribers. It will contain the source-prefix that needs to be install in outside routing context so that the return traffic from the outside can be directed to proper MS-ISA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.30 nat-subscriber-string

nat-subscriber-string

Syntax [**no**] **nat-subscriber-string**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes nat-subscriber-string)

Full Context configure aaa isa-radius-policy acct-include-attributes nat-subscriber-string

Description This command enables the inclusion of the NAT subscriber string attributes.

The **no** form of the command excludes NAT subscriber string attributes.

Default no nat-subscriber-string

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.31 nat-traversal

nat-traversal

Syntax **nat-traversal** [**force**] [**keep-alive-interval** *keep-alive-interval*] [**force-keep-alive**]
no nat-traversal

Context **[Tree]** (config>ipsec>ike-policy nat-traversal)

Full Context configure ipsec ike-policy nat-traversal

Description This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled or in forced mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts the parameters to the default.

Default no nat-traversal

Parameters **force** — Forces to enable NAT-T

keep-alive-interval *keep-alive-interval* — Specifies the keep-alive interval in seconds.

Values 120 to 600

force-keep-alive — When specified, the keep-alive does not expire.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.32 nat64

nat64

Syntax [**no**] **nat64**

Context **[Tree]** (config>service>vprn>inside nat64)

Full Context configure service vprn inside nat64

Description Commands in this context configure NAT64.

The **no** form of the command disables NAT64.

nat64

Syntax [**no**] **nat64**

Context **[Tree]** (config>service>vprn>nat>inside nat64)
[Tree] (config>router>nat>inside nat64)

Full Context configure router nat inside nat64
configure service vprn nat inside nat64

Description Commands in this context configure NAT64 parameters.

The **no** form of the command disables NAT64.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.33 nat64-lsn-sub

nat64-lsn-sub

Syntax [**no**] **nat64-lsn-sub router** *router-instance* **ip** *ipv6-prefix*

Context **[Tree]** (config>li>li-source>nat nat64-lsn-sub)

Full Context configure li li-source nat nat64-lsn-sub

Description This command configures a NAT64 LSN subscriber source.

Parameters *router-instance* — Specifies the routing instance into which to inject the mirrored packets.

ipv6-prefix — Specifies the IPv6 address.

Values

ipv6-prefix:	<prefix>/<length>
prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x to [0 to FFFF]H
	d t o[0t o 255]D
<length>	[0 to 128]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.34 national-bits

national-bits

Syntax **national-bits** *sa4 sa5 sa6 sa7 sa8*
no national-bits

Context **[Tree]** (config>port>tdm>e1 national-bits)

Full Context configure port tdm e1 national-bits

Description This command configures the national use bits.

Parameters *sa-bits* — Disables or enables SA bits.

Values 0, 1

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.35 nbr

nbr

Syntax **nbr** [**detail**]
no nbr

Context **[Tree]** (debug>router>rsvp>event nbr)

Full Context debug router rsvp event nbr

Description This command debugs neighbor events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about neighbor events.

Platforms All

18.36 ncp-renegotiation

ncp-renegotiation

Syntax **ncp-renegotiation** {**ignore** | **terminate-session**}
no ncp-renegotiation

Context **[Tree]** (config>subscr-mgmt>ppp-policy ncp-renegotiation)

Full Context configure subscriber-mgmt ppp-policy ncp-renegotiation

Description This command configures the NCP renegotiation.

The **no** form of the command reverts to the default value.

Default ncp-renegotiation terminate-session

Parameters **ignore** — Specifies that BNG ignore subsequent renegotiation messages after successful IPCP negotiation.

terminate-session — Specifies that the PPP session be terminated.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.37 nd

nd

Syntax **nd**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6 nd)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 nd)

Full Context configure service ies subscriber-interface group-interface ipv6 nd
configure service vprn subscriber-interface group-interface ipv6 nd

Description Commands in this context configure neighbor discovery (ND) parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

nd

Syntax **nd**

Context **[Tree]** (config>service>ies>if>vpls>evpn nd)
[Tree] (config>service>vprn>if>vpls>evpn nd)

Full Context configure service ies interface vpls evpn nd
configure service vprn interface vpls evpn nd

Description Commands in this context configure ND host route parameters.

Platforms All

18.38 nd-host-route

nd-host-route

Syntax **nd-host-route**

Context **[Tree]** (config>service>vprn>if>ipv6 nd-host-route)

Full Context configure service vprn interface ipv6 nd-host-route

Description Commands in this context populate ND host route entries.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.39 nd-learn-unsolicited

nd-learn-unsolicited

Syntax **nd-learn-unsolicited** {**global** | **link-local** | **both**}
no nd-learn-unsolicited

Context **[Tree]** (config>service>ies>if>ipv6 nd-learn-unsolicited)

Full Context configure service ies interface ipv6 nd-learn-unsolicited

Description This command enables the ability to learn neighbor entries out of received unsolicited Neighbor Advertisement messages with or without the solicited flag set. The command can be enabled for global addresses, link-local addresses, or for both.

The **no** form of this command makes the router use standard RFC 4861 behavior, as described below, for learning of neighbor entries.

- If an unsolicited NA, regardless of the S flag, is received from a neighbor that is not yet in the ND cache, the NA is ignored.
- If an NS, RS, RA, or Redirect message with a Link Layer Address (MAC) is received from a neighbor that is not yet in the ND cache, a new neighbor entry is created in the cache to store the received Link Layer MAC. The neighbor is put in the stale state.

Parameters **global** — Learns global neighbor entries out of received unsolicited Neighbor Advertisement messages.

link-local — Learns link local neighbor entries out of received unsolicited Neighbor Advertisement messages.

both — Learns both global and link local neighbor entries out of received unsolicited Neighbor Advertisement messages.

Platforms All

nd-learn-unsolicited

Syntax **nd-learn-unsolicited** {**global** | **link-local** | **both**}
no nd-learn-unsolicited

Context **[Tree]** (config>service>vprn>if>ipv6 nd-learn-unsolicited)

Full Context configure service vprn interface ipv6 nd-learn-unsolicited

Description This command enables the ability to learn neighbor entries out of received unsolicited Neighbor Advertisement messages, with or without the solicited flag set. The command can be enabled for global addresses, link-local addresses, or for both.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command makes the router follow standard RFC 4861 behavior for learning of neighbor entries.

- If an unsolicited NA (regardless of the S flag) is received from a neighbor that is not yet in the ND cache, the NA is ignored in line with RFC 4861.
- If an NS, RS, RA, or Redirect message with a Link Layer Address (MAC) is received from a neighbor that is not yet in the ND cache, a new neighbor entry is created in the cache to store the received Link Layer MAC. The neighbor is put in the STALE state. This is the standard RFC behavior.

Parameters **global** — Learns global neighbor entries out of received unsolicited Neighbor Advertisement messages.

link-local — Learns link local neighbor entries out of received unsolicited Neighbor Advertisement messages.

both — Learns both global and link local neighbor entries out of received unsolicited Neighbor Advertisement messages.

Platforms All

nd-learn-unsolicited

Syntax **nd-learn-unsolicited** {**global** | **link-local** | **both**}
no nd-learn-unsolicited

Context **[Tree]** (config>router>if>ipv6 nd-learn-unsolicited)

Full Context configure router interface ipv6 nd-learn-unsolicited

Description This command enables the ability to learn neighbor entries out of received unsolicited Neighbor Advertisement messages, with or without the solicited flag set. The command can be enabled for global addresses, link-local addresses, or for both.

The **no** form of this command makes the router follow standard RFC 4861 behavior for learning of neighbor entries.

- If an unsolicited NA (regardless of the S flag) is received from a neighbor that is not yet in the ND cache, the NA is ignored in line with RFC 4861.
- If an NS, RS, RA, or Redirect message with a Link Layer Address (MAC) is received from a neighbor that is not yet in the ND cache, a new neighbor entry is created in the cache to store the received Link Layer MAC. The neighbor is put in the STALE state. This is the standard RFC behavior.

Parameters **global** — Learns global neighbor entries out of received unsolicited Neighbor Advertisement messages. This parameter is relevant only to global IPv6 addresses.

link-local — Learns link local neighbor entries out of received unsolicited Neighbor Advertisement messages.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

both — Learns both global and link local neighbor entries out of received unsolicited Neighbor Advertisement messages.

Platforms All

18.40 nd-populate-host-route

nd-populate-host-route

Syntax [**no**] **nd-populate-host-route**

Context **[Tree]** (config>service>ies>interface>ipv6 nd-populate-host-route)

Full Context configure service ies interface ipv6 nd-populate-host-route

Description This command enables the addition or deletion of host routes in the route-table derived from neighbor entries in the neighbor cache. To enable this command, the interface must be shut down. The command triggers the population of host routes in the route table out of their corresponding static, dynamic, or EVPN types in the neighbor table. Neighbor entries installed by subscriber management, local interfaces, and others, do not create host-routes.

Only reachable entries are added to the route table (entries are created from solicited NA messages). Entries created as stale — from Neighbor Solicitation (NS), unsolicited Neighbor Advertisements (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect messages — are not added to the route table because the neighbor is not confirmed as two-way.

- RA, RS, NS, and Redirect messages with a link layer address are added as STALE cache entries. Unsolicited NAs are added as STALE if **nd-learn-unsolicited** is configured.
- To speed up the addition of host routes to the route table for neighbors created as STALE, the following procedure is used:
  - If **nd-populate-host-route** is configured, the router sends an NS (unicast Neighbor Unreachability Detection (NUD) message) to the neighbor created as STALE. Only one NUD message is sent.
  - If **nd-populate-host-route** is not configured, no confirmation message is sent and regular procedures apply.
- When the solicited NA for the neighbor is received, the entry becomes reachable and is then added to the route-table.

The **no** form of this command disables the creation of host routes from the neighbor cache.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.41 nd-proactive-refresh

nd-proactive-refresh

Syntax **nd-proactive-refresh** {**global** | **link-local** | **both**}
no nd-proactive-refresh

Context **[Tree]** (config>service>ies>if>ipv6 nd-proactive-refresh)

Full Context configure service ies interface ipv6 nd-proactive-refresh

Description This command enables a proactive refresh of the neighbor entries. When enabled, at the stale timer expiration, the router sends a NUD message to the host (regardless of the existence of traffic to the IP address on the IOM), so the entry can be refreshed or removed.

This behavior is different from ARP, where the refresh is sent 30 seconds prior to the entry's age out time. The refresh can be optionally enabled for global addresses, link-local addresses, or both.

The **no** form of this command disables the proactive behavior and the router only refreshes an entry if there is traffic that needs to be sent to the IP address.

Parameters **global** — Refreshes global neighbor entries.

link-local — Refreshes link local neighbor entries.

both — Refreshes both global and link local neighbor entries.

Platforms All

nd-proactive-refresh

Syntax **nd-proactive-refresh** {**global** | **link-local** | **both**}
no nd-proactive-refresh

Context **[Tree]** (config>service>vprn>if>ipv6 nd-proactive-refresh)

Full Context configure service vprn interface ipv6 nd-proactive-refresh

Description This command enables a proactive refresh of the neighbor entries. When enabled, at the stale timer expiration, the router sends an NUD message to the host (regardless of the existence of traffic to the IP address on the IOM), so the entry can be refreshed or removed.

This behavior is different from ARP, where the refresh is sent 30 seconds prior to the entry's age out time. The refresh can be optionally enabled for global addresses, link-local addresses, or both.

The **no** form of this command disables the proactive behavior and the router only refreshes an entry if there is traffic that needs to be sent to the IP address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **global** — Refreshes global neighbor entries. This parameter is relevant only to global IPv6 addresses.

link-local — Refreshes link local neighbor entries. This parameter is relevant only to global IPv6 addresses.

both — Refreshes both global and link local neighbor entries. This parameter is relevant only to global IPv6 addresses.

Platforms All

nd-proactive-refresh

Syntax **nd-proactive-refresh** {**global** | **link-local** | **both**}
no nd-proactive-refresh

Context **[Tree]** (config>router>if>ipv6 nd-proactive-refresh)

Full Context configure router interface ipv6 nd-proactive-refresh

Description This command enables a proactive refresh of the neighbor entries. When enabled, at the stale timer expiration, the router sends an NUD message to the host (regardless of the existence of traffic to the IP address on the IOM), so the entry can be refreshed or removed.

This behavior is different from ARP, where the refresh is sent 30 seconds prior to the entry's age out time. The refresh can be optionally enabled for global addresses, link-local addresses, or both.

The **no** form of this command disables the proactive behavior and the router only refreshes an entry if there is traffic that needs to be sent to the IP address.

Parameters **global** — Refreshes global neighbor entries. This parameter is relevant only to global IPv6 addresses.

link-local — Refreshes link local neighbor entries. This parameter is relevant only to global IPv6 addresses.

both — Refreshes both global and link local neighbor entries. This parameter is relevant only to global IPv6 addresses.

Platforms All

18.42 nd-route-tag

nd-route-tag

Syntax **nd-route-tag** *tag*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no nd-route-tag

Context [Tree] (config>service>ies>if>ipv6 nd-route-tag)

Full Context configure service ies interface ipv6 nd-route-tag

Description This command adds a route tag to the ARP-ND host routes generated out of the neighbor entries in the interface. As any other route tag, it can be used to match ARP-ND routes in BGP export policies.

The **no** form of this command removes the route tag for the ARP-ND host routes.

Parameters *tag* — Specifies the route tag to be added when the proxy ND entries are advertised to EVPN.

Values 1 to 255

18.43 neid

neid

Syntax **neid** *hex-string*
no neid

Context [Tree] (config>system>ned>profile neid)

Full Context configure system network-element-discovery profile neid

Description This command configures the NEID for this profile.

The **no** form of this command deletes the NEID for this profile.

Parameters *hex-string* — A hexadecimal string that consists of a subnet ID and basic ID. The first 8 high-order bits indicate the subnet ID and range from 0x1 to 0xFE. The 16 low-order bits indicate the basic ID and ranges from 0x0001 to 0xFFFE. The NEID cannot be configured as 0x90006 to 0x9FF06 or 0x9bff0.

Values 0x10001 to 0xFEFFFE

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.44 neighbor

neighbor

Syntax **neighbor** *ip-address* [**create**]
no neighbor *ip-address*

Context **[Tree]** (config>service>vpls>gsmp>group neighbor)
[Tree] (config>service>vprn>gsmp>group neighbor)

Full Context configure service vpls gsmp group neighbor
configure service vprn gsmp group neighbor

Description Commands in this context configure a GSMP ANCP neighbor parameters.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IP address of the GSMP ANCP neighbor.

create — Keyword used to create the neighbor instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

neighbor

Syntax [**no**] **neighbor** *ip-address* [**create**]

Context **[Tree]** (config>service>vprn>gsmp>group neighbor)

Full Context configure service vprn gsmp group neighbor

Description This command adds a neighbor in the GSMP group.

The **no** form of this command removes the neighbor from the GSMP group.

Parameters *ip-address* — Specifies the IP address in dotted decimal notation.

create — This keyword is mandatory when creating a GSMP group name. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms All

neighbor

Syntax [**no**] **neighbor** *ip-int-name*

Context **[Tree]** (config>router>rip>group neighbor)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ripng>group neighbor)
[Tree] (config>service>vprn>rip>group neighbor)

Full Context configure router rip group neighbor
configure router ripng group neighbor
configure service vprn rip group neighbor

Description This command creates a context for configuring a RIP neighbor interface. By default, group interfaces are not activated with RIP, unless explicitly configured. The BNG only learns RIP routes from IPv4 host on the group interface. The RIP neighbor group interface defaults to **none**. The send operation is unchangeable for group-interface.

The **no** form of this command deletes the RIP interface configuration for this group interface. The shutdown command in the **config>router>rip>group group-name>neighbor** context can be used to disable an interface without removing the configuration for the interface.

Default no neighbor

Parameters *ip-int-name* — Specifies the IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured, an error message will be returned.

Platforms All

neighbor

Syntax **neighbor** *ipv6-address mac-address*
no neighbor *ipv6-address*

Context [Tree] (config>service>ies>if>ipv6 neighbor)

Full Context configure service ies interface ipv6 neighbor

Description This command configures IPv6-to-MAC address mapping on the IES interface.

Parameters *ipv6-address* — The IPv6 address of the interface for which to display information.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-address — Specifies the 48-bit MAC address for the IPv6-to-MAC address mapping in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms All

neighbor

Syntax **neighbor** *ip-address*
no neighbor

Context **[Tree]** (config>port>aps neighbor)

Full Context configure port aps neighbor

Description This command specifies the neighbor's IP address only on a multi-chassis APS where the working and protect circuits are configured on different routers. When the value the neighbor IP address is set to 0.0.0.0, this implies that the APS group is configured as a single-chassis APS group.

The route to the neighbor must not traverse the multi-chassis APS member (working or protect) circuits. It is recommended that the neighbor IP address configured is on a shared network between the routers that own the working and protect circuits.

By default no neighbor address is configured and both the working and protect circuits should be configured on the same router (i.e., single-chassis APS). APS is assumed to be configured wholly on a single chassis.

Parameters *ip-address* — Specifies the neighbor's IP address only on a multi-chassis APS where the working and protect circuits are configured on different routers. The node should be connected with a direct interface to ensure optimum fail-over time.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x:-[0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

neighbor

Syntax [**no**] **neighbor** *ip-address*

Context **[Tree]** (config>router>bgp>group neighbor)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bgp group neighbor

Description This command creates a BGP peer/neighbor instance within the context of the BGP group.

This command can be issued repeatedly to create multiple peers and their associated configuration.

The **no** form of this command is used to remove the specified neighbor and the entire configuration associated with the neighbor. The neighbor must be administratively **shutdown** before attempting to delete it. If the neighbor is not shutdown, the command will not result in any action except a warning message on the console indicating that neighbor is still administratively up.

Default no neighbor

Parameters *ip-address* — Specifies the IP address of the BGP peer router in dotted decimal notation.

Values ipv4-address:

- a.b.c.d (host bits must be 0)

ipv6-address:

- x:x:x:x:x:x:x:x [-interface]
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: 32 characters maximum, mandatory for link local addresses

Platforms All

neighbor

Syntax [**no**] **neighbor** *ip-address*

Context **[Tree]** (config>service>vprn>bgp>group neighbor)

Full Context configure service vprn bgp group neighbor

Description This command creates a BGP peer/neighbor instance within the context of the BGP group.

This command can be issued repeatedly to create multiple peers and their associated configuration.

The **no** form of this command is used to remove the specified neighbor and the entire configuration associated with the neighbor. The neighbor must be administratively **shutdown** before attempting to delete it. If the neighbor is not shut down, the command will not result in any action except a warning message on the console indicating that neighbor is still administratively up.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — The IP address of the BGP peer router in dotted decimal notation.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
	interface: 32 characters maximum, mandatory for link local addresses

The ipv6-address applies to the 7750 SR only.

Platforms All

neighbor

Syntax **neighbor** *ipv6-address mac-address*
no neighbor *ipv6-address*

Context **[Tree]** (config>service>vprn>if>ipv6 neighbor)

Full Context configure service vprn interface ipv6 neighbor

Description This command configures IPv6-to-MAC address mapping on the interface.

Parameters *ipv6-address* — Specifies the IPv6 address on the interface.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D

mac-address — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms All

neighbor

Syntax [**no**] **neighbor** *ip-address*

Context **[Tree]** (config>service>vprn>ospf>area>if neighbor)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>ospf3>area>if neighbor)

Full Context configure service vprn ospf area interface neighbor
configure service vprn ospf3 area interface neighbor

Description This command configures an OSPF non-broadcast multi-access (NBMA) neighbor. The OSPF interface must be configured as an NBMA interface with the **interface-type non-broadcast** command. An NBMA network has no broadcast or multicast capabilities, so the router cannot discover its neighbors dynamically. All neighbors must be configured statically with the **neighbor** command.

In addition to configuring the OSPF NBMA neighbor's IP address, the neighbor's MAC address may need to be configured with the **config>service>vprn>interface>static-arp** command for OSPFv2 neighbors using its IPv4 address, and the **config>service>vprn>interface>ipv6>neighbor** command for OSPFv3 neighbors using its IPv6 link-local address.

The **no** form of this command removes the **neighbor** configuration.

Default No OSPF NBMA neighbors are configured.

Parameters *ip-address* — Specifies the OSPFv2 neighbor's IPv4 address or the OSPFv3 neighbor's IPv6 link-local address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x [-interface]
	x:x:x:x:x:x:d.d.d.d [-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface —32 characters max, for link local addresses.

Platforms All

neighbor

Syntax **neighbor** *ipv6-address mac-address*
no neighbor *ipv6-address*

Context **[Tree]** (config>router>if>ipv6 neighbor)

Full Context configure router interface ipv6 neighbor

Description This command configures an IPv6-to-MAC address mapping on the interface. Use this command if a directly attached IPv6 node does not support ICMPv6 neighbor discovery, or for some reason, a static address must be used. This command can only be used on Ethernet media.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The *ipv6-address* must be on the subnet that was configured from the IPv6 **address** command or a link-local address.

Parameters *ipv6-address* — The IPv6 address assigned to a router interface.

Values		
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

mac-address — Specifies the MAC address for the neighbor in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Platforms All

neighbor

Syntax **neighbor** [*ip-int-name*]
no neighbor

Context **[Tree]** (debug>router>ip neighbor)

Full Context debug router ip neighbor

Description This command enables IPv6 neighbor debugging.

Parameters *ip-int-name* — Specifies the IP interface name.

Platforms All

neighbor

Syntax [**no**] **neighbor** *ipv4-address*
[**no**] **neighbor** *ipv6-address*

Context **[Tree]** (config>router>ospf>area>interface neighbor)
[Tree] (config>router>ospf3>area>interface neighbor)

Full Context configure router ospf area interface neighbor
configure router ospf3 area interface neighbor

Description This command configures an OSPF non-broadcast multi-access (NBMA) neighbor. The OSPF interface must be configured as an NBMA interface with the **interface-type non-broadcast** command. An NBMA network has no broadcast or multicast capabilities, so the router cannot discover its neighbors dynamically. All neighbors must be configured statically with the **neighbor** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In addition to configuring the OSPF NBMA neighbor's IP address, the neighbor's MAC address may need to be configured with the **config>router>interface>static-arp** command for OSPFv2 neighbors using its IPv4 address, and the **config>router>interface>ipv6>neighbor** command for OSPFv3 neighbors using its IPv6 link-local address.

The **no** form of this command removes the **neighbor** configuration.

Default no neighbor

Parameters *ipv4-address* — Specifies the OSPFv2 neighbor's IPv4 address.

Values ipv4-address — a.b.c.d

ipv6-address — Specifies the OSPFv3 neighbor's IPv6 link-local address.

Values

ipv6-address:	x:x:x:x:x:x:x:x [-interface]
	x:x:x:x:x:x:d.d.d.d [-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface — 32 characters maximum for link local addresses.

Platforms All

neighbor

Syntax **neighbor** [*ip-int-name* | *ip-address*]
neighbor [*ip-int-name*] [*router-id*]
no neighbor

Context **[Tree]** (debug>router>ospf neighbor)
[Tree] (debug>router>ospf3 neighbor)

Full Context debug router ospf neighbor
debug router ospf3 neighbor

Description This command enables debugging for an OSPF or OSPF3 neighbor.

Parameters *ip-int-name* — Specifies the neighbor interface name.

ip-address — Specifies neighbor information for the neighbor identified by the specified IP address, in the **debug>router>ospf** context.

router-id — Specifies neighbor information for the neighbor identified by the specified router ID, in the **debug>router>ospf3** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

neighbor

Syntax **neighbor** {*ip-address* | **prefix-list** *name*}
no neighbor

Context **[Tree]** (config>router>policy-options>policy-statement>entry>to neighbor)
[Tree] (config>router>policy-options>policy-statement>entry>from neighbor)

Full Context configure router policy-options policy-statement entry from neighbor
configure router policy-options policy-statement entry to neighbor

Description This command specifies the neighbor address as found in the source address of the actual join and prune message as a filter criterion. If no neighbor is specified, any neighbor is considered a match.

The **no** form of the of the command removes the neighbor IP match criterion from the configuration.

Default no neighbor

Parameters *ip-address* — Specifies the neighbor IP address in dotted decimal notation.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x [-interface]
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: 32 characters maximum, mandatory for link local addresses

prefix-list *name* — Specifies the prefix-list name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The *name* specified must already be defined.

Platforms All

18.45 neighbor-limit

neighbor-limit

Syntax **neighbor-limit** [*value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no neighbor-limit

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>nd neighbor-limit)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>nd neighbor-limit)

Full Context configure service ies subscriber-interface group-interface ipv6 nd neighbor-limit
configure service vprn subscriber-interface group-interface ipv6 nd neighbor-limit

Description This command configures the maximum number of neighbors learned for a single host by doing neighbor discovery.

The **no** form of this command reverts to the default.

Default neighbor-limit 1

Parameters *value* — Specifies the maximum number of neighbors learned.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

neighbor-limit

Syntax **neighbor-limit** *limit* [**log-only**] [**threshold** *percent*]
no neighbor-limit

Context [Tree] (config>service>ies>if>ipv6 neighbor-limit)

Full Context configure service ies interface ipv6 neighbor-limit

Description This command configures the maximum amount of dynamic IPv6 neighbor entries that can be learned on an IP interface.

When the number of dynamic neighbor entries reaches the configured percentage of this limit, an SNMP trap is sent. When the limit is exceeded, no new entries are learned until an entry expires and traffic to these destinations is dropped. Entries that have already been learned is refreshed.

The **no** form of this command removes the **neighbor-limit**.

Default no neighbor-limit

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, entries above the limit is learned.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

limit — The number of entries that can be learned on an IP interface expressed as a decimal integer. If the limit is set to 0, dynamic neighbor learning is disabled and no dynamic neighbor entries are learned.

Values 0 to 102400

Platforms All

neighbor-limit

Syntax **neighbor-limit** *limit* [**log-only**] [**threshold** *percent*]
no neighbor-limit

Context **[Tree]** (config>service>vprn>if>ipv6 neighbor-limit)

Full Context configure service vprn interface ipv6 neighbor-limit

Description This command configures the maximum amount of dynamic IPv6 neighbor entries that can be learned on an IP interface.

When the number of dynamic neighbor entries reaches the configured percentage of this limit, an SNMP trap is sent. When the limit is exceeded, no new entries are learned until an entry expires and traffic to these destinations will be dropped. Entries that have already been learned will be refreshed.

The **no** form of this command removes the **neighbor-limit**.

Default neighbor-limit 90

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, entries above the limit will be learned.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

limit — The number of entries that can be learned on an IP interface expressed as a decimal integer. If the limit is set to 0, dynamic neighbor learning is disabled and no dynamic neighbor entries are learned.

Values 0 to 102400

Platforms All

neighbor-limit

Syntax **neighbor-limit** *limit* [**log-only**] [**threshold** *percent*]
no neighbor-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>if>ipv6 neighbor-limit)

Full Context configure router interface ipv6 neighbor-limit

Description This command configures the maximum amount of dynamic IPv6 neighbor entries that can be learned on an IP interface.

When the number of dynamic neighbor entries reaches the configured percentage of this limit, an SNMP trap is sent. When the limit is exceeded, no new entries are learned until an entry expires and traffic to these destinations will be dropped. Entries that have already been learned will be refreshed.

The **no** form of this command removes the neighbor-limit.

Default no neighbor-limit

Parameters *limit* — The number of entries that can be learned on an IP interface expressed as a decimal integer. If the limit is set to 0, dynamic neighbor learning is disabled and no dynamic neighbor entries are learned.

Values 0 to 102400

log-only — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, entries above the limit will be learned.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

Platforms All

18.46 neighbor-liveness-time

neighbor-liveness-time

Syntax **neighbor-liveness-time** *interval*
no neighbor-liveness-time

Context [Tree] (config>router>ldp>graceful-restart neighbor-liveness-time)

Full Context configure router ldp graceful-restart neighbor-liveness-time

Description This command configures the neighbor liveness time.

The **no** form of this command returns the default value.

Default no neighbor-liveness (which equals a value of 120 seconds)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *interval* — Specifies the length of time in seconds.

Values 5 to 300

Platforms All

18.47 neighbor-resolution

neighbor-resolution

Syntax [**no**] **neighbor-resolution**

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6-relay neighbor-resolution)
[Tree] (config>service>vprn>if>ipv6>dhcp6-relay neighbor-resolution)

Full Context configure service ies interface ipv6 dhcp6-relay neighbor-resolution
configure service vprn interface ipv6 dhcp6-relay neighbor-resolution

Description This command enables neighbor resolution with DHCPv6 relay.

The **no** form of this command disables neighbor resolution.

Platforms All

18.48 neighbor-solicitation

neighbor-solicitation

Syntax [**no**] **neighbor-solicitation**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6>auto-reply neighbor-solicitation)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>auto-reply neighbor-solicitation)

Full Context configure service ies subscriber-interface group-interface ipv6 auto-reply neighbor-solicitation
configure service vprn subscriber-interface group-interface ipv6 auto-reply neighbor-solicitation

Description This command enables auto-reply for neighbor solicitation.

The **no** form of this command disables auto-reply neighbor solicitation.

Default neighbor-solicitation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.49 neighbor-trust

neighbor-trust

Syntax **neighbor-trust** [**vpn-ipv4**] [**vpn-ipv6**]
no neighbor-trust

Context **[Tree]** (config>router>bgp neighbor-trust)

Full Context configure router bgp neighbor-trust

Description This command enables a label security feature for prefixes of a VPN family at an inter-AS boundary.

This label security feature allows the configuration of a router, acting in a PE and/or in an ASBR role, to accept packets of VPRN prefixes only from direct EBGP neighbors to which it advertised a VPRN label.

The untrusted state identifies the participating interfaces. The router supports a maximum of 15 network interfaces that can participate in this feature.

At a high level, BGP tracks each direct EBGP neighbor over an untrusted interface and to which it sent a VPRN prefix label. For each of those VPRN prefixes, BGP programs a bit map in the ILM record that indicates, on per-untrusted interface basis, whether the matching received packets must be forwarded or dropped.

The **no** form of this command disables the inter-AS security feature for the VPN family.

Parameters **vpn-ipv4** — Enables the inter-AS label security for VPN IPv4 family.

vpn-ipv6 — Enables the inter-AS label security for VPN IPv6 family.

Platforms All

18.50 neip

neip

Syntax **neip**

Context **[Tree]** (config>system>ned>profile neip)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system network-element-discovery profile neip

Description Commands in this context configure the NEIP.

Platforms All

18.51 netbios-name-server

netbios-name-server

Syntax **netbios-name-server** *ip-address* [*ip-address*]
no netbios-name-server

Context **[Tree]** (config>router>dhcp>server>pool>options netbios-name-server)
[Tree] (config>service>vprn>dhcp>server>pool>options netbios-name-server)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options netbios-name-server)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>options netbios-name-server)

Full Context configure router dhcp local-dhcp-server pool options netbios-name-server
configure service vprn dhcp local-dhcp-server pool options netbios-name-server
configure subscriber-mgmt local-user-db ipoe host options netbios-name-server
configure subscriber-mgmt local-user-db ppp host options netbios-name-server

Description This command configures up to four Network Basic Input/Output System (NetBIOS) name server IP addresses for a DHCP client.

The **no** form of this command removes the IP address from the netbios-name-server configuration.

Parameters *ip-address* — Specifies up to four NetBIOS name server IP addresses. The address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.52 netbios-node-type

netbios-node-type

Syntax **netbios-node-type** *netbios-node-type*
no netbios-node-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>dhcp>server>pool>options netbios-node-type)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options netbios-node-type)
[Tree] (config>service>vprn>dhcp>server>pool>options netbios-node-type)

Full Context configure router dhcp local-dhcp-server pool options netbios-node-type
configure service vprn dhcp local-dhcp-server pool options netbios-node-type
configure subscriber-mgmt local-user-db ipoe host options netbios-node-type

Description This command configures the Network Basic Input/Output System (NetBIOS) node type.

The **no** form of this command removes the NetBIOS node type parameters from the configuration.

Parameters *netbios-node-type* — Specifies the netbios node type.

Values B — Broadcast node uses broadcasting to query nodes on the network for the owner of a NetBIOS name.

P — Peer-to-peer node uses directed calls to communicate with a known NetBIOS name server for the IP address of a NetBIOS machine name.

M — Mixed node uses broadcast queries to find a node, and if that fails, queries a known P-node name server for the address.

H — Hybrid node is the opposite of the M-node action so that a directed query is executed first, and if that fails, a broadcast is attempted.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.53 netconf

netconf

Syntax **netconf**

Context [Tree] (debug>system netconf)

Full Context debug system netconf

Description Commands in this context debug NETCONF.

Platforms All

netconf

Syntax **netconf**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>security>profile netconf)

Full Context configure system security profile netconf

Description This command authorizes various netconf capabilities for the user.

Platforms All

netconf

Syntax **netconf**

Context [Tree] (config>system>security>management-interface netconf)

Full Context configure system security management-interface netconf

Description Commands in this context configure hash-control for the Netconf interface.

Platforms All

18.54 netconf-stream

netconf-stream

Syntax **netconf-stream** *stream-name*
no netconf-stream

Context [Tree] (config>li>log>log-id netconf-stream)

Full Context configure li log log-id netconf-stream

Description This command is used to associate a NETCONF stream name with a Lawful Intercept log ID. The NETCONF stream name must be unique in the Lawful Intercept context of the SR OS device. For the same Lawful Intercept log ID, the **to netconf** command must be configured for a subscription to that NETCONF stream name to be accepted. If the NETCONF stream is changed, active subscriptions to the changed stream name are terminated by SR OS.

The **no** form of this command removes a NETCONF stream name from a Lawful Intercept log ID. Active subscriptions to the removed stream name are terminated by SR OS.

Parameters *stream-name* — Specifies a NETCONF stream name, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

netconf-stream

Syntax **netconf-stream** *stream-name*
no netconf-steam

Context **[Tree]** (config>log>log-id netconf-stream)

Full Context configure log log-id netconf-stream

Description This command is used to associate a NETCONF stream name with a log ID. The NETCONF stream name must be unique per SR OS device. For the same log ID, **to netconf** must be configured for a subscription to that NETCONF stream name to be accepted. A **netconf-stream** cannot be set to “NETCONF” as “NETCONF” is reserved for log-id 101. If a **netconf-stream** is changed, active subscriptions to the changed stream name are terminated by SR OS.

The **no** form of this command removes a NETCONF stream name from a log ID. Active subscriptions to the removed stream name are terminated by SR OS.

Parameters *stream-name* — Specifies a NETCONF stream name, up to 32 characters.

Platforms All

18.55 network

network

Syntax **network next-hop** *ip-address* [**router** *router-instance*]
network next-hop *ip-address* [**service-name** *service-name*]
no network

Context **[Tree]** (config>subscr-mgmt>steering-profile network)

Full Context configure subscriber-mgmt steering-profile network

Description This command specifies the downstream next-hop IP address and an optional routing instance to be used as a network VAS router in the steering profile.

The **no** form of this command removes the specified next-hop IP address and the router instance if specified.

Parameters *ip-address* — Specifies the IP address to be used as the downstream next-hop IP address in dotted decimal notation.

router-instance — Specifies the router instance to be used as an access VAS router.

Values
router-instance: *router-name* | *vprn-svc-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-name: "Base"
vprn-svc-id: 1 to 2147483647

service-name — Specifies the service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

network

Syntax [**no**] **network**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext network)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext network)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext network
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext network

Description Commands in this context configure network side attributes.

The **no** form of this command resets the network parameters to the default values.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

network

Syntax **network**

Context **[Tree]** (config>card>mda network)
[Tree] (config>port network)

Full Context configure card mda network
configure port network

Description This command enables the network context to configure egress and ingress pool policy parameters.

On the MDA level, network egress pools are only allocated on channelized MDAs.

Platforms All

network

Syntax **network**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>card>fp>ingress network)

Full Context configure card fp ingress network

Description This command specifies the CLI node that contains the network forwarding-plane parameters.

Platforms All

network

Syntax **network**

Context [Tree] (config>port>tdm>ds1>channel-group network)
[Tree] (config>port>tdm>e1>channel-group network)

Full Context configure port tdm ds1 channel-group network
configure port tdm e1 channel-group network

Description Commands in this context configure network channel group parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

network

Syntax **network**

Context [Tree] (config>port>ethernet network)
[Tree] (config>port>sonet-sdh>path network)
[Tree] (config>port>tdm>ds1 network)
[Tree] (config>port>tdm>ds3 network)
[Tree] (config>port>tdm>e1 network)
[Tree] (config>port>tdm>e3 network)

Full Context configure port ethernet network
configure port sonet-sdh path network
configure port tdm ds1 network
configure port tdm ds3 network
configure port tdm e1 network
configure port tdm e3 network

Description This command enables access to the context to configure network port parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path network

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e3 network

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port tdm ds3 network

All

- configure port ethernet network

network

Syntax **network**

Context **[Tree]** (config>service>vpls>vxlan network)

Full Context configure service vpls vxlan network

Description Commands in this context configure network parameters for the VPLS VXLAN service.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

network

Syntax **network**

Context **[Tree]** (config>service>vprn network)

Full Context configure service vprn network

Description Commands in this context configure network parameters for the VPRN service.

Platforms All

network

Syntax **network** *network-policy-id* [**create**] [**name** *name*]
no network *network-policy-id*

Context **[Tree]** (config>qos network)

Full Context configure qos network

Description This command creates or edits a QoS network policy. The network policy defines the treatment that IP or MPLS packets receive as they ingress and egress the network port.

The QoS network policy consists of an ingress and egress component. The ingress component of the policy defines how DiffServ code points and MPLS EXP bits are mapped to internal forwarding class and profile state. The forwarding class and profile state define the Per Hop Behavior (PHB) or the QoS treatment through the router. The mapping on each network interface defaults to the mappings defined in the default network QoS policy until an explicit policy is defined for the network interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The egress component of the network QoS policy defines the queuing parameters associated with each forwarding class. Each of the forwarding classes defined within the system automatically creates a queue on each network interface. This queue gets all the parameters defined within the default network QoS policy 1 until an explicit policy is defined for the network interface access uplink port. If the egressing packet originated on an ingress SAP, or the remarking parameter is defined for the egress interface, the egress QoS policy also defines the IP DSCP, dot1p/DE, or MPLS EXP bit marking based on the forwarding class and the profile state.

Network **policy-id 1** exists as the default policy that is applied to all network interfaces by default. The network **policy-id 1** cannot be modified or deleted. It defines the default DSCP-to-FC mapping and MPLS EXP-to-FC mapping for the ingress. For the egress, it defines six forwarding classes that represent individual queues and the packet marking criteria.

Network **policy-id 1** exists as the default policy that is applied to all network ports by default. This default policy cannot be modified or deleted. It defines the default DSCP-to-FC mapping and default unicast meters for ingress IP traffic. For the egress, it defines the forwarding class to dot1p and DSCP values and the packet marking criteria.

If a new network policy is created (for instance, policy-id 3), only the default action and egress forwarding class parameters are identical to the default policy. A new network policy does not contain the default DSCP-to-FC and MPLS-EXP-to-FC mapping for network QoS policy of type **ip-interface** or the DSCP-to-FC mapping (for network QoS policy of type **port**). The default network policy can be copied (use the copy command) to create a new network policy that includes the default ingress DSCP-to-FC and MPLS EXP-to-FC mapping (as appropriate). Parameters can be modified, or the **no** form of this command can be used to remove an object from the configuration.

Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network interfaces where this policy is applied. For this reason, when many changes are required on a policy, it is highly recommended that the policy be copied to a work area policy-id. That work-in-progress policy can be modified until complete, then written over the original policy-id. Use the config qos copy command to maintain policies in this manner.

The **no** form of this command deletes the network policy. A policy cannot be deleted until it is removed from all entities where it is applied. The default network **policy** *policy-id* 1 cannot be deleted.

Default network 1 — System Default Network Policy 1

Parameters *network-policy-id* — The policy-id uniquely identifies the policy on the router.

Values 1 to 65535

Default 1

create — Required parameter when creating a QoS network policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name *name* — A name that is saved as part of the configuration data. If a name is not specified at creation time, then SR OS assigns a string version of the network policy identifier as the name.

Values A string up to 64 characters

Platforms All

network

Syntax **network** *src-pol dst-pol* [**overwrite**]

Context **[Tree]** (config>qos>copy network)

Full Context configure qos copy network

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

The **copy** command is used to create new policies using existing policies and also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters *src-pol dst-pol* — Indicates that the source and destination policies are network policy IDs. Specify the source policy that the copy command will copy and specify the destination policy to which the command will duplicate the policy to a new or different policy ID.

Values 1 to 65535

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy will be overwritten with the contents of the source policy. If **overwrite** is not specified, the following error occurs if the destination policy ID exists.

```
SR>config>qos# copy network 1 427
MINOR: CLI Destination "427" exists use {overwrite}.
SR>config>qos# copy network 1 427 overwrite
```

Platforms All

18.56 network-address

network-address

Syntax **network-address** {**eq** | **neq**} *ip-address*
network-address {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
no network-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>policy>app-filter>entry network-address)

Full Context configure application-assurance group policy app-filter entry network-address

Description This command configures the network address to use in application definition. The network address will match the destination IP address in a from-sub flow or the source IP address in a to-sub flow.

The **no** form of this command restores the default (removes the network address from application criteria defined by this entry).

Default no network-address

Parameters **eq** — Specifies a comparison operator indicating that the value configured and the value in the flow are equal.

neq — Specifies a comparison operator indicating that the value configured differs from the value in the flow.

ip-address — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D
	prefix-length [1..128]

ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.57 network-domain

network-domain

Syntax [**no**] **network-domain** *network-domain-name*

Context [Tree] (config>router>network-domains network-domain)

Full Context configure router network-domains network-domain

Description This command creates network-domains that can be associated with individual interfaces and SDPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default network-domain “default”

Parameters *network-domain-name* — Specifies the network domain name, up to 32 characters.

Platforms All

network-domain

Syntax [**no**] **network-domain** *network-domain-name*

Context **[Tree]** (config>router>if network-domain)

Full Context configure router interface network-domain

Description This command assigns a given interface to a given network-domain. The network-domain is then taken into account during sap-ingress queue allocation for VPLS SAP.

The network-domain association can only be done in a base-routing context. Associating a network domain with an loop-back or system interface will be rejected. Associating a network-domain with an interface that has no physical port specified will be accepted, but will have no effect as long as a corresponding port, or LAG, is defined.

Single interfaces can be associated with multiple network-domains.

Default network-domain “default”

Platforms All

network-domain

Syntax **network-domain** *network-domain-name*
no network-domain

Context **[Tree]** (config>service>sdp network-domain)

Full Context configure service sdp network-domain

Description This command assigns a given SDP to a given network-domain. The network-domain is then taken into account during sap-ingress queue allocation for VPLS SAP.

The network-domain association can only be done in a base-routing context. Associating a network domain with an loop-back or system interface will be rejected. Associating a network-domain with an interface that has no physical port specified will be accepted, but will have no effect as long as a corresponding port, or LAG, is undefined.

A single SDP can only be associated with a single network-domain.

Default network-domain "default"

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.58 network-domains

network-domains

Syntax **network-domains**

Context **[Tree]** (config>router network-domains)

Full Context configure router network-domains

Description This command opens context for defining network-domains. This command is applicable only in the base routing context.

Platforms All

18.59 network-element-discovery

network-element-discovery

Syntax **network-element-discovery**

Context **[Tree]** (config>system network-element-discovery)

Full Context configure system network-element-discovery

Description Commands in this context configure the network-element discovery parameters and MIB table generation.

Platforms All

18.60 network-interconnect-vxlan

network-interconnect-vxlan

Syntax **network-interconnect-vxlan** *instance*
no network-interconnect-vxlan

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg network-interconnect-vxlan)

Full Context configure service system bgp-evpn ethernet-segment network-interconnect-vxlan

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates the VXLAN instance with the virtual Ethernet Segment. The association of the virtual ES is based on the VXLAN instance and range of services where the VXLAN instance is configured.

The **no** form of this command removes the VXLAN instance from the Ethernet Segment association.

Parameters *instance* — Specifies the VXLAN instance that is to be associated with the virtual ES.

Values 1

Platforms All

18.61 network-interface

network-interface

Syntax **network-interface** *interface-name* [**create**]
no network-interface *interface-name*

Context **[Tree]** (config>service>vprn network-interface)

Full Context configure service vprn network-interface

Description This command configures a network interface in a VPRN that acts as a CSC interface to a CSC-CE in a Carrier Supporting Carrier IP VPN deployment model.

Parameters *interface-name* — Specifies the name of the interface to be added.

create — Keyword used to create the network interface.

Platforms All

18.62 network-ip

network-ip

Syntax **network-ip** *ip-address*[*/mask*]
no network-ip

Context **[Tree]** (config>app-assure>group>transit-prefix-policy>entry>match network-ip)

Full Context configure application-assurance group transit-prefix-policy entry match network-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an entry for an address of prefix transit aa-sub and is used when the site is a remote site on the same opposite side of the system as the parent SAP. The network IP addresses represents the dest-IP in the from-SAP direction and src-IP in the to-SAP direction.

The **no** form of this command removes the network IP address/mask from the match criteria.

Parameters *ip-address[/mask]* — specifies the network address prefix and length associated with this transit prefix policy entry.

Values

ip-address[/mask]: ipv4-address - a.b.c.d[/mask]
mask - [1..32]
ipv6-address - x:x:x:x:x:x:x:x/prefix-length
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D
prefix-length [1..128]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.63 network-queue

network-queue

Syntax **network-queue** *policy-name* [**create**]
no network-queue *policy-name*

Context **[Tree]** (config>qos network-queue)

Full Context configure qos network-queue

Description This command creates a context to configure a network queue policy. Network queue policies define the ingress network queuing at the FP network node level and on the Ethernet port and SONET/SDH path level to define network egress queuing.

Default network-queue “default”

Parameters *policy-name* — The name of the network queue policy.

Values Valid names consist of any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

create — Required keyword when creating a network queue policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

network-queue

Syntax **network-queue** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy network-queue)

Full Context configure qos copy network-queue

Description This command copies or overwrites existing network queue QoS policies to another network queue policy ID.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters **network-queue** — Indicates that the source policy ID and the destination policy ID are network-queue policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy will be overwritten with the contents of the source policy. If **overwrite** is not specified, the following message is generated indicating that the destination policy ID exists.

```
SR7>config>qos# copy network-queue nq1 nq2
MINOR: CLI Destination "nq2" exists - use {overwrite}.
SR7>config>qos# copy network-queue nq1 nq2 overwrite
```

Platforms All

18.64 network-rtt-threshold

network-rtt-threshold

Syntax **network-rtt-threshold** *network-rtt-threshold*
no network-rtt-threshold

Context **[Tree]** (config>app-assure>group>tcp-optimizer network-rtt-threshold)

Full Context configure application-assurance group tcp-optimizer network-rtt-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the threshold of the Route Trip Time (RTT) delay of the network side (between AA and the content provider) above which TCP Optimization (TCPO) is performed. This enables the operator to disable optimization for content that is served from a location close to the TCP optimizer.

Default no network-rtt-threshold

Parameters *network-rtt-threshold* — Specifies the network side RTT delay threshold, inmilliseconds.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.65 network-type

network-type

Syntax **network-type** {**sdh** | **sonet**}

Context **[Tree]** (config>system>ptp network-type)

Full Context configure system ptp network-type

Description This command configures the codeset to be used for the encoding of QL values into PTP clockClass values when the profile is configured for G.8265.1. The codeset is defined in Table 1/G.8265.1. This setting only applies to the range of values observed in the clockClass values transmitted out of the node in Announce messages. The router will support the reception of any valid value in Table 1/G.8265.1

Default network-type sdh

Parameters **sdh** — Specifies the values used on a G.781 Option 1 compliant network.

sonet — Specifies the values used on a G.781 Option 2 compliant network.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

18.66 new-password-at-login

new-password-at-login

Syntax [**no**] **new-password-at-login**

Context **[Tree]** (config>system>security>user>console new-password-at-login)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security user console new-password-at-login

Description This command forces the user to change a password at the next console login. The new password applies to FTP but the change can be enforced only by the console, SSH, or Telnet login.

The **no** form of this command does not force the user to change passwords.

Default no new-password-at-login

Platforms All

18.67 new-qinq-untagged-sap

new-qinq-untagged-sap

Syntax [**no**] **new-qinq-untagged-sap**

Context **[Tree]** (config>system>ethernet new-qinq-untagged-sap)

Full Context configure system ethernet new-qinq-untagged-sap

Description This command controls the behavior of QinQ SAP y.0 (for example, 1/1/1:3000.0). If the flag is not enabled (no new-qinq-untagged-sap), the y.0 SAP works the same as the y.* SAP (for example, 1/1/1:3000.*); all frames tagged with outer VLAN y and no inner VLANs or inner VLAN x where inner VLAN x is not specified in a SAP y.x configured on the same port (for example, 1/1/1:3000.10).

If the flag is enabled, then the following new behavior immediately applies to all existing and future y.0 SAPs: the y.0 SAP maps all the ingress frames tagged with outer tag VLAN-id of y (qinq-etype) and no inner tag or with inner tag of VLAN-id of zero (0). When the flag is disabled, there is no disruption for existing usage of this SAP type.

Default no new-qinq-untagged-sap.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, VSR

18.68 new-session-id

new-session-id

Syntax [**no**] **new-session-id**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gy>efh new-session-id)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling new-session-id

Description This command determines the Diameter session ID when Extended Failure Handling (EFH) is active and an attempt is made to establish a new Diameter Gy session with the Online Charging Server (OCS). An attempt to establish a new Diameter Gy session is made when the allocated interim credit is used or the validity time expires for a rating group of a Diameter Gy session. The first attempt always uses a new Diameter session ID. This command controls the behavior for each subsequent attempt. The behavior is as follows:

- no new-session-id (default) — The same Diameter session ID is used for each subsequent attempt.
- new-session-id — A new Diameter session ID is used for each attempt.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.69 newline

newline

Syntax [**no**] **newline**

Context [Tree] (config>system>management-interface>cli>md-cli>environment>prompt newline)

Full Context configure system management-interface cli md-cli environment prompt newline

Description This command displays a new line before the first prompt line.

The **no** form of this command suppresses the new line before the first prompt line.

Default newline

Platforms All

18.70 next

next

Syntax [**no**] **next**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>nat>pcp-server-policy>option next)

Full Context configure service nat pcp-server-policy option next

Description This command enables support for the **next** option.

The **no** form of this command reverts to the default.

Default no next

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

18.71 next-attempt

next-attempt

Syntax **next-attempt** {**same-preference-level** | **next-preference-level**}
no next-attempt

Context [Tree] (config>router>l2tp next-attempt)
[Tree] (config>service>vprn>l2tp next-attempt)

Full Context configure router l2tp next-attempt
configure service vprn l2tp next-attempt

Description This command enables tunnel selection algorithm based on the tunnel preference level.

The **no** form of this command reverts to the default.

Default next-attempt next-preference-level

Parameters **same-preference-level** — If the **tunnel-spec** selection algorithm evaluates into a tunnel that is currently unavailable (for example, a tunnel in a denylist) then the next elected tunnel, if available, is chosen within the same preference-level as the last attempted tunnel. Only when all tunnels within the same preference level are exhausted, the tunnel selection algorithm moves to the next preference level.

In case that a new session setup request is received while all tunnels on the same preference level are denylisted, the L2TP session tries to be established on denylisted tunnels before the tunnel selection moves to the next preference level.

next-preference-level — If the **tunnel-spec** selection algorithm evaluates into a tunnel that is currently unavailable (for example tunnel in a denylist) then the selection algorithm tries to select the tunnel from the next preference level, even though the tunnels on the same preference level might be available for selection.

Default next-preference-level

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.72 next-header

next-header

Syntax **next-header** *next-header*
no next-header

Context **[Tree]** (config>system>security>mgmt-access-filter>ipv6-filter>entry next-header)

Full Context configure system security management-access-filter ipv6-filter entry next-header

Description This command specifies the next header to match. The protocol type such as TCP, UDP or OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17). IPv6 Extension headers are identified by the next header IPv6 numbers as per RFC2460. This command only applies to the 7750 SR and 7950 XRS.

Parameters *next-header* — Specifies for IPv4 MAF the IP protocol field, and for IPv6 the next header type to be used in the match criteria for this Management Access Filter Entry.

Values

next-header:	0 to 255, protocol numbers accepted in DHB
keywords:	none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, drp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, spf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp

Platforms All

18.73 next-hop

next-hop

Syntax **next-hop** {*ip-address* | *ip-int-name* | *ipv6 address*}

Context **[Tree]** (config>service>vprn>static-route-entry next-hop)

Full Context configure service vprn static-route-entry next-hop

Description This command specifies the directly connected next hop IP address or interface used to reach the destination. If the next hop is over an unnumbered interface or a point-to-point interface, the *ip-int-name* of the unnumbered or point-to-point interface (on this node) can be configured.

If the next hop is over an unnumbered interface in the 7450 ESS router, the *ip-int-name* of the unnumbered interface (on this node) can be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured *ip-address* can be either on the network side or the access side on this node. The address must be associated with a network directly connected to a network configured on this node.

Default no next-hop

Parameters *ip-int-name, ipv4-address, ipv6-address* — the IP-INT, IPv4, and IPv6 addresses

Values The following values apply to the 7750 SR and 7950 XRS:

ip-int-name	32 characters max
ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x-[interface] x:x:x:x:x:x:d.d.d.d[-interface] x: [0 to FFFF]H d: [0 to 255]D interface: 32 characters maximum, mandatory for link local addresses

IPv6 static routes are not supported on the 7450 ESS except in mixed mode.

Platforms All

next-hop

Syntax **next-hop** *ip-address*
no next-hop

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy>nh-grp>bkup next-hop)
[Tree] (config>router>mpls>fwd-policies>fwd-policy>nh-grp>pri next-hop)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group backup-next-hop next-hop
configure router mpls forwarding-policies forwarding-policy next-hop-group primary-next-hop next-hop

Description This command configures the address of primary or backup next hop of an NHG entry in a forwarding policy.

The **no** form of this command removes the address of primary or backup next hop of an NHG entry in a forwarding policy.

Parameters *ip-address* — Specifies the destination IPv4 or IPv6 address.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D

Platforms All

next-hop

Syntax **next-hop** {*ip-int-name* | *ip-address* | *ipv6-address*}

Context **[Tree]** (config>router>static-route-entry next-hop)

Full Context configure router static-route-entry next-hop

Description This command specifies the directly connected next hop IP address or interface used to reach the destination. If the next hop is over a point-to-point unnumbered interface, the **ip-int-name** of the unnumbered point-to-point interface (on this node) can be configured.

If the next hop is over an unnumbered interface in the 7450 ESS router, the *ip-int-name* of the unnumbered interface (on this node) can be configured.

The configured *ip-address* can be either on the network side or the access side on this node. The address must be associated with a network directly connected to a network configured on this node.

Default no next-hop

Parameters *ip-int-name* | *ip-address* | *ipv6-address* — Specifies the interface or IPv4/IPv6 address of the next hop.

Values The following values apply to the 7750 SR, 7450 ESS, and 7950 XRS:

ip-int-name	32 characters max
ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x-[interface] x:x:x:x:x:x:d.d.d.d[-interface] x: [0..FFFF]H d: [0..255]D interface: 32 characters maximum, mandatory for link local addresses

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

next-hop

Syntax [**no**] **next-hop** *ip-address*

Context **[Tree]** (config>vrrp>policy>priority-event>route-unknown next-hop)

Full Context configure vrrp policy priority-event route-unknown next-hop

Description This command enables an allowed next hop IP address to match the IP route prefix for a route-unknown priority control event.

If the next-hop IP address does not match one of the defined *ip-address*, the match is considered unsuccessful and the **route-unknown** event transitions to the set state.

The **next-hop** command is optional. If no **next-hop** *ip-address* commands are configured, the comparison between the RTM prefix return and the **route-unknown** IP route prefix are not included in the next hop information.

When more than one next hop IP addresses are eligible for matching, a **next-hop** command must be executed for each IP address. Defining the same IP address multiple times has no effect after the first instance.

The **no** form of the command removes the *ip-address* from the list of acceptable next hops when looking up the **route-unknown** prefix. If this *ip-address* is the last next hop defined on the **route-unknown** event, the returned next hop information is ignored when testing the match criteria. If the *ip-address* does not exist, the **no next-hop** command returns a warning error, but continues to execute if part of an **exec** script.

Default no next-hop — No next hop IP address for the route unknown priority control event is defined.

Parameters *ip-address* — The IP address for an acceptable next hop IP address for a returned route prefix from the RTM when looking up the **route-unknown** route prefix.

Values The following values apply to the 7450 ESS:
ipv4-address: a.b.c.d

Values The following values apply to the 7750 SR and 7950 XRS:

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x[-interface]	
	x:	[0..FFFF]H
	interface:	32 chars maximum, mandatory for link local addresses

The link-local IPv6 address must have an interface name specified. The global IPv6 address must not have an interface name specified.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

next-hop

Syntax **next-hop** *ip-address*
next-hop prefix-list *name*
no next-hop

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from next-hop)

Full Context configure router policy-options policy-statement entry from next-hop

Description This command enables BGP routes to be matched based on the BGP next-hop address. The match condition is evaluated against the IPv4 or IPv6 address in the NEXT_HOP or MP_REACH_NLRI attribute.

When the next-hop match is applied to VPN-IP routes, the Route Distinguisher (RD) is ignored.

A non-BGP route does not match a policy entry if it contains the **next-hop** command.

Default no next-hop

Parameters *ip-address* — An IPv4 or IPv6 address.

Values a.b.c.d or x:x:x:x:x:x:x:x or x:x:x:x:x:x:d.d.d.d

name — Specifies the name of a prefix-list (up to 32 characters).

prefix-list — Specifies that the BGP next hop should be matched against a prefix-list instead of an individual IP address.

Platforms All

next-hop

Syntax **next-hop** {*ip-address* | **peer-address**}
no next-hop

Context **[Tree]** (config>router>policy-options>policy-statement>default-action next-hop)
[Tree] (config>router>policy-options>policy-statement>entry>action next-hop)

Full Context configure router policy-options policy-statement default-action next-hop
configure router policy-options policy-statement entry action next-hop

Description This command assigns the specified next hop IP address to routes matching the policy statement entry.

If a next-hop IP address is not specified, the next-hop attribute is not changed.

The **no** form of this command disables assigning a next hop address in the route policy entry.

Default no next-hop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the next hop IP address in dotted decimal notation.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
param-name:	The next-hop parameter variable name.
	Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

peer-address — Set the next-hop IP address to the peer’s IP address.

Platforms All

18.74 next-hop-address

next-hop-address

Syntax **next-hop-address** *ip-address*
no next-hop-address

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment>next-hop-id next-hop-address)

Full Context configure router p2mp-sr-tree replication-segment next-hop-id next-hop-address

Description This command configures the IP address of the next hop for the P2MP SR tree replication segment.

The **no** form of this command removes the next hop address.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	where:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0 to FFFF]H
d: [0 to 255]D
interface: up to 32 characters, mandatory for link local addresses

Platforms All

18.75 next-hop-group

next-hop-group

Syntax **next-hop-group** *index* [**resolution-type** {**direct** | **indirect**}]
no next-hop-group *index*

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy next-hop-group)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group

Description This command configures an NHG entry in an MPLS forwarding policy.

Each NHG can have primary and backup next hops of the same type.

The **no** form of this command removes the NHG from the MPLS forwarding policy.

Parameters *index* — Specifies the index value.

Values 1 to 32

direct — Specifies the direct resolution type.

indirect — Specifies the indirect resolution type.

Platforms All

18.76 next-hop-id

next-hop-id

Syntax [**no**] **next-hop-id** *next-hop-id-index*

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment next-hop-id)

Full Context configure router p2mp-sr-tree replication-segment next-hop-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the next-hop ID for the P2MP SR tree replication segment.

A replication policy can have multiple next-hop IDs used at a replication node where there are multiple outgoing interfaces or protection next hops.

The **no** form of this command removes the next-hop ID.

Parameters *next-hop-id-index* — Specifies the index value of the next hop.

Values 1 to 4096

Platforms All

18.77 next-hop-interface-name

next-hop-interface-name

Syntax **next-hop-interface-name** *interface-name*
no next-hop-interface-name

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment>next-hop-id next-hop-interface-name)

Full Context configure router p2mp-sr-tree replication-segment next-hop-id next-hop-interface-name

Description This command provides the outgoing interface name for the P2MP SR tree replication segment.

The **no** form of this command removes the outgoing interface name.

Parameters *interface-name* — Specifies the name of the outgoing interface, up to 32 characters.

Platforms All

18.78 next-hop-resolution

next-hop-resolution

Syntax **next-hop-resolution**

Context **[Tree]** (config>service>vprn>bgp next-hop-resolution)

Full Context configure service vprn bgp next-hop-resolution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure next-hop resolution parameters.

Platforms All

next-hop-resolution

Syntax **next-hop-resolution**

Context **[Tree]** (config>router>bgp next-hop-resolution)

Full Context configure router bgp next-hop-resolution

Description Commands in this context configure next-hop resolution parameters.

Platforms All

18.79 next-hop-self

next-hop-self

Syntax [**no**] **next-hop-self**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy next-hop-self)

Full Context configure subscriber-mgmt bgp-peering-policy next-hop-self

Description This command configures the neighbor to always set the NEXTHOP path attribute to its own physical interface when advertising to a peer.

The **no** form of this command disables the command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

next-hop-self

Syntax [**no**] **next-hop-self**

Context **[Tree]** (config>service>vprn>bgp>group next-hop-self)
[Tree] (config>service>vprn>bgp>group>neighbor next-hop-self)

Full Context configure service vprn bgp group neighbor next-hop-self
configure service vprn bgp group next-hop-self

Description This command configures the group or neighbor to always set the NEXTHOP path attribute to its own physical interface when advertising to a peer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This is primarily used to avoid third-party route advertisements when connected to a multi-access network.

The **no** form of this command used at the group level allows third-party route advertisements in a multi-access network.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no next-hop-self — Third-party route advertisements are allowed.

Platforms All

next-hop-self

Syntax [**no**] **next-hop-self**

Context **[Tree]** (config>router>bgp>group next-hop-self)
[Tree] (config>router>bgp>group>neighbor next-hop-self)

Full Context configure router bgp group neighbor next-hop-self
configure router bgp group next-hop-self

Description This command enables BGP to advertise routes to members of a group or to a specific neighbor using a local address of the BGP instance as the BGP next-hop address. Note that **next-hop-self** is set without exception, regardless of the route source (EBGP or IBGP) or its family. When used with VPN-IPv4 and VPN-IPv6 routes the **enable-rr-vpn-forwarding** command should also be configured.

The **no** form of this command uses protocol standard behavior to decide whether or not to set **next-hop-self** in advertised routes.

Default no next-hop-self

Platforms All

next-hop-self

Syntax [**no**] **next-hop-self**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action next-hop-self)
[Tree] (config>router>policy-options>policy-statement>default-action next-hop-self)

Full Context configure router policy-options policy-statement default-action next-hop-self
configure router policy-options policy-statement entry action next-hop-self

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures BGP to advertise routes that match a policy entry (or that match no other policy entry and, therefore, to which the default action applies) using a local address of the BGP instance as the BGP next-hop address. The command applies to IPv4, IPv6, label-IPv4, and label-IPv6 routes. It also applies to VPN-IPv4 and VPN-IPv6 routes, but only when used in conjunction with the **enable-rr-vpn-forwarding** command.

This command affects how routes are advertised to IBGP peers, regardless of whether or not they were learned from an IBGP or EBGP peer

The **no** form of this command uses protocol standard behavior to decide whether or not to set **next-hop-self** in advertised routes.

Default no next-hop-self

Platforms All

18.80 next-hop-unchanged

next-hop-unchanged

Syntax **next-hop-unchanged** [**label-ipv4**] [**label-ipv6**] [**vpn-ipv4**] [**vpn-ipv6**] [**evpn**]
no next-hop-unchanged

Context **[Tree]** (config>router>bgp>group next-hop-unchanged)
[Tree] (config>router>bgp>group>neighbor next-hop-unchanged)

Full Context configure router bgp group neighbor next-hop-unchanged
configure router bgp group next-hop-unchanged

Description This command enables unchanged BGP next-hops when sending BGP routes to peers in this group or neighbor.

The **no** form of this command disables unchanged BGP next-hops.

Default no next-hop-unchanged

Parameters **evpn** — Specifies BGP next hops are unchanged for the evpn address family.

label-ipv4 — Specifies BGP next hops are unchanged for the label-ipv4 address family.

label-ipv6 — Specifies BGP next hops are unchanged for the label-ipv6 address family.

vpn-ipv4 — Specifies BGP next hops are unchanged for the vpn-ipv4 address family.

vpn-ipv6 — Specifies BGP next hops are unchanged for the vpn-ipv6 address family.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.81 nh-type

nh-type

Syntax **nh-type** {**ip** | **tunnel**}
no nh-type

Context **[Tree]** (config>router>route-next-hop-policy>template nh-type)

Full Context configure router route-next-hop-policy template nh-type

Description This command configures the next-hop type constraint into the route next-hop policy template.

The user can select if tunnel backup next-hop or IP backup next-hop is preferred. The default in SR OS implementation is to prefer IP next-hop over tunnel next-hop. The implementation will fall back to the other type if no LFA next-hop of the preferred type is found.

When the route next-hop policy template is applied to an IP interface, all prefixes using this interface as a primary next-hop will follow the next-hop type preference specified in the template.

The **no** form deletes the next-hop type constraint from the route next-hop policy template.

Default nh-type ip

Parameters **{ip | tunnel}** — Specifies the two possible values for the next-hop type.

Default ip

Platforms All

18.82 nmda

nmda

Syntax **nmda**

Context **[Tree]** (config>system>management-interface>yang-modules nmda)

Full Context configure system management-interface yang-modules nmda

Description Commands in this context configure the attributes for the Network Management Datastores Architecture (NMDA).

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.83 nmda-support

nmda-support

Syntax [**no**] **nmda-support**

Context **[Tree]** (config>system>management-interface>yang-modules>nmda nmda-support)

Full Context configure system management-interface yang-modules nmda nmda-support

Description This command enables the advertisement of NMDA support over NETCONF through the use of YANG library 1.1.

The **no** form of this command disables NMDA advertisement over NETCONF and YANG library 1.0 is used.

Default no nmda-support

Platforms All

18.84 no-match-action

no-match-action

Syntax **no-match-action** *action*
no no-match-action

Context **[Tree]** (config>open-flow>of-switch>flowtable no-match-action)

Full Context configure open-flow of-switch flowtable no-match-action

Description This command configures the action for the flow table when a packet does not match any entry for the controller.

The **no** form of this command restores the default action.

Default no-match-action fall-through

Parameters *action* — Specifies the action for the flow table.

Values drop - Specifies that packets that do not match entries in the flow table as programmed by the OpenFlow switch will be dropped.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fall-through - Specifies that packets that do not match entries in the flow table as programmed by the OpenFlow switch will be forwarded using regular processing by the router. Fall-through applies if an error occurs that prevents a flow table from being installed in a filter policy.

packet-in - Specifies that packets that do not match entries in the flow table as programmed by the OpenFlow switch will be extracted and sent to the controller in a flow-controlled manner. If this action is used, an auxiliary channel should be enabled for packet-in processing using the **aux-channel-enable** command.

Platforms All

18.85 node

node

Syntax **node** *origin-host-string* [**destination-realm** *destination-realm-string*]
no diameter-node

Context **[Tree]** (config>aaa>diam node)

Full Context configure aaa diameter node

Description This command creates a Diameter client node in the SR OS. Multiple Diameter client nodes with their own peer definitions are simultaneously supported in SR OS.

Each such node is defined by a unique DiameterIdentity (the origin host and realm names).

The **no** form of this command removes the origin host string from the configuration.

Parameters *origin-host-string* — Specifies the origin host name, up to 80 characters, is a mandatory parameter that translates to an Origin-Host AVP that is carried in all Diameter messages. The origin host and origin realm form a Diameter Identity that must be unique within the Diameter network in which they participate.

destination-realm-string — Specifies the destination realm name, up to 80 characters, is an optional parameter that translates to an Origin-Realm AVP that is carried in all Diameter messages. The destination host and destination realm form a Diameter Identity that must be unique within the Diameter network in which they participate

If the realm name is not configured, it will be extracted from the host parameter as follows:

- it is set to the string after the first dot (.) in the configured origin-host-string
- it is set to the configured origin-host-string if a dot (.) is not present in the string

create — Keyword used to create the Diameter client node. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

node

Syntax [**no**] **node** *host-name*

Context **[Tree]** (debug>diameter node)

Full Context debug diameter node

Description This command debugs the Diameter node. Node-level debugging can report on all message exchange between the peers. Although this level can report messages that contain session id (app level messages), this level is session unaware. It deals strictly with getting the messages in and out of the system (connection level messages which are not routable, and application level messages which are routable).

Parameters *host-name* — Specifies the host name, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.86 node-id

node-id

Syntax **node-id fqdn** *domain-name*
node-id use-ip-address

Context **[Tree]** (config>subscr-mgmt>pfcp-association node-id)

Full Context configure subscriber-mgmt pfcp-association node-id

Description This command configures the FQDN as sent in PFCP messages. This command can be configured to use the linked interface source IP address, or a pre-configured.

Default node-id use-ip-address

Parameters *domain-name* — Specifies the FQDN, up to 255 characters.

use-ip-address — Specifies to use the IP address of the interface configured for this association.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

node-id

Syntax **node-id** *node-id*
no node-id

Context **[Tree]** (config>router>mpls>mpls-tp node-id)

Full Context configure router mpls mpls-tp node-id

Description This command configures the MPLS-TP Node ID for the node. This is used as the 'from' Node ID used by MPLS-TP LSPs originating at this node. The default value of the node-id is the system interface IPv4 address. The Node ID may be entered in 4-octet IPv4 address format, <a.b.c.d>, or as an unsigned 32 bit integer. The Node ID is not treated as a routable IP address from the perspective of IP routing, and is not advertised in any IP routing protocols.

The MPLS-TP context cannot be administratively enabled unless at least a system interface IPv4 address is configured because MPLS requires that this value is configured.

Default no node-id

Parameters *node-id* — Specifies the MPLS-TP node ID for the node.

Values a.b.c.d or 1 to 4294967295

Default System interface IPv4 address

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

node-id

Syntax **node-id** *mac-address*
no node-id

Context **[Tree]** (config>eth-ring node-id)

Full Context configure eth-ring node-id

Description This optional command configures the MAC address of the RPL control. The default is to use the chassis MAC for the ring control. This command overrides the chassis MAC address with a different MAC address.

The **no** form of the command removes the RPL link.

Default no node-id

Parameters *mac-address* — xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.87 node-id-in-rro

node-id-in-rro

Syntax [**no**] **node-id-in-rro** [**include** | **exclude**]

Context **[Tree]** (config>router>rsvp node-id-in-rro)

Full Context configure router rsvp node-id-in-rro

Description This command enables the option to include node-id sub-object in RRO. Node-ID sub-object propagation is required to provide fast reroute protection for LSP that spans across multiple area domains.

If this option is disabled, then node-id is not included in RRO object.

Default node-id-in-rro exclude

Platforms All

18.88 node-protect

node-protect

Syntax [**no**] **node-protect**

Context **[Tree]** (config>router>mpls>lsp>fast-reroute node-protect)
[Tree] (config>router>mpls>lsp-template>fast-reroute node-protect)

Full Context configure router mpls lsp fast-reroute node-protect
configure router mpls lsp-template fast-reroute node-protect

Description This command enables or disables node and link protection on the specified LSP. Node protection ensures that traffic from an LSP traversing a neighboring router will reach its destination even if the neighboring router fails.

Default node-protect (for a provisioned LSP)

no node-protect (for a P2P LSP template)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

node-protect

Syntax **node-protect** [**max-pq-nodes** *value*]
no node-protect

Context **[Tree]** (config>router>isis>loopfree-alternates>remote-lfa node-protect)

Full Context configure router isis loopfree-alternates remote-lfa node-protect

Description This command enables node-protect in which the router prefers a node-protect over a link-protect repair tunnel for a given prefix if both are found in the Remote LFA or TI-LFA SPF computations. The SPF computations may only find a link-protect repair tunnel for prefixes owned by the protected node.

The **no** form of this command disables node-protect.

Default no node-protect

Parameters *value* — Specifies the maximum number of PQ nodes found in the LFA SPFs for which the node protection check is performed. The node-protect condition means the router must run the original Remote LFA algorithm plus one extra forward SPF on behalf of each PQ node found, potentially after applying the **max-pq-cost** parameter, to check if the path from the PQ node to the destination does not traverse the protected node. Setting this parameter to a lower value means the LFA SPFs will use less computation time and resources but may result in not finding a node-protect repair tunnel.

Values 1 to 32

Default 16

Platforms All

node-protect

Syntax [**no**] **node-protect**

Context **[Tree]** (config>router>isis>loopfree-alternates>ti-lfa node-protect)

Full Context configure router isis loopfree-alternates ti-lfa node-protect

Description This command enables node-protect in which the router prefers a node-protect over a link-protect repair tunnel for a given prefix if both are found in the Remote LFA or TI-LFA SPF computations. The SPF computations may only find a link-protect repair tunnel for prefixes owned by the protected node.

The **no** form of this command disables node-protect.

Default no node-protect

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

node-protect

Syntax **node-protect** [**max-pq-nodes** *value*]
no node-protect

Context **[Tree]** (config>router>ospf>loopfree-alternates>remote-lfa node-protect)
[Tree] (config>router>ospf3>loopfree-alternates>remote-lfa node-protect)

Full Context configure router ospf loopfree-alternates remote-lfa node-protect
configure router ospf3 loopfree-alternates remote-lfa node-protect

Description This command enables node-protect in which the router prefers a node-protect over a link-protect repair tunnel for a given prefix if both are found in the Remote LFA or TI-LFA SPF computations. The SPF computations may only find a link-protect repair tunnel for prefixes owned by the protected node.

The **no** form of this command disables node-protect.

Default no node-protect

Parameters **max-pq-nodes** *value* — Specifies the maximum number of PQ nodes found in the LFA SPFs for which the node protection check is performed. The node-protect condition means the router must run the original Remote LFA algorithm plus one extra forward SPF on behalf of each PQ node found, potentially after applying the **max-pq-cost** parameter, to check if the path from the PQ node to the destination does not traverse the protected node. Setting this parameter to a lower value means the LFA SPFs will use less computation time and resources but may result in not finding a node-protect repair tunnel.

Values 1 to 32

Default 16

Platforms All

node-protect

Syntax [**no**] **node-protect**

Context **[Tree]** (config>router>ospf>loopfree-alternates>ti-lfa node-protect)
[Tree] (config>router>ospf3>loopfree-alternates>ti-lfa node-protect)

Full Context configure router ospf loopfree-alternates ti-lfa node-protect
configure router ospf3 loopfree-alternates ti-lfa node-protect

Description This command enables node-protect in which the router prefers a node-protect over a link-protect repair tunnel for a given prefix if both are found in the Remote LFA or TI-LFA SPF computations. The SPF computations may only find a link-protect repair tunnel for prefixes owned by the protected node.

The **no** form of this command disables node-protect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no node-protect

Platforms All

18.89 node-sid

node-sid

Syntax [**no**] **node-sid**

Context **[Tree]** (config>router>isis>segm-rtng>egress-statistics node-sid)
[Tree] (config>router>ospf>segm-rtng>egress-statistics node-sid)
[Tree] (config>router>ospf3>segm-rtng>egress-statistics node-sid)
[Tree] (config>router>isis>segm-rtng>ingress-statistics node-sid)
[Tree] (config>router>ospf>segm-rtng>ingress-statistics node-sid)
[Tree] (config>router>ospf3>segm-rtng>ingress-statistics node-sid)

Full Context configure router isis segment-routing egress-statistics node-sid
configure router isis segment-routing ingress-statistics node-sid
configure router ospf segment-routing egress-statistics node-sid
configure router ospf segment-routing ingress-statistics node-sid
configure router ospf3 segment-routing egress-statistics node-sid
configure router ospf3 segment-routing ingress-statistics node-sid

Description This command enables the allocation of statistic indices to each node SID (received by means of IGP advertisement). All NHLFEs associated to a given SID share the same index. If a statistics index is not available at allocation time, the allocation fails, then the system re-tries the allocation. The system generates a log on the first fail and a log on the final successful allocation.

The **no** form of this command disables the allocation of statistic indices to each node SID, releases the statistic indices, and clears the associated counters.

Default no node-sid

Platforms All

node-sid

Syntax **node-sid index** *index-value* [**clear-n-flag**]
node-sid label *label-value* [**clear-n-flag**]
no node-sid

Context **[Tree]** (config>router>ospf>area>interface node-sid)
[Tree] (config>router>ospf3>area>interface node-sid)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ospf area interface node-sid
configure router ospf3 area interface node-sid

Description This command assigns a node SID index or label value to the prefix representing the primary address of a network interface of type system or loopback. A separate SID value can be configured for each IPv4 and IPv6 primary address of the interface. The secondary address of an IPv4 interface cannot be assigned a node SID index and does not inherit the SID of the primary IPv4 address.

In OSPFv2 and OSPFv3, the node SID is configured in the primary area but is inherited in any other area in which the interface is added as secondary.

This command fails if the network interface is not of type loopback or if the interface is defined in an IES or VPRN context. Assigning the same SID index or label value to the same interface in two different IGP instances is not allowed within the same node.

The value of the label or index SID is taken from the range configured for this IGP instance. When using the global mode of operation, the segment routing module checks that the same index or label value is not assigned to more than one loopback interface address. When using the per-instance mode of operation, this check is not required because the index, and therefore, the label ranges of IGP instances are not allowed to overlap.

The **clear-n-flag** option allows the user to clear the N-flag (node-sid flag) in an OSPF or OSPF3 prefix SID sub-TLV originated for the prefix of a loopback interface on the system. By default, the prefix SID sub-TLV for the prefix of a loopback interface is tagged as a node SID; that is, it belongs to this node only. However, to configure and advertise an anycast SID using the same loopback interface prefix on multiple nodes, the user must clear the N-flag to assure interoperability with third-party implementations, which may perform a strict check on the receive end and drop duplicate prefix SID sub-TLVs when the N-flag is set.

The SR OS implementation is relaxed on the receive end and accepts duplicate prefix SIDs with the N-flag set or clear. SR OS will resolve to the closest owner, or owners if ECMP, of the prefix SID cost-wise.

Parameters *index-value* — Specifies the node SID index value.

Values 0 to 4294967295

label-value — Specifies the node SID label value.

Values 0 to 4294967295

clear-n-flag — Clears the node SID flag.

Default no clear-n-flag

Platforms All

node-sid

Syntax **node-sid index** [**0..4294967295**]
no node-sid

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ospf>area>if>flex-algo node-sid)

Full Context configure router ospf area interface flex-algo node-sid

Description This command configures a flexible algorithm-aware node SID index.

The **no** form of this command removes the configured node SID index.

Default no node-sid

Platforms All

node-sid

Syntax **node-sid index** [**0..4294967295**]
node-sid label [**1..4294967295**]
no node-sid

Context [Tree] (config>router>ospf>area>if>flex-algo node-sid)

Full Context configure router ospf area interface flex-algo node-sid

Description This command configures a flexible algorithm-aware node SID label.

The **no** form of this command removes the configured node SID label.

Default no node-sid

Platforms All

node-sid

Syntax **node-sid**
no node-sid

Context [Tree] (config>router>segment-routing>sr-mpls>prefix-sids node-sid)

Full Context configure router segment-routing sr-mpls prefix-sids node-sid

Description This command sets the N-flag for the SR SID. The N-flag should be set when the prefix SID is a node SID for the primary prefix. If the N-flag is not set, the SR SID is an SR anycast SID.

The **no** form of this command removes the assigned node SID.

Default no node-sid

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.90 nokia-combined-modules

nokia-combined-modules

Syntax [**no**] **nokia-combined-modules**

Context **[Tree]** (config>system>management-interface>yang-modules nokia-combined-modules)

Full Context configure system management-interface yang-modules nokia-combined-modules

Description This command enables support of the “combined” Nokia SR OS YANG files for both configuration and state data in the NETCONF server.

When **management-interface configuration-mode** is set to **classic**, attempts to access (read or write) the configuration using the Nokia configuration modules or namespace via NETCONF results in errors, even if **nokia-combined-modules** or **nokia-submodules** is enabled.

This command and the **nokia-submodules** command cannot both be enabled at the same time.

The **no** form of this command disables support of the combined Nokia SR OS YANG files.

Default nokia-combined-modules

Platforms All

18.91 nokia-submodules

nokia-submodules

Syntax [**no**] **nokia-submodules**

Context **[Tree]** (config>system>management-interface>yang-modules nokia-submodules)

Full Context configure system management-interface yang-modules nokia-submodules

Description This command enables support of the alternative submodule-based packaging of the Nokia SR OS YANG files for both configuration and state data in the SR OS NETCONF server.

When **management-interface configuration-mode** is set to **classic**, attempts to access (read or write) the configuration using the Nokia configuration modules or namespace via NETCONF results in errors, even if **nokia-combined-modules** or **nokia-submodules** is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command and the **nokia-combined-modules** command cannot both be enabled at the same time.

The **no** form of this command disables support of submodule-based packaging of the Nokia SR OS YANG files.

Default no nokia-submodules

Platforms All

18.92 non-dr-attract-traffic

non-dr-attract-traffic

Syntax [**no**] **non-dr-attract-traffic**

Context **[Tree]** (config>service>vprn>pim non-dr-attract-traffic)

Full Context configure service vprn pim non-dr-attract-traffic

Description This command specifies whether the router should ignore the designated router state and attract traffic even when it is not the designated router.

An operator can configure an interface (router or IES or VPRN interfaces) to IGMP and PIM. The interface IGMP state will be synchronized to the backup node if it is associated with the redundant peer port. The interface can be configured to use PIM which will cause multicast streams to be sent to the elected DR only. The DR will also be the router sending traffic to the DSLAM. Since it may be required to attract traffic to both routers a flag non-dr-attract-traffic can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. While using this flag, the router may not send the stream down to the DSLAM while not DR.

When enabled, the designated router state is ignored. When disabled, **no non-dr-attract-traffic**, the designated router value is honored.

Default no non-dr-attract-traffic

Platforms All

non-dr-attract-traffic

Syntax **non-dr-attract-traffic** [**from-evpn**] [**from-pim-mvpn**]
no non-dr-attract-traffic

Context **[Tree]** (config>service>vpls>bind>evpn-mcast-gateway non-dr-attract-traffic)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls allow-ip-int-bind evpn-mcast-gateway non-dr-attract-traffic

Description This command triggers the required procedures so that multicast traffic can be attracted to the router when it is not elected as DR.

The **no** form of this command disables the attraction of non-DR traffic.

Default non-dr-attract-traffic from-pim-mvpn

Parameters **from-evpn** — Specifies that non-DR traffic generates a wildcard SMET route to attract the MCAST traffic from the OISM domain. No Layer 3 IFF or PIM/C-MCAST route is triggered from received SMET routes on the non-DR.

from-pim-mvpn — Specifies that non-DR traffic does not generate a wildcard SMET route but it does create an IIF or generate PIM/C-MCAST join upon receiving an SMET route. Local joins on a non-SBD service generate PIM/C-MCAST routes or SMETs despite this.

Platforms All

non-dr-attract-traffic

Syntax [**no**] **non-dr-attract-traffic**

Context **[Tree]** (config>router>pim non-dr-attract-traffic)

Full Context configure router pim non-dr-attract-traffic

Description This command specifies whether the router should ignore the designated router state and attract traffic even when it is not the designated router.

An operator can configure an interface (router or IES or VPRN interfaces) to IGMP and PIM. The interface state will be synchronized to the backup node if it is associated with the redundant peer port. The interface can be configured to use PIM which will cause multicast streams to be sent to the elected DR only. The DR will also be the router sending traffic to the DSLAM. Since it may be required to attract traffic to both routers a flag non-dr-attract-traffic can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. While using this flag, the router may not send the stream down to the DSLAM while not DR.

When enabled, the designated router state is ignored.

The **no** form of this command the designated router value is honored.

Default no non-dr-attract-traffic

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.93 non-multi-chassis-tunnel-id-range

non-multi-chassis-tunnel-id-range

Syntax **non-multi-chassis-tunnel-id-range start** *l2tp-tunnel-id* **end** *l2tp-tunnel-id*
non-multi-chassis-tunnel-id-range default
no non-multi-chassis-tunnel-id-range

Context **[Tree]** (config>system>l2tp non-multi-chassis-tunnel-id-range)

Full Context configure system l2tp non-multi-chassis-tunnel-id-range

Description This command sets the tunnel-id range that is used to allocate a new tunnel-id for a tunnel for which no multi-chassis redundancy is configured.

The **no** form of this command is a double negation and means all tunnel-IDs are configured for multi-chassis redundancy.

Default Sets the tunnel-id range to the full tunnel-id range available on this system meaning that by default no tunnel-ID has multi-chassis redundancy.

non-multi-chassis-tunnel-id-range default or non-multi-chassis-tunnel-id-range start 1 end <maximum *tunnel-id*>

The default for **start** *l2tp-tunnel-id* is 1. No tunnel-ids are available for which no multi-chassis redundancy is configured when set to 0.

The default for **end** *l2tp-tunnel-id* is the maximum tunnel-id allowed on this system. The **end** *l2tp-tunnel-id* must be set to 0 when the **start** *l2tp-tunnel-id* is set to 0 and vice versa.

Parameters **start** *l2tp-tunnel-id* — Specifies the start of the range of L2TP tunnel identifiers that can be allocated by L2TP on this system, to be synchronized with Multi Chassis Redundancy Synchronization (MCS).

Values 0 to 16383

end *l2tp-tunnel-id* — Specifies the end of the range of L2TP tunnel identifiers that can be allocated by L2TP on this system, to be synchronized with Multi Chassis Redundancy Synchronization (MCS).

Values 1 to 16383

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.94 non-sub-traffic

non-sub-traffic

Syntax **non-sub-traffic sub-profile** *sub-profile-name* **sla-profile** *sla-profile-name* [**subscriber** *sub-ident-string*] [**app-profile** *app-profile-name*]
no non-sub-traffic

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt>single-sub non-sub-traffic)
[Tree] (config>service>vpls>sap>sub-sla-mgmt>single-sub non-sub-traffic)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt>single-sub non-sub-traffic)
[Tree] (config>subscr-mgmt>msap-policy>sub-sla-mgmt>single-sub non-sub-traffic)

Full Context configure service ies subscriber-interface group-interface sap sub-sla-mgmt single-sub-parameters non-sub-traffic
configure service vpls sap sub-sla-mgmt single-sub-parameters non-sub-traffic
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt single-sub-parameters non-sub-traffic
configure subscriber-mgmt msap-policy sub-sla-mgmt single-sub-parameters non-sub-traffic

Description This command configures traffic profiles for non-IP traffic such as PPPoE packets on a VPLS SAP. It is used in conjunction with the **profiled-traffic-only** command to forward non-IP traffic through the single subscriber SAP without the need for SAP queues.

The **no** form of this command removes any configured profile.

Parameters *sub-profile-name* — Specifies an existing subscriber profile name to be associated with the non-sub-traffic L2 host. The subscriber profile is configured in the **config>subscr-mgmt>sub-profile** context.

sla-profile-name — Specifies an existing SLA profile name to be associated with the non-sub-traffic L2 host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

sub-ident-string — Specifies the subscriber ID to be associated with the non-sub-traffic L2 host. The *sub-ident-string* should match the dynamic subscriber associated with the SAP. If no *sub-ident-string* is configured and no dynamic subscriber is yet associated, then the system will use a default subscriber ID that is overridden when a dynamic subscriber is created on the SAP.

app-profile-name — Specifies an existing app profile name to be associated with the non-sub-traffic L2 host. The application profile is configured in the **config>app-assure>group>policy>app-prof** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.95 non-vid-pid-absent

non-vid-pid-absent

Syntax **non-vid-pid-absent** *milli-seconds*
no non-vid-pid-absent

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms non-vid-pid-absent)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms non-vid-pid-absent)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms non-vid-pid-absent)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms non-vid-pid-absent
configure mcast-management multicast-info-policy bundle channel video analyzer alarms non-vid-pid-absent
configure mcast-management multicast-info-policy bundle video analyzer alarms non-vid-pid-absent

Description This command configures the analyzer to check for a PID within the specified interval.

Default no non-vid-pid-absent

Parameters *milli-seconds* — Specifies the interval, in milliseconds.

Values 100 to 5000

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

18.96 nonce-length

nonce-length

Syntax **nonce-length** *length*
no nonce-length

Context **[Tree]** (config>router>l2tp>l2tpv3 nonce-length)
[Tree] (config>service>vprn>l2tp>l2tpv3 nonce-length)
[Tree] (config>service>vprn>l2tp>group>l2tpv3 nonce-length)

Full Context configure router l2tp l2tpv3 nonce-length
configure service vprn l2tp group l2tpv3 nonce-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn l2tp l2tpv3 nonce-length

Description This command configures the length for the local L2TPv3 nonce (random number) value used in the Nonce AVP.

The **no** form of this command removes the nonce length from the configuration.

Default no nonce-length

Parameters *length* — Specifies the length of the Nonce AVP value.

Values 16 to 64

default — When specified within the **config>service>vprn>l2tp>group>l2tpv3** context, this is referencing to the **nonce-length** configuration within the **config>service>vprn>l2tp>l2tpv3** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.97 normal-state

normal-state

Syntax **normal-state** {**open** | **closed**}

Context **[Tree]** (config>system>alarm-contact-input normal-state)

Full Context configure system alarm-contact-input normal-state

Description This command configures the normal state of the alarm contact input circuit. When the system detects a transition from the normal state, an alarm is generated. The alarm is cleared when the system detects a transition back to the normal state.

Note: Configure the normal state as **closed** if an external power source is used to power the alarm contact inputs.

Default normal-state open

Parameters **open** — Specifies that the normal state of the alarm contact input circuit is open. When the system detects a transition to the closed state, an alarm is generated. The alarm is cleared when the system detects a transition back to the open state.

closed — Specifies that the normal state of the alarm contact input circuit is closed. When the system detects a transition to the open state, an alarm is generated. The alarm is cleared when the system detects a transition back to the closed state.

Platforms 7750 SR-a

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.98 notification

notification

Syntax [**no**] **notification**

Context **[Tree]** (config>port>ethernet>lldp>dstmac notification)

Full Context configure port ethernet lldp dest-mac notification

Description This command enables LLDP notifications.

The **no** form of this command disables LLDP notifications.

Default no notification

Platforms All

notification

Syntax **notification** [**neighbor** *ip-address* | **group** *name*]
no notification

Context **[Tree]** (debug>router>bgp notification)

Full Context debug router bgp notification

Description This command decodes and logs all sent and received notification messages in the debug log.

The **no** form of this command disables the debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.99 notification-bundling

notification-bundling

Syntax **notification-bundling**

Context **[Tree]** (config>system>telemetry notification-bundling)

Full Context configure system telemetry notification-bundling

Description Commands in this context configure SubscribeResponse notification bundling.

Platforms All

18.100 notification-interval

notification-interval

Syntax **notification-interval** *time*
no notification-interval

Context **[Tree]** (config>system>lldp notification-interval)

Full Context configure system lldp notification-interval

Description This command configures the minimum time between change notifications.

The **no** form of this command reverts to the default value.

Default no notification-interval

Parameters *time* — Specifies the minimum time, in seconds, between change notifications.

Values 5 to 3600

Default 5

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.101 notify

notify

Syntax **notify** [**detail**]
no notify

Context **[Tree]** (debug>router>gmpls>packet notify)

Full Context debug router gmpls packet notify

Description This command enables debugging for GMPLS Notify packets.

The **no** form of the command disables debugging for GMPLS Notify packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

18.102 notify-dest-change

notify-dest-change

Syntax [**no**] **notify-dest-change**

Context **[Tree]** (config>filter>redirect-policy notify-dest-change)

Full Context configure filter redirect-policy notify-dest-change

Description This command instructs the system to send notifications (Log, SNMP, …) when the active destination of a redirect policy changes. No notification is sent when there are no more active destinations (as this is covered by a specific other notification). Notifications can be controlled (using the **config>log>event-control** command) using application ID *2017* and event-name *tFilterRPActiveDstChangeEvent*.

The **no** form of the command disables notification generation.

Default no notify-dest-change

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.103 nssa

nssa

Syntax [**no**] **nssa**

Context **[Tree]** (config>service>vprn>ospf>area nssa)
[Tree] (config>service>vprn>ospf3>area nssa)

Full Context configure service vprn ospf area nssa
configure service vprn ospf3 area nssa

Description This command creates the context to configure an OSPF Not So Stubby Area (NSSA) and adds/removes the NSSA designation from the area.

NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF domain.

Existing virtual links of a non-stub or NSSA area are removed when the designation is changed to NSSA or stub.

An area can be designated as stub or NSSA but never both at the same time.

By default, an area is not configured as an NSSA area.

The **no** form of this command removes the NSSA designation and configuration context from the area.

Default no nssa — The OSPF area is not an NSSA.

Platforms All

nssa

Syntax [**no**] **nssa**

Context **[Tree]** (config>router>ospf>area nssa)
[Tree] (config>router>ospf3>area nssa)

Full Context configure router ospf area nssa
configure router ospf3 area nssa

Description This command creates the context to configure an OSPF or OSPF3 Not So Stubby Area (NSSA) and adds/removes the NSSA designation from the area.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF or OSPF3 domain.

Existing virtual links of a non-stub or NSSA area will be removed when the designation is changed to NSSA or stub.

An area can be designated as stub or NSSA but never both at the same time.

By default, an area is not configured as an NSSA area.

The **no** form of this command removes the NSSA designation and configuration context from the area.

Default no nssa

Platforms All

18.104 nssa-range

nssa-range

Syntax **nssa-range** [*ip-address*]
no nssa-range

Context **[Tree]** (debug>router>ospf nssa-range)
[Tree] (debug>router>ospf3 nssa-range)

Full Context debug router ospf nssa-range
debug router ospf3 nssa-range

Description This command enables debugging for an NSSA range.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address range to debug OSPF or OSPF3 leaks.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.105 ntf-logout-retry-count

ntf-logout-retry-count

Syntax **ntf-logout-retry-count** [*value*]
no ntf-logout-retry-count

Context **[Tree]** (config>router>wpp>portals>portal ntf-logout-retry-count)
[Tree] (config>service>vprn>wpp>portals>portal ntf-logout-retry-count)

Full Context configure router wpp portals portal ntf-logout-retry-count
configure service vprn wpp portals portal ntf-logout-retry-count

Description This command configures the number of retransmissions of an NTF_LOGOUT message.

The **no** form of this command reverts to the default.

Default ntf-logout-retry-count 5

Parameters *value* — Specifies the number of retransmissions of an NTF_LOGOUT message.

Values 0 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

18.106 ntp

ntp

Syntax [**no**] **ntp**

Context **[Tree]** (config>service>vprn ntp)

Full Context configure service vprn ntp

Description Commands in this context configure Network Time Protocol (NTP) and its operation. It also enables NTP server mode within the VPRN routing instance so that the router will respond to NTP requests from external clients received inside the VPRN.

The **no** form of this command stops the execution of NTP and removes its configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ntp

Syntax [**no**] **ntp**

Context **[Tree]** (config>system>time ntp)

Full Context configure system time ntp

Description Commands in this context configure Network Time Protocol (NTP) and its operation. This protocol defines a method to accurately distribute and maintain time for network elements. Furthermore, this capability allows for the synchronization of clocks between the various network elements. Use the no form of the command to stop the execution of NTP and remove its configuration.

Default ntp

Platforms All

ntp

Syntax **ntp** [**router** *router-instance*] [**interface** *ip-int-name*]

Context **[Tree]** (debug>system ntp)

Full Context debug system ntp

Description This command enables and configures debugging for NTP.

The **no** form of the command disables debugging for NTP.

Parameters *router-instance* — Specifies the router name or CPM router instance.

Values *router-name* | *vprn-svc-id*
router-name – “Base”, “management”
vprn-svc-id – 1 to 2147483647

Default Base

ip-int-name — Specifies the name of the IP interface. The name can be up to 32 characters and must begin with a letter. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.107 ntp-reply

ntp-reply

Syntax [**no**] **ntp-reply**

Context **[Tree]** (config>service>ies>if>vrrp ntp-reply)
[Tree] (config>service>ies>if>ipv6>vrrp ntp-reply)

Full Context configure service ies interface ipv6 vrrp ntp-reply
configure service ies interface vrrp ntp-reply

Description This command enables the reception and response to NTP Requests directed at the VRRP virtual IP address. This behavior only applies the router currently acting as the master VRRP router.

The **no** form of this command disables NTP Requests from being processed.

Default no ntp-reply

Platforms All

ntp-reply

Syntax [**no**] **ntp-reply**

Context **[Tree]** (config>service>vprn>if>vrrp ntp-reply)
[Tree] (config>service>vprn>if>ipv6>vrrp ntp-reply)

Full Context configure service vprn interface ipv6 vrrp ntp-reply
configure service vprn interface vrrp ntp-reply

Description This command enables the reception and response to NTP Requests directed at the VRRP virtual IP address. This behavior only applies the router currently acting as the master VRRP router.

The **no** form of this command disables NTP Requests from being processed.

Default no ntp-reply

Platforms All

ntp-reply

Syntax [**no**] **ntp-reply**

Context **[Tree]** (config>router>if>vrrp ntp-reply)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>if>ipv6>vrrp ntp-reply)

Full Context configure router interface ipv6 vrrp ntp-reply
configure router interface vrrp ntp-reply

Description This command enables the reception and response to NTP Requests directed at the VRRP virtual IP address. This behavior only applies the router currently acting as the master VRRP router.

The **no** form of this command disables NTP Requests from being processed.

Default no ntp-reply

Platforms All

18.108 ntp-server

ntp-server

Syntax **ntp-server** [**authenticate**]
no ntp-server

Context [Tree] (config>system>time>ntp ntp-server)

Full Context configure system time ntp ntp-server

Description This command configures the node to assume the role of an NTP server. Unless the **server** command is used, this node will function as an NTP client only and will not distribute the time to downstream network elements.

Default no ntp-server

Parameters **authenticate** — Specifies to make authentication a requirement (optional). If authentication is required, the authentication key-id received in a message must have been configured in the **authentication-key** command, and that key-id type and key value must also match.

The authentication key from the received messages will be used for the transmitted messages.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.109 number

number

Syntax **number** {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *event-id*
no number

Context **[Tree]** (config>service>vprn>log>filter>entry>match number)

Full Context configure service vprn log filter entry match number

Description This command adds an SR OS application event number as a match criterion.

SR OS event numbers uniquely identify a specific logging event within an application.

Only one **number** command can be entered per event filter entry. The latest **number** command overwrites the previous command.

The **no** form of this command removes the event number as a match criterion.

Default no event-number — No event ID match criterion is specified.

Parameters **eq | neq | lt | lte | gt | gte** — Specifies the type of match. Valid operators are listed below.

Values

Operator	Note
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

event-id — Specifies the event ID, expressed as a decimal integer.

Values 1 to 4294967295

Platforms All

number

Syntax **number** {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *event-id*
no number

Context **[Tree]** (config>log>filter>entry>match number)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log filter entry match number

Description This command adds an SR OS application event number as a match criterion.

SR OS event numbers uniquely identify a specific logging event within an application.

Only one **number** command can be entered per event filter entry. The latest **number** command overwrites the previous command.

The **no** form of this command removes the event number as a match criterion.

Parameters **eq | neq | lt | lte | gt | gte** — Specifies the type of match. Valid operators are listed in Table 103.

Table 103 **Valid Operators**

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

event-id — The event ID, expressed as a decimal integer.

Values 1 to 4294967295

Platforms All

18.110 number-down

number-down

Syntax **number-down** *number-lag-port-down* **level** *level-id*
no number-down *number-lag-port-down*

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac>mc-constraints number-down)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac mc-constraints number-down

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the number of ports down along with level for multicast CAC policy on an MSAP.

The **no** form of this command reverts to the default.

Parameters *number-lag-port-down* — Specifies the number of port in a LAG group that are down. If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface is as per the levels configured in this context.

Values 1 to 64 (for 64-link LAG)
1 to 32 (for other LAGs)

level-id — Specifies the amount of bandwidth available within a given bundle for MC traffic for a specified level.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

number-down

Syntax **number-down** *number-lag-port-down* **level** *level-id*
no number-down *number-lag-port-down*

Context **[Tree]** (config>service>vpls>sap>igmp-snooping>mcac>mc-constraints number-down)
[Tree] (config>service>vpls>sap>mld-snooping>mcac>mc-constraints number-down)

Full Context configure service vpls sap igmp-snooping mcac mc-constraints number-down
configure service vpls sap mld-snooping mcac mc-constraints number-down

Description This command configure the number of ports down along with level for multicast CAC policy on this interface.

Default no number-down

Parameters *number-lag-port-down* — Specifies that the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

Values 1 to 64 (for 64-link LAG) 1 to 32 (for other LAGs)

Platforms All

number-down

Syntax **number-down** *number-lag-port-down* **level** *level-id*
no number-down

Context **[Tree]** (config>service>vprn>igmp>if>mcac>mc-constraints number-down)
[Tree] (config>service>vprn>mld>if>mcac>mc-constraints number-down)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>pim>if>mcac>mc-constraints number-down)

Full Context configure service vprn igmp interface mcac mc-constraints number-down
configure service vprn mld interface mcac mc-constraints number-down
configure service vprn pim interface mcac mc-constraints number-down

Description This command configures the number of ports down and level for interface's multicast CAC policy.

The **no** form of this command removes the values from the configuration.

Default not enabled

Parameters *number-lag-port-down* — If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

Values 1 to 64 (for 64-link LAG)
1 to 32 (for other LAGs)

level-id — Specifies an entry for the multicast CAC policy constraint level configured on this system.

Values 1 to 8

Platforms All

number-down

Syntax **number-down** *number-lag-port-down* **level** *level-id*
no number-down *number-lag-port-down*

Context [Tree] (config>router>igmp>if>mcac>mc-constraints number-down)
[Tree] (config>router>mld>if>mcac>mc-constraints number-down)
[Tree] (config>router>pim>if>mcac>mc-constraints number-down)

Full Context configure router igmp interface mcac mc-constraints number-down
configure router mld interface mcac mc-constraints number-down
configure router pim interface mcac mc-constraints number-down

Description This command configures the number of ports down along with level for the MCAC policy on this interface.

The **no** form of this command removes the values from the configuration.

Parameters *number-lag-port-down* — Specifies the number of LAG ports down. If the number of ports available in the LAG is reduced by the number of ports configured in this command, then the bandwidth allowed for a bundle or interface will be as per the levels configured in this context.

Values 1 to 64 (for 64-link LAG)
1 to 32 (for other LAGs)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

level *level-id* — Specifies the bandwidth for a given level. Level 1 has the highest priority. Level 8 has the lowest priority.

Values 1 to 8

Platforms All

number-down

Syntax [**no**] **number-down** *number-of-lag-ports-down*

Context **[Tree]** (config>vrrp>policy>priority-event>lag-port-down number-down)

Full Context configure vrrp policy priority-event lag-port-down number-down

Description This command creates a context to configure an event set threshold within a lag-port-down priority control event.

The **number-down** command defines a sub-node within the **lag-port-down** event and is uniquely identified with the *number-of-lag-ports-down* parameter. Each **number-down** node within the same **lag-port-down** event node must have a unique *number-of-lag-ports-down* value. Each **number-down** node has its own **priority** command that takes effect whenever that node represents the current threshold.

The total number of sub-nodes (uniquely identified by the *number-of-lag-ports-down* parameter) allowed in a single **lag-port-down** event is equal to the total number of possible physical ports allowed in a LAG.

A **number-down** node is not required for each possible number of ports that could be down. The active threshold is always the closest lower threshold. When the number of ports down equals a given threshold, that is the active threshold.

The **no** form of the command deletes the event set threshold. The threshold may be removed at any time. If the removed threshold is the current active threshold, the event set thresholds must be re-evaluated after removal.

Default no number-down — No threshold for the LAG priority event is created.

Parameters *number-of-lag-ports-down* — The number of LAG ports down to create a set event threshold. This is the active threshold when the number of down ports in the LAG equals or exceeds *number-of-lag-ports-down*, but does not equal or exceed the next highest configured *number-of-lag-ports-down*.

Values 1 to 64 (applies to 64-link LAG) 1 to 32 (applies to other LAGs)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

18.111 number-paths

number-paths

Syntax **number-paths** *number-of-paths* [**redundant-sfm** *number-of-paths*]

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2-paths>secondary-paths number-paths)

Full Context configure mcast-management bandwidth-policy t2-paths secondary-paths number-paths

Description This command is used to explicitly provision the number of secondary paths (and imply the number of primary paths) supported by the TChip based forwarding plane the bandwidth policy is managing. The default (and minimum) number of secondary paths is 1 and the maximum configurable is 15. The number of primary paths is total number of available paths minus the number of secondary paths.

Secondary paths are used by:

- Expedited VPLS, IES and VPRN service ingress multipoint queues
- Expedited network ingress multipoint queues
- Managed multicast explicit path primary channels (using the primary paths managed multipoint queue)
- All managed multicast dynamic path channels when the primary paths or multicast planes are not at their limit (using the primary paths managed multipoint queue)
- Highest preference managed multicast dynamic path channels when the primary paths or multicast planes are at their limit (using the primary paths managed multipoint queue)

Secondary paths are used by:

- Best-Effort VPLS, IES and VPRN service ingress multipoint queues
- Best-Effort network ingress multipoint queues
- Managed multicast explicit path secondary channels (using the secondary paths managed multipoint queue)
- Lower preference managed multicast dynamic path channels when the primary paths or multicast planes are at their limit (using the secondary paths managed multipoint queue)

The number of secondary paths should be increased from the default value of 1 when a single secondary path is enough for explicit secondary path managed traffic or the amount of best-effort multipoint non-managed queue traffic.

The **no** form of this command restores the default number of secondary paths.

Default number-paths 1 redundant-sfm 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number-of-paths* — Specifies the number of secondary paths when only one switch fabric is active, while the dual-sfm parameter specifies the same value when two switch fabrics are active.

Values 1 to 15

Default 1

18.112 number-retries

number-retries

Syntax **number-retries** *number-retries*
no number-retries

Context **[Tree]** (config>service>vpls>mac-move number-retries)
[Tree] (config>service>template>vpls-template>mac-move number-retries)

Full Context configure service template vpls-template mac-move number-retries
configure service vpls mac-move number-retries

Description This command configures the number of times retries are performed for re-enabling the SAP/SDP.

Default number-retries 3

Parameters *number-retries* — Specifies number of retries for re-enabling the SAP/SDP. A zero (0) value indicates unlimited number of retries.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19 o Commands

19.1 oam

oam

Syntax **oam**

Context **[Tree]** (oam oam)

Full Context oam

Description Commands in this context use the OAM test suite.

Platforms All

oam

Syntax [**no**] **oam**

Context **[Tree]** (config>service>vpls>gsmp>group>ancp oam)
[Tree] (config>service>vprn>gsmp>group>ancp oam)

Full Context configure service vpls gsmp group ancp oam
configure service vprn gsmp group ancp oam

Description This command enables the GSMP ANCP OAM capability to be negotiated at startup of the GSMP connection.

The **no** form of this command disables the feature.

Platforms All

oam

Syntax **oam**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>atm oam)
[Tree] (config>service>vpls>sap>atm oam)
[Tree] (config>service>vprn>interface>sap>atm oam)
[Tree] (config>service>vprn>sub-if>grp-if>sap>atm oam)

Full Context configure service ies subscriber-interface group-interface sap atm oam
configure service vpls sap atm oam

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap atm oam
configure service vprn subscriber-interface group-interface sap atm oam

Description Commands in this context configure OAM functionality for a PVCC delimiting a SAP.

The ATM-capable MDAs support F5 end-to-end OAM functionality (AIS, RDI, Loopback):

- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
- GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
- GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service vprn subscriber-interface group-interface sap atm oam
- configure service ies subscriber-interface group-interface sap atm oam

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service vprn interface sap atm oam
- configure service vpls sap atm oam

oam

Syntax **oam**

Context **[Tree]** (config>service>apipe>sap>atm oam)
[Tree] (config>service>epipe>sap>atm oam)
[Tree] (config>service>ipipe>sap>atm oam)

Full Context configure service apipe sap atm oam
configure service epipe sap atm oam
configure service ipipe sap atm oam

Description Commands in this context configure OAM functionality for a PVCC delimiting a SAP.

- The ATM-capable MDAs support end-to-end and segment OAM functionality (AIS, RDI, Loopback) over both F5 (VC) and end-to-end F4 (VP) OAM:
- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance version 11/95
- GR-1248-CORE - Generic Requirements for Operations of ATM N3 June 1996
- GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) (AAL) Protocols Generic Requirements, Issue 1, July 1994

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

oam

Syntax **oam**

Context **[Tree]** (config>service>ies>if>sap>atm oam)

Full Context configure service ies interface sap atm oam

Description Commands in this context configure OAM functionality for a PVCC delimiting a SAP.

The ATM-capable MDAs support F5 end-to-end OAM functionality (AIS, RDI, Loopback):

- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
- GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
- GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

oam

Syntax **oam**

Context **[Tree]** (debug oam)

Full Context debug oam

Description This command enables OAM debugging.

Platforms All

oam

Syntax **oam**

Context **[Tree]** (config>system>atm oam)

Full Context configure system atm oam

Description This command configures system-wide ATM parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.2 oam-pm

oam-pm

Syntax **oam-pm session** *session-name* {**dm** | **dmm** | **lmm** | **slm** | **twamp-light**} {**start** | **stop**}

Context **[Tree]** (oam oam-pm)

Full Context oam oam-pm

Description This command allows the operator to start and stop on-demand OAM-PM sessions.

Parameters *session-name* — Identifies the session name, up to 32 characters, that the test is associated with.

dm — Specifies the MPLS delay measurement test that is affected by the command.

dmm — Specifies the DMM test that is affected by the command.

lmm — Specifies the LMM test that is affected by the command.

slm — Specifies the SLM test that is affected by the command.

twamp-light — Specifies the TWAMP-light test that is affected by the command.

start — Manually starts the test.

stop — Manually stops the test.

Platforms All

oam-pm

Syntax **oam-pm**

Context **[Tree]** (config oam-pm)

Full Context configure oam-pm

Description This is the top level context that contains the configuration parameters that defines storage parameters (including binning structures), availability/resiliency and the individual proactive, and on-demand tests used to gather the performance/statistical information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.3 oam-template

oam-template

Syntax [**no**] **oam-template** *name*

Context **[Tree]** (config>router>mpls>mpls-tp oam-template)

Full Context configure router mpls mpls-tp oam-template

Description This command creates or edits an OAM template Generally applicable proactive OAM parameters are configured using templates. The top-level template is the OAM template.

Generic MPLS-TP OAM and fault management parameters are configured in the OAM Template.

Proactive CC/CV uses BFD and parameters such as Tx/Rx timer intervals, multiplier and other session/fault management parameters specific to BFD are configured using a BFD Template, which is referenced from the OAM template.

Default no oam-template

Parameters *name* — Specifies a text string name for the template of up to 32 characters in printable 7-bit ASCII, enclosed in double quotes. Named OAM templates are referenced from the MPLS-TP path MEP configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

oam-template

Syntax **oam-template** *name*
no oam-template

Context **[Tree]** (config>router>mpls>lsp>working-tp-path>mep oam-template)
[Tree] (config>router>mpls>lsp>protect-tp-path>mep oam-template)

Full Context configure router mpls lsp protect-tp-path mep oam-template
configure router mpls lsp working-tp-path mep oam-template

Description This command applies an OAM template to an MPLS-TP working or protect path. It contains configuration parameters for proactive OAM mechanisms that can be enabled on the path; for example, BFD. Configuration of an OAM template is optional.

The **no** form of this command removes the OAM template from the path.

Default no oam-template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies a text string name for the template up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.4 ocsp

ocsp

Syntax [**no**] **ocsp**

Context **[Tree]** (debug>certificate ocsp)

Full Context debug certificate ocsp

Description This command enables debug output of the OCSP protocol for a CA profile.

The **no** form of this command disables the debug output.

Platforms All

ocsp

Syntax **ocsp**

Context **[Tree]** (config>system>security>pki>ca-profile ocsp)

Full Context configure system security pki ca-profile ocsp

Description Commands in this context configure OCSP parameters.

Platforms All

19.5 octet-counters

octet-counters

Syntax [**no**] **octet-counters**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes octet-counters)

Full Context configure aaa isa-radius-policy acct-include-attributes octet-counters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the inclusion of the octet-counters attributes.

The **no** form of the command excludes octet-counters attributes.

Default no octet-counters

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.6 octets-admitted-count

octets-admitted-count

Syntax [**no**] **octets-admitted-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr octets-admitted-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr octets-admitted-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters octets-admitted-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters octets-admitted-count

Description This command includes the admitted octet count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of this command excludes the admitted octet count.

Default no octets-admitted-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.7 octets-denied-count

octets-denied-count

Syntax [**no**] **octets-denied-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr octets-denied-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr octets-denied-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters octets-denied-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log accounting-policy custom-record aa-specific to-aa-sub-counters octets-denied-count

Description This command includes the denied octet count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of this command excludes the denied octet count.

Default no octets-denied-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.8 of-controller

of-controller

Syntax [**no**] **of-controller** *ip-address:port*

Context **[Tree]** (config>open-flow>of-switch of-controller)

Full Context configure open-flow of-switch of-controller

Description This command configures the OpenFlow controller for this OpenFlow switch and creates a context for the configuration of additional OpenFlow control channel parameters. Up to two controllers can be configured per OpenFlow switch instance.

The **no** form of this command deletes the controller for this OpenFlow switch instance.

Parameters *ip-address:port* — Specifies the IP address and TCP port for the OpenFlow channel to the controller.

Values

ipv4-address	a.b.c.d:port
ipv6-address	[x:x:x:x:x:x:x:x]:port (eight 16-bit pieces)
	x: [0..FFFF]H
port	1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.9 of-switch

of-switch

Syntax **of-switch** *ofs-name* [**ofs-id** *ofs-id*]
no of-switch *ofs-name*

Context **[Tree]** (config>open-flow of-switch)

Full Context configure open-flow of-switch

Description This command creates an OpenFlow switch instance.

The **no** form of the command deletes the OpenFlow switch instance from the context.

Default no of-switch

Parameters *ofs-name* — specifies the name of the OpenFlow switch instance, a string up to 32 characters.

ofs-id — Specifies the ID of the switch. This is used together with the chassis MAC address to generate the Datapath ID of the OpenFlow switch instance. If it is not configured, an automatically generated Datapath ID is assigned to the switch according to the order in which the OFS instance came up relative to other OFS instances on the node. The configuration should be saved after configuring the OFS ID. If the user originally configures the OFS without an OFS ID, and subsequently adds an OFS ID without saving the new configuration, the OFS may not get the same Datapath ID (which is allocated on a first-come, first-served basis in the absence of an OFS ID).

Values 1 to 8

Platforms All

19.10 offer-selection

offer-selection

Syntax **offer-selection**

Context **[Tree]** (config>service>ies>sub-if>grp-if>dhcp offer-selection)
[Tree] (config>service>vprn>sub-if>dhcp offer-selection)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp offer-selection)

Full Context configure service ies subscriber-interface group-interface dhcp offer-selection
configure service vprn subscriber-interface dhcp offer-selection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface dhcp offer-selection

Description Commands in this context configure a discover delay to influence the offer selection of DHCPv4 clients.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.11 offer-time

offer-time

Syntax **offer-time** [**min** *minutes*] [**sec** *seconds*]
no offer-time

Context **[Tree]** (config>router>dhcp>server>pool offer-time)
[Tree] (config>service>vprn>dhcp>server>pool offer-time)

Full Context configure router dhcp local-dhcp-server pool offer-time
configure service vprn dhcp local-dhcp-server pool offer-time

Description This command configures the time interval during which a DHCP offer is valid.

The **no** form of this command reverts to the default.

Default offer-time min 1

Parameters *time* — Specifies the offer time.

Values

min *minutes*	0 to 10
sec *seconds*	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.12 offered-measurement

offered-measurement

Syntax **offered-measurement**

Context **[Tree]** (config>qos>adv-config-policy>child-control offered-measurement)

Full Context configure qos adv-config-policy child-control offered-measurement

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command modifies the offered rate measurement used to determine the bandwidth the queue or policer is requesting from its parent virtual scheduling context.

This command modifies the parameters that control the child requested bandwidth for all policers and queues associated with the policy.

Platforms All

19.13 offset

offset

Syntax **offset** *offset*

Context **[Tree]** (config>system>time>dst-zone offset)

Full Context configure system time dst-zone offset

Description This command specifies the number of minutes that will be added to the time when summer time takes effect. The same number of minutes will be subtracted from the time when the summer time ends.

Default offset 60

Parameters *offset* — Specifies the number of minutes added to the time at the beginning of summer time and subtracted at the end of summer time, expressed as an integer.

Values 0 to 60

Default 60

Platforms All

19.14 on-cac-failure

on-cac-failure

Syntax [**no**] **on-cac-failure**

Context **[Tree]** (config>router>rsvp>te-threshold-update on-cac-failure)

Full Context configure router rsvp te-threshold-update on-cac-failure

Description This command is used to enable a CAC failure-triggered IGP update.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command should reset on-cac-failure to the default value and disable the CAC failure-triggered IGP update.

Default no on-cac-failure

Platforms All

19.15 on-error

on-error

Syntax [**no**] **on-error**

Context **[Tree]** (debug>diameter>node on-error)

Full Context debug diameter node on-error

Description This command debugs Diameter node errors. Only errors raised before the peer is determined. For example, there is no route for this message in the realm routing table, and therefore the peer cannot be determined.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

on-error

Syntax [**no**] **on-error**

Context **[Tree]** (debug>dia>node>peer on-error)

Full Context debug dia node peer on-error

Description This command reports only peer error conditions.

on-error

Syntax [**no**] **on-error**

Context **[Tree]** (debug>diam>application on-error)
[Tree] (debug>diam>application>policy on-error)

Full Context debug diameter application on-error
debug diameter application policy on-error

Description This command debugs Diameter application errors and reports only peer error conditions, for example, an unknown session-id.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.16 on-failure

on-failure

Syntax **on-failure** [**failover** {**enabled** | **disabled**}] [**handling** {**continue** | **retry-and-terminate** | **terminate**}]
no on-failure

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy on-failure)

Full Context configure subscriber-mgmt diameter-application-policy on-failure

Description This command is applicable only to the R16.0R4 or later implementation of Diameter base in the SR OS.

This command configures session failure handling. The behavior of a Diameter application (Gx, Gy, or NASREQ) that fails to receive a response (an answer message CCA) to a transmitted request message (CCR) for a session, can be controlled by the Diameter server through two AVPs carried in CCA messages that are defined in RFC 4006, *Diameter Credit-Control Application*:

- CC-Session-Failover AVP
  - FAILOVER_NOT_SUPPORTED
  - FAILOVER_SUPPORTED
- Credit-Control-Failure-Handling AVP
  - TERMINATE
  - CONTINUE
  - RETRY_AND_TERMINATE

If those AVPs are not provided by the Diameter server, the local configuration provided by this command takes effect. This command defines the following:

- Retransmission behavior of the application in case that the response to a transmitted request message is not received. The Diameter base notifies the application after the lifetime of the transmitted request message expires (tx timeout) or the route to the destination-realm is unavailable. Depending on the configuration option, the application can then retransmit the message, or suppress retransmission.
- Handling behavior defines whether the session is terminated or continues to exist in absence of the response from the Diameter server.

Default on-failure failover enabled handling terminate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **failover enabled** — Specifies that application session is allowed to retransmit the request message (CCR).

failover disabled — Specifies that the application session is not allowed to retransmit the request message (CCR).

handling continue — Specifies that the sessions continues to exist if the response to a transmitted CCR message is not received. Whether the transmitted message is re-transmitted depends on the failover configuration. In case of session initiation procedure in the Gx case (CCR-I timeout), the subscriber host is nonetheless instantiated with the default parameters, assuming that they are provided. If the default parameter is not provided, the subscriber host initiation fails.

handling retry-and-terminate — Specifies that the message is re-transmitted in case that the failover is enabled. If the response to the retransmitted request message is not received (re-transmission times out), the application session is terminated.

handling terminate — Specifies that the session is terminated if the response to the original request message is not received. No re-transmissions is attempted, regardless of whether or not the failover is enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

on-failure

Syntax **on-failure** [**failover** {**enabled** | **disabled**}] [**handling** {**continue** | **retry-and-terminate** | **terminate**}]
no on-failure

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy on-failure)

Full Context configure subscriber-mgmt diameter-application-policy on-failure

Description This command is applicable to both legacy (pre-Release 16.0.R4) and new (Release 16.0.R4 and later) implementations of Diameter base in the SR OS.

- Legacy Diameter base description:

  This command configures session failure handling. The behavior of the application's session in case of a peer failure can be controlled by the Diameter server through two AVPs carried in CCA messages that are defined in RFC 4006, *Diameter Credit-Control Application*:

  - CC-Session-Failover AVP
    - FAILOVER_NOT_SUPPORTED
    - FAILOVER_SUPPORTED
  - Credit-Control-Failure-Handling AVP
    - TERMINATE
    - CONTINUE
    - RETRY_AND_TERMINATE

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If those AVPs are not provided by the Diameter server, the local configuration provided by this command will take effect. This command defines the following:

- The peer-failover behavior to a secondary peer if the primary peer is unresponsive. From the application point of view, the primary peer is considered unresponsive if the request message that was sent to it, times out. The time out of the message is determined by the tx-timer command.

  The peer-failover action based on the request message timeout is defined per session. In other words, a request message timeout for one session cannot cause the failover for some other session.

  The maximum number of transmissions per session is hard-coded to 2 and the same message is never re-transmitted to the same TCP socket (a TCP socket is defined as a current peering connection defined by the TCP source/destination IP addresses/ports; closing and then reopening a connection to the same peer will result in creation of a new TCP socket). Once the original message for the session times out on the primary peer, the message is re-transmitted to the secondary peer, provided that the secondary peer is available and the failover is enabled with the corresponding handling mechanism. In case that the secondary peer is unavailable, the original message is not be re-transmitted to the same primary peer again.

  Once the reply from a peer is received, the session is tied to that peer until the next timeout. In other words, the session always sticks to the peer from which it received the last response.
- The handling behavior if the response from the peer is not received or the peers are not available at all (all peering connections are closed). If the response to a session initiation message is not received, the fate of the session will depend on the configuration (the session can be terminated or continue to exist with default parameters).

• New Diameter base description:

This command configures session failure handling. The behavior of a Diameter application (Gx, Gy, or NASREQ) that fails to receive a response (an answer message CCA) to a transmitted request message (CCR) for a session, can be controlled by the Diameter server through two AVPs carried in CCA messages that are defined in RFC 4006, *Diameter Credit-Control Application*:

- CC-Session-Failover AVP
  - FAILOVER_NOT_SUPPORTED
  - FAILOVER_SUPPORTED
- Credit-Control-Failure-Handling AVP
  - TERMINATE
  - CONTINUE
  - RETRY_AND_TERMINATE

If those AVPs are not provided by the Diameter server, the local configuration provided by this command takes effect. This command defines the following:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Retransmission behavior of the application in case that the response to a transmitted request message is not received. The Diameter base notifies the application after the lifetime of the transmitted request message expires (tx timeout) or the route to the destination-realm is unavailable. Depending on the configuration option, the application can then retransmit the message, or suppress retransmission.
- Handling behavior defines whether the session is terminated or continues to exist in absence of the response from the Diameter server.

Default on-failure failover enabled handling terminate

Parameters **failover enabled** — Specifies that application session is allowed to switch to the secondary peer (for legacy Diameter base). For new Diameter base, this keyword specifies that application session is allowed to retransmit the request message (CCR).

failover disabled — Specifies that the application session is not allowed to switch to the secondary peer (for legacy Diameter base). For new Diameter base, this keyword specifies that the application session is not allowed to retransmit the request message (CCR).

handling continue — Specifies that the sessions continue to exist if the response to a transmitted CCR message is not received. Whether the transmitted message is re-transmitted depends on the failover configuration. In case of session initiation procedure in the Gx case (CCR-I timeout), the subscriber host is nonetheless instantiated with the default parameters, assuming that they are provided. If the default parameter are not provided, the subscriber host initiation fails.

handling retry-and-terminate — Specifies that the message is re-transmitted if the peer-failover is enabled and the secondary peer is available. Once the retransmitted request message is timed out, the application session is terminated (for legacy Diameter base). For new Diameter base, this keyword specifies that the message is re-transmitted if the failover is enabled. If the response to the retransmitted request message is not received (re-transmission times out), the application session is terminated.

handling terminate — Specifies that the session is terminated if the response to the original request message is not received. No re-transmissions is attempted, regardless if the failover is enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.17 on-link

on-link

Syntax [**no**] **on-link**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>ipv6>rtr-adv>pfx-opt on-link)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv>pfx-opt on-link)
[Tree] (config>service>vprn>router-advert>if on-link)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv>pfx-opt on-link)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv>pfx-opt on-link)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements prefix-options on-link
configure service ies subscriber-interface ipv6 router-advertisements prefix-options on-link
configure service vprn router-advert interface on-link
configure service vprn subscriber-interface group-interface ipv6 router-advertisements prefix-options on-link
configure service vprn subscriber-interface ipv6 router-advertisements prefix-options on-link

Description This command specifies whether the prefix is assigned to an interface on the specified link.

The **no** form of this command reverts to the default.

Default on-link

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

on-link

Syntax [**no**] **on-link**

Context [Tree] (config>subscr-mgmt>rtr-adv>pfx-opt>stateful on-link)
[Tree] (config>subscr-mgmt>rtr-adv>pfx-opt>stateless on-link)

Full Context configure subscriber-mgmt router-advertisement-policy prefix-options stateful on-link
configure subscriber-mgmt router-advertisement-policy prefix-options stateless on-link

Description This command specifies whether the prefix is to be assigned to an interface on the specified link.

The **no** form of this command reverts to the default.

Default on-link

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

on-link

Syntax [**no**] **on-link**

Context [Tree] (config>service>vprn>router-advert>if>prefix on-link)

Full Context configure service vprn router-advertisement interface prefix on-link

Description This command specifies whether the prefix can be used for onlink determination.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default on-link

Platforms All

on-link

Syntax [**no**] **on-link**

Context **[Tree]** (config>router>router-advert>if>prefix on-link)

Full Context configure router router-advertisement interface prefix on-link

Description This command specifies whether the prefix can be used for on link determination.

Default on link

Platforms All

19.18 one-garp-per-sap

one-garp-per-sap

Syntax [**no**] **one-garp-per-sap**

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp one-garp-per-sap)
[Tree] (config>service>vprn>sub-if>grp-if>srrp one-garp-per-sap)

Full Context configure service ies subscriber-interface group-interface srrp one-garp-per-sap
configure service vprn subscriber-interface group-interface srrp one-garp-per-sap

Description This command enables the sending of one gratuitous ARP to each SAP and is applicable to PPPoE only deployments in which there are multiple subnets under the subscriber interface. In such case, if the switchover occurs, it is sufficient to send a single Gratuitous ARP on every VLAN to update the Layer 2 forwarding path in the access aggregation network. This single gratuitous ARP will contain the IP address of the first GW address found under the subscriber interface address.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.19 one-time-http-redirection

one-time-http-redirection

Syntax **one-time-http-redirection ip-filter** *filter-id*
one-time-http-redirection

Context **[Tree]** (config>subscr-mgmt>sla-prof one-time-http-redirection)

Full Context configure subscriber-mgmt sla-profile one-time-http-redirection

Description This command specify the one-time http redirection filter id. This filter will apply to the host when host is created, and is replaced by the sla-profile ingress filter (configured in the **config>subscr-mgmt>sla-prof>ingress** context) after first HTTP request from host has been redirected.

Note: The system does not check if the configured filter include http-redirection entry. If the filter does not include the http-redirection then it will not be replaced in future.

If 7750 SR receives filter insertion via CoA or access-accept when one-time redirection filter is still active then the received filter entries will only be applied to the sla-profile ingress filter. And after 1st http redirection, the original sla-profile ingress filter + received filter will replace the redirection filter.

The **no** form of this command reverts to the default.

Parameters *filter-id* — Specifies the ID of filter that is used for HTTP redirection.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

one-time-http-redirection

Syntax **one-time-http-redirection**

Context **[Tree]** (debug>service>id one-time-http-redirection)

Full Context debug service id one-time-http-redirection

Description This command produces one-time HTTP redirection debug output.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.20 one-time-redirect

one-time-redirect

Syntax **one-time-redirect url** *rdr-url-string* **port** *port-num*
no one-time-redirect

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm one-time-redirect)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm one-time-redirect)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt one-time-redirect
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt one-time-redirect

Description This command enables one-time http-redirect to specify redirect URL for traffic matching the specified destination port.

The **no** form of this command reverts to the default.

Parameters **url** *rdr-url-string* — Specifies the HTTP web address that is sent to the user's browser.

port *port-num* — Specifies the destination port number as a decimal hex or binary.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.21 one-way-delay-test

one-way-delay-test

Syntax **one-way-delay-test** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*]

Context **[Tree]** (oam>eth-cfm one-way-delay-test)

Full Context oam eth-cfm one-way-delay-test

Description This command issues an ETH-CFM one-way delay test.

Parameters *mac-address* — Specifies a unicast destination MAC address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-mepid *mep-id* — Specifies the remote MEP ID of the peer within the association. The domain and association information are derived from the **source mep** for the session. The Layer 2 IEEE MAC address is resolved from previously-learned remote MAC addressing, derived from the reception and processing of the ETH-CC PDU. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

priority — Specifies the priority.

Values 0 to 7

Default 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.22 one-way-delay-threshold

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context **[Tree]** (config>eth-tunnel>path>eth-cfm>mep one-way-delay-threshold)
[Tree] (config>lag>eth-cfm>mep one-way-delay-threshold)
[Tree] (config>port>ethernet>eth-cfm>mep one-way-delay-threshold)

Full Context configure eth-tunnel path eth-cfm mep one-way-delay-threshold
configure lag eth-cfm mep one-way-delay-threshold
configure port ethernet eth-cfm mep one-way-delay-threshold

Description This command enables one way delay threshold time limit.

Default one-way-delay-threshold 3

Parameters *seconds* — Specifies the value, in seconds, for the threshold.

Values 0 to 600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep one-way-delay-threshold)

Full Context configure service epipe sap eth-cfm mep one-way-delay-threshold

Description This command enables/disables eth-test functionality on MEP.

Parameters *seconds* — Specifies the one way-delay threshold in seconds.

Values 0 to 600

Default 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context **[Tree]** (config>service>vpls>sap>eth-cfm>mep one-way-delay-threshold)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep one-way-delay-threshold)

Full Context configure service vpls sap eth-cfm mep one-way-delay-threshold
configure service vpls spoke-sdp eth-cfm mep one-way-delay-threshold

Description This command enables/disables eth-test functionality on MEP.

Parameters *seconds* — Specifies the one way delay threshold, in seconds

Values 0 to 600

Default 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context **[Tree]** (config>service>ies>if>sap>mep one-way-delay-threshold)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep one-way-delay-threshold)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep one-way-delay-threshold)

Full Context configure service ies interface sap mep one-way-delay-threshold
configure service ies interface spoke-sdp eth-cfm mep one-way-delay-threshold
configure service ies subscriber-interface group-interface sap eth-cfm mep one-way-delay-threshold

Description This command enables one way delay threshold time limit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default one-way-delay-threshold 3

Parameters *seconds* — Specifies the value for the threshold.

Values 0 to 600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep one-way-delay-threshold

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep one-way-delay-threshold

one-way-delay-threshold

Syntax **one-way-delay-threshold** *time*

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm one-way-delay-threshold)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm one-way-delay-threshold)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm one-way-delay-threshold)

Full Context configure service vprn interface sap eth-cfm one-way-delay-threshold
configure service vprn interface spoke-sdp eth-cfm one-way-delay-threshold
configure service vprn subscriber-interface group-interface sap eth-cfm one-way-delay-threshold

Description This command enables one way delay threshold time limit.

Default 3 seconds

Parameters *priority* — Specifies the value for the threshold.

Values 0 to 600

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context **[Tree]** (config>router>if>eth-cfm>mep one-way-delay-threshold)

Full Context configure router interface eth-cfm mep one-way-delay-threshold

Description This command enables a one-way delay threshold time limit.

Default one-way-delay-threshold 3

Parameters *seconds* — Specifies the value, in seconds, for the threshold.

Values 0 to 600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep one-way-delay-threshold)

Full Context configure eth-ring path eth-cfm mep one-way-delay-threshold

Description This command configures a one way delay threshold time limit.

Default one-way-delay-threshold 3

Parameters *seconds* — Specifies the value, in seconds, for the threshold.

Values 0 to 600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.23 opaque-data

opaque-data

Syntax **opaque-data** *hex-string*
no opaque-data

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action>insert-nsh>meta-data opaque-data)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action insert-nsh meta-data opaque-data

Description This command specifies 16-byte opaque data HEX string to be inserted in NSH meta-data (with MD-Type set to 1). The opaque data can also be provided (overridden) by AAA server. AAA server has precedence over static configuration. The **opaque-data** and **insert-subscriber-id** commands are mutually exclusive.

The **no** form of this command removes the HEX string from the configuration.

Parameters *hex-string* — Specifies the HEX string up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.24 opcode

opcode

Syntax [**no**] **opcode**

Context **[Tree]** (config>service>nat>pcp-server-policy opcode)

Full Context configure service nat pcp-server-policy opcode

Description This command specifies the PCP opcodes supported by the PCP servers using this PCP policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.25 open

open

Syntax **open** [**neighbor** *ip-address* | **group** *name*]
no open

Context **[Tree]** (debug>router>bgp open)

Full Context debug router bgp open

Description This command decodes and logs all sent and received open messages in the debug log.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

19.26 open-flow

open-flow

Syntax **open-flow**

Context **[Tree]** (config open-flow)

Full Context configure open-flow

Description This command enables configuration content for OpenFlow Hybrid Switch compatibility.

The **no** form of the command removes the OpenFlow configuration from the context.

Platforms All

19.27 oper-down-on-group-degrade

oper-down-on-group-degrade

Syntax [**no**] **oper-down-on-group-degrade**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw oper-down-on-group-degrade)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw oper-down-on-group-degrade)

Full Context configure service ies subscriber-interface group-interface wlan-gw oper-down-on-group-degrade
configure service vprn subscriber-interface group-interface wlan-gw oper-down-on-group-degrade

Description This command operationally brings down the WLAN-GW group if the total number of operational WLAN-GW IOMs in the WLAN-GW group fall below the configured number of active WLAN-GW IOMs. This triggers withdrawal of the route to tunnel endpoint and subscriber subnets in routing.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.28 oper-group

oper-group

Syntax **oper-group** *name*
no oper-group

Context **[Tree]** (config>service>epipe oper-group)

Full Context configure service epipe oper-group

Description This command associates an operational group to the status of the Epipe. When this oper-group is used in Epipes with static VXLAN or BGP-EVPN, the oper-group behaves as follows:

- The Epipe (and the oper-group) goes down if a SAP or spoke SDP go oper-down due to admin shutdown, service shutdown, or non-DF status as a result of EVPN multi-homing single-active election.
- The Epipe (and oper-group) will go down if the Epipe's EVPN destination is removed (due to an EVPN AD per-EVI route withdrawal, for instance).
- The Epipe (and oper-group) will not go down if a static VXLAN destination exists and the egress VTEP is not in the global route-table.

The operational group must be monitored in a different service and not in the service where it is defined.

The **no** version of this command removes the oper-group association.

Parameters *name* — Specifies the name of the **oper-group**, up to 32 characters.

Platforms All

oper-group

Syntax **oper-group** *name*
no oper-group

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls oper-group)
[Tree] (config>service>epipe>bgp-evpn>srv6 oper-group)
[Tree] (config>service>vpls>bgp-evpn>mpls oper-group)
[Tree] (config>service>vpls>bgp-evpn>vxlan oper-group)
[Tree] (config>service>system>bgp-evpn>eth-seg oper-group)

Full Context configure service epipe bgp-evpn mpls oper-group
configure service epipe bgp-evpn segment-routing-v6 oper-group
configure service system bgp-evpn ethernet-segment oper-group
configure service vpls bgp-evpn mpls oper-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls bgp-evpn vxlan oper-group

Description This command adds the BGP EVPN MPLS, SRv6, or VXLAN instance or Ethernet Segment (ES) as a member of the operational group.

When configured on an ES, the state of the operational group depends on the state of the SAPs contained in the ES. The operational group transitions to up if at least one SAP in the ES is up. The operational group goes down when all the associated SAPs are operationally down. The ES operational group should be monitored on the LAG associated to the ES, along with single-active multi-homing, so that the NDF state can be signaled to the CE by LAG standby signaling.

When configured on a BGP EVPN instance, the operational group is up when it is either empty (meaning that the operational group has no members) or at least an EVPN destination is created under the EVPN instance added as member. When configured, no other SAP, SDP binding, or BGP EVPN instance can be added to the same operational group within the same or a different service.

The operational group is down when the following apply:

- on a BGP EVPN instance
- the service is disabled
- the BGP EVPN MPLS, VXLAN or SRv6 instance are disabled
- all the EVPN destinations in the instance are removed

Default no oper-group

Parameters *name* — Specifies the name of the operational group, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service epipe bgp-evpn segment-routing-v6 oper-group

All

- configure service vpls bgp-evpn mpls oper-group
- configure service epipe bgp-evpn mpls oper-group
- configure service vpls bgp-evpn vxlan oper-group
- configure service system bgp-evpn ethernet-segment oper-group

oper-group

Syntax **oper-group** *name*
no oper-group

Context **[Tree]** (config>service>epipe>vxlan>egr-vtep oper-group)

Full Context configure service epipe vxlan egr-vtep oper-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates an operational group to the VXLAN static egress VTEP. If the egress VTEP IP disappears from the routing table, the oper-group status will become operationally down.

The operational group must be monitored in a different service and not in the service where it is defined.

The **no** version of this command removes the oper-group association.

Parameters *name* — Specifies the name of the **oper-group**, up to a maximum of 32 characters.

Platforms All

oper-group

Syntax **oper-group** *group-name*
no oper-group

Context **[Tree]** (config>service>epipe>sap oper-group)

Full Context configure service epipe sap oper-group

Description This command configures the operational group identifier.

The no form of this command removes the group name from the configuration.

Parameters *group-name* — Specifies the Operational-Group identifier up to 32 characters in length.

Platforms All

oper-group

Syntax **oper-group** *group-name*
no oper-group

Context **[Tree]** (config>service>vpls>sap oper-group)
[Tree] (config>service>vpls>spoke-sdp oper-group)
[Tree] (config>service>vpls>bgp>pw-template-binding oper-group)

Full Context configure service vpls bgp pw-template-binding oper-group
configure service vpls sap oper-group
configure service vpls spoke-sdp oper-group

Description This command associates the context to which it is configured to the operational group specified in the *group-name*. The **oper-group** *oper-name* must be already configured under **config>service** context before its name is referenced in this command.

The **no** form of this command removes the association.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no oper-group

Parameters *group-name* — Specifies a character string of maximum 32 ASCII characters identifying the group instance

Platforms All

oper-group

Syntax **oper-group** *group-name*
no oper-group

Context **[Tree]** (config>service>ies>if>vrrp oper-group)

Full Context configure service ies interface vrrp oper-group

Description This command configures VRRP to associate with an operational group. When associated, VRRP notifies the operational group of its state changes so that other protocols can monitor it to provide a redundancy mechanism. When VRRP is the master router (MR), the operational group is up and is down for all other VRRP states.

The **no** form of this command removes the association.

Default no oper-group

Parameters *group-name* — Specifies the operational group identifier up to 32 characters in length.

Platforms All

oper-group

Syntax **oper-group** *group-name*
no oper-group

Context **[Tree]** (config>service>vprn>if>vrrp oper-group)
[Tree] (config>service>vprn>if>ipv6>vrrp oper-group)

Full Context configure service vprn interface ipv6 vrrp oper-group
configure service vprn interface vrrp oper-group

Description This command configures VRRP to associate with an operational group. When associated, VRRP notifies the operational group of its state changes so that other protocols can monitor it to provide a redundancy mechanism. When VRRP is the master router (MR), the operational group is up and is down for all other VRRP states.

The **no** form of this command removes the association.

Default no oper-group — No operational group is configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-name* — Specifies the operational group identifier, up to 32 characters in length.

Platforms All

oper-group

Syntax **oper-group** *group-name*
no oper-group

Context **[Tree]** (config>router>if>vrrp oper-group)
[Tree] (config>router>if>ipv6>vrrp oper-group)

Full Context configure router interface ipv6 vrrp oper-group
configure router interface vrrp oper-group

Description This command configures VRRP to associate with an operational group. When associated, VRRP notifies the operational group of its state changes so that other protocols can monitor it to provide a redundancy mechanism. When VRRP is the master router (MR), the operational group is up; the operational group is down for all other VRRP states.

The **no** form of the command removes the association.

Default no oper-group — No operational group is configured.

Parameters *group-name* — Specifies the operational group identifier, up to 32 characters.

Platforms All

oper-group

Syntax **oper-group** *group-name* [**create**]
no oper-group *group-name*

Context **[Tree]** (config>service oper-group)

Full Context configure service oper-group

Description This command creates a system-wide group (operational group) name which can be used to associate a number of service objects (for example, SAPs or pseudowires). The status of the group is derived from the status of its members. The status of the group can then be used to influence the status of non-member objects. For example, when a group status is marked as down, the object(s) that monitor the group change their status accordingly.

The **no** form of the command removes the group. All the object associations need to be removed before the no form of the command can be executed.

Default no oper-group

Parameters *group-name* — Specifies the operational group identifier up to 32 characters in length.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms All

19.29 oper-members

oper-members

Syntax **oper-members** *oper-members*
no oper-members

Context **[Tree]** (config>service>vprn>isis>link-group>level oper-members)

Full Context configure service vprn isis link-group level oper-members

Description This command sets the threshold for the minimum number of operational links for the associated link-group. If the number of operational links drops below this threshold, the configured offsets are applied. For example, oper-members=3. The metric of the member interfaces is increased when the number of interfaces is lower than 3.

The **no** form of this command reverts the oper-members limit to 1.

Default no oper-members

Parameters *oper-members* — Specifies the number of operational members.

Values 0 to 8

Platforms All

oper-members

Syntax **oper-members** [*value*]
no oper-members

Context **[Tree]** (config>router>isis>link-group>level oper-members)

Full Context configure router isis link-group level oper-members

Description This command sets the threshold for the minimum number of operational links for the associated link-group. If the number of operational links drops below this threshold, the configured offsets are applied. For example, oper-members=3. The metric of the member interfaces is increased when the number of interfaces is lower than 3.

The **no** form of this command reverts the **oper-members** limit to 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default oper-members 1

Parameters *value* — Specifies the threshold for operational members.

Values 1 to 8

Platforms All

19.30 oper-up-on-mhstandby

oper-up-on-mhstandby

Syntax [**no**] **oper-up-on-mhstandby**

Context **[Tree]** (config>service>epipe>pw-port oper-up-on-mhstandby)

Full Context configure service epipe pw-port oper-up-on-mhstandby

Description This command causes the PW port to remain operationally up on the non-DF PE as well as all the PW SAPs contained in the PW port.

The PW port status shows an operationally up status with a flag MH Standby.

The **no** form of this command causes the PW port to remain operationally down on the non-DF PE as well as all the PW SAPs contained in the PW port.

Default no oper-up-on-mhstandby

Platforms All

19.31 oper-up-while-empty

oper-up-while-empty

Syntax [**no**] **oper-up-while-empty**

Context **[Tree]** (config>service>ies>sub-if>grp-if oper-up-while-empty)
[Tree] (config>service>vprn>sub-if>grp-if oper-up-while-empty)

Full Context configure service ies subscriber-interface group-interface oper-up-while-empty
configure service vprn subscriber-interface group-interface oper-up-while-empty

Description This command allows the subscriber interface to treat this group interface to be operationally enabled without any active SAPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command is typically used with MSAPs where advertising the subnet prior to having a MSAP dynamically created is needed.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.32 operations

operations

Syntax **operations**

Context **[Tree]** (config>system>management-interface operations)

Full Context configure system management-interface operations

Description Commands in this context configure operational commands in model-driven interfaces.

Platforms All

19.33 opt-reporting-fields

opt-reporting-fields

Syntax **opt-reporting-fields** [**host-mac**] [**pppoe-session-id**] [**svc-id**] [**sap-id**]
no opt-reporting-fields

Context **[Tree]** (config>subscr-mgmt>igmp-policy>mcast-reporting opt-reporting-fields)

Full Context configure subscriber-mgmt igmp-policy mcast-reporting opt-reporting-fields

Description This command specifies optional data relevant to the IGMP event that can be exported. This optional data includes:

- Host MAC address
- PPPoE session-ID
- Service ID
- SAP

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **host-mac** — Specifies that the host-mac optional field should be included into the multicast reporting messages.

pppoe-session-id — Specifies that the pppoe-session-id optional field should be included into the multicast reporting messages.

svc-id — Specifies that the svc-id optional field should be included into the multicast reporting messages.

sap-id — Specifies that the sap-id optional field should be included into the multicast reporting messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.34 optimal-route-reflection

optimal-route-reflection

Syntax **optimal-route-reflection**

Context **[Tree]** (config>router>bgp optimal-route-reflection)

Full Context configure router bgp optimal-route-reflection

Description This command creates the optimal route reflection context.

Platforms All

19.35 optimized-mode

optimized-mode

Syntax [**no**] **optimized-mode**

Context **[Tree]** (config>system>cpm-http-redirect optimized-mode)

Full Context configure system cpm-http-redirect optimized-mode

Description This command enables the **cpm-http-redirect optimized-mode**. The **optimized-mode** improves the scale of HTTP redirect sessions supported system wide.

Default optimized-mode

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.36 option

option

Syntax **option** *dhcp-option-number* {**present** | **absent**}
option *dhcp-option-number* **match hex** *hex-string* [**exact**] [**invert-match**]
option *dhcp-option-number* **match string** *ascii-string* [**exact**] [**invert-match**]
no option

Context **[Tree]** (config>filter>dhcp-filter>entry option)

Full Context configure filter dhcp-filter entry option

Description This command configures match criteria for the DHCP filter policy entry.

The **no** form of this command reverts to the default.

Parameters *dhcp-option-number* — Specifies the DHCP option number.

Values 0 to 255

present — Specifies that the related DHCP option must be present.

absent — Specifies that the related DHCP option must be absent.

hex-string — Specifies that the option must partially match a specified hex string.

Values 0x0 to 0xFFFFFFFF (up to 254 hex nibbles)

ascii-string — Specifies that the option must partially match a specified ASCII string, up to 127 characters.

exact — Specifies that this option requires an exact match of a hex or ASCII string.

invert-match — Requires the option not to partially match.

Platforms All

option

Syntax **option** *dhcp6-option-number* {**present** | **absent**}
option *dhcp6-option-number* **match hex** *hex-string* [**exact**] [**invert-match**]
option *dhcp6-option-number* **match string** *ascii-string* [**exact**] [**invert-match**]
no option

Context **[Tree]** (config>filter>dhcp6-filter>entry option)

Full Context configure filter dhcp6-filter entry option

Description This command configures match criteria for the DHCP6 filter policy entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *dhcp-option-number* — Specifies the DHCP6 option number.

Values 0 to 255

present — Specifies that the related DHCP6 option must be present.

absent — Specifies that the related DHCP6 option must be absent.

match hex *hex-string* — Specifies that the option must (partially) match a specified hex string.

Values 0x0 to 0xFFFFFFFF (up to 254 hex nibbles)

match string *ascii-string* — Specifies that the option must partially match a specified ASCII string, up to 127 characters.

exact — Specifies that this option requires an exact match of a hex or ASCII string.

invert-match — Requires the option not to partially match.

Platforms All

option

Syntax **option** *option-number* **address** *ipv4-address* [*ipv4-address*]
option *option-number* **hex** *hex-string*
option *option-number* **string** *ascii-string*
no option *option-number*

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>to-client-options>ipv4 option)

Full Context configure subscriber-mgmt local-user-db ipoe host to-client-options ipv4 option

Description This command configures DHCPv4 options via LUDB that are passed in all DHCP messages to the client. The options are blindly appended to any options already present in the DHCP message. In other words, there is no intelligent merging of the options where overlapping options from different sources are further evaluated to determine whether only one option or multiple options should be returned to the client.

Multiple DHCP options can be configured at the same time although each option requires its own option statement. Those options are equivalent to RADIUS VSAs **Alc-ToCLient-Dhcp4-Options**.

DHCPv4 options can be provided via DHCPv4 server in the relay case. In addition, DHCPv4 options provided via LUDB or RADIUS can be supplied and consequently appended to the already existing options. If DHCPv4 options are provided simultaneously via LUDB and RADIUS, the RADIUS as a source of DHCPv4 option is blocked and the options supplied via LUDB are passed to the client. This is valid for the relay and proxy case.

Any DHCP option may be encoded in the option statement. An example of the option statement for DHCPv4 default-gateway is given below:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

option 3 192.168.1.254

DHCPv4 options may be fixed length or variable length. They are appended at the end of DHCPv4 messages. All options begin with a tag octet, which uniquely identifies the option. Fixed-length options without data consist of only a tag octet. Only options 0 and 255 are fixed length. All other options are variable-length.

The **no** form of the removes the option from the configuration.

Parameters *option-number* — Specifies up to four option numbers. This can be a well-known or an anonymous option.

Values 1 to 254

ipv4-address — Specifies an IPv4 address as an option.

Values a.b.c.d

hex-string — Specifies options coded as hex characters.

Values 0x0..0xFFFFFFFF, up to 254 hex nibbles

ascii-string — Specifies options coded as an ASCII string, up to 27 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

option

Syntax **option** *option-number* **address** [*ip-address*]
option *option-number* **hex** *hex-string*
option *option-number* **string** *ascii-string*
option *option-number* **domain** *domain-name*
no option *option-number*

Context **[Tree]** (ipoe>host>to-server-options>ipv6 option)

Full Context configure subscriber-mgmt local-user-db ipoe host to-server-options ipv6 option

Description This command specifies the DHCPv6 options to send to the server.

The **no** form of this command removes the option parameters from the configuration.

Parameters *option-number* — Specifies the option number and the identification string that is inserted in the DHCP client message to the server.

Values 1 to 65535

ip-address — Specifies the IPv6 address.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

d: [0 to 255]D

hex-string — Specifies the hex value of the option.

Values 0x0 to 0xFFFFFFFF, up to 254 hex nibbles

ascii-string — Specifies the string value of the option.

Values up to 127 characters

domain-name — Specifies the domain as in RFC 1035, *Domain Names - Implementation and Specification*, section 3.1.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

option

Syntax **option** *option-number* **address** [*ip-address*]
option *option-number* **hex** *hex-string*
option *option-number* **string** *ascii-string*
option *option-number* **domain** *domain-name*
no option *option-number*

Context **[Tree]** (ipoe>host>to-client-options>ipv6 option)
[Tree] (ppp>host>to-client-options>ipv6 option)

Full Context configure subscriber-mgmt local-user-db ipoe host to-client-options ipv6 option
configure subscriber-mgmt local-user-db ppp host to-client-options ipv6 option

Description This command specifies the DHCPv6 options to send to the client.

The **no** form of this command removes the option parameters from the configuration.

Parameters *option-number* — Specifies the option number and the identification string that is inserted in the DHCP client message to the client.

Values 1 to 65535

ip-address — Specifies the IPv6 address. Up to four addresses can be specified.

Values

ipv6-address:	x:x:x:x:x:x:x:x	(eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d	
	x: [0 to FFFF]H	
	d: [0 to 255]D	

hex-string — Specifies the hex value of the option.

Values 0x0 to 0xFFFFFFFF, up to 254 hex nibbles

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ascii-string — Specifies the string value of the option.

Values up to 127 characters

domain-name — Specifies the domain as in RFC 1035, *Domain Names - Implementation and Specification*, section 3.1.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

option

Syntax [**no**] **option**

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6-relay option)
[Tree] (config>service>vprn>if>ipv6>dhcp6-relay option)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 option)

Full Context configure service ies interface ipv6 dhcp6-relay option
configure service vprn interface ipv6 dhcp6-relay option
configure service vprn subscriber-interface group-interface ipv6 option

Description Commands in this context configure DHCPv6 relay information options.

The **no** form of this command disables DHCPv6 relay information options.

Platforms All

option

Syntax [**no**] **option**

Context **[Tree]** (config>router>if>dhcp option)
[Tree] (config>service>ies>if>dhcp option)
[Tree] (config>service>ies>sub-if>grp-if>dhcp option)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 option)
[Tree] (config>service>vpls>sap>dhcp option)
[Tree] (config>service>vprn>if>dhcp option)
[Tree] (config>service>vprn>sub-if>dhcp option)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp option)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 option)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only-sap-parameters>dhcp option)

Full Context configure router interface dhcp option
configure service ies interface dhcp option
configure service ies subscriber-interface group-interface dhcp option
configure service ies subscriber-interface group-interface ipv6 dhcp6 option
configure service vpls sap dhcp option
configure service vprn interface dhcp option
configure service vprn subscriber-interface dhcp option

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface dhcp option
configure service vprn subscriber-interface group-interface ipv6 dhcp6 option
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option

Description This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enters the context for configuring Option 82 sub-options.

The **no** form of this command reverts to the default.

Default no option

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp option
- configure service ies subscriber-interface group-interface dhcp option
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option
- configure service vprn subscriber-interface group-interface ipv6 dhcp6 option
- configure service ies subscriber-interface group-interface ipv6 dhcp6 option
- configure service vprn subscriber-interface dhcp option

All

- configure service vprn interface dhcp option
- configure router interface dhcp option
- configure service vpls sap dhcp option
- configure service ies interface dhcp option

option

Syntax [**no**] **option**

Context **[Tree]** (config>service>nat>pcp-server-policy option)

Full Context configure service nat pcp-server-policy option

Description This command configures the PCP options supported by the PCP servers using this PCP policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

option

Syntax **option** {**basic** | **isis-enhanced**}
no option

Context **[Tree]** (config>system>security>keychain>direction>bi>entry option)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security keychain direction bi entry option

Description This command configures allows options to be associated with the authentication key.

Parameters **basic** — Specifies that IS-IS should use RFC 5304 encoding of the authentication information. It is only applicable if used with the IS-IS protocol. All other protocols should ignore this configuration command.

isis-enhanced — Specifies that IS-IS should use RFC 5310 encoding of the authentication information. It is only applicable if used with the IS-IS protocol. All other protocols should ignore this configuration command.

Platforms All

19.37 option-present

option-present

Syntax **option-present** {**true** | **false**}

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match option-present)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match option-present)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match option-present
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match option-present

Description This command configures the option-present match condition.

The **no** form of this command reverts to the default.

Parameters **true** — Enables checking for the presence of IP options in the IP header.

false — Disables checking for the presence of IP options in the IP header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

option-present

Syntax **option-present** {**true** | **false**}
no option-present

Context **[Tree]** (config>filter>ip-filter>entry>match option-present)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter ip-filter entry match option-present

Description This command configures matching packets that contain any IP options in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of IP options in the IP header as a match criterion.

Default no option-present

Parameters **true** — Specifies matching on all IP packets that contain any IP options in the IP header. A match will occur for all packets that have any IP option present. An option field of zero is considered as no option present.

false — Specifies matching on IP packets that do not have any IP option present in the IP header. (an option field of zero). An option field of zero is considered as no option present.

Platforms All

option-present

Syntax **option-present** {**true** | **false**}
no option-present

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match option-present)

Full Context configure system security cpm-filter ip-filter entry match option-present

Description This command configures matching packets that contain the option field or have an option field of zero in the IP header as an IP filter match criterion.

The **no** form of this command removes the checking of the option field in the IP header as a match criterion.

Default no option-present

Parameters **true** — Specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of zero is considered as no option present.

false — Specifies matching on IP packets that do not have any option field present in the IP header (an option field of zero). An option field of zero is considered as no option present.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.38 option60

option60

Syntax **option60 hex** *hex-string*
option60 string *ascii-string*
no option60

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident option60)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification option60

Description This command specifies the Vendor-Identifying Vendor Option to match. Option 60 is encoded as Type-Length-Value (TLV). The *hex-string* portion of Option 60 in the received DHCP request is used for matching. Only the first 32 bytes can be defined here. If Option 60 from the message is longer, those bytes are ignored.

Note: This command is only used when **option60** is configured as one of the **match-list** parameters.

The **no** form of this command removes **option60** from the configuration.

Parameters *hex-string* — Specifies the hexadecimal format for this option.

Values 0x0 to 0xFFFFFFFF(maximum 64 hex nibbles)

ascii-string — Specifies the string format for this option, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.39 options

options

Syntax **options**

Context [Tree] (config>router>dhcp6>server>defaults options)
[Tree] (config>router>dhcp>server>pool options)
[Tree] (config>router>dhcp>server>pool>subnet options)
[Tree] (config>router>dhcp6>server>pool options)
[Tree] (config>router>dhcp6>server>pool>prefix options)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host options)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host options)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>dhcp>server>pool options)
[Tree] (config>service>vprn>dhcp6>server>pool options)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix options)

Full Context configure router dhcp local-dhcp-server pool options
configure router dhcp local-dhcp-server pool subnet options
configure router dhcp6 local-dhcp-server defaults options
configure router dhcp6 local-dhcp-server pool options
configure router dhcp6 local-dhcp-server pool prefix options
configure service vprn dhcp local-dhcp-server pool options
configure service vprn dhcp6 local-dhcp-server pool options
configure service vprn dhcp6 local-dhcp-server pool prefix options
configure subscriber-mgmt local-user-db ipoe host options
configure subscriber-mgmt local-user-db ppp host options

Description Commands in this context configure pool options. The options defined here can be overruled by defining the same option in the local user database.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt local-user-db ipoe host options
- configure service vprn dhcp local-dhcp-server pool options
- configure service vprn dhcp6 local-dhcp-server pool prefix options
- configure router dhcp6 local-dhcp-server pool prefix options
- configure service vprn dhcp6 local-dhcp-server pool options
- configure router dhcp local-dhcp-server pool options
- configure subscriber-mgmt local-user-db ppp host options
- configure router dhcp6 local-dhcp-server pool options
- configure router dhcp local-dhcp-server pool subnet options

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure router dhcp6 local-dhcp-server defaults options

options

Syntax **options**

Context [Tree] (config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool options)

Full Context configure subscriber-mgmt vrgw brg brg-profile dhcp-pool options

Description Commands in this context configure options that are reflected in DHCP.

Default none

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

options

Syntax **options**

Context **[Tree]** (config>redundancy>multi-chassis options)

Full Context configure redundancy multi-chassis options

Description This command enables the CLI context to configure multi-chassis options parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

options

Syntax **options**

Context **[Tree]** (config>system>persistence options)

Full Context configure system persistence options

Description This command enables the CLI context to configure persistence options parameters.

Platforms All

19.40 options6

options6

Syntax **options6**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host options6)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host options6)

Full Context configure subscriber-mgmt local-user-db ipoe host options6
configure subscriber-mgmt local-user-db ppp host options6

Description Commands in this context configure IPv6 DNS server information in the local user database.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.41 origin

origin

Syntax **origin** {**igp** | **egp** | **incomplete** | **any** | **aaa** | **dynamic** | **static** | **bonding** | **pfcp**}
no origin

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from origin)

Full Context configure router policy-options policy-statement entry from origin

Description This command configures the match criteria for the origin attribute of the route. The origin attribute is applicable to BGP routes and to the following subscriber-management routes.

- Host routes (for example, IPv4 /32 address, or IPv6 SLAAC prefix) carry the origin attribute with the **aaa**, **dynamic**, or **static** options, depending on the address assignment method. For CUPS hosts, the **pfcp** option is used for the origin attribute. Host routes can also be distinguished using the **sub-mgmt** option for the **protocol** command.
- Dynamically provisioned prefixes or loopback addresses carry the origin attribute with the **aaa** or **pfcp** options, depending on the protocol that provides the prefix and address. Dynamic routes can also be distinguished using the **direct** option for the **protocol** command.
- Statically configured prefixes under the subscriber interface do not have an origin attribute.These routes can be distinguished using the **direct** option for the **protocol** command.
- Framed routes for non-CUPS hosts do not have an origin attribute. Framed routes for CUPS hosts use the **pfcp** option for the origin attribute. Alternatively, framed routes can be distinguished using the **managed** option for the **protocol** command.

These values that are specific to subscriber-management routes are never carried in BGP updates as part of the BGP origin attribute and are not visible within the BGP process.

Default no origin

Parameters **igp** — Specifies path-matching information that originates within the local AS.

egp — Specifies path-matching information that originates in another AS.

incomplete — Configures path-matching information learned by another method.

any — Specifies to ignore this criteria.

aaa — Specifies to use the subscriber-host address that originates from AAA.

Values IPv4 — subscriber-management /32 host routes that originate from the RADIUS framed-ip-address VSA other than 255.255.255.254. The 255.255.255.254 returned by the RADIUS indicates that the BNG (NAS) should assign an IP address from its own pool.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IPv6 — subscriber-management routes that originate through framed-ipv6-prefix (SLAAC), delegated-ipv6-prefix (IA_PD) or alc-ipv6-address (IA_NA) RADIUS attributes. It is also applicable to VSA Alc-IPv6-Sub-If-Prefix, where the subscriber interface prefix can originate from RADIUS. This is valid for IPoE and PPPoE type hosts.

dynamic — Specifies to use the subscriber host address that originates from DHCP, DHCPv6, or the local address server.

Values IPv4 — subscriber-management /32 host routes that originate from the DHCP server (local or remote) or RADIUS framed-ip-address=255.255.255.254 (RFC 2865).

IPv6 — subscriber-management routes that are assigned via local DHCPv6 server pools whose name is obtained through the Alc-Delegated-IPv6-Pool (PD pool) and Framed-IPv6-Pool (NA pool) RADIUS attributes, or the local address server whose name is obtained through the Alc-SLAAC-IPv6-Pool (SLAAC pool) RADIUS attribute. This is valid for IPoE and PPPoE type hosts.

For IPoEv6 only, the pool name can also be obtained from ipv6-delegated-prefix-pool (PD pool) and ipv6-wan-address-pool (NA pool) from the LUDB.

static — Specifies to use the subscriber-host address that originates from the local user database.

Values IPv4 — subscriber-management /32 host routes that originate from the LUDB and also covers the RADIUS fallback category (RADIUS falls back to system defaults or to the LUDB).

IPv6 — subscriber-management routes that originate from the LUDB from ipv6-address (IA_NA) or ipv6-prefix (IA_PD), or ipv6-slaac-prefix (SLAAC).

bonding — Specifies to use bonding.

pfcp — Specifies to use routes learned using the PFCP protocol.

Platforms All

origin

Syntax **origin** {**igp** | **egp** | **incomplete** | *param-name*}
no origin

Context **[Tree]** (config>router>policy-options>policy-statement>default-action origin)
[Tree] (config>router>policy-options>policy-statement>entry>action origin)

Full Context configure router policy-options policy-statement default-action origin
configure router policy-options policy-statement entry action origin

Description This command sets the BGP origin assigned to routes exported into BGP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the routes are exported into protocols other than BGP, this option is ignored.

The **no** form of this command disables setting the BGP origin for the route policy entry.

Default no origin

Parameters **igp** — Sets the path information as originating within the local AS.

egp — Sets the path information as originating in another AS.

incomplete — Sets the path information as learned by some other means.

param-name — The origin parameter variable name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

19.42 origin-host

origin-host

Syntax **origin-host** *origin-host-string*
no origin-host

Context **[Tree]** (config>aaa>diam-peer-plcy origin-host)

Full Context configure aaa diameter-peer-policy origin-host

Description This command configures the Origin-Host AVP that is sent in all Diameter messages. Together with the Origin-Realm AVP, these two AVPs form a Diameter Identity.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command removes the origin host string from the configuration.

Parameters *origin-host-string* — Specifies the Origin-Host AVP (Attribute Value Pair) used by this policy, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.43 origin-invalid-unusable

origin-invalid-unusable

Syntax [**no**] **origin-invalid-unusable**

Context **[Tree]** (config>service>vprn>bgp>best-path-selection origin-invalid-unusable)

Full Context configure service vprn bgp best-path-selection origin-invalid-unusable

Description When this command is configured, all VPRN BGP routes that have an origin validation state of “Invalid” are considered unusable by the best path selection algorithm, meaning they are not used for forwarding, not advertised to BGP peers, and not eligible for export as a VPN-IP route.

With the default value, VPRN BGP routes with an origin validation state of “Invalid” are usable if they are selected.

Default no origin-invalid-unusable

Platforms All

origin-invalid-unusable

Syntax [**no**] **origin-invalid-unusable**

Context **[Tree]** (config>router>bgp>best-path-selection origin-invalid-unusable)

Full Context configure router bgp best-path-selection origin-invalid-unusable

Description When **origin-invalid-unusable** is configured, all routes that have an RPKI origin validation state of ‘Invalid’ are considered unusable by the best path selection algorithm, meaning they are not used for forwarding and not advertised to BGP peers.

With the default of **no origin-invalid-unusable**, routes with an RPKI origin validation state of ‘Invalid’ are compared to other ‘usable’ routes for the same prefix according to the BGP decision process.

Default no origin-invalid-unusable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.44 origin-realm

origin-realm

Syntax **origin-realm** *origin-realm-string*
no origin-realm

Context **[Tree]** (config>aaa>diam-peer-plcy origin-realm)

Full Context configure aaa diameter-peer-policy origin-realm

Description This command configures the Origin-Realm AVP that is sent in all Diameter messages. Together with the Origin-Host AVP, these two AVPs form a Diameter Identity.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Parameters *origin-realm-string* — Specifies the origin-realm AVP (Attribute Value Pair) used by this policy, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

origin-realm

Syntax **origin-realm** *realm*
no origin-realm

Context **[Tree]** (debug>diam origin-realm)

Full Context debug diameter origin-realm

Description This command restricts output to a specific origin-realm.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.45 origin-validation

origin-validation

Syntax **origin-validation**

Context **[Tree]** (config>router origin-validation)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router origin-validation

Description Commands in this context display origin validation information.

Platforms All

19.46 origin-validation-state

origin-validation-state

Syntax **origin-validation-state** state
no origin-validation-state

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from origin-validation-state)

Full Context configure router policy-options policy-statement entry from origin-validation-state

Description This command is used to match BGP routes on the basis of origin validation state:

- Valid (0)
- Not-Found (1)
- Invalid (2)

Default no origin-validation-state

Parameters **valid** — Marks the route as having an origin validation state of valid.

notFound — Marks the route as having an origin validation state of Not Found.

invalid — Marks the route as having an origin validation state of invalid.

Platforms All

origin-validation-state

Syntax **origin-validation-state** {*state* | *param-name*}
no origin-validation-state

Context **[Tree]** (config>router>policy-options>policy-statement>default-action origin-validation-state)
[Tree] (config>router>policy-options>policy-statement>entry>action origin-validation-state)

Full Context configure router policy-options policy-statement default-action origin-validation-state
configure router policy-options policy-statement entry action origin-validation-state

Description This command is used to mark BGP IPv4 and IPv6 routes matching the **default-action** or a specific entry of a route policy with one of the 3 following origin validation states:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Valid (0)
- Not-Found (1)
- Invalid (2)

Default no origin-validation-state

Parameters *state* — Specifies the default operational origin validation state for this policy statement.

Values valid — Marks the route as having an origin validation state of valid.

notFound — Marks the route as having an origin validation state of Not Found.

invalid — Marks the route as having an origin validation state of invalid.

param-name — Specifies the origin parameter variable name. Allowed values are any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

19.47 originate-default-route

originate-default-route

Syntax **originate-default-route** [**type-nssa**] [**adjacency-check**]
no originate-default-route

Context **[Tree]** (config>service>vprn>ospf>area>nssa originate-default-route)
[Tree] (config>service>vprn>ospf3>area>nssa originate-default-route)

Full Context configure service vprn ospf area nssa originate-default-route
configure service vprn ospf3 area nssa originate-default-route

Description This command specifies whether when configuring an NSSA with no summaries, the Area Border Router (ABR) injects a type-7 LSA default route into the NSSA area. The default behavior is to inject a type-3 LSA default route, but some older implementations expect a type-7 LSA default route.

When configuring an NSSA with no summaries, the ABR will inject a type 3 LSA default route into the NSSA area. Some older implementations expect a type 7 LSA default route.

The **no** form of this command disables origination of a default route.

Default no originate-default-route — A default route is not originated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **type-nssa** — Specifies that a type 7 LSA should be used for the default route.

Configure this parameter to inject a type 7 LSA default route into an NSSA configured with no summaries, instead of a type 3 LSA.

To revert to a type 3 LSA, execute the **originate-default-route** command without the **type-nssa** parameter.

Default type 3 LSA default route

adjacency-check — Specifies whether adjacency checks are performed before originating a default route. If this parameter is configured, then no area 0 adjacency is required for the ABR to advertise the default route.

Default Adjacency checks are performed, and an area 0 adjacency is required for the ABR to advertise the default route

Platforms All

originate-default-route

Syntax **originate-default-route** [**type-7**] [**no-adjacency-check**]
originate-default-route [**type-nssa**] [**no-adjacency-check**]
no originate-default-route

Context **[Tree]** (config>router>ospf>area>nssa originate-default-route)
[Tree] (config>router>ospf3>area>nssa originate-default-route)

Full Context configure router ospf area nssa originate-default-route
configure router ospf3 area nssa originate-default-route

Description This command enables the generation of a default route and its LSA type (3 or 7) into a Not So Stubby Area (NSSA) by an NSSA Area Border Router (ABR).

When configuring an NSSA with no summaries, the ABR will inject a type 3 LSA default route into the NSSA area. Some older implementations expect a type 7 LSA default route.

The **no** form of this command disables origination of a default route.

Default no originate-default-route

Parameters **type-7** — Specifies a type 7 LSA should be used for the default route in the **config**>**router**>**ospf**>**area**>**nssa** context.

Configure this parameter to inject a type-7 LSA default route instead the type 3 LSA into the NSSA configured with no summaries.

To revert to a type 3 LSA, enter **originate-default-route** without the **type-7** parameter.

Default Type 3 LSA default route.

type-nssa — Specifies an NSSA-LSA type should be used for the default route in the **config**>**router**>**ospf3**>**area**>**nssa** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no-adjacency-check — Specifies whether or not adjacency checks are performed before originating a default route. If this parameter is configured, then no area 0 adjacency is required for the ABR to advertise the default route.

Default Adjacency checks are performed, and an area 0 adjacency is required for the ABR to advertise the default route.

Platforms All

19.48 originated-qos-marking

originated-qos-marking

Syntax [**no**] **originated-qos-marking** *dscp-name*

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription originated-qos-marking)

Full Context configure system telemetry persistent-subscriptions subscription originated-qos-marking

Description This command configures the QoS marking used for packets carrying telemetry notifications.

The **no** form of this command removes the QoS marking.

Parameters *dscp-name* — Specifies the QoS marking name.

The *dscp-name* parameter is a 6-bit value. It must be one of the predefined DSCP names in the system.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, e f, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms All

originated-qos-marking

Syntax **originated-qos-marking** *dscp-name*
no originated-qos-marking

Context **[Tree]** (config>system>grpc-tunnel>destination-group>destination originated-qos-marking)

Full Context configure system grpc-tunnel destination-group destination originated-qos-marking

Description This command configures the QoS marking used for packets carrying gRPC tunnel packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the QoS marking.

Default no originated-qos-marking

Parameters *dscp-name* — Specifies the QoS marking name.

The *dscp-name* parameter is a 6-bit value. It must be one of the predefined DSCP names in the system.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, e f, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms All

19.49 origination-fpe

origination-fpe

Syntax **origination-fpe** *origination-fpe*
no origination-fpe

Context **[Tree]** (config>router>segment-routing>srv6 origination-fpe)

Full Context configure router segment-routing segment-routing-v6 origination-fpe

Description This command configures the SRv6 FPE ID for origination of SRv6 tunnels on local services. A single FPE can be configured for SRv6 origination.

The **no** form of this command removes the origination FPE from the configuration.

Default no origination-fpe

Parameters *origination-fpe* — Specifies the FPE ID for origination of SRv6 tunnels on local services.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.50 orphan-override

orphan-override

Syntax **orphan-override** [**level** *priority-level*] [**weight** *weight*] [**cir-level** *cir-level*] [**cir-weight** *cir-weight*]
no orphan-override

Context **[Tree]** (config>qos>port-scheduler-policy orphan-override)

Full Context configure qos port-scheduler-policy orphan-override

Description This command overrides the default orphan behavior for port schedulers created using the port scheduler policy. The default orphan behavior is to give all orphan queues and schedulers bandwidth after all other properly parented queues and schedulers. Orphans by default do not receive any within-CIR bandwidth and receive above-CIR bandwidth after priority levels 8 through 1 have been allocated. The orphan-override command accepts the same parameters as the port-parent command in the SAP egress and network queue policy contexts. The defined parameters are used as a default port-parent association for any queue or scheduler on the port that the port scheduler policy is applied.

Orphan queues and schedulers are identified as:

- Any queue or scheduler that does not have a port-parent or parent command applied
- Any queue that has a parent command applied, but the specified scheduler name does not exist on the queue's SAP, MSS, or SLA Profile instance.

A queue or scheduler may be properly parented to an upper level scheduler, but that scheduler may be orphaned. In this case, the queue or scheduler receives bandwidth from its parent scheduler based on the parent schedulers ability to receive bandwidth as an orphan.

Within-CIR Priority Level Parameters

The within-CIR parameters define which port priority level the orphan queues and schedulers should be associated with when receiving bandwidth for the queue or schedulers within-CIR offered load. The within-CIR offered load is the amount of bandwidth the queue or schedulers could use that is equal to or less than its defined or summed CIR value. The summed value is only valid on schedulers and is the sum of the within-CIR offered loads of the children attached to the scheduler. The parameters that control within-CIR bandwidth allocation for orphans are the orphan-override commands cir-level and cir-weight keywords. The cir-level keyword defines the port priority level that the scheduler or queue uses to receive bandwidth for its within-CIR offered load. The cir-weight is used when multiple queues or schedulers exist at the same port priority level for within-CIR bandwidth. The weight value defines the relative ratio that is used to distribute bandwidth at the priority level when more within-CIR offered load exists than the port priority level has bandwidth.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A cir-weight equal to zero (the default value) has special meaning and informs the system that the orphan queues and schedulers do not receive bandwidth from the within-CIR distribution. Instead, all bandwidth for the orphan queues and schedulers must be allocated from the port scheduler's above-CIR pass.

Above-CIR Priority Level Parameters

The above-CIR parameters define which port priority level the orphan queues and schedulers should be associated with when receiving bandwidth for the queue or schedulers above-CIR offered load. The above-CIR offered load is the amount of bandwidth the queue or schedulers could use that is equal to or less than its defined PIR value (based on the queue or schedulers rate command) less any bandwidth that was given to the queue or scheduler during the above-CIR scheduler pass. The parameters that control above-CIR bandwidth allocation for orphans are the orphan-override commands level and weight keywords. The **level** keyword defines the port priority level that the scheduler or queue uses to receive bandwidth for its above-CIR offered load. The weight is used when multiple queues or schedulers exist at the same port priority level for above-CIR bandwidth. The weight value defines the relative ratio that is used to distribute bandwidth at the priority level when more above-CIR offered load exists than the port priority level has bandwidth.

The **no** form of this command removes the orphan override port parent association for the orphan queues and schedulers on port schedulers created with the port scheduler policy. Any orphan queues and schedulers on a port associated with the port scheduler policy will revert to default orphan behavior.

Parameters **level** *priority-level* — Defines the port priority the orphan queues and schedulers will use to receive bandwidth for their above-CIR offered-load.

Values 1 to 8 (8 is the highest priority)

Default 1

weight *weight* — Defines the weight the orphan queues and schedulers will use in the above-CIR port priority level (defined by the level parameter).

Values 1 to 100

Default 1

cir-level *cir-level* — Defines the port priority the orphan queues and schedulers will use to receive bandwidth for their within-CIR offered-load. If the cir-weight parameter is set to a value of 0 (the default value), the orphan queues and schedulers do not receive bandwidth during the port scheduler's within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 1 to 8 (8 is the highest level)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-weight *cir-weight* — Defines the weight the orphan queues and schedulers will use in the within-CIR port priority level (defined by the cir-level parameter). When the cir-weight parameter is set to a value of 0 (the default value), the orphan queues and schedulers do not receive bandwidth during the port scheduler's within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 1 to 100 (100 is the highest weight)

Platforms All

19.51 ospf

ospf

Syntax **ospf** [*router-id*]
no ospf

Context **[Tree]** (config>service>vprn ospf)

Full Context configure service vprn ospf

Description This command enables access to the context to enable an OSPF protocol instance.

OSPF instances are **shutdown** when created, so that all parameters can be configured prior to the instance being enabled.

The **no** form of this command deletes the OSPF protocol instance removing all associated configuration parameters.

Default no ospf

Parameters *router-id* — Specifies the OSPF router ID to be used with the associated OSPF instance. The *router-id* must be given a dot decimal notation format.

Values a.b.c.d

Platforms All

ospf

Syntax **ospf** *ospf-instance* [*router-id*]
[**no**] **ospf** *ospf-instance*

Context **[Tree]** (config>router ospf)

Full Context configure router ospf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates an OSPF routing instance and then enters the associated context to configure the associated protocol parameters.

Additionally, the router ID can be specified as another parameter of the OSPF command. This parameter is required for all non-base OSPF instances.

The default value for the base instance is inherited from the configuration in the **config**>**router** context. When that is not configured, the following apply:

1. the system uses the system interface address (which is also the loopback address)
2. if a system interface address is not configured, it uses the last 32 bits of the chassis MAC address

This is a required command when configuring multiple instances and the instance being configured is not the base instance. When configuring multiple instances of OSPF, there is a risk of loops because networks are advertised by multiple domains configured with multiple interconnections to one another. To prevent this from happening, all routers in a domain should be configured with the same domain ID. Each domain (OSPF-instance) should be assigned a specific bit value in the 32-bit tag mask.

The default value for non-base instances is 0.0.0.0 and is invalid; in this case, the instance of OSPF will not start. When configuring a new router ID, the instance is not automatically restarted with the new router ID. The next time the instance is initialized, the new router ID is used.

Issue the shutdown and no shutdown commands for the instance for the new router ID to be used, or reboot the entire router.

OSPF instances are **shutdown** when created, so that all parameters can be configured prior to the instance being enabled.

The **no** form of this command to reverts to the default value.

Default no ospf

Parameters *ospf-instance* — Specifies a unique integer that identifies a specific instance of a version of the OSPF protocol running in the router instance specified by the router ID.

Values 1 to 31

router-id — Specifies the OSPF router ID to be used with the associated OSPF instance. This IP address must be given a dot decimal notation format.

Platforms All

ospf

Syntax **ospf** [*ospf-instance*]
no ospf [*ospf-instance*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (debug>router ospf)

Full Context debug router ospf

Description Indicates the OSPF instance for debugging purposes.

Parameters *ospf-instance* — Debugs the specified OSPF instance.

Values 0 to 31

Platforms All

19.52 ospf-dynamic-hostnames

ospf-dynamic-hostnames

Syntax [**no**] **ospf-dynamic-hostnames**

Context **[Tree]** (config>system ospf-dynamic-hostnames)

Full Context configure system ospf-dynamic-hostnames

Description This command enables OSPF dynamic hostnames.

The router receiving the new Dynamic Hostname within the OSPF Router Information (RI) LSA is instructed to process the received dynamic hostname information.

The **no** form of this command disables OSPF dynamic hostnames.

Default no ospf-dynamic-hostnames

Platforms All

19.53 ospf3

ospf3

Syntax **ospf3** [*instance-id*] [*router-id*]
[**no**] **ospf3** *instance-id*

Context **[Tree]** (config>service>vprn ospf3)

Full Context configure service vprn ospf3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates an OSPFv3 routing instance and then enters the associated context to configure associated protocol parameters.

OSPF instances are **shutdown** when created, so that all parameters can be configured before the instance is enabled.

The **no** form of this command deletes the OSPFv3 protocol instance, removing all associated configuration parameters.

Default no ospf3

Parameters *instance-id* — Specifies the instance ID for the OSPFv3 instance being created or modified. The instance ID must match the specified range based on the address family.

Values 0 to 31: IPV6 unicast
64 to 95: IPV4 unicast

router-id — Specifies the IP address.

Platforms All

ospf3

Syntax **ospf3** [*ospf-instance*] [*router-id*]
[**no**] **ospf3** *instance-id*

Context **[Tree]** (config>router ospf3)

Full Context configure router ospf3

Description This command creates an OSPFv3 routing instance and then enters the associated context to configure associated protocol parameters.

OSPFv3 instances are **shutdown** when created, so that all parameters can be configured prior to the instance being enabled.

The **no** form of this command deletes the OSPFv3 protocol instance, removing all associated configuration parameters.

Parameters *ospf-instance* — Specifies the instance ID for the OSPFv3 instance being created or modified. The instance ID must match the specified range based on the address family.

Values 0 to 31: IPV6 unicast
64 to 95: IPV4 unicast

router-id — Specifies the OSPF router ID to be used with the associated OSPF instance. This IP address must be given a dot decimal notation format.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ospf3

Syntax **ospf3** [*ospf-instance*]
no ospf3 [*ospf-instance*]

Context **[Tree]** (debug>router ospf3)

Full Context debug router ospf3

Description Indicates the OSPF3 instance for debugging purposes.

Parameters *ospf-instance* — Debugs the specified OSPF3 instance.

Values 0 to 31 | 64 to 95
0 to 31 — IPv6-unicast address-family
64 to 95 — IPv4-unicast address-family

Platforms All

19.54 other-stateful-configuration

other-stateful-configuration

Syntax [**no**] **other-stateful-configuration**

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv other-stateful-configuration)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 other-stateful-configuration)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv other-stateful-configuration)
[Tree] (config>service>vprn>router-advert>if other-stateful-configuration)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv other-stateful-configuration)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 other-stateful-configuration)
[Tree] (config>subscr-mgmt>rtr-adv-plcy other-stateful-configuration)

Full Context configure service ies subscriber-interface group-interface ipv6 other-stateful-configuration
configure service ies subscriber-interface group-interface ipv6 router-advertisements other-stateful-configuration
configure service ies subscriber-interface ipv6 router-advertisements other-stateful-configuration
configure service vprn router-advertisement interface other-stateful-configuration
configure service vprn subscriber-interface group-interface ipv6 other-stateful-configuration
configure service vprn subscriber-interface ipv6 router-advertisements other-stateful-configuration
configure subscriber-mgmt router-advertisement-policy other-stateful-configuration

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the "other configuration" flag. This flag indicates that DHCPv6 is available for auto-configuration of other (non-address) information such as DNS-related information or information on other servers in the network. See RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) for IPv6*.

The **no** form of this command removes the flag.

Default no other-stateful-configuration

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface ipv6 router-advertisements other-stateful-configuration
- configure service vprn subscriber-interface ipv6 router-advertisements other-stateful-configuration
- configure service ies subscriber-interface group-interface ipv6 router-advertisements other-stateful-configuration
- configure subscriber-mgmt router-advertisement-policy other-stateful-configuration

All

- configure service vprn router-advertisement interface other-stateful-configuration

other-stateful-configuration

Syntax [**no**] **other-stateful-configuration**

Context **[Tree]** (config>router>router-advert>if other-stateful-configuration)

Full Context configure router router-advertisement interface other-stateful-configuration

Description This command sets the "Other configuration" flag. This flag indicates that DHCPv6lite is available for autoconfiguration of other (non-address) information such as DNS-related information or information about other servers in the network. See RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) for IPv6*.

Default no other-stateful-configuration

Platforms All

19.55 otu

otu

Syntax [**no**] **otu**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port otu)

Full Context configure port otu

Description This command specifies whether or not to enable OTU encapsulation. The port must be shut down before OTU is enabled. This command is valid only for ports on assemblies that support this encapsulation mode. Refer to the appropriate Installation Guide for ports assembly to determine if OTU encapsulation is supported.

Note that OTU cannot be disabled on OTU3 encapsulated OC768 or 40-Gigabit Ethernet.by the **no otu** command. Therefore, the default depends on the port type. The default for OTU3 encapsulated OC768 or 40-Gigabit Ethernet is **otu**.

The **no** form of this command disables OTU (clear channel 10GE-LAN/WAN or OC192).

Default no otu

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.56 otu2-lan-data-rate

otu2-lan-data-rate

Syntax **otu2-lan-data-rate** {**11.049** | **11.096**}

Context [Tree] (config>port>otu otu2-lan-data-rate)

Full Context configure port otu otu2-lan-data-rate

Description This command specifies the data rate to use when configured for an OTU encapsulated 10GE-LAN signal. The port must be shut down before changing the 10GE LAN OTU2 data rate.

Default otu2-lan-data-rate 11.049

Parameters **11.049** — Configures the port to transmit and receive an 11.049 Gb/s synchronous OTU encapsulated 10GE-LAN signal (No fixed stuffing bytes in the OTU2 frame).

11.096 — Configures the port to transmit and receive an 11.096 Gb/s synchronous OTU encapsulated 10GE-LAN signal (with fixed stuffing bytes in the OTU2 frame).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.57 out-label

out-label

Syntax **out-label** *out-label* **out-link** *if-name* [**next-hop** *ip-address*]
no out-label

Context **[Tree]** (config>router>mpls>lsp>working-tp-path out-label)
[Tree] (config>router>mpls>lsp>protect-tp-path out-label)

Full Context configure router mpls lsp protect-tp-path out-label
configure router mpls lsp working-tp-path out-label

Description This command configures the outgoing label value to use for an MPLS-TP working or protect path. The out-link is the outgoing interface on the node that this path will use, and must be specified. If the out-link refers to a numbered IP interface, the user may optionally configure the **next-hop** parameter and the system will determine the interface to use to reach the configured next-hop, but will check that the user-entered value for the *out-link* corresponds to the link returned by the system. If they do not correspond, then the path will not come up.

Default no out-label

Parameters *out-label* — Specifies the out label.

Values 32 to 16415

if-name — Specifies the interface name.

ip-address — Specifies the IPv4 address in a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.58 out-of-credit-action

out-of-credit-action

Syntax **out-of-credit-action** {**continue** | **disconnect-host** | **block-category** | **change-service-level**}
no out-of-credit-action

Context **[Tree]** (config>subscr-mgmt>credit-control-policy out-of-credit-action)

Full Context configure subscriber-mgmt credit-control-policy out-of-credit-action

Description This command configures the action to be performed when out of credit is reached.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Default out-of-credit-action continue

Parameters *action* — Specifies the action to be taken when out of credit is out reached.

Values continue, disconnect-host, block-category, change-service-level

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.59 out-of-credit-action-override

out-of-credit-action-override

Syntax **out-of-credit-action-override** {**continue** | **block-category** | **change-service-level**}
no out-of-credit-action-override

Context **[Tree]** (config>subscr-mgmt>cat-map>category out-of-credit-action-override)

Full Context configure subscriber-mgmt category-map category out-of-credit-action-override

Description This command specifies the action to be taken if the credit is exhausted.

Parameters **continue** — Specifies to continue when running out of credit.

block-category — Specifies to block the category when running out of credit.

change-service-level — Specifies to change the service level when running out of credit.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.60 out-of-credit-reporting

out-of-credit-reporting

Syntax **out-of-credit-reporting** {**final** | **quota-exhausted**}
no out-of-credit-reporting

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy out-of-credit-reporting)

Full Context configure subscriber-mgmt diameter-application-policy gy out-of-credit-reporting

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command changes the reporting reason in an intermediate interrogation when the final granted units have been consumed and a corresponding **out-of-credit-action** different from **disconnect-host** is started.

The **no** form of this command reverts to the default value.

Default out-of-credit-reporting final

Parameters **final** — Specifies the reporting reason in an intermediate interrogation when the final granted units have been consumed and a corresponding **out-of-credit-action** different from **disconnect-host** is started.

quota-exhausted — Specifies the reporting reason in an intermediate interrogation when the final granted units have been consumed and a corresponding **out-of-credit-action** different from **disconnect-host** is started.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.61 out-profile-octets-discarded-count

out-profile-octets-discarded-count

Syntax [**no**] **out-profile-octets-discarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-counters out-profile-octets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-counters out-profile-octets-discarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters out-profile-octets-discarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters out-profile-octets-discarded-count

Description This command includes the out of profile packets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv6 octets discarded count instead.

The **no** form of this command excludes the out of profile packets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

out-profile-octets-discarded-count

Syntax [**no**] **out-profile-octets-discarded-count**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>log>acct-policy>cr>policer>e-counters out-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters out-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters out-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters out-profile-octets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters out-profile-octets-discarded-count
configure log accounting-policy custom-record queue e-counters out-profile-octets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters out-profile-octets-discarded-count
configure log accounting-policy custom-record ref-queue e-counters out-profile-octets-discarded-count

Description This command includes the out of profile packets discarded count.

The **no** form of this command excludes the out of profile packets discarded count.

Default no out-profile-octets-discarded-count

Platforms All

out-profile-octets-discarded-count

Syntax [**no**] **out-profile-octets-discarded-count**

Context [Tree] (config>log>acct-policy>cr>policer>i-counters out-profile-octets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters out-profile-octets-discarded-count)

Full Context configure log accounting-policy custom-record policer i-counters out-profile-octets-discarded-count
configure log accounting-policy custom-record ref-policer i-counters out-profile-octets-discarded-count

Description This command includes the out of profile octets discarded count.

The **no** form of this command excludes the out of profile octets discarded count.

Default no out-profile-octets-discarded-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.62 out-profile-octets-forwarded-count

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-counters out-profile-octets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>queue>i-counters out-profile-octets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-counters out-profile-octets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters out-profile-octets-forwarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters out-profile-octets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters out-profile-octets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters out-profile-octets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters out-profile-octets-forwarded-count

Description This command includes the out of profile octets forwarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv6 octets forwarded count instead.

The **no** form of this command excludes the out of profile octets forwarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters out-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters out-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters out-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters out-profile-octets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters out-profile-octets-forwarded-count
configure log accounting-policy custom-record queue e-counters out-profile-octets-forwarded-count

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure log accounting-policy custom-record ref-policer e-counters
out-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-queue e-counters
out-profile-octets-forwarded-count

Description This command includes the out of profile octets forwarded count.

The **no** form of this command excludes the out of profile octets forwarded count.

Default no out-profile-octets-forwarded-count

Platforms All

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters out-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>i-counters out-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters out-profile-octets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters out-profile-octets-forwarded-count)

Full Context configure log accounting-policy custom-record policer i-counters
out-profile-octets-forwarded-count
configure log accounting-policy custom-record queue i-counters
out-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-policer i-counters
out-profile-octets-forwarded-count
configure log accounting-policy custom-record ref-queue i-counters
out-profile-octets-forwarded-count

Description This command includes the out of profile octets forwarded count.

The **no** form of this command excludes the out of profile octets forwarded count.

Default no out-profile-octets-forwarded-count

Platforms All

19.63 out-profile-octets-offered-count

out-profile-octets-offered-count

Syntax [**no**] **out-profile-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters out-profile-octets-offered-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>log>acct-policy>cr>ref-policer>e-counters out-profile-octets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters out-profile-octets-offered-count
configure log accounting-policy custom-record ref-policer e-counters out-profile-octets-offered-count

Description This command includes the out of profile octets offered count.

The **no** form of this command excludes the out of profile octets offered count.

Default no out-profile-octets-offered-count

Platforms All

out-profile-octets-offered-count

Syntax [**no**] **out-profile-octets-offered-count**

Context [Tree] (config>log>acct-policy>cr>policer>i-counters out-profile-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters out-profile-octets-offered-count)

Full Context configure log accounting-policy custom-record policer i-counters out-profile-octets-offered-count
configure log accounting-policy custom-record ref-policer i-counters out-profile-octets-offered-count

Description This command includes the out of profile octets offered count.

The **no** form of this command excludes the out of profile octets offered count.

Default no out-profile-octets-offered-count

Platforms All

19.64 out-profile-packets-discarded-count

out-profile-packets-discarded-count

Syntax [**no**] **out-profile-packets-discarded-count**

Context [Tree] (config>subscr-mgmt>acct-plcy>cr>queue>e-counters out-profile-packets-discarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-counters out-profile-packets-discarded-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters out-profile-packets-discarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters out-profile-packets-discarded-count

Description This command includes the out of profile packets discarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv6 packets discarded count instead.

The **no** form of this command excludes the out of profile packets discarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

out-profile-packets-discarded-count

Syntax [**no**] **out-profile-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters out-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters out-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters out-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters out-profile-packets-discarded-count)

Full Context configure log accounting-policy custom-record policer e-counters out-profile-packets-discarded-count
configure log accounting-policy custom-record queue e-counters out-profile-packets-discarded-count
configure log accounting-policy custom-record ref-policer e-counters out-profile-packets-discarded-count
configure log accounting-policy custom-record ref-queue e-counters out-profile-packets-discarded-count

Description This command includes the out of profile packets discarded count.

The **no** form of this command excludes the out of profile packets discarded count.

Default no out-profile-packets-discarded-count

Platforms All

out-profile-packets-discarded-count

Syntax [**no**] **out-profile-packets-discarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters out-profile-packets-discarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters out-profile-packets-discarded-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure log accounting-policy custom-record policer i-counters out-profile-packets-discarded-count
configure log accounting-policy custom-record ref-policer i-counters out-profile-packets-discarded-count

Description This command includes the out of profile packets discarded count.

The **no** form of this command excludes the out of profile packets discarded count.

Default no out-profile-packets-discarded-count

Platforms All

19.65 out-profile-packets-forwarded-count

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>e-counters out-profile-packets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>queue>i-counters out-profile-packets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>e-counters out-profile-packets-forwarded-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters out-profile-packets-forwarded-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue e-counters out-profile-packets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters out-profile-packets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue e-counters out-profile-packets-forwarded-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters out-profile-packets-forwarded-count

Description This command includes the out of profile packets forwarded count.

For queues with **stat-mode v4-v6**, this command includes the IPv6 packets forwarded count instead.

The **no** form of this command excludes the out of profile packets forwarded count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters out-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>e-counters out-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters out-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>e-counters out-profile-packets-forwarded-count)

Full Context configure log accounting-policy custom-record policer e-counters out-profile-packets-forwarded-count
configure log accounting-policy custom-record queue e-counters out-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-policer e-counters out-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-queue e-counters out-profile-packets-forwarded-count

Description This command includes the out of profile packets forwarded count.

The **no** form of this command excludes the out of profile packets forwarded count.

Platforms All

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters out-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>queue>i-counters out-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters out-profile-packets-forwarded-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters out-profile-packets-forwarded-count)

Full Context configure log accounting-policy custom-record policer i-counters out-profile-packets-forwarded-count
configure log accounting-policy custom-record queue i-counters out-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-policer i-counters out-profile-packets-forwarded-count
configure log accounting-policy custom-record ref-queue i-counters out-profile-packets-forwarded-count

Description This command includes the out of profile packets forwarded count.

The **no** form of this command excludes the out of profile packets forwarded count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no out-profile-packets-forwarded-count

Platforms All

19.66 out-profile-packets-offered-count

out-profile-packets-offered-count

Syntax [**no**] **out-profile-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters out-profile-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters out-profile-packets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters
out-profile-packets-offered-count
configure log accounting-policy custom-record ref-policer e-counters
out-profile-packets-offered-count

Description This command includes the out of profile packets offered count.

The **no** form of this command excludes the out of profile packets offered count.

Default no out-profile-packets-offered-count

Platforms All

out-profile-packets-offered-count

Syntax [**no**] **out-profile-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters out-profile-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters out-profile-packets-offered-count)

Full Context configure log accounting-policy custom-record policer i-counters
out-profile-packets-offered-count
configure log accounting-policy custom-record ref-policer i-counters
out-profile-packets-offered-count

Description This command includes the out of profile packets offered count.

The **no** form of this command excludes the out of profile packets offered count.

Default no out-profile-packets-offered-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.67 out-profile-rate

out-profile-rate

Syntax **out-profile-rate** *packet-rate-limit* [**log-event**]
no out-profile-rate

Context **[Tree]** (config>sys>security>cpu-protection>policy out-profile-rate)

Full Context configure system security cpu-protection policy out-profile-rate

Description This command applies a packet arrival rate limit for the entire SAP/interface, above which packets will be market as discard eligible, in other words, out-profile/low-priority/yellow. The rate defined is a global rate limit for the interface regardless of the number of traffic flows. It is a per-SAP/interface rate.

The **no** form of this command sets out-profile-rate parameter back to the default value.

Default out-profile-rate 3000 for cpu-protection-policy-id 1-253

out-profile-rate 6000 for cpu-protection-policy-id 254 (default access interface policy)

out-profile-rate 3000 for cpu-protection-policy-id 255 (default network interface policy)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit in packets per second.

Values 1 to 65535, **max** (max indicates no limit)

log-events — Issues a tmnxCpmProtViolSapOutProf, tmnxCpmProtViolIfOutProf, or tmnxCpmProtViolSdpBindOutProf log event and tracks violating interfaces when the out-profile-rate is exceeded. Supported on CPM3 and above only.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

19.68 out-remark

out-remark

Syntax **out-remark** {**dscp** *dscp-name* | **prec** *ip-prec-value*}
no out-remark

Context **[Tree]** (config>qos>sap-ingress>fc out-remark)

Full Context configure qos sap-ingress fc out-remark

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used in a SAP ingress QoS policy to define an explicit out-of-profile remark action for a forwarding class or subclass. While the SAP ingress QoS policy may be applied to any SAP, the remarking functions are only enforced when the SAP is associated with an IP or subscriber interface (in an IES or VPRN). When the policy is applied to a Layer 2 SAP (for example, Epipe or VPLS), the remarking definitions are silently ignored.

In the case where the policy is applied to a Layer 3 SAP, the out-of-profile remarking definition will be applied to packets that have been classified to the forwarding class or subclass. It is possible for a packet to match a classification command that maps the packet to a particular forwarding class or subclass, only to have a more explicit (higher priority match) override the association. Only the highest priority match forwarding class or subclass association will drive the out-of-profile marking.

The out-remark command is only applicable to ingress IP routed packets that are considered out-of-profile. The profile of a SAP ingress packet is affected by either the explicit in-profile/out-of-profile definitions or the ingress policing function applied to the packet. Table 104 describes the effect of the out-remark command on received SAP ingress packets. Within the out-of-profile IP packet's ToS field, either the six DSCP bits or the three precedence bits are remarked.

Table 104 **Out-remark Command Effect**

SAP Ingress Packet State	out-remark Command Effect
Non-Routed, Policed In-Profile	No Effect (non-routed packet)
Non-Routed, Policed Out-of-Profile	No Effect (non-routed packet)
Non-Routed, Explicit In-Profile	No Effect (non-routed packet)
Non-Routed, Explicit Out-of-Profile	No Effect (non-routed packet)
IP Routed, Policed In-Profile	No Effect (in-profile packet)
IP Routed, Policed Out-of-Profile	out-remark value applied to IP header ToS field
IP Routed, Explicit In-Profile	No Effect (in-of-profile packet)
IP Routed, Explicit Out-of-Profile	out-remark value applied to IP header ToS field

A packet that is explicitly remarked at ingress will not be affected by any egress remarking decision. Explicit ingress remarking has highest priority.

An explicit dscp name or precedence value must be specified for out-of-profile remarking to be applied.

The **no** form of this command disables ingress remarking of out-of-profile packets classified to the forwarding class or subclass.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no out-remark

Parameters **dscp** *dscp-name* — Specifies that the matching packet's DSCP bits should be overridden with the value represented by *dscp-name*.

The *dscp-name* parameter is a 6-bit value. It must be one of the predefined DSCP names defined on the system.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, e f, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

prec *ip-prec-value* — Specifies that the matching packet's precedence bits should be overridden with the value represented by *ip-prec-value*.

The value specified by *ip-prec-value* is used to overwrite the precedence bits within a matching routed packets IP header ToS field.

Values 0 to 7

Platforms All

19.69 outband

outband

Syntax **outband** *service-id*
no outband

Context **[Tree]** (config>system>security>vprn-aaa-server outband)

Full Context configure system security vprn-aaa-server outband

Description This command configures TACACS+ and RADIUS servers in a VPRN to be used for AAA by that VPRN and by sessions on the console or out-of-band (OOB) Ethernet ports.

The **no** form of this command disables the use of servers in out-of-band management.

Default no outband

Parameters *service-id* — Specifies the VPRN server for AAA to use for OOB sessions.

Values *service-id*: 1 to 2147483648
svc-name: 64 characters maximum

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.70 outbound-max-sessions

outbound-max-sessions

Syntax **outbound-max-sessions** *number-of-sessions*
no outbound-max-sessions

Context **[Tree]** (config>system>login-control>telnet outbound-max-sessions)
[Tree] (config>system>login-control>ssh outbound-max-sessions)

Full Context configure system login-control ssh outbound-max-sessions
configure system login-control telnet outbound-max-sessions

Description This parameter limits the number of outbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established from the router. The local serial port cannot be disabled.

The **no** form of this command reverts to the default value.

Default outbound-max-sessions 5

Parameters *value* — Specifies the maximum number of concurrent outbound Telnet sessions, expressed as an integer.

Values 0 to 15

Platforms All

19.71 outbound-route-filtering

outbound-route-filtering

Syntax [**no**] **outbound-route-filtering**

Context **[Tree]** (config>router>bgp outbound-route-filtering)
[Tree] (config>router>bgp>group outbound-route-filtering)
[Tree] (config>router>bgp>group>neighbor outbound-route-filtering)

Full Context configure router bgp group neighbor outbound-route-filtering
configure router bgp group outbound-route-filtering
configure router bgp outbound-route-filtering

Description This command opens the configuration tree for sending or accepting BGP filter lists from peers (outbound route filtering).

Default no outbound-route-filtering

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

outbound-route-filtering

Syntax [**no**] **outbound-route-filtering**

Context **[Tree]** (debug>router>bgp outbound-route-filtering)

Full Context debug router bgp outbound-route-filtering

Description This command enables debugging for all BGP outbound route filtering (ORF) packets. ORF is used to inform a neighbor of targets (using target-list) that it is willing to receive.

Platforms All

19.72 outer-tag

outer-tag

Syntax **outer-tag** *value* [*vid-mask*]
no outer-tag

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match outer-tag)

Full Context configure qos sap-ingress mac-criteria entry match outer-tag

Description This command configures the matching of the first tag that is carried transparently through the service. Service delimiting tags are stripped from the frame and the outer tag on ingress is the first tag after any service delimiting tags. The outer tag is the first tag before any service delimiting tags on egress. This allows matching VLAN tags for explicit filtering or QoS setting when using default or null encapsulations.

On dot1Q SAPs, the outer tag is the only tag that can be matched. On dot1Q SAPs with exact match (sap 2/1/1:50), the outer tag will be populated with the next tag that is carried transparently through the service or 0 if there is no additional VLAN tags on the frame.

On QinQ SAPs that strip a single service delimiting tag, the outer tag will contain the next tag (which is still the first tag carried transparently through the service.) On SAPs with two service delimiting tags (two tags stripped), the **outer-tag** will contain 0 even if there are more than two tags on the frame.

The optional *vid_mask* is defaulted to 4095 (exact match) but may be specified to allow pattern matching. The masking operation is ((value & vid-mask) = = (tag & vid-mask)). A value of 6 and a mask of 7 would match all VIDs with the lower 3 bits set to 6.

For QoS, the VID type cannot be specified on the default QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default vid-mask is set to 4095 for exact match.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

outer-tag

Syntax **outer-tag** *value* [*vid-mask*]
no outer-tag

Context **[Tree]** (config>filter>mac-filter>entry>match outer-tag)

Full Context configure filter mac-filter entry match outer-tag

Description This command configures the matching of the first tag that is carried transparently through the service. Service delimiting tags are stripped from the frame and outer tag on ingress is the first tag after any service delimiting tags. Outer tag is the first tag before any service delimiting tags on egress. This allows matching VLAN tags for explicit filtering or QoS setting when using default or null encapsulations.

On dot1Q SAPs outer-tag is the only tag that can be matched. On dot1Q SAPs with exact match (sap 2/1/1:50) the outer-tag will be populated with the next tag that is carried transparently through the service or 0 if there is no additional VLAN tags on the frame.

On QinQ SAPs that strip a single service delimiting tag, outer-tag will contain the next tag (which is still the first tag carried transparently through the service.) On SAPs with two service delimiting tags (two tags stripped) outer-tag will contain 0 even if there are more than 2 tags on the frame.

The optional *vid-mask* is defaulted to 4095 (exact match) but may be specified to allow pattern matching. The masking operation is ((value & vid-mask) = = (tag & vid-mask)). A value of 6 and a mask of 7 would match all VIDs with the lower 3 bits set to 6.

For QoS the VID type cannot be specified on the default QoS policy.

The default vid-mask is set to 4095 for exact match.

Default no outer-tag

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.73 output

output

Syntax **output**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>sync-if-timing>bits output)

Full Context configure system sync-if-timing bits output

Description This command provides a context to configure and enable or disable the external BITS timing reference output to the central clock of the router. On redundant systems, there are two possible BITS-out interfaces, one for each CPM or CCM.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

19.74 output-authorization

output-authorization

Syntax **output-authorization**

Context [Tree] (config>system>security>management-interface output-authorization)

Full Context configure system security management-interface output-authorization

Description This command configures the authorization of the configuration and state output in model-driven interfaces and telemetry. When enabled, commands that display configuration or state output authorize every element in the output. If a remote AAA server is configured, this can cause delays in displaying output while it is authorized. If a large amount of output is displayed, for example, when displaying the system configuration, the remote AAA server receives a large number of authorization requests.

Input to edit the configuration is not affected by this command, and is always authorized.

Platforms All

19.75 outside

outside

Syntax **outside**

Context [Tree] (config>service>vprn>nat outside)
[Tree] (config>router>nat outside)

Full Context configure router nat outside
configure service vprn nat outside

Description Commands in this context configure the outside NAT instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.76 outside-ip

outside-ip

Syntax [**no**] **outside-ip**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes outside-ip)

Full Context configure aaa isa-radius-policy acct-include-attributes outside-ip

Description This command enables the inclusion of the outside IP attributes.

The **no** form of the command excludes outside IP attributes.

Default no outside-ip

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.77 outside-service-id

outside-service-id

Syntax [**no**] **outside-service-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes outside-service-id)

Full Context configure aaa isa-radius-policy acct-include-attributes outside-service-id

Description This command enables the inclusion of the NAT outside service ID attributes.

The **no** form of the command excludes NAT outside service ID attributes.

Default no outside-service-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.78 overall

overall

Syntax **overall** *max-nr-of-hosts*
no overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits overall)
[Tree] (config>subscr-mgmt>sub-profile>host-limits overall)

Full Context configure subscriber-mgmt sla-profile host-limits overall
configure subscriber-mgmt sub-profile host-limits overall

Description This command configures the maximum number of subscriber hosts per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of subscriber hosts limit.

Parameters *max-nr-of-hosts* — Specifies the maximum number of subscriber hosts.

Values 1 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

overall

Syntax **overall** *max-nr-of-sessions*
no overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>session-limits overall)
[Tree] (config>subscr-mgmt>sub-profile>session-limits overall)

Full Context configure subscriber-mgmt sla-profile session-limits overall
configure subscriber-mgmt sub-profile session-limits overall

Description This command configures the maximum number of subscriber sessions per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of subscriber sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of subscriber sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.79 overall-rate

overall-rate

Syntax **overall-rate** *packet-rate-limit*
no overall-rate

Context **[Tree]** (config>sys>security>cpu-protection>policy overall-rate)

Full Context configure system security cpu-protection policy overall-rate

Description This command applies a maximum packet arrival rate limit (applied per SAP/interface) for the entire SAP/interface, above which packets will be discarded immediately. The rate defined is a global rate limit for the interface regardless of how many traffic flows are present on the SAP/interface. It is a per-SAP/interface rate.

The **no** form of this command sets overall-rate parameter back to the default value.

Default overall max for cpu-protection-policy-id 1 to 253

overall 6000 for cpu-protection-policy-id 254 (default access interface policy)

overall max for cpu-protection-policy-id 255 (default network interface policy)

Parameters *packet-rate-limit* — Specifies a packet arrival rate limit in packets per second.

Values 1 to 65535, **max** (the max indicates no limit)

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

19.80 overflow

overflow

Syntax **overflow** *percent*
no overflow

Context **[Tree]** (config>cflowd overflow)

Full Context configure cflowd overflow

Description This command specifies the percentage of the flow cache entries removed when the maximum number of entries is exceeded. The entries removed are the entries that have not been updated for the longest amount of time.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command resets the number of entries cleared from the flow cache on overflow to the default value.

Default overflow 1

Parameters *percent* — Specifies the percentage of the flow cache entries removed when the maximum number of entries is exceeded.

Values 1 to 50 percent

Platforms All

19.81 overflow-limit

overflow-limit

Syntax **overflow-limit** *number* **threshold** *percent* [**bw** *bandwidth-in-mbps*]
no overflow-limit

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth overflow-limit)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth overflow-limit)

Full Context configure router mpls lsp auto-bandwidth overflow-limit
configure router mpls lsp-template auto-bandwidth overflow-limit

Description This command configures overflow-triggered auto-bandwidth adjustment. It sets the threshold at which bandwidth adjustment is initiated due to the configured number of overflow samples having been reached, regardless of how much time remains until the adjust interval ends.

A sample interval is counted as an overflow if the average data rate during the sample interval is higher than the currently reserved bandwidth by at least the thresholds configured as part of this command.

If overflow-triggered auto-bandwidth adjustment is successful the overflow count, maximum average data rate and adjust count are reset. If overflow-triggered auto-bandwidth adjustment fails then the overflow count is reset but the maximum average data rate and adjust count maintain current values.

The **no** form of this command disables overflow-triggered automatic bandwidth adjustment.

Default no overflow-limit

Parameters *number* — Specifies the number of overflow samples that triggers an overflow auto-bandwidth adjustment attempt.

Values 1 to 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent — Specifies the minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as a percentage of the current bandwidth, for counting an overflow sample.

Values 1 to 100

bandwidth-in-mbps — Specifies the minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as an absolute bandwidth (Mb/s) relative to the current bandwidth, for counting an overflow sample.

Values 1 to 6400000

Platforms All

19.82 overload

overload

Syntax **overload** [**timeout** *seconds*]
no overload

Context **[Tree]** (config>service>vpls>spb overload)

Full Context configure service vpls spb overload

Description This command administratively sets the SPB to operate in the overload state for a specific time period, in seconds, or indefinitely. During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is only used if the destination is reachable by SPB and is not used for other transit traffic.

If a time period is specified, the overload state persists for the configured length of time. If no time is specified, the overload state operation is maintained indefinitely.

The overload command can be useful in circumstances where SPB is overloaded or used prior to executing a shutdown command to divert traffic around the switch.

The **no** form of this command causes the router to exit the overload state.

Default no overload

Parameters *seconds* — The time, in seconds, that this router must operate in overload state.

Values 60 to 1800

Default Infinity (overload state maintained indefinitely)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

overload

Syntax **overload** [**timeout** *seconds*] [**max-metric**]
no overload

Context **[Tree]** (config>service>vprn>isis overload)

Full Context configure service vprn isis overload

Description This command administratively sets the IS-IS router to operate in the overload state for a specific time period, in seconds, or indefinitely.

During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is only used if the destination is reachable by the router and will not be used for other transit traffic.

If a time period is specified, the overload state persists for the configured length of time. If no time is specified, the overload state operation is maintained indefinitely.

The **overload** command can be useful in circumstances where the router is overloaded or used prior to executing a **shutdown** command to divert traffic around the router.

The **max-metric** parameter can be set to advertise transit links with the maximum metric of 0xffffffe (wide metrics) or 0x3f (regular metrics), instead of setting the overload bit when placing the router in overload.

The **no** form of this command causes the router to exit the overload state.

Default no overload

Parameters *seconds* — Specifies the time, in seconds, that this router must operate in overload state.

Values 60 to 1800

Default infinity (overload state maintained indefinitely)

max-metric — Set the maximum metric instead of overload.

Platforms All

overload

Syntax **overload** [**timeout** *seconds*]
no overload

Context **[Tree]** (config>service>vprn>ospf overload)
[Tree] (config>service>vprn>ospf3 overload)

Full Context configure service vprn ospf overload
configure service vprn ospf3 overload

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command changes the overload state of the local router so that it appears to be overloaded. When overload is enabled, the router can participate in OSPF routing, but is not used for transit traffic. Traffic destined to directly attached interfaces continue to reach the router.

To put the IGP in an overload state, enter a **timeout** value. The IGP will enter the overload state until the **timeout** timer expires or a **no overload** command is executed.

If the **overload** command is performed during the execution of an **overload-on-boot** command, the **overload** command takes precedence. This could occur as a result of a saved configuration file in which both parameters are saved. When the file is saved by the system, the **overload-on-boot** command is saved after the **overload** command.

Use the **no** form of this command to return to the default. When the **no overload** command is executed, the overload state is terminated, regardless the reason the protocol entered overload state.

Default no overload

Parameters **timeout** *seconds* — Specifies the number of seconds to reset overloading.

Values 60 to1800

Default 60

Platforms All

overload

Syntax **overload** [**timeout** *seconds*] [**max-metric**]
no overload

Context **[Tree]** (config>router>isis overload)

Full Context configure router isis overload

Description This command administratively sets the IS-IS router to operate in the overload state for a specific time period, in seconds, or indefinitely.

During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is only used if the destination is reachable by the router and will not be used for other transit traffic.

If a time period is specified, the overload state persists for the configured length of time. If no time is specified, the overload state operation is maintained indefinitely.

The overload command is cleared from the configuration after a reboot if **overload-on-boot** is configured with or without a timeout value. To keep the IS-IS router in the overload state indefinitely after rebooting, configure **overload-on-boot** with no timeout value or configure the **overload** command with **no overload-on-boot** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **overload** command can be useful in circumstances where the router is overloaded or used prior to executing a **shutdown** command to divert traffic around the router.

The **max-metric** parameter can be set to advertise transit links with the maximum metric of 0xfffffffe (wide metrics) or 0x3f (regular metrics), instead of setting the overload bit when placing the router in overload.

The **no** form of this command causes the router to exit the overload state.

Default no overload

Parameters *seconds* — Specifies the time, in seconds, that this router must operate in overload state.

Default infinity (overload state maintained indefinitely)

Values 60 to 1800

max-metric — Sets the maximum metric instead of overload.

Platforms All

overload

Syntax **overload** [**timeout** *seconds*]
no overload

Context **[Tree]** (config>router>ospf overload)
[Tree] (config>router>ospf3 overload)

Full Context configure router ospf overload
configure router ospf3 overload

Description This command changes the overload state of the local router so that it appears to be overloaded. When overload is enabled, the router can participate in OSPF routing, but is not used for transit traffic. Traffic destined to directly attached interfaces continues to reach the router.

To put the IGP in an overload state enter a timeout value. The IGP will enter the overload state until the timeout timer expires or a **no overload** command is executed.

If the **overload** command is encountered during the execution of an **overload-on-boot** command then this command takes precedence. This could occur as a result of a saved configuration file where both parameters are saved. When the file is saved by the system the **overload-on-boot** command is saved after the **overload** command. **However**, when **overload-on-boot** is configured under OSPF with no timeout value configured, the router will remain in overload state indefinitely after a reboot.

The **no** form of this command reverts to the default. When the **no overload** command is executed, the overload state is terminated regardless of the reason the protocol entered overload state.

Default no overload

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *timeout seconds* — Specifies the number of seconds to reset overloading.

Values 1 to 1800 in the **config**>**router**>**ospf** context
60 to 1800 in the **config**>**router**>**ospf3** context

Platforms All

19.83 overload-drop

overload-drop

Syntax **overload-drop** [**event-log** *event-log-name*]
no overload-drop

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action overload-drop)

Full Context configure application-assurance group policy app-qos-policy entry action overload-drop

Description This command configures a drop action for cases where flow records are not created (overload).

Parameters *event-log-name* — Specifies the event log name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

overload-drop

Syntax **overload-drop direction** *direction* [**create**]
no overload-drop direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca overload-drop)

Full Context configure application-assurance group statistics threshold-crossing-alert overload-drop

Description This command configures a TCA for the counter capturing drops due to the overload-drop AQP command. An overload-drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating an overload-drop TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

19.84 overload-export-external

overload-export-external

Syntax [**no**] **overload-export-external**

Context **[Tree]** (config>service>vprn>isis overload-export-external)

Full Context configure service vprn isis overload-export-external

Description This command enables external routes that are exported with an IS-IS export policy to continue to be advertised when the router is in overload.

The **no** form of this command causes external routes to be withdrawn when the router is in overload.

Default no overload-export-external

Platforms All

overload-export-external

Syntax [**no**] **overload-export-external**

Context **[Tree]** (config>router>isis overload-export-external)

Full Context configure router isis overload-export-external

Description This command enables external routes that are exported with an IS-IS export policy to continue to be advertised when the router is in overload.

The **no** form of this command causes external routes to be withdrawn when the router is in overload.

Default no overload-export-external

Platforms All

19.85 overload-export-interlevel

overload-export-interlevel

Syntax [**no**] **overload-export-interlevel**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>isis overload-export-interlevel)

Full Context configure service vprn isis overload-export-interlevel

Description This command enables inter-level routes that are exported with an IS-IS export policy to continue to be advertised when the router is in overload.

The **no** form of this command causes inter-level routes to be withdrawn when the router is in overload.

Default no overload-export-interlevel

Platforms All

overload-export-interlevel

Syntax [**no**] **overload-export-interlevel**

Context [Tree] (config>router>isis overload-export-interlevel)

Full Context configure router isis overload-export-interlevel

Description This command enables inter-level routes that are exported with an IS-IS export policy to continue to be advertised when the router is in overload.

The **no** form of this command causes inter-level routes to be withdrawn when the router is in overload.

Default no overload-export-interlevel

Platforms All

19.86 overload-include-ext-1

overload-include-ext-1

Syntax [**no**] **overload-include-ext-1**

Context [Tree] (config>service>vprn>ospf overload-include-ext-1)
[Tree] (config>service>vprn>ospf3 overload-include-ext-1)

Full Context configure service vprn ospf overload-include-ext-1
configure service vprn ospf3 overload-include-ext-1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls whether routes should be re-advertised with a maximum metric value when the system goes into overload state for any reason. When this command is enabled and the router is in overload, all external type-1 routes are advertised with the maximum metric.

The **no** form of this command reverts to the default value.

Default no overload-include-ext-1

Platforms All

overload-include-ext-1

Syntax [**no**] **overload-include-ext-1**

Context **[Tree]** (config>router>ospf overload-include-ext-1)
[Tree] (config>router>ospf3 overload-include-ext-1)

Full Context configure router ospf overload-include-ext-1
configure router ospf3 overload-include-ext-1

Description This command controls whether external type-1 routes should be re-advertised with a maximum metric value when the system goes into overload state for any reason. When this command is enabled and the router is in overload, all external type-1 routes are advertised with the maximum metric.

The **no** form of this command reverts to the default value.

Default no overload-include-ext-1

Platforms All

19.87 overload-include-ext-2

overload-include-ext-2

Syntax [**no**] **overload-include-ext-2**

Context **[Tree]** (config>service>vprn>ospf overload-include-ext-2)
[Tree] (config>service>vprn>ospf3 overload-include-ext-2)

Full Context configure service vprn ospf overload-include-ext-2
configure service vprn ospf3 overload-include-ext-2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls whether external type-2 routes should be re-advertised with a maximum metric value when the system goes into overload state for any reason. When this command is enabled and the router is in overload, all external type-2 routes is advertised with the maximum metric.

The **no** form of this command reverts to the default value.

Default no overload-include-ext-2

Platforms All

overload-include-ext-2

Syntax [**no**] **overload-include-ext-2**

Context **[Tree]** (config>router>ospf overload-include-ext-2)
[Tree] (config>router>ospf3 overload-include-ext-2)

Full Context configure router ospf overload-include-ext-2
configure router ospf3 overload-include-ext-2

Description This command controls whether external type-2 routes should be re-advertised with a maximum metric value when the system goes into overload state for any reason. When this command is enabled and the router is in overload, all external type-2 routes are advertised with the maximum metric.

The **no** form of this command reverts to the default value.

Default no overload-include-ext-2

Platforms All

19.88 overload-include-stub

overload-include-stub

Syntax [**no**] **overload-include-stub**

Context **[Tree]** (config>service>vprn>ospf overload-include-stub)
[Tree] (config>service>vprn>ospf3 overload-include-stub)

Full Context configure service vprn ospf overload-include-stub
configure service vprn ospf3 overload-include-stub

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls whether the OSPF stub networks should be advertised with a maximum metric value when the system goes into overload state for any reason. When enabled, the system uses the maximum metric value. When this command is enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, are advertised at the maximum metric.

The **no** form of this command reverts to the default value.

Default no overload-include-stub

Platforms All

overload-include-stub

Syntax [**no**] **overload-include-stub**

Context **[Tree]** (config>router>ospf overload-include-stub)
[Tree] (config>router>ospf3 overload-include-stub)

Full Context configure router ospf overload-include-stub
configure router ospf3 overload-include-stub

Description This command controls whether the OSPF stub networks should be advertised with a maximum metric value when the system goes into overload state for any reason. When enabled, the system uses the maximum metric value. When this command is enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, are advertised at the maximum metric.

The **no** form of this command reverts to the default value.

Default no overload-include-stub

Platforms All

19.89 overload-on-boot

overload-on-boot

Syntax **overload-on-boot** [**timeout** *seconds*]
no overload-on-boot

Context **[Tree]** (config>service>vpls>spb overload-on-boot)

Full Context configure service vpls spb overload-on-boot

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When the router is in an overload state, SPB the B-VPLS is used only if there is no other SPB B-VPLS to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- The timeout timer expires.
- A manual override of the current overload state is entered with the **no** form of the **config**>**service**>**vpls**>**spb overload** command.

The **no** form of this command does not affect the overload-on-boot function.

If no timeout is specified, SPB IS-IS goes into overload indefinitely after a reboot. After the reboot, the SPB IS-IS status displays a permanent overload state:

```
L1 LSDB Overload: Manual on boot (Indefinitely in overload)
```

This state can be cleared with the **config**>**service**>**vpls**>**spb**>**no overload** command.

When specifying a timeout value, SPB IS-IS goes into overload for the configured timeout after a reboot. After the reboot, SPB IS-IS status displays the remaining time the system stays in overload:

```
L1 LSDB Overload: Manual on boot (Overload Time Left: 17)
```

The overload state can be cleared before the timeout expires with the **no** form of the **config**>**service**>**vpls**>**spb overload** command.

The **no** form of this command removes the overload-on-boot functionality from the configuration.

Default no overload-on-boot

Parameters *seconds* — Specifies the time, in seconds, that this router must operate in overload state.

Values 60 to 1800

Default Infinity (overload state maintained indefinitely)

Platforms All

overload-on-boot

Syntax **overload-on-boot** [**timeout** *seconds*] [**max-metric**]
no overload-on-boot

Context **[Tree]** (config>service>vprn>isis overload-on-boot)

Full Context configure service vprn isis overload-on-boot

Description When the router is in an overload state, it is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The timeout timer expires.
- A manual override of the current overload state is entered with the **config>router>isis>no overload** command.

  The **no overload** command does not affect the **overload-on-boot** function.

If no timeout is specified, IS-IS will go into overload indefinitely after a reboot. After the reboot, the IS-IS status will display a permanent overload state:

- L1 LSDB Overload : Manual on boot (Indefinitely in overload)
- L2 LSDB Overload : Manual on boot (Indefinitely in overload)

This state can be cleared with the **config>router>isis>no overload** command.

When specifying a timeout value, IS-IS will go into overload for the configured timeout after a reboot. After the reboot, the IS-IS status will display the remaining time the system stays in overload:

- L1 LSDB Overload : Manual on boot (Overload Time Left : 17)
- L2 LSDB Overload : Manual on boot (Overload Time Left : 17)

The overload state can be cleared before the timeout expires with the **config>router>isis>no overload** command.

The **no** form of this command removes the overload-on-boot functionality from the configuration.

Use the **show router isis status** command to display the administrative and operational state as well as all timers.

Default no overload-on-boot

Parameters **timeout** *seconds* — Configure the timeout timer for overload-on-boot in seconds.

Values 60 to 1800

max-metric — Set the maximum metric instead of overload.

Platforms All

overload-on-boot

Syntax **overload-on-boot** [**timeout** *seconds*]
no overload

Context **[Tree]** (config>service>vprn>ospf overload-on-boot)
[Tree] (config>service>vprn>ospf3 overload-on-boot)

Full Context configure service vprn ospf overload-on-boot
configure service vprn ospf3 overload-on-boot

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When the router is in an overload state, it is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- The timeout timer expires.
- A manual override of the current overload state is entered with the **no overload** command.

The **no overload** command does not affect the **overload-on-boot** function.

The **no** form of this command removes the overload-on-boot functionality from the configuration.

Default no overload-on-boot

Parameters **timeout** *seconds* — Specifies the number of seconds to reset overloading.

Values 60 to1800

Default 60

Platforms All

overload-on-boot

Syntax **overload-on-boot** [**timeout** *seconds*] [**max-metric**]
no overload-on-boot

Context **[Tree]** (config>router>isis overload-on-boot)

Full Context configure router isis overload-on-boot

Description When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

1. The timeout timer expires.
2. A manual override of the current overload state is entered with the **config>router>isis>no overload** command.

The **no overload** command does not affect the **overload-on-boot** function.

If no timeout is specified, IS-IS will go into overload indefinitely after a reboot. After the reboot, the IS-IS status will display a permanent overload state:

- L1 LSDB Overload : Manual on boot (Indefinitely in overload)
- L2 LSDB Overload : Manual on boot (Indefinitely in overload)

This state can be cleared with the **config>router>isis>no overload** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When specifying a timeout value, IS-IS will go into overload for the configured timeout after a reboot. After the reboot, the IS-IS status will display the remaining time the system stays in overload:

- L1 LSDB Overload : Manual on boot (Overload Time Left : 17)
- L2 LSDB Overload : Manual on boot (Overload Time Left : 17)

The overload state can be cleared before the timeout expires with the **config>router>isis>no overload** command.

The **no** form of this command removes the overload-on-boot functionality from the configuration.

Use the show router isis status command to display the administrative and operational state as well as all timers.

Default no overload-on-boot

Parameters *seconds* — Specifies the timeout timer for overload-on-boot, in seconds.

Values 60 to 1800

max-metric — Sets the maximum metric instead of overload.

Platforms All

overload-on-boot

Syntax **overload-on-boot** [**timeout** *seconds*]
no overload

Context **[Tree]** (config>router>ospf overload-on-boot)
[Tree] (config>router>ospf3 overload-on-boot)

Full Context configure router ospf overload-on-boot
configure router ospf3 overload-on-boot

Description When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- the timeout timer expires
- a manual override of the current overload state is entered with the **no overload** command

The **no overload** command does not affect the **overload-on-boot** function.

The **no** form of this command removes the overload-on-boot functionality from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default timeout value is 60 seconds, which means after 60 seconds overload status the SR will recover (change back to non-overload status). However, when **overload-on-boot** is configured under OSPF with no timeout value the router will remain in overload state indefinitely after a reboot.

Default no overload-on-boot

Parameters *timeout seconds* — Specifies the number of seconds to reset overloading.

Values 1 to 1800 in the **config**>**router**>**ospf** context
60 to 1800 in the **config**>**router**>**ospf3** context

Platforms All

19.90 overload-sub-quarantine

overload-sub-quarantine

Syntax **overload-sub-quarantine**

Context **[Tree]** (config>isa>aa-grp overload-sub-quarantine)

Full Context configure isa application-assurance-group overload-sub-quarantine

Description Commands in this context configure overload subscriber detection for this application assurance group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.91 override

override

Syntax [**no**] **override**

Context **[Tree]** (config>service>vprn>pim>rp>static override)

Full Context configure service vprn pim rp static override

Description This command changes the precedence of static RP over dynamically learned Rendezvous Point (RP).

When enabled, the static group-to-RP mappings take precedence over the dynamically learned mappings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no override

override

Syntax [**no**] **override**

Context **[Tree]** (config>router>pim>rp>static>address override)
[Tree] (config>router>pim>rp>ipv6>static>address override)

Full Context configure router pim rp ipv6 static address override
configure router pim rp static address override

Description This command changes the precedence of static RP over dynamically-learned Rendezvous Points (RPs).

When enabled, the static group-to-RP mappings take precedence over the dynamically learned mappings.

The **no** form of this command reverts to the default.

Default no override

Platforms All

19.92 override-bmi

override-bmi

Syntax **override-bmi** *value*
no override-bmi

Context **[Tree]** (config>router>isis>segm-rtng>msd override-bmi)

Full Context configure router isis segment-routing maximum-sid-depth override-bmi

Description This command provides the ability to override the announced MSD node Base MPLS Imposition (BMI). The MSD-BMI value announced by a router can be used by recipients to understand the number of MPLS labels that can be imposed inclusive of all service, transport, or special labels.

When **override-bmi** is not configured, the router announces the node maximum supported BMI assuming the most simple services and Layer 2 encapsulation.

The **no** form of this command reverts to the default.

Default no override-bmi

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *values* — Specifies the override BMI.

Values 0 to 12

Platforms All

override-bmi

Syntax **override-bmi** *value*
no override-bmi

Context **[Tree]** (config>router>ospf>segm-rtng>msd override-bmi)

Full Context configure router ospf segment-routing maximum-sid-depth override-bmi

Description This command provides the ability to override the announced MSD node Base MPLS Imposition (BMI). The MSD-BMI value announced by a router can be used by recipients to understand the number of MPLS labels that can be imposed inclusive of all service, transport, or special labels.

When **override-bmi** is not configured, the router announces the node maximum supported BMI assuming the most simple services and Layer 2 encapsulation.

The **no** form of this command reverts to the default.

Default no override-bmi

Parameters *values* — Specifies the override BMI. The upper limit depends on the FP chipset used.

Values 0 to 12

Platforms All

19.93 override-erld

override-erld

Syntax **override-erld** *value*
no override-erld

Context **[Tree]** (config>router>isis>segm-rtng>msd override-erld)

Full Context configure router isis segment-routing maximum-sid-depth override-erld

Description This command provides the ability to override the announced MSD node Entropy Readable Label Depth (ERLD). It is useful for ingress LSRs to know each intermediate LSR's capability of reading the maximum label stack depth and performing EL-based load balancing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When **override-erld** is not configured, then the router announces the node maximum supported ERLD assuming the most simple Layer 2 encapsulation.

The **no** form of this command reverts to the default.

Default no override-erld

Parameters *values* — Specifies the override ERLD.

Values 0 to 15

Platforms All

override-erld

Syntax **override-erld** *value*
no override-erld

Context **[Tree]** (config>router>ospf>segm-rtng>msd override-erld)

Full Context configure router ospf segment-routing maximum-sid-depth override-erld

Description This command provides the ability to override the announced MSD node Entropy Readable Label Depth (ERLD). It is useful for ingress LSRs to know each intermediate LSR's capability of reading the maximum label stack depth and performing EL-based load balancing.

When **override-erld** is not configured, then the router announces the node maximum supported ERLD assuming the most simple Layer 2 encapsulation.

Default no override-erld

Parameters *values* — Specifies the override ERLD. The upper limit depends on the FP chipset used.

Values 0 to 15

Platforms All

19.94 override-slaac

override-slaac

Syntax [**no**] **override-slaac**

Context **[Tree]** (config>service>vprn>sub-if>ipv6>dhcp6 override-slaac)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6 override-slaac)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 override-slaac)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 override-slaac)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 override-slaac
configure service ies subscriber-interface ipv6 dhcp6 override-slaac
configure service vprn subscriber-interface group-interface ipv6 dhcp6 override-slaac
configure service vprn subscriber-interface ipv6 dhcp6 override-slaac

Description This command allows a DHCP IA_NA address to override and replace a host existing SLAAC address. When this feature is enabled, a subscriber SLAAC address is removed once the DHCP IA_NA address assignment is completed. If used with conjunction with the **allow-multiple-wan-address** command, the DHCP IA_NA address will also override the SLAAC address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

19.95 override-tunnel-elc

override-tunnel-elc

Syntax [**no**] **override-tunnel-elc**

Context **[Tree]** (config>router>bgp override-tunnel-elc)

Full Context configure router bgp override-tunnel-elc

Description This command enables or disables entropy label capability (ELC) on BGP tunnels.

When this command is enabled, the system assumes that all far ends for BGP tunnels are entropy-label-capable, regardless of any received capability signaling. This ensures that the entropy label will be inserted on BGP tunnels in the absence of capability signaling support by the far end.

This is a system-wide configuration, since efficient entropy label operation requires that all LSRs in a network support entropy labels. This command should be used with care, particularly in inter-AS use cases, since entropy label capability may differ between domains.

Default no override-tunnel-elc

Platforms All

override-tunnel-elc

Syntax [**no**] **override-tunnel-elc**

Context **[Tree]** (config>router>isis>entropy-label override-tunnel-elc)
[Tree] (config>router>ospf>entropy-label override-tunnel-elc)

Full Context configure router isis entropy-label override-tunnel-elc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf entropy-label override-tunnel-elc

Description This command configures the ability to override any received entropy label capability advertisement. When enabled, the system assumes that all nodes for an IGP domain are capable of receiving and processing the entropy label on segment routed tunnels. This command can only be configured if **entropy-label** is enabled via the **config**>**router**>**isis**>**segment-routing**>**entropy-label** or **config**>**router**>**ospf**>**segment-routing**>**entropy-labe**l command.

The **no** form of this command disables the override. The system assumes entropy label capability for other nodes in the IGP instance if capability advertisements are received.

Default no override-tunnel-elc

Platforms All

override-tunnel-elc

Syntax [**no**] **override-tunnel-elc**

Context **[Tree]** (config>router>mpls>lsp override-tunnel-elc)
[Tree] (config>router>mpls>lsp-template override-tunnel-elc)

Full Context configure router mpls lsp override-tunnel-elc
configure router mpls lsp-template override-tunnel-elc

Description This command allows the system to override any received entropy label capability advertisement.

This command is enabled under the LSP context or in LSP templates of type **pce-init-p2p-srte** and **on-demand-p2p-srte**, the system assumes that all nodes along the path of the SR-TE LSP are capable of receiving and processing the entropy label. This includes SR-TE LSPs that have a PCE-computed path, PCE-initiated SR-TE LSPs, and on-demand SR-TE LSPs.

The **no** form of this command disables the override.

Default no override-tunnel-elc

Platforms All

19.96 own-auth-method

own-auth-method

Syntax **own-auth-method** {**psk** | **cert** | **eap-only**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no own-auth-method

Context [Tree] (config>ipsec>ike-policy own-auth-method)

Full Context configure ipsec ike-policy own-auth-method

Description This command configures the authentication method used with this IKE policy on its own side.

Default no own-auth-method

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

19.97 owner

owner

Syntax **owner** {**bgp-ad** | **bgp-vpls** | **bgp-evpn-mpls**}
no owner

Context [Tree] (config>service>vpls>provider-tunnel>inclusive owner)

Full Context configure service vpls provider-tunnel inclusive owner

Description This command selects the owner protocol of the inclusive PMSI tunnel in the service. Only one of the protocols will support the provider tunnel.

The **bgp-vpls** and **bgp-evpn-mpls** parameters cannot be configured together in the same service. Although **bgp-ad** and **bgp-evpn** can coexist in the same service, **bgp-ad** cannot be configured as the owner of the provider-tunnel. In addition, the following applies to this configuration:

- The owner must be explicitly set before the provider-tunnel can be **no shutdown**.
- If the owner is **bgp-ad**, then BGP-EVPN MPLS and BGP-EVPN VXLAN will fail to **no shutdown**.
- The provider-tunnel must be shutdown to change the owner; on the fly change is not allowed.

Default no owner

Parameters **bgp-ad** — Specifies that bgp-ad is the owner of the provider-tunnel.

bgp-vpls — Specifies that bgp-vpls is the owner of the provider-tunnel.

bgp-evpn-mpls — Specifies that BGP-EVPN MPLS is the owner of the provider-tunnel.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20 p Commands

20.1 p2mp

p2mp

Syntax **p2mp** {**enable** | **disable**}

Context **[Tree]** (config>router>ldp>session-params>peer>fec-type-capability p2mp)

Full Context configure router ldp session-parameters peer fec-type-capability p2mp

Description This command enables or disables P2MP FEC capability for the session.

Platforms All

20.2 p2mp-candidate-path

p2mp-candidate-path

Syntax [**no**] **p2mp-candidate-path** *candidate-path-name*

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy p2mp-candidate-path)

Full Context configure router p2mp-sr-tree p2mp-policy p2mp-candidate-path

Description This command configures a candidate path in the P2MP policy entry for the P2MP SR tree.

A P2MP SR policy can contain multiple candidate paths, which are redundant trees. Each candidate path represents a P2MP SR tree with its own traffic engineering constraints. Each candidate path has its own preference; the candidate path with the highest preference is the active P2MP SR tunnel.

The **no** form of this command removes the specified candidate path from the P2MP SR policy.

Parameters *candidate-path-name* — Specifies the name of the candidate path, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.3 p2mp-id

p2mp-id

Syntax **p2mp-id** *id*

Context **[Tree]** (config>router>mpls>lsp p2mp-id)

Full Context configure router mpls lsp p2mp-id

Description This command configures the identifier of an RSVP P2MP LSP. An RSVP P2MP LSP is fully identified by the combination of: <P2MP ID, tunnel ID, extended tunnel ID> part of the P2MP session object, and <tunnel sender address, LSP ID> fields in the p2mp sender_template object.

The **p2mp-id** is a 32-bit identifier used in the session object that remains constant over the life of the P2MP tunnel. It is unique within the scope of the ingress LER.

The **no** form restores the default value of this parameter.

This command is not supported on the 7450 ESS.

Default 0

Parameters *id* — Specifies a P2MP identifier.

Values 0 to 65535

Platforms All

20.4 p2mp-ipv4

p2mp-ipv4

Syntax **p2mp** {**enable** | **disable**}

Context **[Tree]** (config>router>ldp>if-params>if>ipv4>fec-type-capability p2mp-ipv4)
[Tree] (config>router>ldp>if-params>if>ipv6>fec-type-capability p2mp-ipv4)
[Tree] (config>router>ldp>session-params>peer>fec-cap p2mp-ipv4)

Full Context configure router ldp interface-parameters interface ipv4 fec-type-capability p2mp-ipv4
configure router ldp interface-parameters interface ipv6 fec-type-capability p2mp-ipv4
configure router ldp session-parameters peer fec-type-capability p2mp-ipv4

Description This command enables or disables IPv4 P2MP FEC capability on the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **config>router>ldp>if-params>if>ipv6>fec-type-capability>p2mp-ipv4** command is not supported on the 7450 ESS.

Platforms All

20.5 p2mp-ipv6

p2mp-ipv6

Syntax **p2mp** {**enable** | **disable**}

Context **[Tree]** (config>router>ldp>if-params>if>ipv4>fec-type-capability p2mp-ipv6)
[Tree] (config>router>ldp>if-params>if>ipv6>fec-type-capability p2mp-ipv6)
[Tree] (config>router>ldp>session-params>peer>fec-cap p2mp-ipv6)

Full Context configure router ldp interface-parameters interface ipv4 fec-type-capability p2mp-ipv6
configure router ldp interface-parameters interface ipv6 fec-type-capability p2mp-ipv6
configure router ldp session-parameters peer fec-type-capability p2mp-ipv6-address

Description This command enables or disables IPv6 P2MP FEC capability on the interface.

This command is not supported on the 7450 ESS.

Platforms All

20.6 p2mp-ldp-tree-join

p2mp-ldp-tree-join

Syntax **p2mp-ldp-tree-join**
p2mp-ldp-tree-join ipv4
p2mp-ldp-tree-join ipv6
p2mp-ldp-tree-join ipv4 ipv6
no p2mp-ldp-tree-join [**ipv4**] [**ipv6**]

Context **[Tree]** (config>service>vprn>pim>if p2mp-ldp-tree-join)

Full Context configure service vprn pim interface p2mp-ldp-tree-join

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the option to join P2MP LDP tree towards the multicast source for the VPRN service. If p2mp-ldp-tree-join is enabled, a PIM multicast join received on an interface is processed to join P2MP LDP LSP using the in-band signaled P2MP tree for the same multicast flow. LDP P2MP tree is setup towards the multicast source. Route to source of the multicast node is looked up from the RTM. The next-hop address for the route to source is set as the root of LDP P2MP tree.

The **no** form of command disables joining P2MP LDP tree for IPv4 or IPv6 or both (if both or none is specified).

Default no p2mp-ldp-tree-join

Parameters *ipv4* — Enables dynamic mLDP in-band signaling for IPv4 PIM joins. IPv4 multicast must be enabled; see **ipv4-multicast-disable**. For backward compatibility **p2mp-ldp-tree-join** is equivalent to **p2mp-ldp-tree-join ipv4**.

ipv6 — Enables dynamic mLDP in-band signaling for IPv6 PIM joins. IPv6 multicast must be enabled; see **ipv6-multicast-disable**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

p2mp-ldp-tree-join

Syntax [**no**] **p2mp-ldp-tree-join** [**ipv4**] [**ipv6**]

Context **[Tree]** (config>router>pim>interface p2mp-ldp-tree-join)

Full Context configure router pim interface p2mp-ldp-tree-join

Description This command configures the option to join the P2MP LDP tree towards the multicast source. If **p2mp-ldp-tree-join** is enabled, a PIM multicast join received on an interface is processed to join the P2MP LDP LSP, using the in-band signaled P2MP tree for the same multicast flow. LDP P2MP tree is set up towards the multicast source. The route to the multicast node source is looked up from the RTM. The next-hop address for the route to source is set as the root of LDP P2MP tree.

The **no** form of this command disables joining the P2MP LDP tree for IPv4 or IPv6 or for both (if both or none is specified).

Default no p2mp-ldp-tree-join

Parameters *ipv4* — Enables dynamic MLDP in-band signaling for IPv4 PIM joins. IPv4 multicast must be enabled. For backward compatibility **p2mp-ldp-tree-join** is equivalent to **p2mp-ldp-tree-join ipv4**.

ipv6 — Enables dynamic MLDP in-band signaling for IPv6 PIM joins. IPv6 multicast must be enabled.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.7 p2mp-lsp-ping

p2mp-lsp-ping

Syntax **p2mp-lsp-ping** *lsp-name* [**p2mp-instance** *instance-name* [**s2l-dest-address** *ipv4-address* [*ipv4-address*]]] [**ttl** *label-ttl*]
p2mp-lsp-ping ldp *p2mp-identifier* [**vpn-recursive-fec**] [**sender-addr** *ipv4-address*] [**leaf-addr** *ipv4-address* [*ipv4-address*]]
p2mp-lsp-ping ldp-ssm source *ip-address* **group** *ip-address* [{**router** *router-instance* | **service-name** *service-name*}] [**sender-addr** *ipv4-address*] [**leaf-addr** *ipv4-address* [*ipv4-address*]]
NOTE: Options common to all **p2mp-lsp-ping** cases**:** [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**timeout** *timeout*] [**detail**]

Context **[Tree]** (oam p2mp-lsp-ping)

Full Context oam p2mp-lsp-ping

Description This command performs an in-band connectivity test for an RSVP P2MP LSP. The echo request message is sent on the active P2MP instance and is replicated in the data path over all branches of the P2MP LSP instance. By default, all egress LER nodes that are leaves of the P2MP LSP instance replies to the echo request message.

LDP P2MP generic-identifier along with source IP address of the head-end node can be used to uniquely identify LDP P2MP LSP in a 7750 SR or 7950 XRS network. LDP **p2mp-identifier** is a mandatory parameter to test LSP ping. LDP P2MP identifier specified to configure a tunnel-interface on head-end node must be used as **p2mp-identifier** to test an LSP.

To reduce the scope of the echo reply messages, explicitly enter a list of addresses for the egress LER nodes that are required to reply. A maximum of five addresses can be specified in a single run of the **p2mp-lsp-ping** command. An LER node can parse the list of egress LER addresses and, if its address is included, it replies with an echo reply message.

The output of the command without the **detail** option provides a high-level summary of received error codes and success codes. The output of the command with the **detail** option shows a line for each replying node, as in the output of the LSP ping for a P2P LSP.

The display is delayed until all responses are received or the timer configured in the *timeout* parameter expires. No other CLI commands can be entered while waiting for the display. Entering A ^C aborts the ping operation. Note that **p2mp-lsp-ping** is not supported in a VPLS/B-VPLS PMSI context.

The timestamp format to be sent, and to be expected when received in a PDU, is as configured by the **config>test-oam>mpls-time-stamp-format** command. If RFC 4379 (obsoleted by RFC 8029) is selected, then the timestamp is in seconds and microseconds since 1900, otherwise it is in seconds and microseconds since 1970.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *lsp-name* — Specifies the name, up to 64 characters, that identifies an P2MP LSP to ping.

instance-name — Specifies the name, up to 32 characters, of the specific instance of the P2MP LSP to send the echo request.

s2l-dest-addr *ipv4-address* — Specifies up to five egress LER system addresses that are required to reply to the LSP ping echo request message.

label-ttl — Specifies the TTL value for the MPLS label, expressed as a decimal integer.

Values 1 to 255

Default 255

p2mp-identifier — Specifies the identifier for an LDP P2MP LSP to ping (applies to the 7750 SR and 7950 XRS only).

Values 1 to 4294967295

vpn-recursive-fec — Adds a VPN recursive FEC element to the launched packet (useful for pinging a VPN BGP inter-AS Option B leaf). This parameter issues an OAM **p2mp-lsp-ping** with RFC 6512 VPN recursive opaque FEC type 8.

Refer to the “OAM” subsection of the LDP chapter in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for more information.

sender-addr *ipv4-address* — Specifies any local IP sender address for mLDP (applies to the 7750 SR and 7950 XRS only).

leaf-addr *ipv4-address* — Specifies up to five egress LER system addresses that are required to reply to LSP ping echo request message (applies to the 7750 SR and 7950 XRS only).

Values ipv4-address: a.b.c.d

ldp-ssm — Specifies a specific multicast stream to be tested when using dynamic multicast in mLDP. The source and group addresses correspond to the <S,G> being advertised by this mLDP FEC.

Values

source	*ipv4-address*	*a.b.c.d*|
	ipv6-address	*x:x:x:x:x:x:x:x* (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0t o 255]D
group	*mcast-address*	
	mcast-v6-address	
router	*router-name*	Base | management
		Default - Base
	service-id	[1 to 2147483647]
	service-name	up to 64 characters
sender-addr	*ipv4-address*	*a.b.c.d*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

leaf-addr *ipv4-address* *a.b.c.d*

fc-name — Specifies the **fc** and **profile** parameters used to indicate the forwarding class and profile of the MPLS echo request packet.

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified fc and profile parameter values. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface.

When the MPLS echo request packet is received on the responding node, the **fc** and **profile** parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in an egress network queue. The egress network queue is selected according to the **fc** and **profile** parameter values determined by the classification of the echo request packet that is being replied to at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. The ToS byte is not modified. Table 105 summarizes this behavior.

Table 105 **p2mp-lsp-ping Request Packet and Behavior**

Request Packet	Behavior
CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by the user in the OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • packet queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet {tos=1, fc2, profile2}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 105 **p2mp-lsp-ping Request Packet and Behavior**

Request Packet	Behavior
Outgoing interface (responder node)	Echo reply packet: • packet queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile of the LSP ping echo request message.

Default out

octets — Specifies the size in octets, expressed as a decimal integer, of the MPLS echo request packet, including the IP header but not the label stack. The request payload is padded with zeros to the specified size. Note that an OAM command is not failed if the user enters a size lower than the minimum required to build the packet for the echo request message. The payload is automatically padded to meet the minimum size.

Values 1 to 9786

Default 1

timeout — Specifies the time, in seconds, that is used to override the default *timeout* value and is the amount of time that the router waits for an echo reply message from all leaves of the P2MP LSP after sending the message request message. Upon the expiration of the message time out, the requesting router no longer waits for reply messages. Any echo reply message received after the request times out is silently discarded.

Values 1 to 120

Default 10

detail — Displays P2MP LSP detailed information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.8 p2mp-lsp-trace

p2mp-lsp-trace

Syntax **p2mp-lsp-trace** *lsp-name* **p2mp-instance** *instance-name* **s2l-dest-address** *ip-address* [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**max-fail** *no-response-count*] [**probe-count** *probes-per-hop*] [**min-ttl** *min-label-ttl*] [**max-ttl** *max-label-ttl*] [**timeout** *timeout*] [**interval** *interval*] [**detail**]

Context **[Tree]** (oam p2mp-lsp-trace)

Full Context oam p2mp-lsp-trace

Description This command discovers and displays the hop-by-hop path for a source-to-leaf (S2L) sub-LSP of an RSVP P2MP LSP.

The LSP trace capability allows the user to trace the path of a single S2L path of a P2MP LSP. Its operation is like **p2mp-lsp-ping**, but the sender of the echo reply request message includes the downstream mapping TLV to request the downstream branch information from a branch LSR or bud LSR. The branch LSR or bud LSR also includes the downstream mapping TLV to report the information about the downstream branches of the P2MP LSP. An egress LER does not include this TLV in the echo response message.

The parameter probe-count operates in the same way as in LSP Trace on a P2P LSP. It represents the maximum number of probes sent per TTL value before stops waiting for echo reply messages. If a response is received from the traced node before reaching maximum number of probes, then no more probes are sent for the same TTL. The sender of the echo request then increments the TTL and uses the information it received in the downstream mapping TLV to start sending probes to the node downstream of the last node which replied. This continues until the egress LER for the traced S2L path replies.

Like **p2mp-lsp-ping**, an LSP trace probe reports on all egress LER nodes that eventually receive the echo request message, but only the traced egress LER node replies to the last probe.

Any branch LSR node or bud LSR node in the P2MP LSP tree may receive a copy of the echo request message with the TTL in the outer label expiring at this node. However, only a branch LSR or bud LSR that has a downstream branch over which the traced egress LER is reachable responds.

When a branch LSR or bud LSR responds, it sets the global return code in the echo response message to RC=14 - “See DDMAP TLV for Return Code and Return Sub-Code” and the return code in the DDMAP TLV corresponding to the outgoing interface of the branch used by the traced S2L path to RC=8 - “Label switched at stack-depth <RSC>”. Note that **p2mp-lsp-trace** is not supported in a VPLS/B-VPLS PMSI context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The timestamp format to be sent, and to be expected when received in a PDU, is as configured by the **config>test-oam>mpls-time-stamp-format** command. If RFC 4379 (obsoleted by RFC 8029) is selected, then the timestamp is in seconds and microseconds since 1900, otherwise it is in seconds and microseconds since 1970.

Parameters *lsp-name* — Specifies the name that identifies an P2MP LSP, up to 64 characters, to ping.

instance-name — Specifies the name, up to 32 characters, of the specific instance of the P2MP LSP to send the echo request.

ip-address — Specifies the egress LER system address of the S2L sub-LSP path which is being traced.

Values a.b.c.d

fc-name — Specifies the **fc** and **profile** parameters are used to indicate the forwarding class and profile of the MPLS echo request packet.

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified FC and profile parameter values. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface.

When the MPLS echo request packet is received on the responding node, the **fc** and **profile** parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in an egress network queue. The egress network queue is selected according to the **fc** and **profile** parameter values determined by the classification of the echo request packet that is being replied to at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. The ToS byte is not modified. Table 106 summarizes this behavior.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 106 **p2mp-lsp-trace Request Packet and Behavior**

Request Packet	Behavior
CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • packet queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet {tos=1, fc2, profile2}
Outgoing interface (responder node)	Echo reply packet: • packet queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet{tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile of the LSP trace echo request message.

Default out

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

octets — Specifies the size in octets, expressed as a decimal integer, of the MPLS echo request packet, including the IP header but not the label stack. The request payload is padded with zeros to the specified size. Note that an OAM command is not failed if the user enters a size lower than the minimum required to build the packet for the echo request message. The payload is automatically padded to meet the minimum size.

Values 1 to 9786

Default 1

no-response-count — Specifies the maximum number of consecutive MPLS echo requests, expressed as a decimal integer that do not receive a reply before the trace operation fails for a given TTL.

Values 1 to 10

Default 5

probes-per-hop — Specifies the number of LSP trace echo request messages to send per TTL value.

Values 1 to 10

Default 1

min-label-ttl — Specifies the minimum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Values 1 to 255

Default 1

max-label-ttl — Specifies the maximum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Values 1 to 255

Default 30

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for an echo reply message from all leaves of the P2MP LSP after sending the message request message. Upon the expiration of the message time out, the requesting router no longer waits for reply messages. Any echo reply message received after the request times out is silently discarded.

Values 1 to 60

Default 3

interval — Specifies the time, in seconds, used to override the default echo request message send interval and defines the minimum amount of time that must expire before the next echo request message is sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the **interval** is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of an echo reply message corresponding to the outstanding message request.

Values 1 to 10

Default 1

Output The following is an example of p2mp-lsp-trace information.

Sample Output

```
*A:Dut-C# oam p2mp-lsp-trace "p2mp_1" p2mp-instance "1" s2l-dest-address 10.20.1.
10.20.1.4  10.20.1.5  10.20.1.6
*A:Dut-C# oam p2mp-lsp-trace "p2mp_1" p2mp-instance "1" s2l-dest-
address 10.20.1.5 detail
P2MP LSP p2mp_1: 132 bytes MPLS payload
P2MP Instance 1, S2L Egress 10.20.1.5

  1  10.20.1.1  rtt=3.78 ms rc=8(DSRtrMatchLabel)
     DS 1: ipaddr 10.20.1.2 iftype 'ipv4Unnumbered' ifaddr 2 MRU=1500 label=131060
proto=4(RSVP-TE) B/E flags:0/0
  2  10.20.1.2  rtt=3.54 ms rc=8(DSRtrMatchLabel)
     DS 1: ipaddr 10.20.1.4 iftype 'ipv4Unnumbered' ifaddr 3 MRU=1500 label=131061
proto=4(RSVP-TE) B/E flags:0/0
  3  10.20.1.5  rtt=5.30 ms rc=5(DSMappingMismatched)

Probe returned multiple responses. Result may be inconsistent.

*A:Dut-C#
```

Platforms All

20.9 p2mp-merge-point-abort-timer

p2mp-merge-point-abort-timer

Syntax **p2mp-merge-point-abort-timer** *seconds*
no p2mp-merge-point-abort-timer

Context **[Tree]** (config>router>rsvp p2mp-merge-point-abort-timer)

Full Context configure router rsvp p2mp-merge-point-abort-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a configurable timer to abort Merge-Point (MP) node procedures for an S2L of a P2MP LSP instance. When a value higher than zero is configured for this timer, it will enter into effect anytime this node activates Merge-Point procedures for one or more P2MP LSP S2L paths. As soon an ingress interface goes operationally down, the Merge-Point node starts the abort timer. Upon expiry of the timer, MPLS will clean up all P2MP LSP S2L paths which ILM is on the failed interface and which have not already received a Path refresh over the bypass LSP.

The **no** form of this command disables the timer.

Default no p2mp-merge-point-abort-timer

Parameters *seconds* — Specifies the length of the abort timer in seconds

Values 1 to 65535

Platforms All

20.10 p2mp-policy

p2mp-policy

Syntax [**no**] **p2mp-policy** *policy-name*

Context **[Tree]** (config>router>p2mp-sr-tree p2mp-policy)

Full Context configure router p2mp-sr-tree p2mp-policy

Description This command creates a P2MP policy entry for the P2MP SR tree.

The **no** form of this command deletes the specified policy entry.

Parameters *policy-name* — Specifies the policy name, up to 32 characters.

Platforms All

p2mp-policy

Syntax [**no**] **p2mp-policy**

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>p2mp-sr p2mp-policy)
[Tree] (config>service>vprn>mvpn>pt>selective>multistream-spmsi p2mp-policy)
[Tree] (config>service>vprn>mvpn>pt>selective>p2mp-sr p2mp-policy)

Full Context configure service vprn mvpn provider-tunnel inclusive p2mp-sr p2mp-policy
configure service vprn mvpn provider-tunnel selective multistream-spmsi p2mp-policy
configure service vprn mvpn provider-tunnel selective p2mp-sr p2mp-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables a P2MP policy for the MVPN provider tunnel.

The **no** form of this command disables the P2MP policy.

Platforms All

20.11 p2mp-resignal-timer

p2mp-resignal-timer

Syntax **p2mp-resignal-timer** *minutes*
no p2mp-resignal-timer

Context **[Tree]** (config>router>mpls p2mp-resignal-timer)

Full Context configure router mpls p2mp-resignal-timer

Description This command configures the re-signal timer for a P2MP LSP instance. MPLS will request CSPF to re-compute the whole set of S2L paths of a given active P2MP instance each time the P2MP re-signal timer expires. The P2MP re-signal timer is configured separately from the P2P LSP parameter. MPLS performs a global MBB and moves each S2L sub-LSP in the instance into its new path using a new P2MP LSP ID if the global MBB is successful, regardless of the cost of the new S2L path.

This command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

The **no** form of this command disables the timer-based re-signaling of P2MP LSPs on this system.

Parameters *minutes* — Specifies the time MPLS waits before attempting to re-signal the P2MP LSP instance.

Values 60 to 10080

Platforms All

20.12 p2mp-s2l-fast-retry

p2mp-s2l-fast-retry

Syntax **p2mp-s2-fast-retry** *seconds*
no p2mp-s2l-fast-retry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>mpls p2mp-s2l-fast-retry)
[Tree] (config>router>rsvp p2mp-s2l-fast-retry)

Full Context configure router mpls p2mp-s2l-fast-retry
configure router rsvp p2mp-s2l-fast-retry

Description This command configures a global parameter to allow the user to apply a shorter retry timer for the first try after an active LSP path went down due to a local failure or the receipt of a ResvTear. This timer is used only in the first try. Subsequent retries will continue to be governed by the existing LSP level retry-timer.

The config>router>mpls>p2mp-s2l-fast-retry command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

The **no** form of this command disables the timer.

Default no p2mp-s2l-fast-retry

Parameters *seconds* — Specifies the length of time for retry timer, in seconds

Values 1 to 10 seconds

Platforms All

20.13 p2mp-sr

p2mp-sr

Syntax [**no**] **p2mp-sr**

Context [Tree] (config>service>vprn>mvpn>pt>inclusive p2mp-sr)
[Tree] (config>service>vprn>mvpn>pt>selective p2mp-sr)

Full Context configure service vprn mvpn provider-tunnel inclusive p2mp-sr
configure service vprn mvpn provider-tunnel selective p2mp-sr

Description This command enables P2MP SR for the MVPN provider tunnel.

The **no** form of this command disables P2MP SR.

Default no p2mp-sr

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.14 p2mp-sr-tree

p2mp-sr-tree

Syntax [**no**] **p2mp-sr-tree**

Context **[Tree]** (config>router p2mp-sr-tree)

Full Context configure router p2mp-sr-tree

Description Commands in this context configure P2MP SR parameters.

Default no p2mp-sr-tree

Platforms All

20.15 p2mp-template-lsp

p2mp-template-lsp

Syntax [**no**] **p2mp-template-lsp rsvp-session-name** *SessionNameString* **sender** *sender-address*

Context **[Tree]** (config>router>mpls>ingress-stats p2mp-template-lsp)

Full Context configure router mpls ingress-statistics p2mp-template-lsp

Description This command configures an ingress statistics context matching on the RSVP session name for a RSVP P2MP LSP at the egress LER.

This command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

When the ingress LER signals the path of the S2L sub-LSP, it includes the name of the LSP and that of the path in the Session Name field of the Session Attribute object in the Path message. The encoding is as follows:

Session Name: <lsp-name::path-name>, where lsp-name component is encoded as follows:

- P2MP LSP through the user configuration for L3 multicast in global routing instance: “LspNameFromConfig”
- P2MP LSP as I-PMSI or S-PMSI in L3 mVPN: templateName-SvcId-mTTmIndex
- P2MP LSP as I-PMSI in VPLS/B-VPLS: templateName-SvcId-mTTmIndex

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The ingress statistics CLI configuration allows the user to match either on the exact name of the P2MP LSP as configured at the ingress LER or on a context that matches on the template name and the service-id as configured at the ingress LER.

When the matching is performed on a context, the user must enter the RSVP session name string in the format “templateName-svcId” to include the LSP template name as well as the mVPN VPLS/B-VPLS service ID as configured at the ingress LER. In this case, one or more P2MP LSP instances signaled by the same ingress LER could be associated with the ingress statistics configuration and the user is provided with CLI parameter max-stats to limit the maximum number of stat indices that can be assigned to this context. If the context matches more than this value, the additional request for stat indices from this context will be rejected. A background tasks monitors the ingress statistics templates which have one or more matching LSP instances with unassigned stat index and assigns one to them as they are freed.

Note the following rules when configuring an ingress statistics context based on template matching:

- max-stats, once allocated, can be increased but not decreased unless the entire ingress statistics context matching a template name is deleted.
- In order to delete ingress statistics context matching a template name, a shutdown is required.
- An accounting policy cannot be configured or de-configured until the ingress statistics context matching a template name is shut down.
- After deleting an accounting policy from an ingress statistics context matching a template name, the policy is not removed from the log until a “no shut” is performed on the ingress statistics context.

If there are no stat indices available at the time the session of the P2MP LSP matching a template context is signaled and the session state installed by the egress LER, no stats are allocated to the session.

Furthermore, the assignment of stat indices to the LSP names that match the context will also be not deterministic. The latter is due to the fact that a stat index is assigned and released following the dynamics of the LSP creation or deletion by the ingress LER. For example, a multicast stream crosses the rate threshold and is moved to a newly signaled S-PMSI dedicated to this stream. Later on, the same steam crosses the threshold downwards and is moved back to the shared I-PMSI and the P2MP LSP corresponding to the S-PMSI is deleted by the ingress LER.

The **no** form deletes the ingress statistics context matching on the RSVP session name.

Parameters **rsvp-session-name** *SessionNameString* — Specifies the name of the RSVP P2MP session in the format of “templateName-svcId”. This field can hold up to 64 characters.

sender *sender-address* — Specifies a string of 15 characters representing the IP address of the ingress LER for the LSP.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.16 p2p-active-path-fast-retry

p2p-active-path-fast-retry

Syntax **p2p-active-path-fast-retry** *seconds*
no p2p-active-path-fast-retry

Context **[Tree]** (config>router>mpls p2p-active-path-fast-retry)

Full Context configure router mpls p2p-active-path-fast-retry

Description This command configures a global parameter to allow the user to apply a shorter retry timer for the first try after an active LSP path went down due to a local failure or the receipt of a ResvTear. This timer is used only in the first try. Subsequent retries will continue to be governed by the existing LSP level retry-timer.

The **no** form of this command disables the timer.

Default no p2p-active-path-fast-retry

Parameters *seconds* — Specifies the length of time for retry timer, in seconds

Values 1 to 10 seconds

Platforms All

20.17 p2p-merge-point-abort-timer

p2p-merge-point-abort-timer

Syntax **p2p-merge-point-abort-timer** *seconds*
no p2p-merge-point-abort-timer

Context **[Tree]** (config>router>rsvp p2p-merge-point-abort-timer)

Full Context configure router rsvp p2p-merge-point-abort-timer

Description This command configures a timer to abort Merge-Point (MP) node procedures for a P2P LSP path. When a value higher than zero is configured for this timer, it will enter into effect anytime this node activates Merge-Point procedures for one or more P2P LSP paths. As soon an ingress interface goes operationally down, the Merge-Point node starts the abort timer. Upon expiry of the timer, MPLS will clean up all P2P LSP paths which ILM is on the failed interface and which have not already received a Path refresh over the bypass LSP.

The **no** form of this command disables the timer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no p2p-merge-point-abort-timer

Parameters *seconds* — Specifies the length of the abort timer in seconds

Values 1 to 65535

Platforms All

20.18 p2p-template-lsp

p2p-template-lsp

Syntax [**no**] **p2p-template-lsp rsvp-session-name** *SessionNameString* **sender** *sender-address*

Context **[Tree]** (config>router>mpls>ingress-stats p2p-template-lsp)

Full Context configure router mpls ingress-statistics p2p-template-lsp

Description This command configures an ingress statistics context matching on the RSVP session name for a RSVP P2P auto-LSP at the egress LER.

When the ingress LER signals the path of a template based **one-hop-p2p** or **mesh-p2p auto-lsp**, it includes the name of the LSP and that of the path in the Session Name field of the Session Attribute object in the Path message. The encoding is as follows:

Session Name: *lsp-name::path-name*, where *lsp-name* component is encoded as follows:

P2MP LSP through the user configuration for Layer 3 multicast in global routing instance: “LspNameFromConfig”

- P2MP LSP as I-PMSI or S-PMSI in L3 mVPN: templateName-SvcId-mTTmIndex
- P2MP LSP as I-PMSI in VPLS/B-VPLS: templateName-SvcId-mTTmIndex.

The ingress statistics CLI configuration allows the user to match either on the exact name of the P2P auto-LSP or on a context that matches on the template name and the destination of the LSP at the ingress LER.

When the matching is performed on a context, the user must enter the RSVP session name string in the format “templateName-svcId” to include the LSP template name as well as the mVPN VPLS/B-VPLS service ID as configured at the ingress LER. In this case, one or more P2MP LSP instances signaled by the same ingress LER could be associated with the ingress statistics configuration. In this case, the user is provided with CLI parameter max-stats to limit the maximum number of stat indices which can be assigned to this context. If the context matches more than this value, the additional request for stat indices from this context will be rejected.

Note the following rules when configuring an ingress statistics context based on template matching:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **max-stats**, once allocated, can be increased but not decreased unless the entire ingress statistics context matching a template name is deleted.
- In order to delete ingress statistics context matching a template name, a shutdown is required.
- An accounting policy cannot be configured or de-configured until the ingress statistics context matching a template name is shut down.
- After deleting an accounting policy from an ingress statistics context matching a template name, the policy is not removed from the log until a **no shut** is performed on the ingress statistics context.

If there are no stat indices available at the time the session of the P2P LSP matching a template context is signaled and the session state installed by the egress LER, no stats are allocated to the session.

Furthermore, the assignment of stat indices to the LSP names that match the context will also be not deterministic. The latter is due to the fact that a stat index is assigned and released following the dynamics of the LSP creation or deletion by the ingress LER. For example, a multicast stream crosses the rate threshold and is moved to a newly signaled S-PMSI dedicated to this stream. Later on, the same steam crosses the threshold downwards and is moved back to the shared I-PMSI and the P2MP LSP corresponding to the S-PMSI is deleted by the ingress LER.

The **no** form deletes the ingress statistics context matching on the RSVP session name.

Parameters **rsvp-session-name** *SessionNameString* — Specifies the name of the RSVP P2MP session in the format of “templateName-svcId”. This field can hold up to 64 characters.

sender *sender-address* — Specifies a string of 15 characters representing the IP address of the ingress LER for the LSP.

Platforms All

20.19 packet

packet

Syntax **packet detail-level** {**high** | **low**}
packet mode {**all** | **dropped**}
no packet

Context **[Tree]** (debug>gtp packet)

Full Context debug gtp packet

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging of GTP packets sent or received by the system's control plane.

The **no** form of this command disables debugging of GTP packets.

Parameters **detail-level** {**high** | **low**} — Specifies how much detail is to be displayed when debugging a GTP packet.

Values

high	Specifies to display and decode all data in the packet.
low	Specifies to display and decode only the most important data.

Default low

mode {**all** | **dropped**} — Specifies which packets is debugged.

Values

all	Specifies to debug all packets.
dropped	Specifies to debug only dropped packets.

Default dropped

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

packet

Syntax [**no**] **packet**

Context **[Tree]** (debug>router>l2tp packet)
[Tree] (debug>router>l2tp>assignment-id packet)
[Tree] (debug>router>l2tp>group packet)
[Tree] (debug>router>l2tp>peer packet)

Full Context debug router l2tp assignment-id packet
debug router l2tp group packet
debug router l2tp packet
debug router l2tp peer packet

Description This command enables packet debugging.

The **no** form of this command disables packet debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packet

Syntax [**no**] **packet**

Context **[Tree]** (debug>service>id>ppp packet)

Full Context debug service id ppp packet

Description This command enables debugging for specific PPPoE packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

packet

Syntax [**no**] **packet**

Context **[Tree]** (debug>router>wpp packet)
[Tree] (debug>router>wpp>portal packet)

Full Context debug router wpp packet
debug router wpp portal packet

Description This command enables WPP packet debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

packet

Syntax **packet jitter-buffer** *milliseconds* [**payload-size** *bytes*]
packet payload-size *bytes*
no packet

Context **[Tree]** (config>service>cpipe>sap>cem packet)
[Tree] (config>service>epipe>sap>cem packet)

Full Context configure service cpipe sap cem packet
configure service epipe sap cem packet

Description This command specifies the jitter buffer size, in milliseconds, and payload size, in bytes.

Default The default value depends on the CEM SAP endpoint type, and if applicable, the number of timeslots as shown in Table 107.

Table 107 **Packet CEM SAP Endpoint Types**

Endpoint Type	Timeslots	Default Jitter Buffer (in ms)
unstructuredE1	—	5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 107 **Packet CEM SAP Endpoint Types**

Endpoint Type	Timeslots	Default Jitter Buffer (in ms)
unstructuredT1	—	5
nxDS0 (E1/T1)	—	32
	N = 1	16
	N = 2 to 4	8
	N = 5 to 15	5
nxDS0WithCas (E1)	N	8
nxDS0WithCas (T1)	N	12

Parameters *milliseconds* — Specifies the jitter buffer size in milliseconds (ms).

Configuring the payload size and jitter buffer to values that result in less than 2 packet buffers or greater than 32 packet buffers is not allowed. Setting the jitter butter value to 0 sets it back to the default value.

Values 1 to 250

payload-size *bytes* — Specifies the payload size (in bytes) of packets transmitted to the packet service network (PSN) by the CEM SAP. This determines the size of the data that will be transmitted over the service. If the size of the data received is not consistent with the payload size then the packet is considered malformed.

Values 0 | 16 to 2048

Default The default value depends on the CEM SAP endpoint type, and if applicable, the number of timeslots as shown in Table 108.

Table 108 **CEM SAP Endpoint Types**

Endpoint Type	Timeslots	Default Payload Size (in bytes)
unstructuredE1	—	256
unstructuredT1	—	192
nxDS0 (E1/T1)	N = 1	64
	N = 2 to 4	N x 32
	N = 5 to 15	N x 16
	N >= 16	N x 8
nxDS0WithCas (E1)	N	N x 16
nxDS0WithCas (T1)	N	N x 24

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For all endpoint types except for nxDS0WithCas, the valid payload size range is from the default to 2048 bytes.

For nxDS0WithCas, the payload size divide by the number of timeslots must be an integer factor of the number of frames per trunk multi-frame (for example, 16 for E1 trunk and 24 for T1 trunk).

For 1xDS0, the payload size must be a multiple of 2.

For NxDS0, where N > 1, the payload size must be a multiple of the number of timeslots.

For unstructuredE1 and unstructuredT1, the payload size must be a multiple of 32 bytes.

Configuring the payload size and jitter buffer to values that result in less than 2 packet buffers or greater than 32 packet buffer is not allowed.

Setting the payload size to 0 sets it back to the default value.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap cem packet

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service epipe sap cem packet

packet

Syntax **packet** [**hello** | **jp**]
packet [**hello** | **jp**] **evpn-mpls**
packet [**hello** | **jp**] [**sap** *sap-id*]
packet [**hello** | **jp**] [**sdp** *sdp-id:vc-id*]
packet [**hello** | **jp**] **vxlan vtep** *ip-address* **vni** *vni-id*
no packet

Context **[Tree]** (debug>service>id>pim-snooping packet)

Full Context debug service id pim-snooping packet

Description This command enables or disables debugging for PIM packets.

Parameters **hello | jp** — PIM packet types

sap-id — Debugs packets associated with the specified SAP

sdp-id:vc-id — Debugs packets associated with the specified SDP

evpn-mpls — Debugs PIM snooping statistics for EVPN-MPLS destinations

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packet

Syntax **packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]
packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}] **group-interface** *ip-int-name*
packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address* [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]
no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*]
no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **group-interface** *ip-int-name*
no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address*

Context **[Tree]** (debug>router>igmp packet)

Full Context debug router igmp packet

Description This command enables/disables debugging for IGMP packets.

Parameters **query** — Specifies to log the IGMP group- and source-specific queries transmitted and received on this interface.

v1-report — Specifies to debug IGMP V1 reports transmitted and received on this interface.

v2-report — Specifies to debug IGMP V2 reports transmitted and received on this interface.

v3-report — Specifies to debug IGMP V3 reports transmitted and received on this interface.

v2-leave — Specifies to debug the IGMP Leaves transmitted and received on this interface.

ip-int-name — Debugs the information associated with the specified IP interface name.

Values IP interface address

ip-address — Debugs the information associated with the specified IP address.

Platforms All

packet

Syntax **packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]
packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}] **group-interface** *ip-int-name*
packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address* [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]
no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*]
no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **group-interface** *ip-int-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address*

Context **[Tree]** (debug>router>igmp packet)

Full Context debug router igmp packet

Description This command enables/disables debugging for IGMP packets.

Parameters **query** — Specifies to log the IGMP group- and source-specific queries transmitted and received on this interface.

v1-report — Specifies to debug IGMP V1 reports transmitted and received on this interface.

v2-report — Specifies to debug IGMP V2 reports transmitted and received on this interface.

v3-report — Specifies to debug IGMP V3 reports transmitted and received on this interface.

v2-leave — Specifies to debug the IGMP Leaves transmitted and received on this interface.

ip-int-name — Debugs the information associated with the specified IP interface name.

Values IP interface address

ip-address — Debugs the information associated with the specified IP address.

Platforms All

packet

Syntax [**no**] **packet**

Context **[Tree]** (debug>router>gmpls packet)

Full Context debug router gmpls packet

Description This command enables and disables debugging for specific GMPLS packets.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

packet

Syntax **packet** [**detail**]
no packet

Context **[Tree]** (debug>router>ldp>if packet)
[Tree] (debug>router>ldp>peer packet)

Full Context debug router ldp interface packet
debug router ldp peer packet

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for specific LDP packets.

The **no** form of the command disables the debugging output.

Parameters **detail** — Displays detailed information.

Platforms All

packet

Syntax [**no**] **packet**

Context **[Tree]** (debug>router>rsvp packet)

Full Context debug router rsvp packet

Description Commands in this context debug packets.

Platforms All

packet

Syntax **packet** [*pkt-type*] [**peer** *ip-address*]

Context **[Tree]** (debug>router>msdp packet)

Full Context debug router msdp packet

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) packets.

The **no** form of the command disables MSDP packet debugging.

Parameters *pkt-type* — Debugs information associated with the specified packet type.

Values keep-alive, source-active, sa-request, sa-response

ip-address — Debugs information associated with the specified peer IP address.

Platforms All

packet

Syntax **packet** [**hello** | **register** | **register-stop** | **jp** | **bsr** | **assert** | **crp** | **mdt-tlv** | **auto-rp-announcement** | **auto-rp-mapping** | **graft** | **graft-ack**] [*ip-int-name* | *mt-int-name* | *int-ip-address* | *mpls-if-name*] [**family** {**ipv4** | **ipv6**}] [**send** | **receive**]
no packet

Context **[Tree]** (debug>router>pim packet)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router pim packet

Description This command enables debugging for PIM packets.

The **no** form of this command disables debugging for PIM packets.

Parameters **hello** | **register** | **register-stop** | **jp** | **bsr** | **assert** | **crp | mdt-tlv | auto-rp-announcement | auto-rp-mapping | graft | graft-ack** — Specifies PIM packet types.

ip-int-name — Debugs the information associated with the specified IP interface name, up to 32 characters.

mt-int-name — Debugs the information associated with the specified VPRN ID and group address.

Values *vprn-id*-mt-*grp-ip-address*

int-ip-address — Debugs the information associated with the specified IP address.

ipv4 — Specifies to display IPv4 packets.

ipv6 — Specifies to display IPv6 packets.

mpls-if-name — Debugs the information associated with the specified MPLS interface.

Values mpls-if-*index*

receive — Specifies to display received packets.

send — Specifies to display sent packets.

family — Debugs database packet information.

Values ipv4, ipv6

Platforms All

packet

Syntax **packet jitter-buffer** *milliseconds* [**payload-size** *bytes*]
packet payload-size *bytes*
no packet

Context **[Tree]** (config>mirror>mirror-dest>sap>cem packet)

Full Context configure mirror mirror-dest sap cem packet

Description This command specifies the jitter buffer size, in milliseconds, and payload size, in bytes.

Default The default value depends on the CEM SAP endpoint type, and if applicable, the number of timeslots:

Endpoint Type	Timeslots	Default Jitter Buffer (in ms)
unstructuredE1	n/a	5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Endpoint Type	Timeslots	Default Jitter Buffer (in ms)
unstructuredT1	n/a	5
unstructuredE3	n/a	5
unstructuredT3	n/a	5
nxDS0 (E1/T1)	N = 1	32
	N = 2 to 4	16
	N = 5 to 15	8
	N >= 16	5
nxDS0WithCas (E1)	N	8
nxDS0WithCas (T1)	N	12

Parameters *milliseconds* — Specifies the jitter buffer size in milliseconds (ms).

Configuring the payload size and jitter buffer to values that result in less than 2 packet buffers or greater than 32 packet buffers is not allowed.

Setting the jitter butter value to 0 sets it back to the default value.

Values 1 — 250

bytes — Specifies the payload size (in bytes) of packets transmitted to the packet service network (PSN) by the CEM SAP. This determines the size of the data that will be transmitted over the service. If the size of the data received is not consistent with the payload size then the packet is considered malformed.

Default The default value depends on the CEM SAP endpoint type, and if applicable, the number of timeslots:

Endpoint Type	Timeslots	Default Payload Size (in bytes)
unstructuredE1	n/a	256
unstructuredT1	n/a	192
unstructuredE3	n/a	1024
unstructuredT3	n/a	1024
nxDS0 (E1/T1)	N = 1	64
	N = 2 to 4	N x 32
	N = 5 to 15	N x 16
	N >= 16	N x 8
nxDS0WithCas (E1)	N	N x 16
nxDS0WithCas (T1)	N	N x 24

For all endpoint types except for nxDS0WithCas, the valid payload size range is from the default to 2048 bytes.

For nxDS0WithCas, the payload size divide by the number of timeslots must be an integer factor of the number of frames per trunk multiframe (for example, 16 for E1 trunk and 24 for T1 trunk).

For 1xDS0, the payload size must be a multiple of 2.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For NxDS0, where N > 1, the payload size must be a multiple of the number of timeslots.

For unstructuredE1, unstructuredT1, unstructuredE3 and unstructuredT3, the payload size must be a multiple of 32 bytes.

Configuring the payload size and jitter buffer to values that result in less than 2 packet buffers or greater than 32 packet buffer is not allowed.

Setting the payload size to 0 sets it back to the default value.

Values 16 to 2048

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

packet

Syntax **packet** *packet-number* [**create**]
no packet *packet-number*

Context **[Tree]** (debug>oam>build-packet packet)

Full Context debug oam build-packet packet

Description This command configures a packet to be launched by the OAM **find-egress** tool.

The **no** form of this command removes the packet number value.

Parameters *packet-number* — Specifies a packet to be launched by the OAM **find-egress** tool.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

packet

Syntax **packet all**
packet cfm-opcode *opcode* [*opcode*]
no packet

Context **[Tree]** (debug>eth-cfm>mep packet)
[Tree] (debug>eth-cfm>mip packet)

Full Context debug eth-cfm mep packet
debug eth-cfm mip packet

Description This command defines the ETH-CFM opcodes of interest to be debugged.

The **no** form of this command stops packet debugging and the collection of PDUs.

Parameters **all** — Specifies that debugging is enabled for all ETH-CFM packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

opcode — Specifies a standard numerical reference or common three-letter acronym (TLA) that identifies the CFM PDU type. Up to five opcodes can be specified, and a combination of both numbers and TLAs can be used.

MEPs support all opcodes.

MIPs support 2 (LBR), 3 (LBM), 4 (LTR), and 5 (LTM).

Unknown or unsupported opcodes in TLA form are rejected. The applicable numerical opcode can be used instead. When numerical references are used, they are converted to a known TLA or left in numerical form if the TLA is unknown.

Re-entering the **packet** command overwrites the previous opcode entries for the MEP or MIP.

Values MEP: 1 to 255 | common TLA
MIP: 2 to 5 | common TLA

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

packet

Syntax **packet** [{*ip-int-name* | *ip-address*}] [**headers**] [*protocol-id*]
no packet [{*ip-int-name* | *ip-address*}]

Context **[Tree]** (debug>router>ip packet)

Full Context debug router ip packet

Description This command enables debugging for IP packets.

Parameters *ip-int-name* — Only displays the interface information associated with the specified IP interface name.

Values 32 characters maximum

ip-address — Only displays the interface information associated with the specified IP address.

headers — Only displays information associated with the packet header.

protocol-id — Specifies the decimal value representing the IP protocol to debug. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form the command removes the protocol from the criteria.

Values 0 to 255 (values can be expressed in decimal, hexadecimal, or binary)

Platforms All

packet

Syntax [**no**] **packet**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>router>pcp>pcp-server packet)

Full Context debug router pcp pcp-server packet

Description This command enables packet debugging.

The **no** form of this command disables packet debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

packet

Syntax [**no**] **packet** [{**query** | **request** | **response**}]

Context [Tree] (debug>router>mtrace packet)

Full Context debug router mtrace packet

Description This command enables debugging for mtrace packets.

Platforms All

packet

Syntax [**no**] **packet** [{**query** | **request** | **reply**}]

Context [Tree] (debug>router>mtrace2 packet)

Full Context debug router mtrace2 packet

Description This command enables debugging for mtrace2 packets.

Platforms All

packet

Syntax [**no**] **packet**

Context [Tree] (debug>router>rpki-session packet)

Full Context debug router rpki-session packet

Description This command enables debugging for specific RPKI packets.

The **no** form of this command disables debugging for specific RPKI packets.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packet

Syntax **packet** [*packet-type*] [*ip-int-name* | *ip-address*] [**detail**]

Context **[Tree]** (debug>router>isis packet)

Full Context debug router isis packet

Description This command enables debugging for IS-IS packets.

The **no** form of the command disables debugging.

Parameters *ip-address* — When specified, only packets with the specified interface address are debugged.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

ip-int-name — When specified, only packets with the specified interface name are debugged.

packet-type — When specified, only packets of the specified type are debugged.

Values ptop-hello | l1-hello | l2-hello | l1-psnp | l2-psnp | l1-csnp | l2-csnp | l1-lsp | l2-lsp

detail — All output is displayed in the detailed format.

Platforms All

packet

Syntax **packet** [*packet-type*] [*interface-name*] [**ingress** | **egress**] [**detail**]
packet [*packet-type*] [*interface-name*] [**ingress** | **egress** | **drop**] [**detail**]
no packet

Context **[Tree]** (debug>router>ospf packet)
[Tree] (debug>router>ospf3 packet)

Full Context debug router ospf packet
debug router ospf3 packet

Description This command enables debugging for OSPF packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *packet-type* — Specifies the OSPF packet type to debug.

Values hello, dbdescr, lsrequest, lsupdate, lsack

interface-name — Specifies the interface to debug, up to 32 characters.

ingress — Specifies to display ingress packets.

egress — Specifies to display egress packets.

drop — Specifies to display dropped packets.

Platforms All

packet

Syntax **packet** [**high-detail**] [**dropped-only**]
no packet

Context **[Tree]** (debug>subscr-mgmt>pfcp packet)

Full Context debug subscriber-mgmt pfcp packet

Description This command debugs PFCP packets that are received or sent. The **no** form of this command disables any PFCP packet debugging.

Parameters **high-detail** — Specifies to provide a full packet dump; without this parameter only basic packet information is provided.

dropped-only — Specifies to only debug dropped packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.20 packet-byte-offset

packet-byte-offset

Syntax **packet-byte-offset** {**add** *bytes* | **subtract** *bytes*}
no packet-byte-offset

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>policer packet-byte-offset)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>policer packet-byte-offset)

Full Context configure subscriber-mgmt sla-profile egress qos policer packet-byte-offset
configure subscriber-mgmt sla-profile ingress qos policer packet-byte-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to modify the size of each packet handled by the policer by adding or subtracting a number of bytes. The actual packet size is not modified; only the size used to determine the bucket depth impact is changed. The **packet-byte-offset** command is meant to be an arbitrary mechanism the can be used to either add downstream frame encapsulation or remove portions of packet headers. Both the policing metering and profiling throughput is affected by the offset as well as the stats associated with the policer.

When child policers are adding to or subtracting from the size of each packet, the parent policer's **min-thresh-separation** value should also need to be modified by the same amount.

The policer's **packet-byte-offset** defined in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. Packet byte offset settings are not included in the applied rate when (queue) frame based accounting is configured and the policer is managed by HQoS, however the offsets are applied to the statistics.

The **no** form of this command removes the per packet size modifications from the policer.

Parameters **add** *bytes* — Specifies the packet byte offset. The **add** keyword is mutually exclusive to the **subtract** keyword. Either **add** or **subtract** must be specified. When **add** is defined the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 0 to 31

subtract *bytes* — Specifies the packet byte offset. The **subtract** keyword is mutually exclusive to the **add** keyword. Either **add** or **subtract** must be specified. When b is defined the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.

Note: The minimum resulting packet size used by the system is 1 byte.

Values ingress 1 to 32
egress: 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context **[Tree]** (config>card>fp>ingress>access>qgrp>policer-over>plcr packet-byte-offset)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>card>fp>ingress>network>qgrp>policer-over>plcr packet-byte-offset)

Full Context configure card fp ingress access queue-group policer-override policer packet-byte-offset
configure card fp ingress network queue-group policer-override policer packet-byte-offset

Description This command modifies the size of each packet handled by the policer by adding or subtracting a number of bytes. The actual packet size is not modified; only the size used to determine the bucket depth impact is changed. The **packet-byte-offset** command is meant to be an arbitrary mechanism the can be used to either add downstream frame encapsulation or remove portions of packet headers. Both the policing metering and profiling throughput is affected by the offset as well as the stats associated with the policer.

When child policers are adding to or subtracting from the size of each packet, the parent policer's **min-thresh-separation** value should also need to be modified by the same amount.

The policer's **packet-byte-offset** defined in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command removes per packet size modifications from the policer.

Parameters *add-bytes* — The **add** keyword is mutually exclusive to the **subtract** keyword. Either **add** or **subtract** must be specified. When **add** is defined the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 1 to 31

sub-bytes — The **subtract** keyword is mutually exclusive to the **add** keyword. Either **add** or **subtract** must be specified. When b is defined the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet. Note that the minimum resulting packet size used by the system is 1 byte.

Values 0 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context [Tree] (config>service>apipe>sap>egress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>apipe>sap>ingress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>cpipe>sap>egress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>cpipe>sap>ingress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>epipe>sap>egress>policer-over>plcr packet-byte-offset)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>epipe>sap>ingress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>fpipe>sap>egress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>fpipe>sap>ingress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>ipipe>sap>egress>policer-over>plcr packet-byte-offset)
[Tree] (config>service>ipipe>sap>ingress>policer-over>plcr packet-byte-offset)

Full Context

configure service apipe sap egress policer-override policer packet-byte-offset
configure service apipe sap ingress policer-override policer packet-byte-offset
configure service cpipe sap egress policer-override policer packet-byte-offset
configure service cpipe sap ingress policer-override policer packet-byte-offset
configure service epipe sap egress policer-override policer packet-byte-offset
configure service epipe sap ingress policer-override policer packet-byte-offset
configure service fpipe sap egress policer-override policer packet-byte-offset
configure service fpipe sap ingress policer-override policer packet-byte-offset
configure service ipipe sap egress policer-override policer packet-byte-offset
configure service ipipe sap ingress policer-override policer packet-byte-offset

Description

This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured packet-byte-offset parameter for the specified policer-id. Packet byte offset settings are not included in the applied rate when (queue) frame based accounting is configured; however, the offsets are applied to the statistics.

The **no** packet-byte-offset command is used to restore the policer's packet-byte-offset setting to the policy defined value.

Default

no packet-byte-offset

Parameters

add-bytes — Specifies the number of bytes that are added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 1 to 31

sub-bytes — Specifies the number of bytes that are subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.

Values 1 to 64

Platforms

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress policer-override policer packet-byte-offset
- configure service fpipe sap egress policer-override policer packet-byte-offset
- configure service fpipe sap ingress policer-override policer packet-byte-offset
- configure service cpipe sap ingress policer-override policer packet-byte-offset

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service epipe sap ingress policer-override policer packet-byte-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ipipe sap egress policer-override policer packet-byte-offset
- configure service ipipe sap ingress policer-override policer packet-byte-offset
- configure service epipe sap egress policer-override policer packet-byte-offset

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap egress policer-override policer packet-byte-offset
- configure service apipe sap ingress policer-override policer packet-byte-offset

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context **[Tree]** (config>service>vpls>sap>egress>policer-override>plcr packet-byte-offset)
[Tree] (config>service>vpls>sap>ingress>policer-override>plcr packet-byte-offset)

Full Context configure service vpls sap egress policer-override policer packet-byte-offset
configure service vpls sap ingress policer-override policer packet-byte-offset

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured packet-byte-offset parameter for the specified policer-id. Packet byte offset settings are not included in the applied rate when (queue) frame based accounting is configured, however the offsets are applied to the statistics.

The **no** form of this command restores the policer's packet-byte-offset setting to the policy defined value.

Default no packet-byte-offset

Parameters *add-bytes* — The add keyword is mutually exclusive to the subtract keyword. Either add or subtract must be specified. When add is defined the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 0 to 31

sub-bytes — The subtract keyword is mutually exclusive to the add keyword. Either add or subtract must be specified. When subtract is defined the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context [Tree] (config>service>ies>if>sap>egress>policer-override>plcr packet-byte-offset)
[Tree] (config>service>ies>if>sap>ingress>policer-override>plcr packet-byte-offset)

Full Context configure service ies interface sap egress policer-override policer packet-byte-offset
configure service ies interface sap ingress policer-override policer packet-byte-offset

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured packet-byte-offset parameter for the specified policer-id. Packet byte offset settings are not included in the applied rate when (queue) frame based accounting is configured, however the offsets are applied to the statistics.

The **no** form of this command restores the policer's packet-byte-offset setting to the policy defined value.

Default no packet-byte-offset

Parameters **add** *add-bytes* — The **add** keyword is mutually exclusive to the **subtract** keyword. Either **add** or **subtract** must be specified. When **add** is defined, the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 0 to 31

subtract *sub-bytes* — The **subtract** keyword is mutually exclusive to the **add** keyword. Either **add** or **subtract** must be specified. When **subtract** is defined, the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

packet-byte-offset

Syntax **packet-byte-offset add** *add-bytes*
packet-byte-offset subtract *sub-bytes*
no packet-byte-offset

Context [Tree] (config>service>vprn>if>sap>egress>policer-override>plcr packet-byte-offset)
[Tree] (config>service>vprn>if>sap>ingress>policer-override>plcr packet-byte-offset)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap egress policer-override policer packet-byte-offset
configure service vprn interface sap ingress policer-override policer packet-byte-offset

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured packet-byte-offset parameter for the specified policer-id. Packet byte offset settings are not included in the applied rate when (queue) frame based accounting is configured, however the offsets are applied to the statistics.

The **no** form of this command restores the policer's packet-byte-offset setting to the policy defined value.

Default no packet-byte-offset

Parameters **add** *add-bytes* — The **add** keyword is mutually exclusive to the **subtract** keyword. Either **add** or **subtract** must be specified. When **add** is defined, the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 0 to 31

subtract *sub-bytes* — The **subtract** keyword is mutually exclusive to the **add** keyword. Either **add** or **subtract** must be specified. When **subtract** is defined, the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub- bytes*}
no packet-byte-offset

Context **[Tree]** (config>qos>sap-ingress>dyn-policer packet-byte-offset)
[Tree] (config>qos>sap-egress>dyn-policer packet-byte-offset)
[Tree] (config>qos>sap-ingress>policer packet-byte-offset)
[Tree] (config>qos>sap-egress>policer packet-byte-offset)

Full Context configure qos sap-egress dynamic-policer packet-byte-offset
configure qos sap-egress policer packet-byte-offset
configure qos sap-ingress dynamic-policer packet-byte-offset
configure qos sap-ingress policer packet-byte-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to modify the size of each packet handled by the policer by adding or subtracting a number of bytes. The actual packet size is not modified; only the size used to determine the bucket depth impact is changed. The **packet-byte-offset** command is meant to be an arbitrary mechanism that can be used to either add downstream frame encapsulation or remove portions of packet headers. Both the policing metering and profiling throughput is affected by the offset as well as the stats associated with the policer.

When child policers are adding to or subtracting from the size of each packet, the parent policer's **min-thresh-separation** value should also need to be modified by the same amount.

The policer's **packet-byte-offset** defined in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. Packet byte offset settings are not included in the applied rate when (queue) frame-based accounting is configured and the policer is managed by HQoS; however, the offsets are applied to the statistics.

The **no** form of this command is used to remove per packet size modifications from the policer.

Parameters **add** *add-bytes* — The **add** keyword is mutually exclusive to the **subtract** keyword. Either **add** or **subtract** must be specified. When **add** is defined, the corresponding bytes parameter specifies the number of bytes that is added to the size of each packet associated with the policer for rate metering, profiling, and accounting purposes. From the policer's perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 0 to 31

subtract *sub-bytes* — The **subtract** keyword is mutually exclusive to the **add** keyword. Either **add** or **subtract** must be specified. When **subtract** is defined, the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling, and accounting purposes. From the policer's perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet. The minimum resulting packet size used by the system is 1 byte.

Values 1 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure qos sap-ingress dynamic-policer packet-byte-offset
- configure qos sap-egress dynamic-policer packet-byte-offset

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-ingress policer packet-byte-offset
- configure qos sap-egress policer packet-byte-offset

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no packet-byte-offset

Context **[Tree]** (config>qos>sap-ingress>queue packet-byte-offset)

Full Context configure qos sap-ingress queue packet-byte-offset

Description This command modifies the size of each packet handled by the queue by adding or subtracting the specified number of bytes. The actual packet size is not modified, only the size used to determine the ingress scheduling and profiling is changed. The **packet-byte-offset** command is an arbitrary mechanism that can be used to either add downstream frame encapsulation or remove portions of packet headers. Both the scheduling and profiling throughput is affected by the offset as well as the statistics (accounting) associated with the queue. The **packet-byte-offset** does not apply to drop statistics, received valid statistics, or the offered managed and unmanaged statistics used by Ingress Multicast Path Management.

The **no** form of this command removes per-packet size modifications from the queue.

Parameters *add-bytes* — Specifies the number of bytes added to the size of each packet associated with the queue for scheduling, profiling, and accounting purposes. From the queue's perspective, the packet size is increased by the amount specified.

Values 0 to 30, in increments of 2

sub-bytes — Specifies the number of bytes subtracted from the size of each packet associated with the queue for scheduling, profiling, and accounting purposes. From the queue's perspective, the packet size is reduced by the amount specified. The minimum resulting packet size used by the system is 1 byte.

Values 0 to 64, in increments of 2

Platforms All

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context **[Tree]** (config>qos>sap-egress>queue packet-byte-offset)

Full Context configure qos sap-egress queue packet-byte-offset

Description This command is used to modify the size of each packet handled by the queue by adding or subtracting a number of bytes. The actual packet size is not modified; only the size used to determine the bucket depth impact is changed.

The packet-byte-offset command is meant to be an arbitrary mechanism the can be used to either add downstream frame encapsulation or remove portions of packet headers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a packet-byte-offset value is applied to a queue instance, it adjusts the immediate packet size. This means that the queue rates, i.e., operational PIR and CIR, and queue bucket updates use the adjusted packet size. In addition, the queue statistics will also reflect the adjusted packet size. Scheduler policy rates, which are data rates, will use the adjusted packet size.

The port scheduler max-rate and the priority level rates and weights, if a Weighted Scheduler Group is used, are always on-the-wire rates and thus use the actual frame size. The same applies for the agg-rate-limit on a SAP, a subscriber, or a multiservice Site (MSS) when the queue is port-parented.

When the user enables frame-based-accounting in a scheduler policy or queue-frame-based-accounting with agg-rate-limit in a port scheduler policy, the queue rate will be capped to a user-configured on-the-wire rate and the packet-byte-offset is not included. However, the offsets are applied to the statistics.

The **no** form of this command is used to remove per packet size modifications from the queue.

Parameters *add-bytes* — The **add** keyword is mutually exclusive to the **subtract** keyword. Either parameter must be specified. When **add** is defined, the corresponding bytes parameter specifies the number of bytes that is added to the size of each packet associated with the queue for scheduling and accounting purposes.

Values 0 to 32

sub-bytes — The **subtract** keyword is mutually exclusive to the **add** keyword. Either parameter must be specified. When subtract is defined, the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the queue for scheduling and accounting purposes. The minimum resulting packet size used by the system is 1 byte.

Values 0 to 64

Platforms All

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context **[Tree]** (config>qos>qgrps>ing>qgrp>policer packet-byte-offset)

Full Context configure qos queue-group-templates ingress queue-group policer packet-byte-offset

Description This command configures a packet byte offset for the QoS ingress queue-group policer.

Default no packet-byte-offset

Parameters *add-bytes* — Specifies the number of bytes to add as the offset amount.

Values 0 to 31

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-bytes — Specifies the number of bytes to add as the offset amount.

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

packet-byte-offset

Syntax **packet-byte-offset** {**add** *add-bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context **[Tree]** (config>qos>qgrps>ing>qgrp>queue packet-byte-offset)

Full Context configure qos queue-group-templates ingress queue-group queue packet-byte-offset

Description This command is used to modify the size of each packet handled by the queue by adding or subtracting a number of bytes. The actual packet size is not modified; only the size used to determine the ingress scheduling and profiling is changed. The packet-byte-offset command is meant to be an arbitrary mechanism that can be used to either add downstream frame encapsulation or remove portions of packet headers. Both the scheduling and profiling throughput is affected by the offset as well as the stats (accounting) associated with the queue. The packet-byte-offset does not apply to drop statistics, received valid statistics, or the offered managed and unmanaged statistics used by Ingress Multicast Path Management.

The **no** form of this command is used to remove per packet size modifications from the queue.

Parameters *add-bytes* — The add keyword is mutually exclusive to the subtract keyword. Either add or subtract must be specified. When add is defined, the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the queue for scheduling, profiling and accounting purposes. From the queue's perspective, the packet size is increased by the amount being added to the size of each packet.

Values 0 to 30, in steps of 2

sub-bytes — The subtract keyword is mutually exclusive to the add keyword. Either add or subtract must be specified. When subtract is defined, the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the queue for scheduling, profiling and accounting purposes. From the queue's perspective, the packet size is reduced by the amount being subtracted from the size of each packet. The minimum resulting packet size used by the system is 1 byte.

Values 0 to 64, in steps of 2

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packet-byte-offset

Syntax **packet-byte-offset** {**add add-***bytes* | **subtract** *sub-bytes*}
no packet-byte-offset

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer packet-byte-offset)
[Tree] (config>qos>qgrps>egr>qgrp>queue packet-byte-offset)

Full Context configure qos queue-group-templates egress queue-group policer packet-byte-offset
configure qos queue-group-templates egress queue-group queue packet-byte-offset

Description This command is used to modify the size of each packet handled by the queue by adding or subtracting a number of bytes. The actual packet size is not modified; only the size used to determine the bucket depth impact is changed.

The packet-byte-offset command is meant to be an arbitrary mechanism that can be used to either add downstream frame encapsulation or remove portions of packet headers.

When a packet-byte-offset value is applied to a queue or policer instance, it adjusts the immediate packet size. This means that the queue rates (i.e., operational PIR and CIR) and policer or queue bucket updates use the adjusted packet size. In addition, the statistics will also reflect the adjusted packet size. Scheduler policy rates, which are data rates, will use the adjusted packet size.

The port scheduler **max-rate** and the priority level rates and weights, if a Weighted Scheduler Group is used, are always on-the-wire rates and thus use the actual frame size. The same applies for the agg-rate-limit on a SAP, a subscriber, or a Multiservice Site (MSS) when the queue is port-parented.

When the user enables **frame-based-accounting** in a scheduler policy or **queue-frame-based-accounting** with agg-rate-limit in a port scheduler policy, the policer or queue rate will be capped to a user-configured on-the-wire rate and the packet-byte-offset is not included; however, the offsets are applied to the statistics.

The **no** form of this command is used to remove per packet size modifications from the queue.

Parameters *add-bytes* — Specifies that the corresponding bytes parameter specifies the number of bytes that is added to the size of each packet associated with the queue for scheduling and accounting purposes.

Values 0 to 32

sub-bytes — Specifies that the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the queue for scheduling and accounting purposes. The minimum resulting packet size used by the system is 1 byte.

Values 0 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos queue-group-templates egress queue-group policer packet-byte-offset

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure qos queue-group-templates egress queue-group queue packet-byte-offset

20.21 packet-length

packet-length

Syntax **packet-length** {**lt** | **gt** | **eq**} *packet-length-value*
packet-length range *packet-length-value packet-length-value*
no packet-length

Context **[Tree]** (config>filter>ip-filter>entry>match packet-length)

Full Context configure filter ip-filter entry match packet-length

Description This command configures the IPv4 packet length value match criterion. The IPv4 packet length represents the total packet length including the IPv4 header and the payload.

Default no packet-length

Parameters **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

packet-length-value — Specifies the packet length value.

Values 0 to 65535

range — Specifies an inclusive range. When range is used, the beginning of the range must have a value less than the second value of the range.

Platforms All

packet-length

Syntax **packet-length** {**lt** | **gt** | **eq**} *packet-length-value*
packet-length range *packet-length-value packet-length-value*
no packet-length

Context **[Tree]** (config>filter>ipv6-filter>entry>match packet-length)

Full Context configure filter ipv6-filter entry match packet-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the IPv6 packet length value match criterion. The IPv6 packet length represents the total packet length including the IPv6 header and the payload.

Default no packet-length

Parameters **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

packet-length-value — Specifies the packet length value.

Values 40 to 65575

range — Specifies an inclusive range. When range is used, the beginning of the range must have a value less than the second value of the range.

Platforms All

20.22 packet-rate-high-wmark

packet-rate-high-wmark

Syntax **packet-rate-high-wmark** *high-watermark*

Context **[Tree]** (config>app-assure packet-rate-high-wmark)

Full Context configure application-assurance packet-rate-high-wmark

Description This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent.

Default packet-rate-high-wmark max

Parameters *high-watermark* — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the **packet-rate-low-wmark** *low-watermark* value.

Values 1 to 14880952 packets/sec, **max** (disabled)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.23 packet-rate-low-wmark

packet-rate-low-wmark

Syntax **packet-rate-low-wmark** *low-watermark*
no packet-rate-low-wmark

Context **[Tree]** (config>app-assure packet-rate-low-wmark)

Full Context configure application-assurance packet-rate-low-wmark

Description This command configures the packet rate on the ISA-AA when a packet rate alarm will be cleared by the agent.

The **no** form of this command reverts to the default.

Default packet-rate-low-wmark 0

Parameters *low-watermark* — Specifies the low watermark for packet rate alarms. The value must be lower than or equal to the **packet-rate-high-wmark** *high-watermark* value.

Values 0 to 14880952 packets per second

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.24 packet-rx

packet-rx

Syntax **packet-rx** [**client** *client-ip* [**source-port** *src-port*]] [**fcc-join**] [**fcc-leave**] [**ret-nack**]
no packet-rx

Context **[Tree]** (debug>service>id>video-interface packet-rx)

Full Context debug service id video-interface packet-rx

Description This command enables debugging of received RTCP messages. The options for this command allow the user to filter only certain types of messages to appear in the debug traces.

Parameters **client** *client-ip* — Specifies the client IP address.

source-port *src-port* — Specifies the source port.

fcc-join — Enables debugging for FCC joins.

fcc-leave — Enables debugging for FCC leaves.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ret-nack — Enables debugging for retransmission nack packets.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.25 packet-sanity

packet-sanity

Syntax **packet-sanity direction** *direction* [**create**]
no packet-sanity direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>sctp-filter packet-sanity)

Full Context configure application-assurance group statistics threshold-crossing-alert sctp-filter packet-sanity

Description This command configures a TCA for the counter capturing packet sanity hits for the specified SCTP filter. A packet sanity TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.26 packet-size

packet-size

Syntax **packet-size** *bytes*
no packet-size

Context **[Tree]** (config>system>snmp packet-size)

Full Context configure system snmp packet-size

Description This command configures the maximum SNMP packet size generated by this node.

The **no** form of this command restores the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default packet-size 1500

Parameters *bytes* — Specifies the SNMP packet size in bytes.

Values 484 to 9216

Platforms All

20.27 packet-too-big

packet-too-big

Syntax **packet-too-big** [*number seconds*]
no packet-too-big

Context **[Tree]** (config>service>ies>if>ipv6>icmp6 packet-too-big)

Full Context configure service ies interface ipv6 icmp6 packet-too-big

Description This command specifies whether packet-too-big ICMP messages should be sent. When enabled, ICMPv6 packet-too-big messages are generated by this interface.

The **no** form of this command disables the sending of ICMPv6 packet-too-big messages.

Default packet-too-big 100 10

Parameters *number* — Specifies the number of ICMP messages that are too large to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time frame, in seconds, that is used to limit the number of "packet-too-big" ICMP messages issued.

Values 1 to 60

Default 10

Platforms All

packet-too-big

Syntax **packet-too-big** [*number seconds*]
no packet-too-big

Context **[Tree]** (config>service>vprn>if>ipv6>icmp6 packet-too-big)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface ipv6 icmp6 packet-too-big

Description This command configures the rate for Internet Control Message Protocol version 6 (ICMPv6) packet-too-big messages.

Parameters *number* — Specifies the number of packet-too-big messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time frame, in seconds, that is used to limit the number of packet-too-big messages issued.

Values 1 to 60

Default 10

Platforms All

packet-too-big

Syntax **packet-too-big**
packet-too-big number [**10..1000**] **seconds** [**1..60**]
no packet-too-big

Context **[Tree]** (config>service>vprn>if>sap>ip-tunnel>icmp6-gen packet-too-big)

Full Context configure service vprn interface sap ip-tunnel icmp6-generation packet-too-big

Description This command enables the system to send ICMPv6 PTB (Packet Too Big) messages on the private side and optionally specifies the rate.

With this command configured, the system sends PTB back if it received an IPv6 packet on the private side that is bigger than 1280 bytes and also exceeds the private MTU of the tunnel.

The **ip-mtu** command (under **ipsec-tunnel** or **tunnel-template**) specifies the private MTU for the ipsec-tunnel or dynamic tunnel.

The **no** form of this command reverts **interval** and **message-count** values to their default values.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

packet-too-big

Syntax **packet-too-big** [*number seconds*]
no packet-too-big

Context **[Tree]** (config>router>if>ipv6>icmp6 packet-too-big)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface ipv6 icmp6 packet-too-big

Description This command configures the rate for ICMPv6 packet-too-big messages.

Parameters *number* — Limits the number of packet-too-big messages issued per time frame specified in the *seconds* parameter.

Values 10 to 1000

seconds — Determines the time frame, in seconds, that is used to limit the number of packet-too-big messages issued per time frame.

Values 1 to 60

Platforms All

20.28 packet-tx

packet-tx

Syntax **packet-tx** [**group** *grp-addr* [**source** *srcAddr*]] [**ret-nack**]
no packet-tx

Context **[Tree]** (debug>service>id>video-interface packet-tx)

Full Context debug service id video-interface packet-tx

Description This command enables debugging transmitted RTCP packets.

Parameters **client** *client-ip* — Specifies the client IP address.

source *src-srcAddr* — Specifies the source port's IP address.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.29 packet-type

packet-type

Syntax **packet-type** [**authentication**] [**accounting**] [**coa**]
no packet-type

Context **[Tree]** (debug>router>radius packet-type)

Full Context debug router radius packet-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the RADIUS packet type filter of command **debug router radius**.

Default authentication accounting coa

Parameters **authentication** — Specifies the RADIUS authentication packet.

accounting — Specifies the RADIUS accounting packet.

coa — Specifies the RADIUS change of authorization packet.

Platforms All

20.30 packets

packets

Syntax [**no**] **packets** [**interface** *ip-int-name*]

Context **[Tree]** (debug>router>srrp packets)

Full Context debug router srrp packets

Description This command enables debugging for SRRP packets.

The **no** form of this command disables debugging.

Platforms All

packets

Syntax [**no**] **packets**
[**no**] **packets interface** *ip-int-name* [**vrid** *virtual-router-id*]
[**no**] **packets interface** *ip-int-name* **vrid** *virtual-router-id* **ipv6**

Context **[Tree]** (debug>router>vrrp packets)

Full Context debug router vrrp packets

Description This command enables or disables debugging for VRRP packets.

Parameters *ip-int-name* — Specifies the interface name, up to 32 characters.

virtual-router-id — Specifies the router ID.

Values 1 to 255

ipv6 — Debugs the specified IPv6 VRRP interface.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packets

Syntax **packets** [**neighbor** *ip-address* | **group** *name*]
no packets

Context **[Tree]** (debug>router>bgp packets)

Full Context debug router bgp packets

Description This command decodes and logs all sent and received BGP packets in the debug log.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

packets

Syntax **packets** [**station** *station-name*]
no packets

Context **[Tree]** (debug>router>bmp packets)

Full Context debug router bmp packets

Description This command enables debugging for all BMP packets.

The **no** form of the command disables debugging for all BMP packets.

Parameters *station-name* — Specifies the station name of the BMP monitoring station, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

packets

Syntax [**no**] **packets** [**neighbor** *ip-int-name* | *ip-addr*]

Context **[Tree]** (debug>router>rip packets)

Full Context debug router rip packets

Description This command enables debugging for RIP packets.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP packets sent on the neighbor IP address or interface.

Platforms All

packets

Syntax [**no**] **packets** [**neighbor** *ip-int-name* | *ipv6-address*]

Context **[Tree]** (debug>router>ripng packets)

Full Context debug router ripng packets

Description This command enables debugging for RIPng packets.

Parameters *ip-int-name* | *ipv6-address* — Debugs the RIPng packets sent on the neighbor IP address or interface.

Platforms All

20.31 packets-admitted-count

packets-admitted-count

Syntax [**no**] **packets-admitted-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr packets-admitted-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr packets-admitted-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters packets-admitted-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters packets-admitted-count

Description This command includes the admitted packet count in the AA subscriber's custom record and only applies to the 7750 SR.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command excludes the admitted packet count.

Default no packets-admitted-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.32 packets-denied-count

packets-denied-count

Syntax [**no**] **packets-denied-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-from-sub-cntr packets-denied-count)
[Tree] (config>log>acct-policy>cr>aa>aa-to-sub-cntr packets-denied-count)

Full Context configure log accounting-policy custom-record aa-specific from-aa-sub-counters packets-denied-count
configure log accounting-policy custom-record aa-specific to-aa-sub-counters packets-denied-count

Description This command includes the denied packet count in the AA subscriber's custom record and only applies to the 7750 SR.

The **no** form of this command excludes the denied packet count.

Default no packets-denied-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.33 pad-size

pad-size

Syntax **pad-size** *octets*
no pad-size

Context **[Tree]** (config>oam-pm>session>ip>twamp-light pad-size)

Full Context configure oam-pm session ip twamp-light pad-size

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the amount by which the TWAMP Light packet is padded. TWAMP session controller packets are 27 bytes smaller than TWAMP session reflector packets. If symmetrical packet sizes in the forward and backward direction are required, the pad size must be configured to a minimum of 27 bytes.

The **no** form of this command removes all padding.

Default pad-size 0

Parameters *octets* — Specifies the value, in octets, to pad the TWAMP Light packet.

Values 0 to 2000

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.34 pad-tlv-size

pad-tlv-size

Syntax **pad-tlv-size** *octets*
no pad-tlv-size

Context **[Tree]** (config>oam-pm>session>mpls>dm pad-tlv-size)

Full Context configure oam-pm session mpls dm pad-tlv-size

Description This command allows the operator to add an optional Pad TLV to PDU and increase the frame on the wire by the specified amount. Note that this command only configures the size of the padding added to the PDU, and does not configure the total size of the frame on the wire. Since the bit count for the length is a maximum of 255 (8bits) the maximum pad per pad-tlv is between 0, 2 and 257 (type 1B, Length 1B, Length 255). Only a single pad-tlv can be added.

The **no** form of this command removes the optional TLV.

Parameters *octets* — Specifies the overall length of the pad-tlv.

Values 0, 2 to 257

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.35 padding-size

padding-size

Syntax **padding-size** *padding-size*
no padding-size

Context **[Tree]** (config>service>vprn>static-route-entry>indirect>cpe-check padding-size)
[Tree] (config>service>vprn>static-route-entry>next-hop>cpe-check padding-size)

Full Context configure service vprn static-route-entry indirect cpe-check padding-size
configure service vprn static-route-entry next-hop cpe-check padding-size

Description This optional parameter specifies the amount of padding to add to the ICMP packet in bytes. The parameter is only applicable when the **cpe-check** option is used with the associated static route.

Default padding-size 56

Parameters *padding-size* — An integer value.

Values 0 to 16384 bytes

Platforms All

padding-size

Syntax **padding-size** *padding-size*
no padding-size

Context **[Tree]** (config>router>static-route-entry>indirect>cpe-check padding-size)
[Tree] (config>router>static-route-entry>next-hop>cpe-check padding-size)

Full Context configure router static-route-entry indirect cpe-check padding-size
configure router static-route-entry next-hop cpe-check padding-size

Description This command specifies the amount of padding to add to the ICMP packet in bytes. The parameter is only applicable when the **cpe-check** option is used with the associated static route.

Default padding-size 56

Parameters *padding-size* — Specifies the integer value.

Values 0 to 16384 bytes

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

padding-size

Syntax **padding-size** *size*
no padding-size

Context **[Tree]** (config>vrrp>priority-event>host-unreachable padding-size)

Full Context configure vrrp priority-event host-unreachable padding-size

Description This command allows the operator to increase the size of IP packet by padding the PDU.

The **no** form of the command reverts to the default.

Default padding-size 0

Parameters *size* — Specifies amount of increase to the ICMP PDU.

Values 0 to 16384

20.36 padi-auth-policy

padi-auth-policy

Syntax **padi-auth-policy** *policy-name*
no padi-auth-policy

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host padi-auth-policy)

Full Context configure subscriber-mgmt local-user-db ppp host padi-auth-policy

Description This command configures the PADI authentication policy of this host.

Parameters *policy-name* — Specifies the authentication policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.37 pado-ac-name

pado-ac-name

Syntax **pado-ac-name** *name*
no pado-ac-name

Context **[Tree]** (config>subscr-mgmt>ppp-policy pado-ac-name)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt ppp-policy pado-ac-name

Description This command configures the Access Concentrator name that is used in the PPPoE PADO message.

By default, the system name or if not configured, the chassis Serial Number is used.

Parameters *name* — Specifies the string up to 128 characters to be used as AC name in the PPPoE PADO message.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.38 pado-delay

pado-delay

Syntax **pado-delay** *deci-seconds*
no pado-delay

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host pado-delay)

Full Context configure subscriber-mgmt local-user-db ppp host pado-delay

Description This command configures the delay timeout before sending a PPPoE Active Discovery Offer (PADO).

Parameters *deci-seconds* — Specifies the delay timeout before sending a PADO.

Values 1 to 30

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pado-delay

Syntax **pado-delay** *deci-seconds*
no pado-delay

Context **[Tree]** (config>subscr-mgmt>ppp-policy pado-delay)

Full Context configure subscriber-mgmt ppp-policy pado-delay

Description This command configures the delay timeout before sending a PPP Active Discovery Offer (PADO) packet.

Parameters *deci-seconds* — Specifies the delay timeout before sending a PADO.

Values 1 to 30

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.39 pairing-button

pairing-button

Syntax **pairing-button** *admin-state*

Context **[Tree]** (config>system>bluetooth pairing-button)

Full Context configure system bluetooth pairing-button

Description This command is used to allow or block the function of the pairing button. This can be used to block the accidental triggering of a pairing operation while there is already a paired device.

The actual behavior of the Bluetooth pairing is dependent on both this command and the **power** command.

If normal operation is to use the pairing button on the router and on the external device to initiate the Bluetooth connection, then set:

config>system>bluetooth>power enabled-manual

config>system>bluetooth>pairing-button enable

If normal operation is to only require the pairing to be initiated by the external device, then set:

config>system>bluetooth>power enabled-automatic

config>system>bluetooth>pairing-button disable

If normal operation is to not allow the local operator to connect without permission from the central management location, then set:

config>system>bluetooth>power enabled-manual

config>system>bluetooth>pairing-button disable

Then when a connection is desired, the central management station must change the configuration to one of the two options shown above for the time the local operator is connecting. The central management station can change the setting back to block local access after the operations is complete.

Default pairing-button disable

Parameters *admin-state* — Specifies the administrative state.

Values enable — pairing button can trigger a pairing operation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

disable — pairing button does not trigger a pairing operation

Platforms 7750 SR-1, 7750 SR-s

20.40 parallel

parallel

Syntax **parallel** [**no-advertise**]
no parallel

Context **[Tree]** (config>router>ospf>segm-rtng>adjacency-set parallel)
[Tree] (config>router>isis>segm-rtng>adjacency-set parallel)

Full Context configure router isis segment-routing adjacency-set parallel
configure router ospf segment-routing adjacency-set parallel

Description This command indicates that all members of the adjacency set must terminate on the same neighboring node. The system raises a trap if a user attempts to add an adjacency terminating on a neighboring node that differs from the existing members of the adjacency set. In addition, the system stops advertising the adjacency set in IS-IS or OSPF and locally deprograms it.

By default, parallel adjacency sets are advertised in the IGP. The **no-advertise** option prevents an adjacency set from being advertised in the IGP. It is only allowed in CLI and SNMP if the **parallel** command is configured.

The **no** form of this command indicates that the adjacency set can include adjacencies to different next hop nodes.

Default parallel

Platforms All

20.41 param-problem

param-problem

Syntax **param-problem** [*number seconds*]
no param-problem

Context **[Tree]** (config>service>ies>if>ipv6>icmp6 param-problem)
[Tree] (config>service>ies>sub-if>grp-if>icmp param-problem)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>if>icmp param-problem)
[Tree] (config>service>vprn>sub-if>grp-if>icmp param-problem)

Full Context configure service ies interface icmp param-problem
configure service ies interface ipv6 icmp6 param-problem
configure service ies subscriber-interface group-interface icmp param-problem
configure service vprn subscriber-interface group-interface icmp param-problem

Description This command specifies whether parameter-problem ICMP/ICMPv6 messages should be sent. When enabled, parameter-problem ICMP/ICMPv6 messages are generated by this interface.

The **no** form of this command disables the sending of parameter-problem ICMP/ICMPv6 messages.

Default param-problem 100 10

Parameters *number* — Specifies the number of parameter-problem ICMPv6 messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time frame, in seconds, that is used to limit the number of parameter-problem ICMPv6 messages issued.

Values 1 to 60

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface icmp param-problem
- configure service ies subscriber-interface group-interface icmp param-problem

All

- configure service ies interface ipv6 icmp6 param-problem
- configure service ies interface icmp param-problem

param-problem

Syntax **param-problem** [**number** *number*] [**seconds** *seconds*]
no param-problem

Context [Tree] (config>subscr-mgmt>git>ipv4>icmp param-problem)

Full Context configure subscriber-mgmt group-interface-template ipv4 icmp param-problem

Description This command configures the parameter-problem ICMPv4 messages that are generated by this interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the sending of parameter-problem ICMPv4 messages.

Default param-problem number 100 seconds 10

Parameters *number* — Specifies the number of parameter-problem ICMPv4 messages sent in the time specified by the *seconds* parameter.

Values 10 to 1000

seconds — Specifies the time, in seconds, that is used to limit the number of parameter-problem ICMPv4 messages issued.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

param-problem

Syntax **param-problem** *number seconds*
no param-problem [*number seconds*]

Context **[Tree]** (config>service>vprn>if>icmp param-problem)
[Tree] (config>service>vprn>if>ipv6>icmp6 param-problem)
[Tree] (config>service>vprn>nw-if>icmp param-problem)

Full Context configure service vprn interface icmp param-problem
configure service vprn interface ipv6 icmp6 param-problem
configure service vprn network-interface icmp param-problem

Description This command specifies whether parameter-problem ICMP messages should be sent. When enabled, parameter-problem ICMP messages are generated by this interface. The **no** form of this command disables the sending of parameter-problem ICMP messages.

Parameters *number* — Specifies the number of parameter-problem ICMP messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time frame, in seconds, that is used to limit the number of parameter-problem ICMP messages issued.

Values 1 to 60

Default 10

Platforms All

param-problem

Syntax **param-problem** [*number seconds*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no param-problem

Context [Tree] (config>router>if>icmp param-problem)

Full Context configure router interface icmp param-problem

Description This command specifies whether parameter-problem ICMP messages should be sent. When enabled, parameter-problem ICMP messages are generated by this interface.

The **no** form of this command disables the sending of parameter-problem ICMP messages.

Parameters *number* — Specifies the number of parameter-problem ICMP messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time frame, in seconds, that is used to limit the number of parameter-problem ICMP messages issued.

Values 1 to 60

Default 10

Platforms All

param-problem

Syntax **param-problem** [*number seconds*]
no param-problem

Context [Tree] (config>router>if>ipv6>icmp6 param-problem)

Full Context configure router interface ipv6 icmp6 param-problem

Description This command specifies whether parameter-problem ICMPv6 messages should be sent. When enabled, parameter-problem ICMPv6 messages are generated by this interface.

The **no** form of this command disables the sending of parameter-problem ICMPv6 messages.

Parameters *number* — Specifies the number of parameter-problem ICMPv6 messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time frame, in seconds, that is used to limit the number of parameter-problem ICMPv6 messages issued.

Values 1 to 60

Default 10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.42 parent

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]
no parent

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover>q parent)

Full Context configure port ethernet access egress queue-group queue-overrides queue parent

Description This command, when used in the *queue-overrides* context for a queue group queue, defines an optional **weight** and **cir-weight** for the queue treatment by the parent scheduler that further governs the available bandwidth given the queue aside from the queue PIR setting. When multiple schedulers and/or queues share a child status with the parent scheduler, the weight or level parameters define how this queue contends with the other children for the parent bandwidth.

Parameters *weight* — Specifies the relative weight of this queue in comparison to other child schedulers and queues while vying for bandwidth on the parent scheduler-name. Any queues or schedulers defined as weighted receive no parental bandwidth until all strict queues and schedulers on the parent have reached their maximum bandwidth or are idle. In this manner, weighted children are considered to be the lowest priority.

Values 0 to 100

Default 1

cir-weight — Specifies the weight the queue uses at the within-cir port priority level. The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-cir pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 100

Platforms All

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]
no parent

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>sched-override>scheduler parent)
[Tree] (config>port>ethernet>access>ing>qgrp>sched-override>scheduler parent)

Full Context configure port ethernet access egress queue-group scheduler-override scheduler parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet access ingress queue-group scheduler-override scheduler parent

Description This command can be used to override the scheduler's parent weight and CIR weight. The weights apply to the associated level/cir-level configured in the applied scheduler policy. The scheduler name must exist in the applied scheduler policy.

The override weights are ignored if the scheduler does not have a parent command configured in the scheduler policy - this allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the queue group overrides. If the parent scheduler does not exist, causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non-default weightings for fostered schedulers.

The **no** form of this command returns the scheduler's parent weight and cir-weight to the value configured in the applied scheduler policy.

Default no parent

Parameters *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict level defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total distributes the available bandwidth at that level. A weight is considered to be active when the queue or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

cir-weight — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same cir-level defined by the cir-level parameter in the applied scheduler policy. Within the strict cir-level, all cir-weight values from active children at that level are summed and the ratio of each active child's cir-weight to the total distributes the available bandwidth at that level. A cir-weight is considered to be active when the policer, queue, or scheduler that the cir-weight pertains to has not reached the CIR and still has packets to transmit.

A 0 (zero) cir-weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Platforms All

parent

Syntax **parent** {[**weight** *weight*] [**cir-weight** *cir-weight*]}
no parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context

[Tree] (config>service>apipe>sap>egress>queue-override>queue parent)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue parent)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue parent)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue parent)
[Tree] (config>service>epipe>sap>egress>queue-override>queue parent)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue parent)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue parent)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue parent)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue parent)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue parent)

Full Context

configure service apipe sap egress queue-override queue parent
configure service apipe sap ingress queue-override queue parent
configure service cpipe sap egress queue-override queue parent
configure service cpipe sap ingress queue-override queue parent
configure service epipe sap egress queue-override queue parent
configure service epipe sap ingress queue-override queue parent
configure service fpipe sap egress queue-override queue parent
configure service fpipe sap ingress queue-override queue parent
configure service ipipe sap egress queue-override queue parent
configure service ipipe sap ingress queue-override queue parent

Description

This command defines an optional parent scheduler that further governs the available bandwidth given the queue aside from the queue's PIR setting. When multiple schedulers and/or queues share a child status with the parent scheduler, the **weight** or **level** parameters define how this queue contends with the other children for the parent's bandwidth.

Checks are not performed to see if a *scheduler-name* exists when the parent command is defined on the queue. Scheduler names are configured in the **config>qos>scheduler-policy>tier** *level* context. Multiple schedulers can exist with the *scheduler-name* and the association pertains to a scheduler that should exist on the egress SAP as the policy is applied and the queue created. When the queue is created on the egress SAP, the existence of the *scheduler-name* is dependent on a scheduler policy containing the *scheduler-name* being directly or indirectly applied (through a multi-service customer site) to the egress SAP. If the *scheduler-name* does not exist, the queue is placed in the orphaned operational state. The queue will accept packets but will not be bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP. The orphaned state must generate a log entry and a trap message. The SAP which the queue belongs to must also depict an orphan queue status. The orphaned state of the queue is automatically cleared when the *scheduler-name* becomes available on the egress SAP.

The parent scheduler can be made unavailable due to the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the queue enters the orphaned state and automatically returns to normal operation when the parent scheduler is available again.

When a parent scheduler is defined without specifying weight or strict parameters, the default bandwidth access method is weight with a value of 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and returns without an error. Once a parent association has been removed, the former child queue attempts to operate based on its configured rate parameter. Removing the parent association on the queue within the policy takes effect immediately on all queues using the SAP egress QoS policy.

Parameters

weight — These optional keywords are mutually exclusive to the **level** keyword. Specifies the relative weight of this queue in comparison to other child schedulers, policers, and queues while vying for bandwidth on the parent *scheduler-name*. Any policers, queues, or schedulers defined as weighted receive no parental bandwidth until all policers, queues, and schedulers with a higher (numerically larger) priority on the parent have reached their maximum bandwidth or are idle.

All **weight** values from all weighted active policers, queues, and schedulers with a common parent scheduler are added together. Then, each individual active weight is divided by the total, deriving the percentage of remaining bandwidth provided to the policer, queue, or scheduler. A weight is considered to be active when the pertaining policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit. All child policers, queues, and schedulers with a weight of 0 are considered to have the lowest priority level and are not serviced until all non-zero weighted policers, queues, and schedulers at that level are operating at the maximum bandwidth or are idle.

Values 0 to 100

Default 1

cir-weight — Specifies the weight the queue or scheduler will use at the within-cir port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the policer, queue, or scheduler does not receive bandwidth during the port schedulers within-cir pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress queue-override queue parent
- configure service cpipe sap egress queue-override queue parent
- configure service fpipe sap egress queue-override queue parent
- configure service fpipe sap ingress queue-override queue parent

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue parent
- configure service apipe sap ingress queue-override queue parent

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap egress queue-override queue parent
- configure service ipipe sap egress queue-override queue parent
- configure service ipipe sap ingress queue-override queue parent
- configure service epipe sap ingress queue-override queue parent

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]
no parent

Context **[Tree]** (config>service>apipe>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>apipe>sap>egress>sched-override>scheduler parent)
[Tree] (config>service>cpipe>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>cpipe>sap>egress>sched-override>scheduler parent)
[Tree] (config>service>epipe>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>epipe>sap>egress>sched-override>scheduler parent)
[Tree] (config>service>fpipe>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>fpipe>sap>egress>sched-override>scheduler parent)
[Tree] (config>service>ipipe>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>ipipe>sap>egress>sched-override>scheduler parent)

Full Context configure service apipe sap egress scheduler-override scheduler parent
configure service apipe sap ingress scheduler-override scheduler parent
configure service cpipe sap egress scheduler-override scheduler parent
configure service cpipe sap ingress scheduler-override scheduler parent
configure service epipe sap egress scheduler-override scheduler parent
configure service epipe sap ingress scheduler-override scheduler parent
configure service fpipe sap egress scheduler-override scheduler parent
configure service fpipe sap ingress scheduler-override scheduler parent
configure service ipipe sap egress scheduler-override scheduler parent
configure service ipipe sap ingress scheduler-override scheduler parent

Description This command can be used to override the scheduler's parent weight and cir-weight information. The weights apply to the associated level/cir-level configured in the applied scheduler policy. The scheduler name must exist in the scheduler policy applied to the ingress or egress of the SAP or multi-service site.

The override weights are ignored if the scheduler does not have a parent command configured in the scheduler policy – this allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the SAP/MSS overrides. If the parent scheduler does not exist causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non-default weightings for fostered schedulers.

The **no** form of this command returns the scheduler's parent weight and cir-weight to the value configured in the applied scheduler policy.

Default no parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers, policers, and queues at the same strict **level** defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the policer, queue, or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

cir-weight — Specifies the relative weight of this scheduler in comparison to other child schedulers, policers, and queues at the same *cir-level* defined by the **cir-level** parameter in the applied scheduler policy. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the policer, queue, or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit.

A 0 (zero) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress scheduler-override scheduler parent
- configure service cpipe sap ingress scheduler-override scheduler parent
- configure service fpipe sap egress scheduler-override scheduler parent
- configure service fpipe sap ingress scheduler-override scheduler parent

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress scheduler-override scheduler parent
- configure service apipe sap egress scheduler-override scheduler parent

All

- configure service ipipe sap egress scheduler-override scheduler parent
- configure service ipipe sap ingress scheduler-override scheduler parent
- configure service epipe sap ingress scheduler-override scheduler parent
- configure service epipe sap egress scheduler-override scheduler parent

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no parent

Context [Tree] (config>service>vpls>sap>egress>queue-override>queue parent)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue parent)

Full Context configure service vpls sap egress queue-override queue parent
configure service vpls sap ingress queue-override queue parent

Description This command defines an optional parent scheduler that further governs the available bandwidth given the queue aside from the queue's PIR setting. When multiple schedulers and/or queues share a child status with the parent scheduler, the **weight** or **level** parameters define how this queue contends with the other children for the parent's bandwidth.

Checks are not performed to see if a *scheduler-name* exists when the parent command is defined on the queue. Scheduler names are configured in the **config>qos>scheduler-policy>tier** *level* context. Multiple schedulers can exist with the *scheduler-name* and the association pertains to a scheduler that should exist on the egress SAP as the policy is applied and the queue created. When the queue is created on the egress SAP, the existence of the *scheduler-name* is dependent on a scheduler policy containing the *scheduler-name* being directly or indirectly applied (through a multi-service customer site) to the egress SAP. If the *scheduler-name* does not exist, the queue is placed in the orphaned operational state. The queue will accept packets but will not be bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP. The orphaned state must generate a log entry and a trap message. The SAP which the queue belongs to must also depict an orphan queue status. The orphaned state of the queue is automatically cleared when the *scheduler-name* becomes available on the egress SAP.

The parent scheduler can be made unavailable due to the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the queue enters the orphaned state mentioned above and automatically return to normal operation when the parent scheduler is available again.

When a parent scheduler is defined without specifying weight or strict parameters, the default bandwidth access method is weight with a value of 1.

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and returns without an error. Once a parent association has been removed, the former child queue attempts to operate based on its configured rate parameter. Removing the parent association on the queue within the policy takes effect immediately on all queues using the SAP egress QoS policy.

Parameters *weight* — These optional keywords are mutually exclusive to the **level** keyword. The weight defines the relative weight of this queue in comparison to other child schedulers, policers, and queues while vying for bandwidth on the parent *scheduler-name*. Any policers, queues, or schedulers defined as weighted receive no parental bandwidth until all policers, queues, and schedulers with a higher (numerically larger) priority on the parent have reached their maximum bandwidth or are idle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All **weight** values from all weighted active policers, queues, and schedulers with a common parent scheduler are added together. Then, each individual active weight is divided by the total, deriving the percentage of remaining bandwidth provided to the policer, queue, or scheduler. A weight is considered to be active when the pertaining policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit. All child policers, queues, and schedulers with a weight of 0 are considered to have the lowest priority level and are not serviced until all non-zero weighted policers, queues, and schedulers at that level are operating at the maximum bandwidth or are idle.

Values 0 to 100

Default 1

cir-weight — Specifies the weight the queue or scheduler will use at the within-cir port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the policer, queue, or scheduler does not receive bandwidth during the port schedulers within-cir pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 100

Platforms All

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]
no parent

Context **[Tree]** (config>service>vpls>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>vpls>sap>egress>sched-override>scheduler parent)

Full Context configure service vpls sap egress scheduler-override scheduler parent
configure service vpls sap ingress scheduler-override scheduler parent

Description This command can be used to override the scheduler's parent weight and cir-weight information. The weights apply to the associated level/cir-level configured in the applied scheduler policy. The scheduler name must exist in the scheduler policy applied to the ingress or egress of the SAP or multi-service site.

The override weights are ignored if the scheduler does not have a parent command configured in the scheduler policy – this allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the SAP/MSS overrides. If the parent scheduler does not exist causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non-default weightings for fostered schedulers.

The **no** form of this command returns the scheduler's parent weight and cir-weight to the value configured in the applied scheduler policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no parent

Parameters *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict **level** defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the policer, queue, or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

cir-weight — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same *cir-level* defined by the **cir-level** parameter in the applied scheduler policy. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the policer, queue, or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit.

A 0 (zero) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Platforms All

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue parent)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue parent)
[Tree] (config>service>ies>if>sap>egress>sched-override>scheduler parent)
[Tree] (config>service>ies>if>sap>ingress>sched-override>scheduler parent)

Full Context configure service ies interface sap egress queue-override queue parent
configure service ies interface sap egress scheduler-override scheduler parent
configure service ies interface sap ingress queue-override queue parent
configure service ies interface sap ingress scheduler-override scheduler parent

Description This command can be used to override the scheduler's parent weight and cir-weight information. The weights apply to the associated level/cir-level configured in the applied scheduler policy. The scheduler name must exist in the scheduler policy applied to the ingress or egress of the SAP or multi-service site.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The override weights are ignored if the scheduler does not have a parent command configured in the scheduler policy – this allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the SAP/MSS overrides. If the parent scheduler does not exist causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non default weightings for fostered schedulers.

The **no** form of this command returns the scheduler's parent weight and cir-weight to the value configured in the applied scheduler policy.

Default no parent

Parameters **weight** *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict **level** defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the queue or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

cir-weight *cir-weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same *cir-level* defined by the **cir-level** parameter in the applied scheduler policy. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the policer, queue, or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit.

A 0 (zero) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Platforms All

parent

Syntax **parent** [**weight** *weight*] [**cir-weight cir-***weight*]
no parent

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue parent)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue parent)

Full Context configure service vprn interface sap egress queue-override queue parent
configure service vprn interface sap ingress queue-override queue parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command can be used to override the scheduler's parent weight and cir-weight information. The weights apply to the associated level/cir-level configured in the applied scheduler policy. The scheduler name must exist in the scheduler policy applied to the ingress or egress of the SAP or multi-service site.

The override weights are ignored if the scheduler does not have a parent command configured in the scheduler policy – this allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the SAP/MSS overrides. If the parent scheduler does not exist causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non default weightings for fostered schedulers.

The **no** form of this command returns the scheduler's parent weight and cir-weight to the value configured in the applied scheduler policy.

Default no parent

Parameters **weight** *weight* — Specifes the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict **level** defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the queue or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

Default 1

cir-weight *cir-weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same *cir-level* defined by the **cir-level** parameter in the applied scheduler policy. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the policer, queue, or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit.

A 0 (zero) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Default 1

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]
no parent

Context **[Tree]** (config>service>vprn>if>sap>ingress>sched-override>scheduler parent)
[Tree] (config>service>vprn>if>sap>egress>sched-override>scheduler parent)

Full Context configure service vprn interface sap egress scheduler-override scheduler parent
configure service vprn interface sap ingress scheduler-override scheduler parent

Description This command can be used to override the scheduler's parent weight and cir-weight information. The weights apply to the associated level/cir-level configured in the applied scheduler policy. The scheduler name must exist in the scheduler policy applied to the ingress or egress of the SAP or multi-service site.

The override weights are ignored if the scheduler does not have a parent command configured in the scheduler policy – this allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the SAP/MSS overrides. If the parent scheduler does not exist causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non default weightings for fostered schedulers.

The no form of this command returns the scheduler's parent weight and cir-weight to the value configured in the applied scheduler policy.

Default no parent

Parameters **weight** *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict **level** defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the policer, queue, or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

cir-weight *cir-weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same *cir-level* defined by the **cir-level** parameter in the applied scheduler policy. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the policer, queue, or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A 0 (zero) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Platforms All

parent

Syntax **parent** {**root** | *arbiter-name*} [**level** *priority-level*] [**weight** *weight-within-level*]
no parent

Context **[Tree]** (config>qos>plcr-ctrl-plcy>tier>arbiter parent)

Full Context configure qos policer-control-policy tier arbiter parent

Description This command is used to define from where the tiered arbiter receives bandwidth. Both tier 1 and tier 2 arbiters default to parenting to the root arbiter. Tier 2 arbiters may be modified to parent to a tier 1 arbiter. The tier 1 arbiter parent cannot be changed.

The **no** form of this command is used to return the tiered arbiter to the default parenting behavior.

Default parent root level 1 weight 1

Parameters **root** — In tier 1, *arbiter-name* is not allowed and only **root** is accepted. When **root** is specified, the arbiter will receive all bandwidth directly from the root arbiter. This is the default parent for tiered arbiters.

arbiter-name — In tier 1, *arbiter-name* is not allowed and only **root** is accepted. The specified *arbiter-name* must exist within the policer-control-policy at tier 1 or the parent command will fail. When a tiered arbiter is acting as a parent for another tiered arbiter, the parent arbiter cannot be removed from the policy. The child arbiter will receive all bandwidth directly from its parent arbiter (that receives bandwidth from the root arbiter).

priority-level — Each child arbiter attaches to its parent on one of the parent's eight strict levels. Level 1 is the lowest and 8 is the highest. The level attribute is used to define which level the child arbiter uses on its parent. The parent distributes its available bandwidth based on strict priority starting with priority level 8 and proceeding towards level 1.

Values 1 to 8

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

weight-within-level — The **weight** attribute is used to define how multiple children at the same parent strict level compete when insufficient bandwidth exists on the parent for that level. Each child's weight is divided by the sum of the active children's weights and the result is multiplied by the available bandwidth. If a child cannot receive its entire weighted fair share of bandwidth due to a defined child rate limit, the remainder of its bandwidth is distributed between the other children based on their weights.

Values 1 to 100

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

parent

Syntax **parent** *arbiter-name* [**weight** *weight-within-level*] [**level** *level*]
no parent

Context **[Tree]** (config>qos>sap-ingress>dyn-policer parent)
[Tree] (config>qos>sap-egress>dyn-policer parent)
[Tree] (config>qos>sap-ingress>policer parent)
[Tree] (config>qos>sap-egress>policer parent)

Full Context configure qos sap-egress dynamic-policer parent
configure qos sap-egress policer parent
configure qos sap-ingress dynamic-policer parent
configure qos sap-ingress policer parent

Description This command is used to create a child-to-parent mapping between each instance of the policer and either the **root** arbiter or a specific tiered **arbiter** on the object where the policy is applied. Defining a parent association for the policer causes the policer to compete for the parent policer's available bandwidth with other child policers mapped to the policer control hierarchy.

Policer control hierarchies may be created on SAPs or on a subscriber or multiservice site context. To create a policer control hierarchy on an ingress or egress SAP context, a **policer-control-policy** must be applied to the SAP. When applied, the system will create a parent policer that is bandwidth limited by the policy's **max-rate** value under the root arbiter. The root arbiter in the policy also provides the information used to determine the various priority-level discard-unfair and discard-all thresholds. Besides the root arbiter, the policy may also contain user-defined tiered arbiters that provide arbitrary bandwidth control for subsets of child policers that are either directly or indirectly parented by the arbiter.

When the QoS policy containing the policer with a **parent** mapping to an arbiter name exists on the SAP, the system will scan the available arbiters on the SAP. If an arbiter exists with the appropriate name, the policer to arbiter association is created. If the specified arbiter does not exist either because a **policer-control-policy** is not currently applied to the SAP or the arbiter name does not exist within the applied policy, the policer is placed in an orphan state. Orphan policers operate as if they are not parented and are not subject to any bandwidth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

constraints other than their own PIR. When a policer enters the orphan state, it is flagged as operationally degraded due to the fact that it is not operating as intended and a trap is generated. Whenever a **policer-control-policy** is added to the SAP or the existing policy is modified, the SAP's policer's parenting configurations must be reevaluated. If an orphan policer becomes parented, the degraded flag is cleared, and a resulting trap is generated.

For subscribers, the policer control hierarchy is created through the **policer-control-policy** applied to the **sub-profile** used by the subscriber. A unique policer control hierarchy is created for each subscriber associated with the **sub-profile**. The QoS policy containing the policer with the parenting command comes into play through the subscriber **sla-profile**, which references the QoS policy. The combining of the **sub-profile** and the **sla-profile** at the subscriber level provides the system with the proper information to create the policer control hierarchy instance for the subscriber. This functionality is available only for the 7450 ESS and 7750 SR.

Executing the **parent** command will fail if:

- The policer’s stat-mode in the QoS policy is set to no-stats
- A stat-mode no-stats override exists on an instance of the policer on a SAP or subscriber or multiservice site context

A policer with a **parent** command applied cannot be configured with **stat-mode no-stats** in either the QoS policy or as an override on an instance of the policer.

When a policer is successfully parented to an arbiter, the **parent** commands **level** and **weight** parameters are used to determine at what priority level and at which weight in the priority level that the child policer competes with other children (policers or other arbiters) for bandwidth.

The **no** form of this command is used to remove the parent association from all instances of the policer.

Parameters **{root |** *arbiter-name***}** — When the **parent** command is executed, either the keyword **root** or an *arbiter-name* must be specified.

root — Specifies that the policer is intended to become a child to the **root** arbiter where an instance of the policer is created. If the **root** arbiter does not exist, the policer will be placed in the orphan state.

Default **root**

arbiter-name — Specifies that the policer is intended to become a child to one of the tiered arbiters with the given arbiter-name where an instance of the policer is created. If the specified *arbiter-name* does not exist, the policer will be placed in the orphan state.

weight *weight-within-level* — The **weight** *weight-within-level* keyword and parameter are optional when executing the **parent** command. When **weight** is not specified, a default level of 1 is used in the parent arbiter’s priority level. When **weight** is specified, the *weight-within-level* parameter must be specified as an integer value from 1 through 100.

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure qos sap-ingress dynamic-policer parent
- configure qos sap-egress dynamic-policer parent

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-ingress policer parent
- configure qos sap-egress policer parent

parent

Syntax **parent** *scheduler-name* [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no parent

Context **[Tree]** (config>qos>sap-ingress>queue parent)
[Tree] (config>qos>sap-egress>queue parent)

Full Context configure qos sap-egress queue parent
configure qos sap-ingress queue parent

Description This command defines an optional parent scheduler that further governs the available bandwidth given the queue aside from the queue's PIR setting. When multiple schedulers, policers (at egress only), and/or queues share a child status with the parent scheduler, the **weight** or **level** parameters define how this queue contends with the other children for the parent's bandwidth.

Checks are not performed to see if a *scheduler-name* exists when the parent command is defined on the queue. Scheduler names are configured in the **config>qos>scheduler-policy>tier** *level* context. Multiple schedulers can exist with the *scheduler-name* and the association pertains to a scheduler that should exist on the egress SAP as the policy is applied and the queue created. When the queue is created on the egress SAP, the existence of the *scheduler-name* is dependent on a scheduler policy containing the *scheduler-name* being directly or indirectly applied (through a multiservice customer site) to the egress SAP. If the *scheduler-name* does not exist, the queue is placed in the orphaned operational state. The queue will accept packets but will not be bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP. The SAP that the queue belongs to also depicts an orphan queue status. The orphaned state of the queue is automatically cleared when the *scheduler-name* becomes available on the egress SAP.

The parent scheduler can be made unavailable due to the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the queue enters the orphaned state and automatically returns to normal operation when the parent scheduler is available again.

When a parent scheduler is defined without specifying the weight parameter, the default is a weight of 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and returns without an error. When a parent association has been removed, the former child queue attempts to operate based on its configured rate parameter. Removing the parent association on the queue within the policy takes effect immediately on all queues using the SAP egress QoS policy.

Parameters *scheduler-name* — The defined *scheduler-name* conforms to the same input criteria as the schedulers defined within a scheduler policy. Scheduler names are configured in the config>qos>scheduler-policy>tier *level* context. There are no checks performed at the time of definition to ensure that the *scheduler-name* exists within an existing scheduler policy. For the queue to use the defined *scheduler-name*, the scheduler exists on each egress SAP that the queue is eventually created on. For the duration where *scheduler-name* does not exist on the egress SAP, the queue operates in an orphaned state.

Values Any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

weight — Specifies the relative weight of this queue in comparison to other child schedulers, policers, and queues, while vying for bandwidth on the parent *scheduler-name*. Any queues, policers, or schedulers defined as weighted receive no parental bandwidth until all policers, queues, and schedulers with a higher (numerically larger) priority on the parent have reached their maximum bandwidth or are idle.

All **weight** values from all weighted active queues, policers, and schedulers with a common parent scheduler are added together. Then, each individual active weight is divided by the total, deriving the percentage of remaining bandwidth provided to the queue, policer, or scheduler. A weight is considered to be active when the pertaining queue, policer, or scheduler has not reached its maximum rate and still has packets to transmit. All child queues, policers, and schedulers with a weight of 0 are considered to have the lowest priority level and are not serviced until all non-zero weighted queues, policers, and schedulers at that level are operating at the maximum bandwidth or are idle.

Values 0 to 100

Default 1

level — The optional **level** parameter defines the level of hierarchy when compared to other schedulers and queues competing for bandwidth on the parent *scheduler-name*. Queues or schedulers will not receive parental bandwidth until all queues, policers, and schedulers with a higher (numerically larger) priority on the parent have reached their maximum bandwidth or are idle.

Children of the parent scheduler with a lower strict priority will not receive bandwidth until all children with a higher strict priority have either reached their maximum bandwidth or are idle. Children with the same strict level are serviced in relation to their relative weights.

Values 1 to 8

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-weight — Specifies the weight that the queue or scheduler uses at the within-CIR port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 100

Default 1

cir-level — Specifies the port priority that the queue or scheduler will use to receive bandwidth for its within-CIR offered-load. If the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms All

parent

Syntax **parent** {**root** | *arbiter-name*} [**level** *level*] [**weight** *weight-within-level*]
no parent

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer parent)
[Tree] (config>qos>qgrps>ing>qgrp>policer parent)

Full Context configure qos queue-group-templates egress queue-group policer parent
configure qos queue-group-templates ingress queue-group policer parent

Description This command is used to create a child-to-parent mapping between each instance of the policer and either the **root** arbiter or a specific tiered **arbiter** on the object where the policy is applied. Defining a parent association for the policer causes the policer to compete for the parent policer's available bandwidth with other child policers mapped to the policer control hierarchy.

Policer control hierarchies may be created on SAPs or on a subscriber or multiservice site context. To create a policer control hierarchy on an ingress or egress SAP context, a **policer-control-policy** must be applied to the SAP. When applied, the system will create a parent policer that is bandwidth limited by the policy's **max-rate** value under the root arbiter. The root arbiter in the policy also provides the information used to determine the various priority level discard-unfair and discard-all thresholds. Besides the root arbiter, the policy may also contain user-defined tiered arbiters that provide arbitrary bandwidth control for subsets of child policers that are either directly or indirectly parented by the arbiter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the QoS policy containing the policer with a **parent** mapping to an arbiter name exists on the SAP, the system will scan the available arbiters on the SAP. If an arbiter exists with the appropriate name, the policer to arbiter association is created. If the specified arbiter does not exist either because a **policer-control-policy** is not currently applied to the SAP or the arbiter name does not exist within the applied policy, the policer is placed in an orphan state. Orphan policers operate as if they are not parented and are not subject to any bandwidth constraints other than their own PIR. When a policer enters the orphan state, it is flagged as operationally degraded due to the fact that it is not operating as intended and a trap is generated. Whenever a **policer-control-policy** is added to the SAP or the existing policy is modified, the SAP's policer's parenting configurations must be reevaluated. If an orphan policer becomes parented, the degraded flag is cleared and a resulting trap is generated.

For subscribers, the policer control hierarchy is created through the **policer-control-policy** applied to the **sub-profile** used by the subscriber. A unique policer control hierarchy is created for each subscriber associated with the **sub-profile**. The QoS policy containing the policer with the parenting command comes into play through the subscriber **sla-profile** that references the QoS policy. The combining of the **sub-profile** and the **sla-profile** at the subscriber level provides the system with the proper information to create the policer control hierarchy instance for the subscriber. This functionality is available only for the 7450 ESS and 7750 SR.

Executing the **parent** command will fail if:

- The policer’s stat-mode in the QoS policy is set to no-stats
- A stat-mode no-stats override exists on an instance of the policer on a SAP or subscriber or multiservice site context

A policer with a **parent** command applied cannot be configured with **stat-mode no-stats** in either the QoS policy or as an override on an instance of the policer.

When a policer is successfully parented to an arbiter, the **parent** commands **level** and **weight** parameters are used to determine at what priority level and at which weight in the priority level that the child policer competes with other children (policers or other arbiters) for bandwidth.

The **no** form of this command is used to remove the parent association from all instances of the policer.

Parameters **{root |** *arbiter-name***}** — When the **parent** command is executed, either the keyword **root** or an *arbiter-name* must be specified.

Default **root**

root — The **root** keyword specifies that the policer is intended to become a child to the **root** arbiter where an instance of the policer is created. If the **root** arbiter does not exist, the policer will be placed in the orphan state.

arbiter-name — The *arbiter-name* parameter specifies that the policer is intended to become a child to one of the tiered arbiters with the given arbiter-name where an instance of the policer is created. If the specified arbiter-name does not exist, the policer will be placed in the orphan state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

weight *weight-within-level* — The **weight** *weight-within-level* keyword and parameter are optional when executing the **parent** command. When **weight** is not specified, a default level of 1 is used in the parent arbiters priority level. When **weight** is specified, the *weight-within-level* parameter must be specified as an integer value from 1 through 100.

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

parent

Syntax **parent** *scheduler-name* [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no parent

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue parent)
[Tree] (config>qos>qgrps>ing>qgrp>queue parent)

Full Context configure qos queue-group-templates egress queue-group queue parent
configure qos queue-group-templates ingress queue-group queue parent

Description This command defines an optional parent scheduler that further governs the available bandwidth given the queue aside from the queue's PIR setting. When multiple schedulers, policers (at egress only), and/or queues share a child status with the parent scheduler, the **weight** or **level** parameters define how this queue contends with the other children for the parent's bandwidth.

Checks are not performed to see if a *scheduler-name* exists when the parent command is defined on the queue. Scheduler names are configured in the config>qos>scheduler-policy>tier *level* context. Multiple schedulers can exist with the *scheduler-name* and the association pertains to a scheduler that should exist on the egress SAP as the policy is applied and the queue created. When the queue is created on the egress SAP, the existence of the *scheduler-name* is dependent on a scheduler policy containing the *scheduler-name* being directly or indirectly applied (through a multiservice customer site) to the egress SAP. If the *scheduler-name* does not exist, the queue is placed in the orphaned operational state. The queue will accept packets but will not be bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP. The SAP that the queue belongs to must also depict an orphan queue status. The orphaned state of the queue is automatically cleared when the *scheduler-name* becomes available on the egress SAP.

The parent scheduler can be made unavailable due to the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the queue enters the orphaned state and automatically returns to normal operation when the parent scheduler is available again.

When a parent scheduler is defined without specifying weight or strict parameters, the default bandwidth access method is weight with a value of 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and returns without an error. When a parent association has been removed, the former child queue attempts to operate based on its configured rate parameter. Removing the parent association on the queue within the policy takes effect immediately on all queues using the SAP egress QoS policy.

Parameters *scheduler-name* — The defined *scheduler-name* conforms to the same input criteria as the schedulers defined within a scheduler policy. Scheduler names are configured in the config>qos>scheduler-policy>tier *level* context. There are no checks performed at the time of definition to ensure that the *scheduler-name* exists within an existing scheduler policy. For the queue to use the defined *scheduler-name*, the scheduler exists on each egress SAP the queue is eventually created on. For the duration where *scheduler-name* does not exist on the egress SAP, the queue operates in an orphaned state.

Values Any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

weight *weight* — *weight* defines the relative weight of this queue in comparison to other child schedulers and queues while vying for bandwidth on the parent *scheduler-name*. Any queues or schedulers defined as weighted receive no parental bandwidth until all policers, queues, and schedulers with a higher (numerically larger) priority on the parent have reached their maximum bandwidth or are idle.

All **weight** values from all weighted active queues, policers, and schedulers with a common parent scheduler are added together. Then, each individual active weight is divided by the total, deriving the percentage of remaining bandwidth provided to the queue, policer, or scheduler. A weight is considered to be active when the pertaining queue or scheduler has not reached its maximum rate and still has packets to transmit. All child policers, queues, and schedulers with a weight of 0 are considered to have the lowest priority level and are not serviced until all non-zero weighted queues, policers, and schedulers at that level are operating at the maximum bandwidth or are idle.

Values 0 to 100

Default 1

level *level* — The optional **level** parameter defines the level of hierarchy when compared to other schedulers and queues when vying for bandwidth on the parent *scheduler-name*. Queues or schedulers will not receive parental bandwidth until all queues and schedulers with a higher (numerically larger) priority on the parent have reached their maximum bandwidth or are idle.

Children of the parent scheduler with a lower strict priority will not receive bandwidth until all children with a higher strict priority have either reached their maximum bandwidth or are idle. Children with the same strict level are serviced relative to their weights.

Values 1 to 8

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-weight *cir-weight* — Specifies the weight the queue or scheduler will use at the within-CIR port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 100

Default 1

cir-level *cir-level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its within-CIR offered-load. If the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms All

parent

Syntax **parent** *scheduler-name* [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no parent

Context **[Tree]** (config>qos>scheduler-policy>tier>scheduler parent)

Full Context configure qos scheduler-policy tier scheduler parent

Description This command defines an optional parent scheduler that is higher up the policy hierarchy. Only schedulers in tier levels 2 and 3 can have a parental association. When multiple schedulers, policers (at egress only), and/or queues share a child status with the scheduler on the parent, the weight or strict parameters define how this scheduler contends with the other children for the parent's bandwidth. The parent scheduler can be removed or changed at any time and is immediately reflected on the schedulers created by association of this scheduler policy.

When a parent scheduler is defined without specifying weight or strict parameters, the default bandwidth access method is weight with a value of 1.

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and returns without an error. When a parent association has been removed, the former child scheduler attempts to operate based on its configured rate parameter. Removing the parent association on the scheduler within the policy will take effect immediately on all schedulers with *scheduler-name* that have been created using the *scheduler-policy-name*.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *scheduler-name* — Specifies a scheduler name. The *scheduler-name* must already exist within the context of the scheduler policy in a tier that is higher (numerically lower).

Values Any valid *scheduler-name* existing on a higher tier within the scheduler policy.

weight *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict level defined by the **level** parameter. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the queue or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit.

A zero (0) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

Default 1

level *level* — Specifies the strict priority level of this scheduler in comparison to other child schedulers and queues vying for bandwidth on the parent scheduler-name during the above-CIR distribution phase of bandwidth allocation. During the above-CIR distribution phase, any queues or schedulers defined at a lower strict level receive no parental bandwidth until all queues and schedulers defined with a higher (numerically larger) strict level on the parent have reached their maximum bandwidth or have satisfied their offered load requirements.

When the similar **cir-level** parameter default (undefined) are retained for the child scheduler, bandwidth is only allocated to the scheduler during the above-CIR distribution phase.

Children of the parent scheduler with a lower strict priority level will not receive bandwidth until all children with a higher strict priority level have either reached their maximum bandwidth or are idle. Children with the same strict level are serviced in relation to their relative weights.

Values 1 to 8

Default 1

cir-weight *cir-weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same **cir-level** defined by the **cir-level** parameter. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the queue or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit.

A zero (0) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-level *cir-level* — Specifies the strict priority CIR level of this scheduler in comparison to other child schedulers and queues vying for bandwidth on the parent *scheduler-name* during the within-CIR distribution phase of bandwidth allocation. During the within-CIR distribution phase, any queues or schedulers defined at a lower strict CIR level receive no parental bandwidth until all queues and schedulers defined with a higher (numerically larger) strict CIR level on the parent have reached their CIR bandwidth or have satisfied their offered load requirements.

If the scheduler's **cir-level** parameter retains the default (undefined) state, bandwidth is only allocated to the scheduler during the above-CIR distribution phase.

Children with the same strict cir-level are serviced according to their cir-weight.

Values 0 to 8

Default 0

Platforms All

parent

Syntax **parent** [**weight** *weight*] [**cir-weight** *cir-weight*]
no parent

Context **[Tree]** (config>service>cust>multi-service-site>ingress>sched-override>scheduler parent)
[Tree] (config>service>cust>multi-service-site>egress>sched-override>scheduler parent)

Full Context configure service customer multi-service-site egress scheduler-override scheduler parent
configure service customer multi-service-site ingress scheduler-override scheduler parent

Description This command overrides the scheduler's parent weight and CIR weight information. The weights apply to the associated level or cir-level configured in the applied scheduler policy. The scheduler name must exist in the scheduler policy applied to the ingress or egress of the SAP or multi-service site.

The override weights are ignored if the scheduler does not have a **parent** command configured in the scheduler policy. This allows the parent of the scheduler to be removed from the scheduler policy without having to remove all of the SAP/MSS overrides. If the parent scheduler does not exist causing the configured scheduler to be fostered on an egress port scheduler, the override weights will be ignored and the default values used; this avoids having non-default weightings for fostered schedulers.

The **no** form of the command returns the scheduler's parent weight and CIR weight to the value configured in the applied scheduler policy.

Default no parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *weight* — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same strict **level** defined by the level parameter in the applied scheduler policy. Within the level, all weight values from active children at that level are summed and the ratio of each active child's weight to the total is used to distribute the available bandwidth at that level. A weight is considered to be active when the policer, queue or scheduler the weight pertains to has not reached its maximum rate and still has packets to transmit. A 0 (zero) weight value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict level.

Values 0 to 100

Default 1

cir-weight — Specifies the relative weight of this scheduler in comparison to other child schedulers and queues at the same *cir-level* defined by the **cir-level** parameter in the applied scheduler policy. Within the strict **cir-level**, all **cir-weight** values from active children at that level are summed and the ratio of each active child's **cir-weight** to the total is used to distribute the available bandwidth at that level. A **cir-weight** is considered to be active when the policer, queue or scheduler that the **cir-weight** pertains to has not reached the CIR and still has packets to transmit. A 0 (zero) **cir-weight** value signifies that the child scheduler will receive bandwidth only after bandwidth is distributed to all other non-zero weighted children in the strict cir-level.

Values 0 to 100

Default 0

Platforms All

20.43 parent-location

parent-location

Syntax **parent-location** {**default** | **sla**}
no parent-location

Context **[Tree]** (config>qos>sap-egress parent-location)

Full Context configure qos sap-egress parent-location

Description This command determines the expected location of the parent schedulers for queues configured with a parent command within the sap-egress policy. All parent schedulers must be configured within a scheduler-policy applied at the location corresponding to the parent-location parameter.

If a parent scheduler name does not exist at the specified location, the queue will not be parented and will be orphaned.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Default parent-location default

Parameters **default** — When the sap-egress policy is applied to an sla-profile for a subscriber, the parent schedulers of the queues need to be configured in the scheduler-policy applied to the subscriber's sub-profile.

When the sap-egress policy is applied to a SAP, the parent schedulers of the queues need to be configured in the scheduler-policy applied to the SAP or the multiservice site.

sla — When the sap-egress policy is applied to an sla-profile for a subscriber, the parent schedulers of the queues need to be configured in the scheduler-policy applied to the same sla-profile.

If this parameter is configured within a sap-egress policy that is applied to any object except of the egress of an sla-profile, the configured parent schedulers will not be found and so the queues will not be parented and will be orphaned. This parameter is not supported when **policers-hqos-manageable** is configured in the SAP egress QoS policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

parent-location

Syntax **parent-location** {**none** | **sub** | **vport**}
no parent-location

Context **[Tree]** (config>qos>scheduler-policy>tier parent-location)

Full Context configure qos scheduler-policy tier parent-location

Description This command determines the expected location of the parent schedulers for the tier 1 schedulers configured with a parent command within the scheduler-policy. The parent schedulers must be configured within a scheduler-policy applied at the location corresponding to the parent-location parameter.

If a parent scheduler name does not exist at the specified location, the schedulers will not be parented and will be orphaned.

The configuration of **parent-location** and **frame-based-accounting** in a scheduler policy is mutually exclusive in order to ensure consistency between the different scheduling levels.

The **no** form of this command reverts to the default.

Default parent-location none

Parameters **none** — This parameter indicates that the tier 1 schedulers do not have a parent scheduler and the configuration of the parent under a tier 1 scheduler is blocked. Conversely, this parameter is blocked when any tier 1 scheduler has a parent configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub — When the scheduler-policy is applied to an sla-profile for a subscriber, the parent schedulers of the tier 1 schedulers need to be configured in the scheduler-policy applied to the subscriber's sub-profile.

If this parameter is configured within a scheduler-policy that is applied to any object except for the egress of an sla-profile, the configured parent schedulers will not be found and so the tier 1 schedulers will not be parented and will be orphaned.

vport — When the scheduler-policy is applied to an sla-profile, a sub-profile for a subscriber, or to the egress of a pseudowire SAP, the parent schedulers of the tier 1 schedulers need to be configured in the scheduler-policy applied to the Vport to which the subscriber will be assigned.

If this parameter is configured within a scheduler-policy that is applied to any object except for the egress of an sla-profile or sub-profile, or to the egress of a PW SAP, the configured parent schedulers will not be found and so the tier 1 schedulers will not be parented and will be orphaned.

Platforms All

20.44 parent-mid-pool

parent-mid-pool

Syntax **parent-mid-pool** *mid-pool-id*
no parent-mid-pool

Context **[Tree]** (config>qos>hs-port-pool-policy>alt-port-class-pools>class-pool parent-mid-pool)
[Tree] (config>qos>hs-port-pool-policy>std-port-class-pools>class-pool parent-mid-pool)

Full Context configure qos hs-port-pool-policy alt-port-class-pools class-pool parent-mid-pool
configure qos hs-port-pool-policy std-port-class-pools class-pool parent-mid-pool

Description This command creates the buffer allocation mapping between the associated class pool and the specified mid-pool. Use care when selecting a mid-pool in an active state (properly mapped to a root-pool with a non-zero allocation percentage). If a port-class pool is parented by an inactive mid-pool, the queues using the port-class pool are forced into an operational MBS setting of 0, causing all packet to be discarded. A port-class pool can be made inactive (no available buffers) by executing **parent-mid-pool none** in the port-class pool context.

The **no** form of the command reverts to the class-pool parenting value. For the standard port-class pools, this default is 1. For alternate port-class pools the default is none.

Default alt-port-class-pools: none

std-port-class-pools: 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mid-pool-id* — Specifies the mid-pool identifier in the HS pool policy. Either a valid mid-pool ID or **none** must be specified when executing the **parent-mid-pool** command. The *mid-pool-id* parameter defines the parent mid-pool to which the port-class is associated. The **none** keyword deactivates the port-class pool, causing the pool to have a zero size. A queue can still map to an inactive port-class pool although all packets are discarded by the queue.

Values 1 to 16, none

Platforms 7750 SR-7/12/12e

20.45 parent-root-pool

parent-root-pool

Syntax **parent-root-pool** *root-pool-id*
no parent-root-pool

Context **[Tree]** (config>qos>hs-pool-policy>mid-tier>mid-pool parent-root-pool)

Full Context configure qos hs-pool-policy mid-tier mid-pool parent-root-pool

Description This command creates a buffer allocation mapping between the associated **mid-pool** *mid-pool-id* and the specified **parent-root-pool** *root-pool-id*. The specified root pool ID must have a non-zero allocation-weight or the command fails. After a mid-pool is successfully associated with a root-pool, the parent root-pool's **allocation-weight** value cannot be set to zero.

When the *root-pool-id* is set to **none**, no buffers are assigned to the mid-tier pool.

The **no** form of the command reverts to the default.

Default parent-root-pool 1

Parameters *root-pool-id* — Specifies the parent root pool to which the mid-pool is associated. This parameter is required when executing the **parent-root-pool** command.

Values 1 to 16, none

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.46 participant-id

participant-id

Syntax **participant-id** *participant-id*
no participant-id

Context **[Tree]** (config>app-assure>group>http-error-redirect participant-id)

Full Context configure application-assurance group http-error-redirect participant-id

Description This command specifies a 32-character string assigned to the operator by Barefruit. It is used by barefruit landing servers (applies to template # 1 only).

Default no participant-id

Parameters *participant-id* — Specifies the 32-character string supplied by Barefruit.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.47 participate

participate

Syntax [**no**] **participate**

Context **[Tree]** (config>router>isis>flex-algos>flex-algo participate)

Full Context configure router isis flexible-algorithms flex-algo participate

Description This command enables IS-IS participation in a specific flexible algorithm.

The router advertises its capability to participate in a specific flexible algorithm within the IS-IS router-capability TLV. Router participation in a flexible algorithm assumes that segment routing and, consequently the **advertise-router-capability area** is enabled. However, a router only advertises flexible algorithm participation when it can support the corresponding winning flexible algorithm definition. The flexible algorithm participation is not enabled by default.

The **no** form of this command disables participation for a particular flexible algorithm.

Default no participate

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

participate

Syntax [**no**] **participate**

Context **[Tree]** (config>router>ospf>flex-algos>flex-algo participate)

Full Context configure router ospf flexible-algorithms flex-algo participate

Description This command enables OSPFv2 participation in a specific flexible algorithm.

The router advertises its capability to participate in a specific flexible algorithm within the OSPFv2 SR algorithm TLV of the router information opaque LSA. Router participation in a flexible algorithm assumes that segment routing and, consequently, the **advertise-router-capability area** is enabled. However, a router only advertises flexible algorithm participation when it can support the corresponding winning flexible algorithm definition. The flexible algorithm participation is not enabled by default.

The **no** form of this command disables participation for a specific flexible algorithm.

Default no participate

Platforms All

20.48 partitions

partitions

Syntax [**no**] **partitions**

Context **[Tree]** (config>isa>aa-grp partitions)

Full Context configure isa application-assurance-group partitions

Description This command enables partitions within an ISA-AA group. When enabled, partitions can be created.

The **no** form of this command disables partitions within an ISA-AA group.

Default no partitions

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.49 partner-down-delay

partner-down-delay

Syntax **partner-down-delay** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no partner-down-delay

Context **[Tree]** (config>router>dhcp>server>failover partner-down-delay)
[Tree] (config>router>dhcp>server>pool>failover partner-down-delay)
[Tree] (config>service>vprn>dhcp>server>failover partner-down-delay)
[Tree] (config>service>vprn>dhcp>server>pool>failover partner-down-delay)
[Tree] (config>router>dhcp6>server>failover partner-down-delay)
[Tree] (config>router>dhcp6>server>pool>failover partner-down-delay)
[Tree] (config>service>vprn>dhcp6>server>failover partner-down-delay)
[Tree] (config>service>vprn>dhcp6>server>pool>failover partner-down-delay)

Full Context configure router dhcp local-dhcp-server failover partner-down-delay
configure router dhcp local-dhcp-server pool failover partner-down-delay
configure router dhcp6 local-dhcp-server failover partner-down-delay
configure router dhcp6 local-dhcp-server pool failover partner-down-delay
configure service vprn dhcp local-dhcp-server failover partner-down-delay
configure service vprn dhcp local-dhcp-server pool failover partner-down-delay
configure service vprn dhcp6 local-dhcp-server failover partner-down-delay
configure service vprn dhcp6 local-dhcp-server pool failover partner-down-delay

Description This command configures the partner down delay time. Since the DHCP lease synchronization failure can be caused by the failure of the intercommunication link (and not necessary the entire node), there is a possibility the redundant DHCP servers become isolated in the network. In other words, they can serve DHCP clients but they cannot synchronize the lease. This can lead to duplicate assignment of IP addresses, since the servers have configured overlapping IP address ranges but they are not aware of each other's leases.

The purpose of the partner down delay is to prevent the IP lease duplication during the intercommunication link failure by not allowing new IP addresses to be assigned from the remote IP address range. This timer is intended to provide the operator with enough time to remedy the failed situation and to avoid duplication of IP addresses or prefixes during the failure.

During the partner-down-delay time, the prefix designated as remote is eligible only for renewals of the existing DHCP leases that have been synchronized by the peering node. Only after the sum of the partner-down-delay and the maximum-client-lead-time will the prefix designated as remote be eligible for delegation of the new DHCP leases. When this occurs, we say that the remote IP address range has been taken over.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

It is possible to expedite the takeover of a remote IP address range so that the new IP leases can start being delegated from that range shortly after the intercommunication failure is detected. This can be achieved by configuring the partner-down-delay timer to 0 seconds, along with enabling the ignore-mclt-on-takeover CLI flag. Caution must be taken before enabling this functionality. It is safe to bypass safety timers (partner-down-delay + MCLT) only in cases where the operator is certain that the intercommunication between the nodes has failed due to the entire node failure and not due to the intercommunication (MCS) link failure. Failed intercommunication due to the nodal failure would ensure that only one node is present in the network for IP address delegation (as opposed to two isolated nodes with overlapping IP address ranges where address duplication can occur). For this reason, the operator must ensure that there are redundant paths between the nodes to ensure uninterrupted synchronization of DHCP leases.

In access-driven mode of operation, partner-down-delay has no effect.

The **no** form of this command reverts to the default.

Default partner-down-delay hrs 23 min 59 sec 59

Parameters *partner-down-delay* — Specifies the partner down delay time.

Values

hrs *hours*	1 to 23
min *minutes*	1 to 59
sec *seconds*	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.50 passive

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy passive)

Full Context configure subscriber-mgmt bgp-peering-policy passive

Description This command enables the passive mode for the BGP neighbors.

The **no** form of this command disables the passive mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>service>vprn>bgp>group passive)
[Tree] (config>service>vprn>bgp>group>neighbor passive)

Full Context configure service vprn bgp group neighbor passive
configure service vprn bgp group passive

Description This command enables passive mode for the BGP group or neighbor.

When in passive mode, BGP will not attempt to actively connect to the configured BGP peers but responds only when it receives a connect open request from the peer.

The **no** form of this command used at the group level disables passive mode where BGP actively attempts to connect to its peers.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no passive — BGP will actively try to connect to all the configured peers.

Platforms All

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>service>vprn>isis>if passive)
[Tree] (config>service>vprn>isis>if>level passive)

Full Context configure service vprn isis interface level passive
configure service vprn isis interface passive

Description This command adds the passive attribute which causes the interface to be advertised as an IS-IS interface without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interfaces at the level that they are configured.

When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS protocol PDUs and does not transmit IS-IS protocol PDUs.

The **no** form of this command removes the passive attribute.

Default no passive

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>service>vprn>ospf>area>if passive)
[Tree] (config>service>vprn>ospf3>area>if passive)

Full Context configure service vprn ospf area interface passive
configure service vprn ospf3 area interface passive

Description This command adds the passive property to the OSPF interface where passive interfaces are advertised as OSPF interfaces but do not run the OSPF protocol.

By default, only interface addresses that are configured for OSPF are advertised as OSPF interfaces. The **passive** parameter allows an interface to be advertised as an OSPF interface without running the OSPF protocol.

While in passive mode, the interface ignores ingress OSPF protocol packets and does not transmit any OSPF protocol packets.

The **no** form of this command removes the passive property from the OSPF interface.

Default no passive

Platforms All

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>router>bgp>group passive)
[Tree] (config>router>bgp>group>neighbor passive)

Full Context configure router bgp group neighbor passive
configure router bgp group passive

Description Enables/disables passive mode for the BGP group or neighbor**.**

When in passive mode, BGP will not attempt to actively connect to the configured BGP peers but responds only when it receives a connect open request from the peer.

The **no** form of this command used at the group level disables passive mode where BGP actively attempts to connect to its peers.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no passive

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>router>isis>if passive)
[Tree] (config>router>isis>if>level passive)

Full Context configure router isis interface level passive
configure router isis interface passive

Description This command adds the passive attribute which causes the interface to be advertised as an IS-IS interface without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interfaces at the level that they are configured.

When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS protocol PDUs and does not transmit IS-IS protocol PDUs.

The **no** form of this command removes the passive attribute.

Default no passive

Platforms All

passive

Syntax [**no**] **passive**

Context **[Tree]** (config>router>ospf>area>interface passive)
[Tree] (config>router>ospf3>area>interface passive)

Full Context configure router ospf area interface passive
configure router ospf3 area interface passive

Description This command adds the passive property to the OSPF interface where passive interfaces are advertised as OSPF interfaces but do not run the OSPF protocol.

By default, only interface addresses that are configured for OSPF will be advertised as OSPF interfaces. The **passive** parameter allows an interface to be advertised as an OSPF interface without running the OSPF protocol.

While in passive mode, the interface will ignore ingress OSPF protocol packets and not transmit any OSPF protocol packets.

The **no** form of this command removes the passive property from the OSPF interface.

Default no passive

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.51 passive-mode

passive-mode

Syntax [**no**] **passive-mode**

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ep passive-mode)

Full Context configure redundancy multi-chassis peer mc-endpoint passive-mode

Description This command configures the passive mode behavior for the MC-EP protocol. When in passive mode the MC-EP pair will be dormant until two of the pseudowires in a MC-EP will be signaled as active by the remote PEs, being assumed that the remote pair is configured with regular MC-EP. As soon as more than one pseudowire is active, dormant MC-EP pair will activate. It will use the regular exchange to select the best pseudowire between the active ones and it will block the Rx and Tx directions of the other pseudowires.

The **no** form of this command will disable the passive mode behavior.

Default no passive-mode

Platforms All

20.52 passkey

passkey

Syntax **passkey** *passkey*

Context **[Tree]** (config>system>bluetooth passkey)

Full Context configure system bluetooth passkey

Description This command is used to define the Bluetooth pass key that is used during paring. This passkey must match in both devices attempting the pairing operation.

Default passkey 123456

Parameters *passkey* — Must be six digits.

Values 000000 to 999999

Platforms 7750 SR-1, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.53 password

password

Syntax **password** {**ignore** | **chap** *password* | **pap** *password*} [**hash** | **hash2** | **custom**]
no password

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host password)

Full Context configure subscriber-mgmt local-user-db ppp host password

Description This command specifies a password type or configures password string for **pap** or **chap**. The pap and chap passwords are stored in a hashed format in the config files. The **hash|hash2** optional keywords are used for config execution.

This command will only be interpreted if the local user database is connected directly to the PPPoE node under the VPRN/IES group interface. It is not used if the local user database is accessed by a local DHCP server.

The **no** form of this command reverts to the default.

Parameters **ignore** — Specifies that the password be ignored, in which case authentication is always succeed, independent of the password used by the PPPoE client. The client must still perform authentication.

chap *password* — Specifies that the password, up to 64 characters, for Challenge-Handshake Authentication Protocol) (CHAP) is used. Only a password received with the CHAP protocol is accepted.

pap *password* — Specifies that the Password Authentication Protocol (PAP) is used, up to 64 characters. Only a password received with the PAP protocol is accepted, even though the CHAP protocol is proposed to the client first because it is unknown at the time of the offer which password type is allowed to the client.

hash | hash2 — Specifies hashing scheme.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *password* [{**hash** | **hash2** | **custom**}]
no password

Context **[Tree]** (config>router>l2tp password)
[Tree] (config>router>l2tp>group password)
[Tree] (config>router>l2tp>group>tunnel password)
[Tree] (config>router>l2tp>l2tpv3 password)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>l2tp>group>l2tpv3 password)
[Tree] (config>service>vprn>l2tp password)
[Tree] (config>service>vprn>l2tp>l2tpv3 password)
[Tree] (config>service>vprn>l2tp>group password)
[Tree] (config>service>vprn>l2tp>group>l2tpv3 password)
[Tree] (config>service>vprn>l2tp>group>tunnel password)

Full Context configure router l2tp group l2tpv3 password
configure router l2tp group password
configure router l2tp group tunnel password
configure router l2tp l2tpv3 password
configure router l2tp password
configure service vprn l2tp group l2tpv3 password
configure service vprn l2tp group password
configure service vprn l2tp group tunnel password
configure service vprn l2tp l2tpv3 password
configure service vprn l2tp password

Description This command configures the password between L2TP LAC and LNS

The **no** form of this command removes the password.

Default no password

Parameters *password* — Configures the password used for challenge/response calculation and AVP hiding. The maximum length is up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *password* [**hash** | **hash2** | **custom**]
no password

Context [Tree] (config>service>dynsvc>plcy>auth password)

Full Context configure service dynamic-services dynamic-services-policy authentication password

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the password to be used for RADIUS authentication of data-triggered dynamic services.

The **no** form of this command removes the password from the configuration.

Parameters *password* — Specifies the password that is used in RADIUS authentication of a data-triggered dynamic service. The maximum length is 20 characters if unhashed, 32 characters if hashed, and 54 characters if the **hash2** keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *password* [**hash** | **hash2**| **custom**]
no password

Context **[Tree]** (config>subscr-mgmt>auth-policy password)

Full Context configure subscriber-mgmt authentication-policy password

Description This command sets a password that is sent with **user-name** in every RADIUS authentication request sent to the RADIUS server upon receipt of DHCP discover or request messages. If no password is configured, no password AVP is sent.

The **no** form of this command reverts to the default value.

Parameters *password* — Specifies a text string containing the password. Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

hash — Specifies that the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *password* [**hash** | **hash2** | **custom**]
no password

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>nasreq password)

Full Context configure subscriber-mgmt diameter-application-policy nasreq password

Description This command sets a password that is sent with **user-name** in every RADIUS authentication request sent to the RADIUS server upon receipt of DHCP discover or request messages. If no password is provided, an empty password is sent.

The **no** form of this command reverts to the default value.

Parameters *password* — Specifies a text string containing the password. Allowed values are any string up to 64 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

hash — Specifies that the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *password* [**hash** | **hash2** | **custom**]
no password

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>aaa>route-downloader password)

Full Context configure aaa route-downloader password

Description This command specifies the password that is used in the RADIUS access requests.

The **no** form of this command resets the password to the default which is an empty string.

Parameters *password* — Specifies a password string up to 32 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *password* [**hash** | **hash2**| **custom**]
no password

Context [Tree] (config>aaa>radius-srv-plcy>servers>health-check>test-account password)
[Tree] (config>subscr-mgmt>vrgw>brg>brg-profile>radius-authentication password)

Full Context configure aaa radius-server-policy servers health-check test-account password
configure subscriber-mgmt vrgw brg brg-profile radius-authentication password

Description This command specifies the password that the test account will use to send access requests to probe the RADIUS servers.

Parameters *password* — Specifies the probing password up to 64 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password**

Context **[Tree]** (config>system>security password)

Full Context configure system security password

Description Commands in this context configure password-related parameters.

Platforms All

password

Syntax **password** *password* [**hash** | **hash2** | **custom**]
no password

Context **[Tree]** (config>ipsec>rad-auth-plcy password)

Full Context configure ipsec radius-authentication-policy password

Description This command specifies the password that is used in the RADIUS access requests.

The **no** form of this command resets the password to its default of **ALU** and will be stored using hash/hash2 encryption.

Default no password

Parameters *password* — Specifies a password string up to 64characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

password

Syntax **password** *password* [**hash** | **hash2** | **custom**]
no password

Context **[Tree]** (config>aaa>isa-radius-plcy password)

Full Context configure aaa isa-radius-policy password

Description This command specifies the password that is used in the RADIUS access requests. It shall be specified as a string of up to 32 characters in length.

The **no** form of the command resets the password to its default of **ALU** and will be stored using hash/hash2 encryption.

Default no password

Parameters *password* — Specifies a password string up to 32 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

password

Syntax **password** *hex-string*
no password

Context **[Tree]** (config>li>x-interfaces>lics>lic>authentication password)

Full Context configure li x-interfaces lics lic authentication password

Description This command configures the password for the X1 and X2 interfaces.

The **no** form of this command reverts to the default.

Parameters *hex-string* — Specifies the password. Must contain exactly 32 hex nibbles.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

password

Syntax **password**

Context **[Tree]** (global password)

Full Context global password

Description This command changes a user's CLI login password.

When a user logs in after the administrator forces a **new-password-at-login,** or the password has expired (**aging**), then this command is automatically invoked.

When invoked, the user is prompted to enter the old password, the new password, and then the new password again to verify the correct input.

If a user fails to create a new password after the administrator forces a **new-password-at-login** or after the password has expired, the user is not allowed to access the CLI.

A user cannot configure a non-conformant password for themselves using the global **password** command. A password value that does not conform to the minimum-length or other password complexity rules can be configured using the **config>system>security>user>password** command (for example, by an administrator), but a warning is provided in the CLI. This allows, for example, an administrator to configure a non-conformant password for a user.

password

Syntax **password** [*password*]

Context **[Tree]** (config>system>security>user password)

Full Context configure system security user password

Description This command configures the user password for console and FTP access.

The password is stored in an encrypted format in the configuration file when specified. Passwords should be encased in double quotes (" ") at the time of the password creation. The double quote character (") is not accepted inside a password. It is interpreted as the start or stop delimiter of a string.

The password can be entered as plain text or a hashed value. SR OS can distinguish between hashed passwords and plain text passwords and take the appropriate action to store the password correctly.

```
config>system>security>user# password testuser1
```

The password is hashed by default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For example:

```
config>system>security# user testuser1
config>system>security>user$ password xyzabcd1
config>system>security>user# exit


config>system>security# info
------------------------------------
...
            user "testuser1"
                password "$2y$10$pFoehOg/tCbBMPDJ/
kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK"
            exit
...
------------------------------------
config>system>security#
```

The **password** command allows you also to enter the password as a hashed value.

For example:

```
config>system>security# user testuser1
config>system>security>user$ password "$2y$10$pFoehOg/tCbBMPDJ/
kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK"
config>system>security>user# exit
config>system>security# info
------------------------------------
...
user "testuser1"
password "$2y$10$pFoehOg/tCbBMPDJ/kqpu.8af0AoVGY2xsR7WFqyn5fVTnwRzGmOK"
exit
...
------------------------------------
config>system>security#
```

Parameters *password* — This is the password for the user that must be entered by this user during the login procedure. The minimum length of the password is determined by the **minimum-length** command. The maximum length can be up to 20 chars if unhashed, 32 characters if hashed. The complexity requirements for the password is determined by the **complexity-rules** command and must be followed; otherwise, the password will not be accepted.

All password special characters (#, $, spaces, and so on) must be enclosed within double quotes.

For example: config>system>security>user# password “south#bay?”

The question mark character (?) cannot be directly inserted as input during a telnet connection because the character is bound to the **help** command during a normal Telnet/console connection.

To insert a # or ? characters, they must be entered inside a notepad or clipboard program and then cut and pasted into the Telnet session in the password field that is encased in the double quotes as delimiters for the password.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a **password** is entered without any parameters, a password length of zero is implied: (carriage return).

Platforms All

password

Syntax **password** *password* [**hash** | **hash2** | **custom**]
no password

Context **[Tree]** (bof password)

Full Context bof password

Description This command configures the password to access the BOF interactive menu at startup.

If a password is configured, the BOF interactive menu is accessible only when the correct password is entered. If the correct password is not entered in 30 s, the node reboots.

The **no** form of this command removes the configured password.

Default no password

Parameters *password* — Specifies the password.

If the **hash**, **hash2**, or **custom** parameter is not configured, the password is entered in plaintext and the password length must be between 8 and 32 characters. A plaintext password cannot contain embedded nulls or end with “ hash”, “ hash2”, or “ custom”.

If the **hash**, **hash2**, or **custom** parameter is configured, the password is hashed and the password length must be between 1 and 64 characters.

hash — Keyword to specify that the password is entered in an encrypted form.

hash2 — Keyword to specify that the password is entered in a more complex encrypted form. The **hash2** encryption scheme is node-specific and the password cannot be transferred between nodes.

custom — Keyword to specify that the password uses custom encryption.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.54 password-history

password-history

Syntax **password-history** {**user** *user-name* | **all**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (admin>clear password-history)

Full Context admin clear password-history

Description This command is used to clear old passwords used by a specific user, or for all users.

Parameters *user-name* — Clears the password history information about the specified user, up to 32 characters.

all — Clears the password history information for all users.

Platforms All

20.55 pat-repetition

pat-repetition

Syntax **pat-repetition** [**tnc** *tnc-milli-seconds* **qos** *qos-milli-seconds* **poa** *poa-milli-seconds*]
no pat-repetition

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms pat-repetition)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms pat-repetition)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms pat-repetition)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms pat-repetition
configure mcast-management multicast-info-policy bundle channel video analyzer alarms pat-repetition
configure mcast-management multicast-info-policy bundle video analyzer alarms pat-repetition

Description This command configures the analyzer to check for the program association table (PAT). It is expected that the PAT arrives periodically within a certain interval range. It is possible to configure the type of alarm that is raised when the PAT fails to arrive within the specified interval. As the delay increases between two consecutive PATs, the type of alarm raised becomes more critical, from TNC to POA.

Default no pat-repetition

Parameters *tnc-milli-seconds* — Specifies the time, in milliseconds, for which a TNC alarm is raised if the interval between two consecutive PATs is greater than or equal to this configured value.

Values 100 to 800 in multiples of 100 only

Default 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos-milli-seconds — Specifies the time, in milliseconds, for which a QoS alarm is raised if the interval between two consecutive PATs is greater than or equal to this configured value.

Values 200 to 900 in multiples of 100 only and higher than the *tnc-milli-seconds* value

Default 200

poa-milli-seconds — Specifies the time, in milliseconds, for which a POA alarm is raised if the interval between two consecutive PATs is greater than or equal to this configured value.

Values 300 to 1000 in multiples of 100 only and higher than the *qos-milli-seconds* value

Default 500

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.56 pat-syntax

pat-syntax

Syntax [**no**] **pat-syntax**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms pat-syntax)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms pat-syntax)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms pat-syntax)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms pat-syntax
configure mcast-management multicast-info-policy bundle channel video analyzer alarms pat-syntax
configure mcast-management multicast-info-policy bundle video analyzer alarms pat-syntax

Description This command configures the analyzer to check for PAT syntax errors.

Default no pat-syntax

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.57 path

path

Syntax **path xc-a** *lag-id* **xc-b** *lag-id*
path pxc *pxc-id*
no path

Context **[Tree]** (config>fwd-path-ext>fpe path)

Full Context configure fwd-path-ext fpe path

Description This command references a PXC (pair of PXC sub-ports) and consequently create an association between the PXC and the application which is referenced under the same FPE object. Each application will utilize the PXC in the form of an internal cross-connect. The exact use and internal provisioning of this cross-connect depends on the application itself.

The **no** form of this command removes the reference and association from the configuration.

Default no path

Parameters **xc-a** *lag-id* — Specifies the LAG identifier associated with one side of the cross-connect. The operator has the freedom to associate **xc-a** with LAG ID containing either sub-ports.a or sub-ports.b. In other words, the system does not perform automatic check that will ensure a match between **xc-a** and the LAG ID containing sub-ports.a.

Values 1 to 800

xc-b *lag-id* — Specifies the LAG identifier associated with one side of the cross-connect. The operator has the freedom to associate **xc-a** with LAG ID containing either sub-ports.a or sub-ports.b.

Values 1 to 800

pxc-id — Specifies the PXC identifier, the PXC construct that contains a physical port in a loopback mode that provides the cross-connect capability. The system creates two paired sub-ports on top of this physical port and each of these two sub-ports forwards traffic in one direction over the loopback. One sub-port is associated with the transit side of the loopback, while the other sub-port is associated with the termination side (see PXC Configuration Guides for further explanation).

Values 1 to 64

Platforms All

path

Syntax **path** *path-id* **pxc** *pxc-id*
path *path-id* **xc-a** *lag-id* **xc-b** *lag-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no path *path-id*

Context **[Tree]** (config>fwd-path-ext>fpe>multi-path-list path)

Full Context configure fwd-path-ext fpe multi-path-list path

Description This command configures a multipath FPE forwarding path. A single path in a multipath FPE can contain a single PXC port or LAG of PXC ports.

The PXC references a physical port in loopback mode that provides the cross-connect capability. The system creates two paired subports on top of the physical port, each of which forwards traffic in one direction over the loopback. One subport is associated with the transit side of the loopback, while the other is associated with the termination side.

The **no** form of the command removes the path.

Parameters *path-id* — Specifies a path ID for the forwarding path.

Values 1 to 64

pxc-id — Specifies a dedicated PXC ID for the forwarding path.

Values 1 to 64

xc-a *lag-id* — Specifies the LAG ID associated with one side (transit or termination) of the cross-connect. The operator can associate **xc-a** with the LAG containing either subports.a or subports.b. The system does not enforce a match between **xc-a** and the LAG ID containing subports.a.

Values lag-[1 to 800]

xc-b *lag-id* — Specifies the LAG ID associated with the other side of the cross-connect (not designated for **xc-a**). The operator can associate **xc-b** with the LAG containing either subports.a or subports.b. The system does not enforce a match between **xc-b** and the LAG ID containing subports.b.

Values lag-[1 to 800]

Platforms All

path

Syntax [**no**] **path** [*sonet-sdh-index*]

Context **[Tree]** (config>port>sonet-sdh path)

Full Context configure port sonet-sdh path

Description This command defines the SONET/SDH path.

The **no** form of this command removes the specified SONET/SDH path.

This command is supported on TDM satellite.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default full channel (or clear channel)

Parameters *sonet-sdh-index* — Specifies the components making up the specified SONET/SDH path. Depending on the type of SONET/SDH port the *sonet-sdh-index* must specify more path indexes to specify the payload location of the path. The *sonet-sdh-index* differs for SONET and SDH ports.

Values sts192 (for the 7950 XRS only)
sts1-*x.x* (for the 7450 ESS and 7750 SR), tu3, vt2, vt15

SONET		SDH	
OC-192	STS-48-index	STM-64	AUG-16-index
	STS-12-index		AUG-4-index
	STS-3-index		AUG-1-index
	STS-1-index		AU-3-index
OC-48	STS-12-index	STM-16	AUG-4-index
	STS-3-index		AUG-1-index
	STS-1-index		AU-3-index
OC-12	STS-3-index	STM-4	AUG-1-index
	STS-1-index		AU-3-index
OC-3	STS-1-index	STM-1	AU-3-index

In addition the support of virtual tributary circuits adds an additional level of complexity and several addition levels of indexes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

path

Syntax [**no**] **path** *path-index*

Context **[Tree]** (config>eth-tunnel path)

Full Context configure eth-tunnel path

Description This command configures one of the two paths supported under the Ethernet tunnel.

The **no** form of this command removes the path from under the Ethernet tunnel. If this is the last path, the associated SAP need to be unconfigured before the path can be deleted.

Default no path

Parameters **path-index** — Specifies the identifier for the path.

Values 1 to 16

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

path

Syntax **path** *name*
no path

Context **[Tree]** (config>service>epipe>spoke-sdp-fec path)

Full Context configure service epipe spoke-sdp-fec path

Description This command specifies the explicit path, containing a list of S-PE hops, that should be used for this spoke SDP. The path-name should correspond to the name of an explicit path configured in the **config>service>pw-routing** context.

If no path is configured, then each next-hop of the MS-PW used by the spoke SDP will be chosen locally at each T-PE and S-PE.

Default no path

Parameters *name* — The name of the explicit path to be used, as configured under the **config>service>pw-routing** context.

Platforms All

path

Syntax **path** *path-index* **tag** *qtag*[.*qtag*]
no path *path-index*

Context **[Tree]** (config>service>epipe>sap>eth-tunnel path)
[Tree] (config>service>ipipe>sap>eth-tunnel path)

Full Context configure service epipe sap eth-tunnel path
configure service ipipe sap eth-tunnel path

Description This command configures Ethernet tunnel SAP path parameters.

The **no** form of this command removes the values from the configuration.

Parameters *path-index* — Specifies the path index value.

Values 1 to 16

qtag[.*qtag*] — Specifies the qtag value.

Values 0 to 4094 | *

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

path

Syntax **path** *path-index* **tag** *qtag*[.*qtag*]
no path *path-index*

Context **[Tree]** (config>service>vpls>sap>eth-tunnel path)

Full Context configure service vpls sap eth-tunnel path

Description This command configures Ethernet tunnel SAP path parameters.

The **no** form of this command removes the values from the configuration.

Parameters *path-index* — Specifies the path index value.

Values 1 to 16

tag *qtag*[.*qtag*] — Specifies the qtag value.

Values 0 to 4094, * (wildcard)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

path

Syntax **path** *path-name*
no path *path-name*

Context **[Tree]** (config>router>gmpls path)

Full Context configure router gmpls path

Description This command creates the path to be used for a GMPLS LSP. A path can be used by multiple GMPLS LSPs. A path can specify some or all hops from ingress to egress and they can be either strict or loose.

Paths are created in a **no shutdown** state. A path must be shut down before making any changes (adding or deleting hops) to the path. When a path is shut down, any GMPLS LSP using the path becomes operationally down.

The **no** form of this command deletes the path and all its associated configuration information. All the GMPLS LSPs that are currently using this path will be affected. A path must be shut down and unbound from all GMPLS LSPs using the path before it can be deleted. The **no path** *path-name* command will not result in any action except a warning message on the console indicating that the path may be in use.

Parameters *path-name* — Specifies a unique case-sensitive name label for the LSP path.

Values 32 characters maximum alphanumeric string

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

path

Syntax [**no**] **path**

Context **[Tree]** (debug>router>gmpls>event path)

Full Context debug router gmpls event path

Description This command enables and disables debugging for GMPLS Path events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

path

Syntax **path** [**detail**]
no path

Context **[Tree]** (debug>router>gmpls>packet path)

Full Context debug router gmpls packet path

Description This command enables debugging for GMPLS Path packets.

The **no** form of the command disables debugging for GMPLS Path packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

path

Syntax [**no**] **path** *path-name*

Context **[Tree]** (config>router>mpls path)

Full Context configure router mpls path

Description This command creates the path to be used for an LSP. A path can be used by multiple LSPs. A path can specify some or all hops from ingress to egress and they can be either **strict** or **loose**. A path can also be empty (no *path-name* specified) in which case the LSP is set up based on IGP (best effort) calculated shortest path to the egress router. Paths are created in a **shutdown** state. A path must be shutdown before making any changes (adding or deleting hops) to the path. When a path is shutdown, any LSP using the path becomes operationally down.

To create a strict path from the ingress to the egress router, the ingress and the egress routers must be included in the path statement.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the path and all its associated configuration information. All the LSPs that are currently using this path will be affected. Additionally all the services that are actively using these LSPs will be affected. A path must be **shutdown** and unbound from all LSPs using the path before it can be deleted. The **no path** *path-name* command will not result in any action except a warning message on the console indicating that the path may be in use.

Parameters *path-name* — Specifies a unique case-sensitive alphanumeric name label for the LSP path up to 32 characters in length.

Platforms All

path

Syntax **path** [**detail**]
no path

Context **[Tree]** (debug>router>rsvp>event path)

Full Context debug router rsvp event path

Description This command debugs path-related events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about path-related events.

Platforms All

path

Syntax **path** [**detail**]
no path

Context **[Tree]** (debug>router>rsvp>packet path)

Full Context debug router rsvp packet path

Description This command enables debugging for RSVP path packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about path-related events.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

path

Syntax **path** *name* [**create**]
no path *name*

Context **[Tree]** (config>service>pw-routing path)

Full Context configure service pw-routing path

Description This command configures an explicit path between this T-PE and a remote T-PE. For each path, one or more intermediate S-PE hops must be configured. A path can be used by multiple multi-segment pseudowires. Paths are used by a 7450 ESS, 7750 SR, or 7950 XRS T-PE to populate the list of Explicit Route TLVs included in the signaling of a dynamic MS-PW.

A path may specify all or only some of the hops along the route to reach a T-PE.

The **no** form of the command removes a specified explicit path from the configuration.

Parameters *path-name* — Specifies a locally-unique case-sensitive alphanumeric name label for the MS-PW path of up to 32 characters in length.

Platforms All

path

Syntax **path** {**a** | **b**} [{*port-id* | *lag-id*} **raps-tag** *qtag1*[.*qtag2*]]
no path {**a** | **b**}

Context **[Tree]** (config>eth-ring path)

Full Context configure eth-ring path

Description This command assigns the ring (major or sub-ring) path to a port and defines the Ring APS tag. Rings typically have two paths: a and b.

The **no** form of this command removes the path a or b.

Default no path

Parameters *port-id* — Specifies the port ID.

Values *slot*/*mda*/*port*

lag-id — Specifies the LAG ID.

Values **lag** — Keyword.
id — Specifies the LAG ID number.

raps-tag — Specifies the member encapsulation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qtag1 — Specifies the top or outer VLAN ID.

Values 1 to 4094

qtag2 — Specifies the bottom or inner VLAN ID.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

path

Syntax **path** *path-name* [**create**]
no path *name*

Context **[Tree]** (config>system>telemetry>sensor-groups>sensor-group path)

Full Context configure system telemetry sensor-groups sensor-group path

Description This command configures a sensor path for the specified sensor-group. Multiple sensor paths can be defined for a single sensor-group. The path is defined in the form of an XML Path (XPath) syntax that refers to single or multiple objects within the YANG model.

The **no** form of the command removes the specified explicit path from the configuration.

Parameters *path-name* — Specifies a sensor path, up to 512 characters.

create — Keyword used to create the sensor path.

Platforms All

20.58 path-b

path-b

Syntax [**no**] **path-b**

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring path-b)

Full Context configure redundancy multi-chassis peer mc-ring ring path-b

Description This command specifies the set of upper-VLAN IDs associated with the SAPs that belong to path B with respect to load-sharing. All other SAPs belong to path A.

Default If not specified, the default is an empty set.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.59 path-computation-method

path-computation-method

Syntax **path-computation-method** *path-computation-method*
no path-computation-method

Context **[Tree]** (config>router>mpls>lsp path-computation-method)
[Tree] (config>router>mpls>lsp-template path-computation-method)

Full Context configure router mpls lsp path-computation-method
configure router mpls lsp-template path-computation-method

Description This command configures the path computation method of a RSVP-TE or SR-TE LSP.

The user can select among the **hop-to-label** translation, the local CSPF or the PCE for a configured SR-TE LSP. For SR-TE LSP templates, the PCE option is supported with the SR-TE LSP template type **on-demand-p2p-srte** and not other template types.

The user can select among the IGP-based path, the local CSPF, or the PCE for a configured RSVP-TE LSP. The PCE option is not supported with the RSVP-TE LSP template.

By default, the IGP-based path is used for an RSVP-TE LSP and the **hop-to-label** path computation method is used for an SR-TE LSP.

The **no** form of this command returns to the default path computation method for the type of LSP.

Default no path-computation-method

Parameters *path-computation-method* — Specifies the path computation method for the LSP.

Values local-cspf — Selects the local router CSPF for path computation.
pce — Selects the PCE for path computation.

Platforms All

20.60 path-cost

path-cost

Syntax **path-cost** *sap-path-cost*
no path-cost [*sap-path-cost*]

Context **[Tree]** (config>service>vpls>sap>stp path-cost)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>template>vpls-sap-template>stp path-cost)
[Tree] (config>service>vpls>spoke-sdp>stp path-cost)

Full Context configure service template vpls-sap-template stp path-cost
configure service vpls sap stp path-cost
configure service vpls spoke-sdp stp path-cost

Description This command configures the Spanning Tree Protocol (STP) path cost for the SAP or spoke-SDP.

The path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that SAP or spoke-SDP. When BPDUs are sent out of other egress SAPs or spoke-SDPs, the newly calculated root path cost is used. These are the values used for CIST when running MSTP.

STP suggests that the path cost is defined as a function of the link bandwidth. Since SAPs and spoke-SDPs are controlled by complex queuing dynamics, in the 7450 ESS, 7750 SR, and 7950 XRS the STP path cost is a purely static configuration.

The **no** form of this command returns the path cost to the default value.

Parameters *path-cost* — The path cost for the SAP or spoke-SDP

Values 1 to 200000000 (1 is the lowest cost)

Default 10

Platforms All

path-cost

Syntax **path-cost** *sap-path-cost*
no path-cost

Context [Tree] (config>service>pw-template>stp path-cost)

Full Context configure service pw-template stp path-cost

Description This command configures the Spanning Tree Protocol (STP) path cost for the SAP or spoke SDP.

The path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that SAP or spoke SDP. When BPDUs are sent out other egress SAPs or spoke SDPs, the newly calculated root path cost is used. These are the values used for CIST when running MSTP.

STP suggests that the path cost is defined as a function of the link bandwidth. Since SAPs and spoke SDPs are controlled by complex queuing dynamics, the STP path cost is a purely static configuration.

The **no** form of this command returns the path cost to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default path-cost 10

Parameters *path-cost* — Specifies the path cost for the SAP or spoke SDP.

Values 1 to 200000000 (1 is the lowest cost)

Default 10

Platforms All

20.61 path-destination

path-destination

Syntax **path-destination** *ip-address* **interface** *if-name*
path-destination *ip-address* [**next-hop** *ip-address*]
no path-destination

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy path-destination)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy path-destination)

Full Context configure saa test type-multi-line lsp-ping sr-policy path-destination
configure saa test type-multi-line lsp-trace sr-policy path-destination

Description This command configures the IP address of the path destination from the range 127/8. When the LDP FEC prefix is IPv6, the user must enter a 127/8 IPv4 mapped IPv6 address, that is, in the range ::ffff:127/104.

The **no** form of this command removes the configuration.

Parameters *ip-address* — Specifies the IP address.

Values
ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

if-name — Specifies the name of an IP interface, up 32 characters, to send the MPLS echo request to. The name must already exist in the **config>router>interface** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.62 path-discovery

path-discovery

Syntax **path-discovery**

Context **[Tree]** (config>test-oam>ldp-treetrace path-discovery)

Full Context configure test-oam ldp-treetrace path-discovery

Description This command creates the context to configure the LDP ECMP OAM path discovery.

The ingress LER builds the ECMP tree for a given FEC (egress LER) by sending LSP Trace messages and including the LDP IPv4 Prefix FEC TLV as well as the downstream mapping TLV. It inserts an IP address range drawn from the 127/8 space. When received by the downstream LSR, it uses this range to determine which ECMP path is exercised by any IP address or a sub-range of addresses within that range based on its internal hash routine. When the MPLS Echo reply is received by the ingress LER, it records this information and proceeds with the next echo request message targeted for a node downstream of the first LSR node along one of the ECMP paths. The sub-range of IP addresses indicated in the initial reply is used since the objective is to have the LSR downstream of the ingress LER pass this message to its downstream node along the first ECMP path.

The user configures the frequency of running the tree discovery using the command **config>test-oam>ldp-treetrace>path-discovery>interval**.

The ingress LER gets the list of FECs from the LDP FEC database. New FECs are added to the discovery list at the next tree discovery and not when they are learned and added into the FEC database. The maximum number of FECs to be discovered with the tree building feature is limited to 500. The user can configure FECs to include or exclude using a policy profile by applying the command **config>test-oam>ldp-treetrace>path-discovery>policy-statement**.

Platforms All

20.63 path-excl

path-excl

Syntax [**no**] **path-excl**

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring path-excl)

Full Context configure redundancy multi-chassis peer mc-ring ring path-excl

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the set of upper-VLAN IDs associated with the SAPs that are to be excluded from control by the multi-chassis ring.

Default If not specified, the default is an empty set.

Platforms All

20.64 path-id

path-id

Syntax **path-id** {**lsp-num** *lsp-num* | **working-path** | **protect-path** [**src-global-id** *src-global-id*] **src-node-id** *src-node-id* **src-tunnel-num** *src-tunnel-num* [**dest-global-id** *dest-global-id*] **dest-node-id** *dest-node-id* [**dest-tunnel-num** *dest-tunnel-num*]}
no path-id

Context **[Tree]** (config>router>mpls>mpls-tp>transit-path path-id)

Full Context configure router mpls mpls-tp transit-path path-id

Description This command configures path ID for an MPLS-TP transit path at an LSR. The path ID is equivalent to the MPLS-TP LSP ID and is used to generate the maintenance entity group intermediate point (MIP) identifier for the LSP at the LSR. A path-id must be configured for on-demand OAM to verify an LSP at the LSR.

The path-id must contain at least the following parameters: **lsp-num, src-node-id, src-global-id, src-tunnel-num, dest-node-id**.

The path-id must be unique on a node. It is recommended that his is also configured to be a globally unique value.

The **no** form of this command removes the path ID from the configuration.

Default no path-id

Parameters *lsp-num* — Specifies the LSP number.

Values 1 to 65535, or **working path**, or **protect-path**. A **working-path** is equivalent to an lsp-num of 1, and a **protect-path** is an lsp-num of 2.

src-global-id — Specifies the source global ID.

Values 0 to 4294967295

src-node-id — Specifies the source node ID.

Values a.b.c.d or 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-tunnel-num — Specifies the source tunnel number.

Values 1 to 61440

dest-global-id — Specifies the destination global ID. If the destination global ID is not entered, then it is set to the same value as the source global ID.

Values 0 to 4294967295

dest-node-id — Specifies the destination node ID.

Values a.b.c.d or 1 to 4294967295

dest-tunnel-num — Specifies the destination tunnel number. If the destination tunnel number is not entered, then it is set to the same value as the source tunnel number.

Values 1 to 61440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.65 path-mtu

path-mtu

Syntax **path-mtu** [*bytes*]
no path-mtu *bytes*

Context **[Tree]** (config>service>sdp path-mtu)

Full Context configure service sdp path-mtu

Description This command configures the Maximum Transmission Unit (MTU) in bytes that the Service Distribution Point (SDP) can transmit to the far-end device router without packet dropping or IP fragmentation overriding the SDP-type default path-mtu.

The default SDP-type **path-mtu** can be overridden on a per SDP basis. Dynamic maintenance protocols on the SDP like RSVP may override this setting.

If the physical **mtu** on an egress interface or PoS channel indicates the next hop on an SDP path cannot support the current **path-mtu**, the operational **path-mtu** on that SDP will be modified to a value that can be transmitted without fragmentation.

The **no** form of this command removes any **path-mtu** defined on the SDP and the SDP will use the system default for the SDP type.

Default no path-mtu — Specifies the default path-mtu defined on the system for the type of SDP is used.

Parameters *bytes* — Specifies the bytes.

Values 576 to 9800

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

20.66 path-mtu-discovery

path-mtu-discovery

Syntax [**no**] **path-mtu-discovery**

Context **[Tree]** (config>router>ldp>tcp-session-params>peer-transport path-mtu-discovery)

Full Context configure router ldp tcp-session-parameters peer-transport path-mtu-discovery

Description This command enables Path MTU discovery for the associated TCP connections. When enabled, the MTU for the associated TCP session is initially set to the egress interface MTU. The DF bit is also set so that if a router along the path of the TCP connection cannot handle a packet of a particular size without fragmenting, it sends back an ICMP message to set the path MTU for the given session to a lower value that can be forwarded without fragmenting.

If one or more transport addresses used in the Hello adjacencies to the same peer LSR are different from the LSR-ID value, the user must add each of the transport addresses to the path MTU discovery configuration as a separate peer. This means when the TCP connection is bootstrapped by a given Hello adjacency, the path MTU discovery can operate over that specific TCP connection by using its specific transport address.

Default no path-mtu-discovery

Platforms All

path-mtu-discovery

Syntax [**no**] **path-mtu-discovery**

Context **[Tree]** (config>router>bgp path-mtu-discovery)
[Tree] (config>router>bgp>group path-mtu-discovery)
[Tree] (config>router>bgp>group>neighbor path-mtu-discovery)

Full Context configure router bgp group neighbor path-mtu-discovery
configure router bgp group path-mtu-discovery
configure router bgp path-mtu-discovery

Description This command enables Path MTU Discovery (PMTUD) for the associated TCP connections.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When enabled, PMTUD is activated toward an IPv4 BGP neighbor. The Don't Fragment (DF) bit is set in the IP header of all IPv4 packets sent to the peer. If any device along the path toward the peer cannot forward the packet because the IP MTU of the interface is smaller than the IP packet size, the device drops the packet and sends an ICMP or ICMPv6 error message encoding the interface MTU. When the router receives the ICMP or ICMPv6 message, it lowers the TCP maximum segment size limit from the previous value to accomodate the IP MTU constraint.

When PMTUD is disabled and there is no **tcp-mss** configuration to associate with a BGP neighbor (in either the BGP configuration or the first-hop IP interface configuration), the router advertises a TCP MSS option of only 1024 bytes, limiting received TCP segments to that size.

The **no** form of this command disables PMTUD.

Default no path-mtu-discovery

Platforms All

20.67 path-preference

path-preference

Syntax **path-preference** *value*
no path-preference

Context **[Tree]** (config>router>mpls>lsp>secondary path-preference)

Full Context configure router mpls lsp secondary path-preference

Description This command enables the use of path preference among configured standby secondary paths per LSP. If all standby secondary paths have a default path-preference value then a non-standby secondary path will remain the active path while a standby secondary is available. A standby secondary path configured with the highest priority (for example, the lowest path-preference value) is made the active path when the primary is not in use. If multiple standby secondary paths have the same, lowest, path-preference value then the system will select the path with the highest up-time. Path preference can only be configured on the standby secondary paths.

The **no** form of this command resets the path-preference to the default value.

Default path-preference 255

Parameters *value* — Specifies an alternate path for the LSP if the primary path is not available.

Values 1 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.68 path-probing

path-probing

Syntax **path-probing**

Context **[Tree]** (config>test-oam>ldp-treetrace path-probing)

Full Context configure test-oam ldp-treetrace path-probing

Description This command creates the context to configure the LDP tree trace path probing phase.

The periodic path exercising runs in the background to test the LDP ECMP paths discovered by the path discovery capability. The probe used is an LSP Ping message with an IP address drawn from the sub-range of 127/8 addresses indicated by the output of the tree discovery for this FEC.

The user configures the frequency of running the path probes using the **config>test-oam>ldp-treetrace>path-probing>interval** command. If an I/F is down on the ingress LER performing the LDP tree trace, then LSP Ping probes that normally go out this interface are not sent but the ingress LER node does not raise alarms.

The LSP Ping routine updates the content of the MPLS echo request message, specifically the IP address, as soon as the LDP ECMP path discovery phase has output the results of a new computation for the path in question.

Platforms All

20.69 path-profile

path-profile

Syntax **path-profile** *profile-id* [**path-group** *group-id*]
no path-profile *profile-id*

Context **[Tree]** (config>router>mpls>lsp path-profile)
[Tree] (config>router>mpls>lsp-template path-profile)

Full Context configure router mpls lsp path-profile
configure router mpls lsp-template path-profile

Description This command configures the PCE path profile and path group ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The PCE supports the computation of disjoint paths for two different LSPs originating and/or terminating on the same or different PE routers. To indicate this constraint to the PCE, the user must configure the PCE path profile ID and path group ID to which the PCE computed or PCE controlled LSP belongs to. These parameters are passed transparently by the PCC to the PCE and are thus opaque data to the router.

The association of the optional path-group ID is to allow the PCE to determine the profile ID that must be used with this path-group ID. One path-group ID is allowed per profile ID. The user can, however, enter the same path-group ID with multiple profile IDs by executing this command multiple times. A maximum of five **path-profile** [**path-group**] entries can be associated with the same LSP.

The **no** form of this command removes the path profile association with the LSP.

Parameters *profile-id* — Specifies the profile ID.

Values 1 to 4294967295

path-group *group-id* — Specifies the path group ID.

Values 0 to 4294967295

Platforms All

20.70 path-restoration-time

path-restoration-time

Syntax **path-restoration-time** *minutes*
no path-restoration-time

Context **[Tree]** (config>subscr-mgmt>pfcp-association path-restoration-time)

Full Context configure subscriber-mgmt pfcp-association path-restoration-time

Description This command configures the time sessions are kept after a PFCP path failure is detected. When the timer expires, or if it is not configured, all sessions associated with the path are removed. If the path recovers without a restart before the timer expires, the timer is canceled, and no sessions are removed.

The **no** form of this command removes the path restoration configuration.

Default no path-restoration-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *minutes* — Specifies the time, in minutes, that sessions are kept after a PFCP path failure. This timer should be configured to a value that is at least twice the sum of the **heartbeat interval** plus the total heartbeat timeout (heartbeat retries x heartbeat timeout = N1 x T1).

Values 5 to 1440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.71 path-threshold

path-threshold

Syntax **path-threshold** *num-paths*
no path-threshold

Context **[Tree]** (config>eth-tunnel>lag-emulation path-threshold)

Full Context configure eth-tunnel lag-emulation path-threshold

Description This command configures the behavior for the eth-tunnel if the number of operational members is equal to or below a threshold level

Default no path-threshold

Parameters *num-paths* — Specifies the threshold for the Ethernet Tunnel group.

Values 0 to 15

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.72 path-type

path-type

Syntax **path-type** {**ibgp** | **ebgp**}
no path-type

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from path-type)

Full Context configure router policy-options policy-statement entry from path-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command matches BGP routes based on their path type (EBGP or IBGP). A route learned from an EBGP peer has path-type **ebgp**. A route learned from an IBGP or confed-EBGP peer has path-type **ibgp**.

A non-BGP route does not match a policy entry if it contains the **path-type** command.

Default no path-type

Parameters **ibgp** — Matches routes from internal BGP peers.

ebgp — Matches routes from external BGP peers.

Platforms All

20.73 patherr

patherr

Syntax **patherr** [**detail**]
no patherr

Context **[Tree]** (debug>router>gmpls>packet patherr)

Full Context debug router gmpls packet patherr

Description This command enables debugging for GMPLS PathErr packets.

The **no** form of the command disables debugging for GMPLS PathErr packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

patherr

Syntax **patherr** [**detail**]
no patherr

Context **[Tree]** (debug>router>rsvp>packet patherr)

Full Context debug router rsvp packet patherr

Description This command debugs path error packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about path error packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

20.74 pathtear

pathtear

Syntax **pathtear** [**detail**]
no pathtear

Context **[Tree]** (debug>router>gmpls>packet pathtear)

Full Context debug router gmpls packet pathtear

Description This command enables debugging for GMPLS PathTear packets.

The **no** form of the command disables debugging for GMPLS PathTear packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

pathtear

Syntax **pathtear** [**detail**]
no pathtear

Context **[Tree]** (debug>router>rsvp>packet pathtear)

Full Context debug router rsvp packet pathtear

Description This command debugs path tear packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about path tear packets.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.75 pattern

pattern

Syntax **pattern** *pad-value*
no pattern

Context **[Tree]** (config>oam-pm>session>ip pattern)

Full Context configure oam-pm session ip pattern

Description This command configures the pattern value to be repeated in the padding portion of the TWAMP Light packet.

The **no** form of this command uses an incrementing byte pattern beginning with 00 and ending with FF, wrapping back to 00.

Default pattern 0

Parameters *pad-value* — Specifies the specific pattern to use.

Values 0 to 65535

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

pattern

Syntax **pattern** *pad-value*
no pattern

Context **[Tree]** (config>oam-pm>session>mpls pattern)

Full Context configure oam-pm session mpls pattern

Description This command configures the pattern value to be repeated in the padding portion of pad-tlv length field of the dm PDU.

The **no** form of this command uses an incrementing byte pattern beginning with 00 and ending with FF, wrapping back to 00.

Parameters *pad-value* — Specifies a two octet pattern to be repeated to fill the padding field of each echo request packet launched for each test belonging to the specified session. For example, if 255 is specified, the padding field is filled with the octet values 00, FF, 00, FF, ... (hexadecimal).

Values 0 to 65535

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.76 payload

payload

Syntax **payload** {**sts3** | **tug3** | **ds3** | **e3** | **vt2** | **vt15** | **ds1** | **e1**}

Context **[Tree]** (config>port>sonet-sdh>path payload)

Full Context configure port sonet-sdh path payload

Description This command specifies if the associated SONET/SDH path is an asynchronous circuit or a virtual tributary group (VT). This command is only applicable to channelized MDAs.

This command is supported on TDM satellite, however the sts3, ds3, and e3 parameters are not supported.

Parameters **sts3** — Configures STS3/STM1 payload as clear channel.

tu3 — Configures STS3/STM1 payload as Tributary Unit Group 3 (TUG3).

ds3 — Configures the port or channel as DS-3 STS1/VC3 payload as DS-3.

e3 — Configures the port or channel as E-3 STS1/VC3 payload as E-3.

vt2 — Configures the path STS1 payload as vt2 as a virtual tributary group. Only allowed on STS-1 nodes (SONET VT container).

vt15 — Configures the path as a virtual tributary group. Only allowed on STS-1 nodes (SONET VT container).

ds1 — Configures the port or channel as DS1.vt15 or vt2 payload as DS-1.

e1 — Configures VT2 payload as E-1.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.77 pbb

pbb

Syntax **pbb**

Context **[Tree]** (config>service pbb)
[Tree] (config>service>vpls pbb)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service pbb
configure service vpls pbb

Description Commands in this context configure the PBB parameters.

Platforms All

pbb

Syntax **pbb**

Context **[Tree]** (config>test-oam>build-packet>header pbb)
[Tree] (debug>oam>build-packet>packet>field-override>header pbb)

Full Context configure test-oam build-packet header pbb
debug oam build-packet packet field-override header pbb

Description This command configures a test Provider Backbone Bridge (PBB) packet header to be launched by the OAM **find-egress** tool.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.78 pbb-etype

pbb-etype

Syntax **pbb-etype** [*ethertype-value*]
no pbb-etype

Context **[Tree]** (config>port>ethernet pbb-etype)

Full Context configure port ethernet pbb-etype

Description This command configures the Ethertype used for PBB encapsulation.

Default no pbb-etype

Parameters *ethertype-value* — Specifies the Ethertype value in the form of 0x600 to 0xfff.

Values 1536 to 65535 (accepted in decimal or hex)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pbb-etype

Syntax **pbb-etype** *type*
no pbb-etype [*type*]

Context **[Tree]** (config>service>sdp pbb-etype)

Full Context configure service sdp pbb-etype

Description This command configures the Ethertype used for PBB.

Default no pbb-etype

Parameters *type* — Specifies the Ethertype.

Values 0x0600..0xffff or 1536 to 65535 (accepted in decimal or hex)

Platforms All

20.79 pbr-down-action-override

pbr-down-action-override

Syntax **pbr-down-action-override** *filter-action*
no pbr-down-action-override

Context **[Tree]** (config>filter>ip-filter>entry pbr-down-action-override)
[Tree] (config>filter>ipv6-filter>entry pbr-down-action-override)
[Tree] (config>filter>mac-filter>entry pbr-down-action-override)

Full Context configure filter ip-filter entry pbr-down-action-override
configure filter ipv6-filter entry pbr-down-action-override
configure filter mac-filter entry pbr-down-action-override

Description This command allows overriding the default action that is applied for entries with PBR/PBF action defined, when the PBR/PBF target is down.

The **no** form of the command preserves default behavior when PBR/PBF target is down.

Default no pbr-down-action-override

Parameters *filter-action* — Specifies the packets matching the entry.

drop — Specifies that packets matching the entry will be dropped if PBR/PBF target is down.

forward — Specifies that packets matching the entry will be forwarded if PBR/PBF target is down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

filter-default-action — Specifies that packets matching the entry will be processed as per **default-action** configuration for this filter if PBR/PBF target is down.

Platforms All

20.80 pcap

pcap

Syntax **pcap** *session-name* [**create**]
no pcap *session-name*

Context **[Tree]** (config>mirror>mirror-dest pcap)

Full Context configure mirror mirror-dest pcap

Description This command specifies a PCAP instance used for packet capture.

The **no** form of this command removes the PCAP instance and stops the packet capture and file transfer session.

Parameters *session-name* — Specifies the session name, up to 32 characters.

Platforms All

pcap

Syntax **pcap** *session-name*

Context **[Tree]** (debug pcap)

Full Context debug pcap

Description This command specifies the session for the packet capture process.

Parameters *session-name* — Specifies the session name, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.81 pcc

pcc

Syntax [**no**] **pcc**

Context **[Tree]** (debug>router>mpls>event pcc)

Full Context debug router mpls event pcc

Description This command debugs pcc events.

The **no** form of the command disables the debugging.

Platforms All

pcc

Syntax **pcc**

Context **[Tree]** (config>router>pcep pcc)

Full Context configure router pcep pcc

Description Commands in this context configure PCC parameters.

Platforms All

20.82 pce-control

pce-control

Syntax [**no**] **pce-control**

Context **[Tree]** (config>router>mpls>lsp pce-control)
[Tree] (config>router>mpls>lsp-template pce-control)

Full Context configure router mpls lsp pce-control
configure router mpls lsp-template pce-control

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables a PCE controlled LSP mode of operation. The **pce-control** option means the router delegates full control of the LSP to the PCE (PCE controlled). Enabling it means the PCE is acting in stateful-active mode for this LSP and the PCE will be able to reroute the path following a failure or re-optimize the path and update the router without a request from the router.

The user can delegate CSPF and non-CSPF LSPs, or LSPs that have the **path-computation-method pce** option enabled or disabled. The LSP maintains its latest active path computed by PCE or the router at the time it is delegated. The PCE only makes an update to the path at the next network event or reoptimization.

When configured to no, the PCE controlled mode of operation for the LSP has not effect.

Default no pce-control

Platforms All

20.83 pce-initiated-lsp

pce-initiated-lsp

Syntax [**no**] **pce-initiated-lsp**

Context **[Tree]** (config>router>mpls pce-initiated-lsp)

Full Context configure router mpls pce-initiated-lsp

Description This command creates a context to configure support for PCE-initiated LSPs.

The **no** form of this command removes PCE-initiated LSP support. All PCE-initiated LSPs are deleted.

Platforms All

20.84 pce-report

pce-report

Syntax **pce-report rsvp-te** {**enable** | **disable**}
pce-report sr-te {**enable** | **disable**}

Context **[Tree]** (config>router>mpls pce-report)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls pce-report

Description This command separately configures the reporting modes to a PCE for RSVP-TE or SR-TE LSPs. The PCC LSP database is synchronized with the PCE LSP database using the PCEP PCRpt (PCE Report) message for PCC-controlled, PCE-computed, and PCE-controlled LSPs.

The global MPLS level **pce-report** command can be used to enable or disable PCE reporting for all SR-TE LSPs or RSVP-TE LSPs during PCE LSP database synchronization. This configuration is inherited by all LSPs of the specified type. The PCC reports both CSPF and non-CSPF LSPs. The default value is disabled for both types of LSP. This default value is meant to control the introduction of the PCE into an existing network and to let the operator decide if all LSPs of a particular type need to be reported.

The LSP-level **pce-report** command overrides the global configuration for the reporting of LSPs to the PCE. The default value is to inherit the global MPLS level value. The **enable** or **disable** value allows for the override of the inherited value. The **inherit** value explicitly resets the LSP to inherit the global configuration for that LSP type.

If PCE reporting is disabled for the LSP, either due to inheritance or due to LSP-level configuration, then enabling the **pce-control** option for the LSP has no effect.

Default pce-report rsvp-te disable

pce-report sr-te disable

Parameters **rsvp-te** — Specifies the PCE reporting mode for all TE LSPs of RSVP-TE type.

Values **enable** — enables PCE reporting for all TE LSPs of RSVP-TE type
disable — disables PCE reporting for all TE LSPs of RSVP-TE type

sr-te — Specifies the PCE reporting mode for all TE LSPs of SR-TE type.

Values **enable** — enables PCE reporting for all TE LSPs of SR-TE type
disable — disables PCE reporting for all TE LSPs of SR-TE type

Platforms All

pce-report

Syntax **pce-report** {**enable** | **disable** | **inherit**}

Context **[Tree]** (config>router>mpls>lsp pce-report)
[Tree] (config>router>mpls>lsp-template pce-report)

Full Context configure router mpls lsp pce-report
configure router mpls lsp-template pce-report

Description This command separately configures the reporting modes to a PCE for RSVP-TE or SR-TE LSPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The PCC LSP database is synchronized with the PCE LSP database using the PCEP PCRpt (PCE Report) message for PCC-controlled, PCE-computed and PCE-controlled LSPs.

The global MPLS-level **pce-report** command can be used to enable or disable PCE reporting for all SR-TE LSPs or RSVP-TE LSPs during PCE LSP database synchronization. This configuration is inherited by all LSPs of the specified type. The PCC reports both CSPF and non-CSPF LSPs. The default value is disabled for both types of LSP. This default value is meant to control the introduction of the PCE into an existing network and to let the operator decide if all LSPs of a particular type need to be reported.

The LSP-level **pce-report** command overrides the global configuration for the reporting of LSP to the PCE. The default value is to inherit the global MPLS level value. The **enable** or **disable** value allows for the override of the inherited value. The **inherit** value explicitly resets the LSP to inherit the global configuration for that LSP type.

If PCE reporting is disabled for the LSP, either due to inheritance or due to LSP-level configuration, then enabling the **pce-control** option for the LSP has no effect.

Default pce-report inherit

Parameters **enable** — Enables PCE reporting.

disable — Disables PCE reporting.

inherit — Inherits the global configuration for PCE reporting.

Platforms All

20.85 pcep

pcep

Syntax [**no**] **pcep**

Context **[Tree]** (config>router pcep)

Full Context configure router pcep

Description This command enables Path Computation Element communications Protocol (PCEP), and enters the context to configure PCEP parameters.

The **no** form of the command disables PCEP.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.86 pcm

pcm

Syntax [**no**] **pcm** *pcm-slot* [**chassis** *chassis-id*]

Context **[Tree]** (config>system>power-management pcm)

Full Context configure system power-management pcm

Description This command sets the PCM slot number. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Parameters *pcm-slot* — Identifies the PCM slot.

Values 1 to 12

chassis-id — Specifies chassis ID for the router chassis.

Values 1, 2

Default 1

20.87 pcp

pcp

Syntax **pcp**

Context **[Tree]** (debug>router pcp)

Full Context debug router pcp

Description This command enables debugging for the PCP servers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.88 pcp-server

pcp-server

Syntax **pcp-server**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>router pcp-server)

Full Context configure router pcp-server

Description Commands in this context configure a Port Control Policy (PCP) server.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pcp-server

Syntax **pcp-server** *name*

Context **[Tree]** (debug>router>pcp pcp-server)

Full Context debug router pcp pcp-server

Description This command enables debugging for the PCP servers.

Parameters *name* — Debugs the PCP server associated with the specified name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.89 pcp-server-policy

pcp-server-policy

Syntax **pcp-server-policy** *name* [**create**]
no pcp-server-policy *name*

Context **[Tree]** (config>service>nat pcp-server-policy)

Full Context configure service nat pcp-server-policy

Description This command configures a PCP server policy name.

The **no** form of the command removes the name from the configuration.

Parameters *name* — Specifies a PCP server policy name up to 32 characters.

create — Keyword used to create the PCP server policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pcp-server-policy

Syntax **pcp-server-policy** *name*
no pcp-server-policy

Context **[Tree]** (config>router>pcp-server>server pcp-server-policy)

Full Context configure router pcp-server server pcp-server-policy

Description This command configures the PCP server policy.

The **no** form of this command reverts to the default value.

Default no pcp-server-policy

Parameters *name* — Specifies the PCP server policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.90 pcr-repetition

pcr-repetition

Syntax **pcr-repetition** [**tnc** *tnc-milli-seconds* **qos** *qos-milli-seconds* **poa** *poa-milli-seconds*]
no pcr-repetition

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms pcr-repetition)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms pcr-repetition)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms pcr-repetition)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms pcr-repetition
configure mcast-management multicast-info-policy bundle channel video analyzer alarms pcr-repetition
configure mcast-management multicast-info-policy bundle video analyzer alarms pcr-repetition

Description This command configures the analyzer to check for the program clock reference (PCR). It is expected that the PCR arrives periodically within a certain interval range. It is possible to configure the type of alarm that is raised when the PCR fails to arrive within the specified interval. As the delay increases between two consecutive PCRs, the type of alarm raised becomes more critical, from TNC to POA.

Default no pcr-repetition

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *tnc-milli-seconds* — Specifies the time, in milliseconds, for which a TNC alarm is raised if the interval between two consecutive PCRs is greater than or equal to this configured value.

Values 100 to 800 in multiples of 100 only

Default 100

qos-milli-seconds — Specifies the time, in milliseconds, for which a QoS alarm is raised if the interval between two consecutive PCRs is greater than or equal to this configured value.

Values 200 to 900 in multiples of 100 only and higher than the *tnc-milli-seconds* value

Default 200

poa-milli-seconds — Specifies the time, in milliseconds, for which a POA alarm is raised if the interval between two consecutive PCRs is greater than or equal to this configured value.

Values 300 to 1000 in multiples of 100 only and higher than the *qos-milli-seconds* value

Default 500

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.91 pd-managed-route

pd-managed-route

Syntax **pd-managed-route** [**next-hop** {**ipv4** | **ipv6**}]
no pd-managed-route

Context **[Tree]** (config>service>vprn>sub-if>ipv6>dhcp6 pd-managed-route)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6 pd-managed-route)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 pd-managed-route)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 pd-managed-route)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 pd-managed-route
configure service ies subscriber-interface ipv6 dhcp6 pd-managed-route
configure service vprn subscriber-interface group-interface ipv6 dhcp6 pd-managed-route
configure service vprn subscriber-interface ipv6 dhcp6 pd-managed-route

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables DHCP IA-PD (delegated prefix) to be modeled as managed (framed) route instead of as a subscriber-host. Antispoof filtering for the subscriber host associated with the IA-PD route must be set to **nh-mac**. The subscriber specific parameters (such as **sla-profile** or **sub-profile**) are ignored during the authentication phase because IA-PD is not modeled as a subscriber host. Other subscriber host-specific functions (for example, host overrides via CoA or host accounting) are not possible with a PD as the managed route.

By default, or when configured with the **next-hop ipv6** parameter, the next-hop for PD managed route is an IPv6 WAN sub-host (DHCP IA-NA or SLAAC) with the same mac address as the one in the DHCP lease state for the managed IA-PD. The DHCP IA-NA next-hop host will always override the SLAAC next-hop host if both are available. If the IPv6 next-hop is not present when the framed IA-PD is instantiated, the IA-PD is set up but the PD managed route will not be installed in the IPv6 route table and the DHCPv6 lease state for the IA-PD will have the managed route status (DHCP6 MRt Status) set to “noNextHop”.

When configured with the **next-hop ipv4** parameter the next-hop for PD managed route is a DHCPv4 sub-host that belongs to the same IPoE session or PPPoE session. For IPoE, **ipoe-session** must be enabled on the group-interface. If **ipoe-session** is disabled, an IPv4 next-hop will not be found. If the IPv4 next-hop is not found or not present at the time when the framed IA-PD is instantiated, the IA-PD is set up but the PD managed route is not installed in the IPv6 route table. In this case, the DHCPv6 lease state for the IA-PD will have the managed route status (DHCP6 MRt Status) set to noNextHop.

Note: IPv6 filters, QoS IPv6 criteria, and IPv6 multicast are not supported for DHCPv6 IA-PD as managed route pointing to an IPv4 subscriber host as next-hop.

The DHCP IA-PD modeled as a route is displayed differently than regular subscriber hosts in **show** commands related to subscriber host state. The PD managed route is always shown directly below the host it is using as the next hop. The forwarding status of the PD managed route is also shown, where (N) indicate that the PD managed route is not forwarding. In addition, DHCP IA-PD route is displayed as a managed route for the corresponding IPv6 subscriber host (DHCP IA-NA or SLAAC) or DHCPv4 subscriber host.

DHCP IA-PD information for managed IA-PD route is still maintained in the DHCPv6 lease state.

The **no** form of this command reverts to the default.

Parameters **next-hop** — Specifies the next-hop type for the DHCP IA-PD managed route

Values **ipv4** - The next-hop for PD managed route is a DHCPv4 sub-host that belongs to the same IPoE session (based on the IPoE session key which is **sap-mac** by default). IPoE session must be enabled on the group-interface.

ipv6 - The next-hop for PD managed route is an IPv6 WAN sub-host (DHCP IA-NA or SLAAC) with the same MAC address as the one in the DHCP lease state for the managed IA-PD. This is the default when no next-hop is specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.92 pdn-connection-id

pdn-connection-id

Syntax [**no**] **pdn-connection-id**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp pdn-connection-id)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp pdn-connection-id

Description This command enables the inclusion of the PDN-Connection-Id AVP, which contains the APN as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the AVP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.93 pdn-type

pdn-type

Syntax **pdn-type** {**ipv4** | **ipv6** | **ipv4v6**}
no pdn-type

Context **[Tree]** (config>router>gtp>uplink pdn-type)
[Tree] (config>service>vprn>gtp>uplink pdn-type)

Full Context configure router gtp uplink pdn-type
configure service vprn gtp uplink pdn-type

Description This command configures the PDP type to be signaled in GTP, determining which addresses are requested from the P-GW/GGSN and which hosts are set up afterwards. This can be overridden by RADIUS. If the **ipv4v6** keyword is used, the P-GW/GGSN can fall back to either IPv4 or IPv6.

The **no** form of this command reverts to the default configuration.

Default pdn-type ipv4

Parameters **ipv4** — Specifies the GTP connection requests an IPv4 address.

ipv6 — Specifies the GTP connection requests an IPv6 address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4v6 — Specifies the GTP connection requests both an IPv4 and an IPv6 address.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.94 pdp-context-type

pdp-context-type

Syntax [**no**] **pdp-context-type**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp pdp-context-type)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp pdp-context-type

Description This command includes the [3GPP-1247] PDP-Context-Type AVP in Diameter DCCA CCR-Initial messages.

The **no** form of this command removes the PDP-Context-Type AVP from the Diameter DCCA CCR-Initial messages.

Default pdp-context-type

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.95 pe-id-mac-flush-interop

pe-id-mac-flush-interop

Syntax [**no**] **pe-id-mac-flush-interop**

Context **[Tree]** (config>router>ldp>session-params>peer pe-id-mac-flush-interop)

Full Context configure router ldp session-parameters peer pe-id-mac-flush-interop

Description This command enables the addition of the PE-ID TLV in the LDP MAC withdrawal (mac-flush) message, under certain conditions, and modifies the mac-flush behavior for interoperability with other vendors that do not support the flush-all-from-me vendor-specific TLV. This flag can be enabled on a per LDP peer basis and allows the flush-all-from-me interoperability with other vendors. When the pe-id-mac-flush-interop flag is enabled for a given peer, the current mac-flush behavior is modified in terms of mac-flush generation, mac-flush propagation and behavior upon receiving a mac-flush.

The mac-flush generation will be changed depending on the type of event and according to the following rules:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Any all-from-me mac-flush event will trigger a mac-flush all-but-mine message (RFC 4762 compliant format) with the addition of a PE-ID TLV. The PE-ID TLV contains the IP address of the sending PE.
- Any all-but-mine mac-flush event will trigger a mac-flush all-but-mine message WITHOUT the addition of the PE-ID TLV, as long as the source spoke SDP is not part of an end-point.
- Any all-but-mine mac-flush event will trigger a mac-flush all-but-mine message WITH the addition of the PE-ID TLV, if the source spoke SDP is part of an end-point and the spoke-sdp goes from down/standby state to active state. In this case, the PE-ID TLV will contain the IP address of the PE to which the previous active spoke-sdp was connected to.

Any other case will follow the existing mac-flush procedures.

When the pe-id-mac-flush-interop flag is enabled for a given LDP peer, the mac-flush ingress processing is modified according to the following rules:

- Any received all-from-me mac-flush will follow the existing mac-flush all-from-me rules regardless of the existence of the PE-ID.
- Any received all-but-mine mac-flush will take into account the received PE-ID, that is all the mac addresses associated to the PE-ID will be flushed. If the PE-ID is not included, the mac addresses associated to the sending PE will be flushed.
- Any other case will follow the existing mac-flush procedures.

When a mac-flush message has to be propagated (for an ingress sdp-binding to an egress sdp-binding) and the pe-id-mac-flush-interop flag is enabled for the ingress and egress TLDP peers, the following behavior is observed:

- If the ingress and egress bindings are spoke SDP, the PE will propagate the mac-flush message with its own PE-ID.
- If the ingress binding is an spoke SDP and the egress binding a mesh SDP, the PE will propagate the mac-flush message without modifying the PE-ID included in the PE-ID TLV.
- If the ingress binding is a mesh SDP and the egress binding an spoke SDP, the PE will propagate the mac-flush message with its own PE-ID.
- When ingress and egress bindings are mesh-sdp, the mac-flush message is never propagated. This is the behavior regardless of the pe-id-mac-flush-interop flag configuration.

The PE-ID TLV is never added when generating a mac-flush message on a B-VPLS if the **send-bvpls-flush** command is enabled in the I-VPLS. In the same way, no PE-ID is added when propagating mac-flush from a B-VPLS to a I-VPLS when the **propagate-mac-flush-from-bvpls** command is enabled. Mac-flush messages for peers within the same I-VPLS or within the same B-VPLS domain follow the procedures described above.

Default no pe-id-mac-flush-interop

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.96 peak-rate

peak-rate

Syntax **peak-rate** *rate*
no peak-rate

Context **[Tree]** (config>router>policy-acct-template>policer peak-rate)

Full Context configure router policy-acct-template policer peak-rate

Description This command sets the peak rate (the fill or drain rate of the bucket).

Each policer has a peak information rate and a maximum burst size. The default **peak-rate** (when no value is configured or the configured value is max) is the line rate of the ingress port.

The **no** form of this command reverts to the default value.

Default peak-rate max

Parameters *rate* — Specifies the peak rate in Kb/s

Values 1 to 6400000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

20.97 peer

peer

Syntax **peer** *ip-address* **tag** *sync-tag*
no peer

Context **[Tree]** (config>router>dhcp>server>failover peer)
[Tree] (config>router>dhcp>server>pool>failover peer)
[Tree] (config>router>dhcp6>server>failover peer)
[Tree] (config>router>dhcp6>server>pool>failover peer)
[Tree] (config>service>vprn>dhcp>server peer)
[Tree] (config>service>vprn>dhcp>server>pool peer)
[Tree] (config>service>vprn>dhcp6>server peer)
[Tree] (config>service>vprn>dhcp6>server>pool peer)

Full Context configure router dhcp local-dhcp-server failover peer
configure router dhcp server pool failover peer
configure router dhcp6 local-dhcp-server failover peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router dhcp6 server pool failover peer
configure service vprn dhcp server peer
configure service vprn dhcp server pool peer
configure service vprn dhcp6 server peer
configure service vprn dhcp6 server pool peer

Description This command creates a sync tag. DHCP leases can be synchronized per DHCP server or DHCP pool. The pair of synchronizing servers or pools is identified by a tag. The synchronization information is carried over the Multi-Chassis Synchronization (MCS) link between the two peers. MCS link is a logical link (IP, or MPLS).

MCS runs over TCP, port 45067 and it is using either data traffic or keepalives to detect failure on the communication link between the two nodes. In the absence of any MCS data traffic for more than 0.5sec, MCS will send its own keepalive to the peer. If a reply is **not** received within three sec, MCS will declare its operation state as DOWN and the DB Sync state as out-of-sync. MCS will consequently notify its clients (DHCP Server being one of them) of this. It can take up to three seconds before the DHCP client realizes that the inter-chassis communication link has failed.

The inter-chassis communication link failure does not necessarily assume the same failed fate for the access links. The two redundant nodes can become isolated from each other in the network. This occurs when only the intercommunication (MCS) link fails. It is important that this MCS link be highly redundant.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the peer.

Values

ipv4-address:	a.b.c.d	
:	x:ipv6-addressx:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

tag *sync-tag* — Specifies a tag, up to 32 characters, that identifies the synchronizing DHCP servers or pools.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax [**no**] **peer router** *router-instance* **address** *ip-address* [**udp-port** *port*]

Context **[Tree]** (debug>gtp peer)

Full Context debug gtp peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command restricts debugging to only data related to the specified GTP peer. This command can be repeated multiple times, where only data for any of the specified peers is debugged.

The **no** form of this command removes the restriction for the specified peer. When the last peer filter is removed, all data is debugged again, but may be restricted by other filters.

Parameters *router-instance* — Specifies the ID of the VRF where the peer is connected.

Values

router-instance:	*router-name* | *vprn-svc-id*
router-name:	"Base"
vprn-svc-id	1 to 2147483647

ip-address — Specifies the IP address of the peer.

Values a.b.c.d

port — Specifies the GTP-C port used by the peer.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer** *ip-address*
no peer

Context **[Tree]** (config>router>l2tp>group>tunnel peer)
[Tree] (config>service>vprn>l2tp>group>tunnel peer)

Full Context configure router l2tp group tunnel peer
configure service vprn l2tp group tunnel peer

Description This command configures the peer address.

The **no** form of this command removes the IP address from the tunnel configuration.

Default no peer

Parameters *ip-address* — Sets the LNS IP address for the tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer** *ip-address* [**udp-port** *port*] [**ip**]

Context **[Tree]** (debug>router>l2tp peer)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router l2tp peer

Description This command enables and configures debugging for an L2TP peer.

Parameters *ip-address* — Specifies the IP address of the L2TP peer.

port — Specifies the UDP port for the L2TP peer. This parameter is only supported with L2TPv2 peers.

ip — Displays debugging information for peers using IP transport.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer** *name* [**create**]
no peer name

Context **[Tree]** (config>aaa>diam-peer-plcy peer)

Full Context configure aaa diameter-peer-policy peer

Description This command creates context for diameter peer configuration. Up to five Diameter peers can be configured inside a **diameter-peer-policy**. Only the two peers with the highest preference in the peer table are considered for use (the primary and secondary). Other peers can be the Open state and merely run keepalives (watchdog-request or answer messages). After the primary peer fails, the secondary peer is used as long as the last transaction on it has succeeded (stickiness). Another peer in the Open state becomes secondary. Load balancing between peers is not supported.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies the peer name, up to of 32 characters.

create — Keyword used to create the peer. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer index** *index* [*destination-host-string*][**create**]
no peer index *index*

Context **[Tree]** (config>aaa>diam>node peer)

Full Context configure aaa diameter node peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates context for diameter peer configuration within a Diameter client node in SR OS. Up to five Diameter peers can be configured within a given Diameter client node.

This command is not applicable to legacy Diameter base.

The **no** form of this command removes the peer index information from the configuration.

Parameters *index* — Specifies the index of a peer. Index is used to break a tie if a Diameter route for a given host or realm destination points to multiple diameter peers with the same preference. In such scenario, the peer with the lowest index will be selected as next-hop in traffic forwarding.

Values 1 to 5

destination-host-string — Identifies the peer by its name, up to 80 characters (of type DiameterIdentity). This peer name must match the one in Origin-Host AVP received in Capability Exchange Answer message. In case of a mismatch, the TCP connection will be terminated.

create — Keyword used to create the peer index. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer** *ip-address* [**create**]
no peer *ip-address*

Context **[Tree]** (config>redundancy>multi-chassis peer)

Full Context configure redundancy multi-chassis peer

Description This command configures the IP address of the peer in a redundant multi-chassis setup, and enters the context for further, application-specific configuration options.

Parameters *ip-address* — Specifies a peer IP address. Multicast addresses are not allowed.

Values ipv4-address: a.b.c.d
ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF] H
- d: [0 to 255] D

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

peer

Syntax [**no**] **peer** *destination-host*

Context **[Tree]** (debug>diameter>node peer)

Full Context debug diameter node peer

Description This command debugs Diameter node peers. At this level, the forwarding/routing phase is completed and the peer is known. All messages flowing between this node and the peer are reported. Although the messages displayed can contain session-ids, this debugging level is session unaware (the session states are not maintained at this level).

Parameters *destination-host* — Specifies the host name, up to 80 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer ip-address** *ip-address*
no peer

Context **[Tree]** (config>subscr-mgmt>pfcp-association peer)

Full Context configure subscriber-mgmt pfcp-association peer

Description This command configures PFCP peer IP address.

The **no** form of this command removes the PFCP IP address.

Default no peer

Parameters *ip-address* — Specifies the PFCP peer IP address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax **peer** *a.b.c.d* [**create**]

Context **[Tree]** (config>service>vprn>ptp peer)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ptp peer

Description This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer.

Up to 20 remote PTP peers may be configured.

The **no** form of this command deletes the specified peer.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last peer cannot be deleted. This prevents the user from having PTP enabled without any peer configured and enabled.

Peers are created within the routing instance associated with the context of this command. All configured PTP peers must use the same routing instance.

Parameters *a.b.c.d* — Specifies the IP address of the remote peer.

Values ipv4-address a.b.c.d

create — Keyword used to create the peer.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax **peer** *ip-address* [**create**]
no peer *ip-address*

Context **[Tree]** (config>system>ptp peer)

Full Context configure system ptp peer

Description This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer.

Up to 20 remote PTP peers may be configured.

The **no** form of the command deletes the specified peer. The specific address being deleted must be included.

If the **clock-type** is **ordinary slave** or **boundary**, and PTP is no shutdown, the last peer cannot be deleted. This prevents the user from having PTP enabled without any peer configured and enabled.

Peers are created within the routing instance associated with the context of this command. All configured PTP peers must use the same routing instance.

Parameters *ip-address* — Specifies the IP address of the remote peer.

create — Creates the remote PTP peer.

Values ipv4 address: a.b.c.d.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax [**no**] **peer** *peer-address*

Context **[Tree]** (config>service>vprn>msdp peer)
[Tree] (config>service>vprn>msdp>group peer)

Full Context configure service vprn msdp group peer
configure service vprn msdp peer

Description This command configures peer parameters. Multicast Source Discovery Protocol (MSDP) must have at least one peer configured. A peer is defined by configuring a local-address that can be used by this node to set up a peering session and the address of a remote MSDP router, It is the address of this remote peer that is configured in this command and it identifies the remote MSDP router address.

After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. It may be required to have multiple peering sessions in which case multiple peer statements should be included in the configurations.

By default, the options applied to a peer are inherited from the global or group-level. To override these inherited options, include peer-specific options within the peer statement.

If the peer address provided is already a configured peer, then this command only provides the context to configure the parameters pertaining to this peer.

If the peer address provided is not already a configured peer, then the peer instance must be created and the context to configure the parameters pertaining to this peer should be provided. In this case, the $ prompt to indicate that a new entity (peer) is being created should be used.

The peer address provided will be validated and, if valid, will be used as the remote address for an MSDP peering session.

When the **no** form of this command is entered, the existing peering address will be removed from the configuration and the existing session will be terminated. Whenever a session is terminated, all source active information pertaining to and learned from that peer will be removed. Whenever a new peering session is created or a peering session is lost, an event message should be generated.

At least one peer must be configured for MSDP to function.

Parameters *peer-address* — The address configured in this statement must identify the remote MSDP router that the peering session must be established with.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

peer

Syntax **peer** *ipv4-address*
no peer

Context **[Tree]** (config>router>nat>inside>redundancy peer)
[Tree] (config>service>vprn>nat>inside>redundancy peer)

Full Context configure router nat inside redundancy peer
configure service vprn nat inside redundancy peer

Description This command is used in LSN44 multi-chassis redundancy in conjunction with filters. The configured peer address is an IPv4 address that is configured under an interface on the peering LSN44 node (active or standby). This IPv4 interface address is advertised via routing on the inside in order to attract traffic from the standby to the active LSN44 node.

If configured, the steering-route will be advertised only from the active LSN44 node. Consequently, upstream traffic for LSN44 will be attracted to the active LSN44 node. The nat action in the ipv4-filter on the active LSN44 node will forward traffic to the local MS-ISA where LSN44 function is performed. However, in that case that upstream traffic somehow arrives on the standby LSN44 node, the nat action in the IPv4-filter will forward traffic to the peer address (active LSN44 node).

The **no** form of the command removes the peer ipv4-address from the configuration.

Default none

Parameters *ipv4-address* — Specifies the IP address of the NAT redundancy peer.

Values ipv4-address:a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax [**no**] **peer** *peer-node-id*

Context **[Tree]** (config>router>lmp peer)

Full Context configure router lmp peer

Description This command creates a context to enable the specification of the LMP peer parameters. It also specifies the LMP peer node. For a GMPLS UNI, this is the UNI-N node at the far end of the IP control channel for the GMPLS UNI. If the peer loopback address is entered using the **peer-loopback-address** command, then this is used as the routable peer address; otherwise the *peer-node-id* is assumed to correspond to a routable peer loopback

Default no peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *peer-node-id* — An identifier for the LMP peer node. This may be an IPv4-formatted address or a 32-bit unsigned integer.

Values a.b.c.d | 1 to 4294967295

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax **peer** *peer-node-id*
no peer

Context **[Tree]** (config>router>gmpls>lsp>working-path peer)
[Tree] (config>router>gmpls>lsp>protect-path peer)

Full Context configure router gmpls lsp protect-path peer
configure router gmpls lsp working-path peer

Description This command specifies a peer node to use for the first hop of the GMPLS LSP. If specified, this command forces the GMPLS LSP to use a specific UNI-N node on ingress to the optical network. This command is only applicable if 1toN end to end protection is used.

The **no** form of the command removes the list of SRLG groups to exclude.

Parameters *peer-node-id* — The node ID of the peer UNI-N. This may be an ipv4-formatted address or a 32-bit unsigned integer.

Values a.b.c.d | 1 – 4294967295

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax [**no**] **peer** *peer-node-id*

Context **[Tree]** (config>router>gmpls peer)

Full Context configure router gmpls peer

Description This command specifies parameters for the RSVP session to a neighboring GMPLS UNI-N node. The *peer-node-id* is the control plane identifier for the adjacent UNI-N node.

The **no** form of this command deletes the configuration.

Parameters *peer-node-id* — Specifies the control plane node ID of the neighboring GMPLS UNI-N node. This can be an ipv4 address or a 32-bit unsigned integer.

Values {a.b.c.d | 1 to 4294967295}

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

peer

Syntax [**no**] **peer**

Context **[Tree]** (debug>router>gmpls>event peer)

Full Context debug router gmpls event peer

Description This command enables and disables debugging for GMPLS NBR events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax [**no**] **peer** *ip-address*

Context **[Tree]** (config>router>ldp>session-parameters peer)

Full Context configure router ldp session-parameters peer

Description This command configures parameters for an LDP peer.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the LDP peer in dotted decimal notation.

Platforms All

peer

Syntax [**no**] **peer** *ip-address*

Context **[Tree]** (config>router>ldp>targeted-session peer)

Full Context configure router ldp targeted-session peer

Description This command configures parameters for an LDP peer.no

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the LDP peer in dotted decimal notation.

Platforms All

peer

Syntax [**no**] **peer** *ip-address*

Context **[Tree]** (debug>router>ldp peer)

Full Context debug router ldp peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Use this command for debugging an LDP peer.

Parameters **ip-address** — The IP address of the LDP peer.

Platforms All

peer

Syntax **peer** *ip-address* [**preference** *preference*]
no peer *ip-address*

Context **[Tree]** (config>router>pcep>pcc peer)

Full Context configure router pcep pcc peer

Description This command configures the IP address of a peer PCEP speaker. The address is used as the destination address in the PCEP session messages to a PCEP peer.

The **preference** parameter allows the PCC to select the preferred PCE when both have their PCEP sessions successfully established. A maximum of two PCEP peers is supported.

The PCE peer that is not in overload is always selected by the PCC as the active PCE. However, if neither of the PCEs are signaling the overload state, the PCE with the higher numerical preference value is selected, and in case of a tie, the PCE with the lower IP address is selected.

Note: The system does not support two or more simultaneously active PCEs.

The **no** form of the command removes the specified peer PCEP speaker.

Parameters *ip-address* — The IP address of the PCEP peer to be used as the destination address in the PCEP session.

preference — The preference value of the peer.

Values 0 to 100

Default 1

Platforms All

peer

Syntax **peer** *ip-address*
no peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>aarp peer)

Full Context configure application-assurance aarp peer

Description This command defines the IP address of the peer router which must be a routable system IP address.

If no peer is configured and the AARP is **no shutdown**, it is configured as a single node AARP instance.

The **no** form of this command removes the IP address from the AARP instance.

Default no peer

Parameters *ip-address* — Specifies the IP address in the a.b.c.d format.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

peer

Syntax [**no**] **peer** *peer-address*

Context [Tree] (config>router>msdp peer)
[Tree] (config>router>msdp>group peer)

Full Context configure router msdp group peer
configure router msdp peer

Description This command configures peer parameters. Multicast Source Discovery Protocol (MSDP) must have at least one peer configured. A peer is defined by configuring a local-address that can be used by this node to set up a peering session and the address of a remote MSDP router, It is the address of this remote peer that is configured in this command and it identifies the remote MSDP router address.

After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. It may be required to have multiple peering sessions in which case multiple peer statements should be included in the configurations.

By default, the options applied to a peer are inherited from the global or group-level. To override these inherited options, include peer-specific options within the peer statement.

If the peer address provided is already a configured peer, then this command only provides the context to configure the parameters pertaining to this peer.

If the peer address provided is not already a configured peer, then the peer instance must be created and the context to configure the parameters pertaining to this peer should be provided. In this case, the $ prompt to indicate that a new entity (peer) is being created should be used.

The peer address provided will be validated and, if valid, will be used as the remote address for an MSDP peering session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the **no** form of this command is entered, the existing peering address will be removed from the configuration and the existing session will be terminated. Whenever a session is terminated, all source active information pertaining to and learned from that peer will be removed. Whenever a new peering session is created or a peering session is lost, an event message should be generated.

At least one peer must be configured for MSDP to function.

Parameters *peer-address* — Specifies the peer IP address. address configured in this statement must identify the remote MSDP router that the peering session must be established with.

Platforms All

peer

Syntax **peer** *lic-name*
no peer

Context **[Tree]** (config>li>x-interfaces>x1 peer)

Full Context configure li x-interfaces x1 peer

Description This command configures the LIC name for X1 interface communication, which is configured under **config**>**li**>**x-interfaces**>**lics**>**lic**.

The **no** form of this command reverts to the default.

Parameters *lic-name* — Specifies the LIC name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax **peer** *lic-name*
no peer

Context **[Tree]** (config>li>x-interfaces>x2 peer)

Full Context configure li x-interfaces x2 peer

Description This command configures the LIC name for X2 interface communication, which is configured under **config**>**li**>**x-interfaces**>**lics**>**lic**.

The **no** form of this command reverts to the default.

Parameters *lic-name* — Specifies the LIC name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

peer

Syntax [**no**] **peer** *lic-name*

Context **[Tree]** (config>li>x-interfaces>x3>peers peer)

Full Context configure li x-interfaces x3 peers peer

Description This command configures the LIC name for X3 interface communication, which is configured under **config**>**li**>**x-interfaces**>**lics**>**lic**.

The **no** form of this command removes the LIC name.

Parameters *lic-name* — Specifies the name for the LIC peer, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer

Syntax [**no**] **peer** {*ip-address* | *ipv6-address*}

Context **[Tree]** (config>router>bfd>seamless-bfd peer)

Full Context configure router bfd seamless-bfd peer

Description This command specifies the context for the local mapping, used by an S-BFD initiator, between a discriminator for a far-end S-BFD reflector and its discriminator value.

The **no** form of this command removes the mapping for the peer.

Parameters *ip-address* — Specifies the IPv4 address of the peer.

Values a.b.c.d

ipv6-address — Specifies the IPv6 address of the peer.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

Platforms All

peer

Syntax **peer** [**router** *router-instance* | **service-name** *service-name*] {*ip-address* | *ipv6-address*} [**key-id** *key-id*] [**version** *version*] [**prefer**]
no peer [**router** *router-instance* | **service-name** *service-name*] {*ip-address* | *ipv6-address*}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>time>ntp peer)

Full Context configure system time ntp peer

Description This command configures symmetric active mode for an NTP peer. It is recommended to configure authentication and to only configure known time servers as peers. Peers may exist within a VPRN service.

Note: For symmetric peering to operate correctly with a peer accessible through a VPRN, local NTP server functionality must be enabled within the VPRN using the **config**>**service**>**vprn**>**ntp** command.

The **no** form of the command removes the configured peer.

Parameters *router-instance* — Specifies the routing context that contains the interface.

Values *router-name* —Base | Management
service-id — 1 to 2147483647

Default Base

service name — Specifies the service name for the VPRN, up to 64 characters. CPM routing instances are not supported.

ip-address — Configures the IPv4 address of the peer that requires a peering relationship to be set up.

Values a.b.c.d

Default None

ipv6-address — Configures the IPv6 address of the peer that requires a peering relationship to be set up.

Values
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF] H
- d: [0 to 255] D

Default None

key-id — Specifies the key ID. Successful authentication requires that both peers must have the same authentication key-id, type, and key value.

Specify the *key-id* that identifies the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP peer. If an NTP packet is received by these nodes, the authentication key-id, type, and key value must be valid, otherwise the packet will be rejected and an event or trap will be generated.

Values 1 to 255

Default None

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

version — Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode, in which case all versions are accepted.

Values 2 to 4

Default 4

prefer — When configuring more than one peer, one remote system can be configured as the preferred peer. When a second peer is configured as preferred, then the new entry overrides the old entry.

Platforms All

20.98 peer-address-change-policy

peer-address-change-policy

Syntax **peer-address-change-policy** {**accept** | **ignore** | **reject**}

Context **[Tree]** (config>router>l2tp peer-address-change-policy)
[Tree] (config>service>vprn>l2tp peer-address-change-policy)

Full Context configure router l2tp peer-address-change-policy
configure service vprn l2tp peer-address-change-policy

Description This command specifies what to do in case the system receives a L2TP response from another address than the one the request was sent to.

Default peer-address-change-policy reject

Parameters **accept** — Specifies that this system accepts any source IP address change of received L2TP control messages related to a locally originated tunnel in the state waitReply and rejects any peer address change for other tunnels; in case the new peer IP address is accepted, it is learned and used as destination address in subsequent L2TP messages.

ignore — Specifies that this system ignores any source IP address change of received L2TP control messages, does not learn any new peer IP address, and does not change the destination address in subsequent L2TP messages.

reject — Specifies that this system rejects any source IP address change of received L2TP control messages and drops those messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.99 peer-as

peer-as

Syntax **peer-as** *as-number*
no peer-as

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy peer-as)

Full Context configure subscriber-mgmt bgp-peering-policy peer-as

Description This command configures the autonomous system number for the remote peer. The peer AS number must be configured for each configured peer.

The **no** form of this command removes the *as-number* from the configuration.

Parameters *as-number* — Specifies the AS number for the remote peer.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

peer-as

Syntax **peer-as** *as-number*

Context **[Tree]** (config>service>vprn>bgp>group peer-as)
[Tree] (config>service>vprn>bgp>group>neighbor peer-as)

Full Context configure service vprn bgp group neighbor peer-as
configure service vprn bgp group peer-as

Description This command configures the autonomous system number for the remote peer. The peer AS number must be configured for each configured peer.

For EBGP peers, the peer AS number configured must be different from the autonomous system number configured for this router under the global level since the peer will be in a different autonomous system than this router

For IBGP peers, the peer AS number must be the same as the autonomous system number of this router configured under the global level.

This is a required command for each configured peer. This may be configured under the group level for all neighbors in a particular group.

Default No AS numbers are defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *as-number* — The autonomous system number, expressed as a decimal integer.

Values 1 to 65535

Platforms All

peer-as

Syntax **peer-as** *as-number*

Context **[Tree]** (config>router>bgp>group peer-as)
[Tree] (config>router>bgp>group>neighbor peer-as)

Full Context configure router bgp group neighbor peer-as
configure router bgp group peer-as

Description This command configures the autonomous system number for the remote peer. The peer AS number must be configured for each configured peer.

For EBGP peers, the peer AS number configured must be different from the autonomous system number configured for this router under the global level since the peer will be in a different autonomous system than this router.

For IBGP peers, the peer AS number must be the same as the autonomous system number of this router configured under the global level.

This is required command for each configured peer. This may be configured under the group level for all neighbors in a particular group.

Parameters *as-number* — Specifies the autonomous system number expressed as a decimal integer.

Values 1 to 4294967295

Platforms All

20.100 peer-endpoint

peer-endpoint

Syntax **peer-endpoint sap** *sap-id* **encap-type** {**dot1q** | **null** | **qinq**}
peer-endpoint spoke-sdp *sdp-id:vc-id*
no peer-endpoint

Context **[Tree]** (config>app-assure>aarp peer-endpoint)

Full Context configure application-assurance aarp peer-endpoint

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the peer endpoint ID of the SAP or spoke-SDP parent-aa-sub of the AARP peer.

The **no** form of this command removes the peer endpoint from the AARP instance.

Default no peer-endpoint

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 to 32767
1 to 4294967295

dot1q | **null** | **qinq** — Specifies the encapsulation type.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.101 peer-group

peer-group

Syntax **peer-group** *tunnel-group-id*
no peer-group

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group peer-group)

Full Context configure redundancy multi-chassis peer mc-ipsec tunnel-group peer-group

Description This command specifies the corresponding tunnel-group ID on peer node. The peer tunnel-group ID does not necessary equals to local tunnel-group ID.

The **no** form of this command removes the tunnel-group ID from the configuration.

Parameters *tunnel-group-id* — Specifies the tunnel-group identifier.

Values 1 to 16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.102 peer-interface-address

peer-interface-address

Syntax **peer-interface-address** *ip-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>lmp>peer>control-channel peer-interface-address)

Full Context configure router lmp peer control-channel peer-interface-address

Description This command configures the mandatory **peer-interface-address**. It is the destination address of the IPCC on the peer UNI-N used to reach the GMPLS Router ID of the UNI-N peer. It corresponds to the lmpCcRemoteIpAddr in RFC 4631.

Parameters *ip-address* — The interface address of the IPCC next-hop.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x to [0 to FFFF]H
d to [0 to 255]D

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.103 peer-ip-address

peer-ip-address

Syntax **peer-ip-address** *ip-address*
no peer-ip-address

Context [Tree] (config>service>ies>if>ipcp peer-ip-address)

Full Context configure service ies interface ipcp peer-ip-address

Description This command defines the remote IP address to be assigned to the far-end of the associated PPP or MLPPP link via IPCP extensions. This command is only applicable if the associated SAP or port is a PPP or MLPPP interface with an IPCP encapsulation.

The **no** form of this command reverts to the default value.

Default no peer-ip-address (0.0.0.0)

Parameters *ip-address* — Specifies a unicast IPv4 address to be signaled to the far-end of the associated PPP or MLPPP link by IPCP extensions.

Platforms All

peer-ip-address

Syntax **peer-ip-address** *ip-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no peer-ip-address

Context **[Tree]** (config>service>vprn>if>ipcp peer-ip-address)

Full Context configure service vprn interface ipcp peer-ip-address

Description This command defines the remote IP address to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface with an IPCP encapsulation.

The interface must be shut down to modify the IPCP configuration.

The **no** form of this command deletes the IPCP extension peer-ip-address configuration.

Default no peer-ip-address (0.0.0.0)

Parameters *ip-address* — Specifies a unicast IPv4 address to be signaled to the far-end of the associated PPP/MLPPP link by IPCP extensions.

Platforms All

20.104 peer-ip-prefix

peer-ip-prefix

Syntax **peer-ip-prefix** *ip-prefix/ip-prefix-length*
peer-ip-prefix ipv4-any
peer-ip-prefix ipv6-any
no peer-ip-prefix

Context **[Tree]** (config>ipsec>client-db>client>client-id peer-ip-prefix)

Full Context configure ipsec client-db client client-identification peer-ip-prefix

Description This command specifies match criteria that uses the peer's tunnel IP address as the input. Only one peer-ip-prefix criteria can be configured for a given client entry.

The **no** form of this command reverts to the default.

Default no peer-ip-prefix

Parameters *ip-prefix/ip-prefix-length* — Specifies an IPv4 or IPv6 prefix. It is considered a match if the peer's tunnel IP address is within the specified prefix.

ipv4-any — Matches any IPv4 address.

ipv6-any — Matches any IPv6 address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

peer-ip-prefix

Syntax [**no**] **peer-ip-prefix**

Context **[Tree]** (config>ipsec>client-db>match-list peer-ip-prefix)

Full Context configure ipsec client-db match-list peer-ip-prefix

Description This command enables the use of the peer's tunnel IP address as the match input.

The **no** form of this command disables the peer IP prefix matching process.

Default no peer-ip-prefix

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.105 peer-limit

peer-limit

Syntax **peer-limit** *limit*
no peer-limit

Context **[Tree]** (config>service>vprn>ptp peer-limit)

Full Context configure service vprn ptp peer-limit

Description This command specifies an upper limit to the number of discovered peers permitted within the routing instance. This command can ensure that a routing instance does not consume all the possible discovered peers and blocking discovered peers in other routing instances.

If it is desired to reserve a fixed number of discovered peers per router instance, then all router instances supporting PTP should have values specified with this command and the sum of all the peer-limit values must not exceed the maximum number of discovered peers supported by the system.

If the user attempts to specify a peer-limit, and there are already more discovered peers in the routing instance than the new limit being specified, the configuration is not accepted.

The **no** form of this command removes the limit from the configuration.

Default no limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *limit* — Specifies the maximum number of discovered peers allowed in the routing instance.

Values 0 to 50

Default 0 (The maximum number of discovered peers supported by the system).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

peer-limit

Syntax **peer-limit** *limit*
no peer-limit

Context **[Tree]** (config>system>ptp peer-limit)

Full Context configure system ptp peer-limit

Description This command specifies an upper limit to the number of discovered peers permitted within the routing instance. This can be used to ensure that a routing instance does not consume all the possible discovered peers and blocking discovered peers in other routing instances.

If it is desired to reserve a fixed number of discovered peers per router instance, then all router instances supporting PTP should have values specified with this command and the sum of all the peer-limit values must not exceed the maximum number of discovered peers supported by the system.

If the user attempts to specify a peer-limit, and there are already more discovered peers in the routing instance than the new limit being specified, the configuration will not be accepted.

Default no peer-limit

Parameters *limit* — Specifies the maximum number of discovered peers allowed in the routing instance.

Values 0 to 512

Default 1 (The maximum number of discovered peers supported by the system.)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.106 peer-loopback-address

peer-loopback-address

Syntax **peer-loopback-address** *ip-address*
no peer-loopback-address

Context **[Tree]** (config>router>lmp>peer peer-loopback-address)

Full Context configure router lmp peer peer-loopback-address

Description The IP address corresponding to the GMPLS loopback address configured on the LMP peer. If **peer-loopback-address** is entered, then this is used as the routable peer address, otherwise the *peer-node-id* is assumed to correspond to a routable peer loopback.

peer-loopback-address is an optional configurable field. If **peer-loopback-address** is not configured, the router will use **lmp-peer-node-id** (that is LmpNbrNodeId as per RFC 4631) as the dstIpAddr in the IP-header for the peer-specific messages (that is, Link summary msgs, RSVP msgs).

Note: The **peer-interface-address** is mandatory; it is the destination address of the IPCC on the peer UNI-N used to reach the GMPLS Router ID of the UNI-N peer. It corresponds to the lmpCcRemoteIpAddr in RFC 4631.

Default no peer-loopback-address

Parameters *ip-address* — The GMPLS control plane loopback address of the IPCC next-hop.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x to [0 to FFFF]H
d to [0 to 255]D

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.107 peer-name

peer-name

Syntax **peer-name** *name*
no peer-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>redundancy>multi-chassis>peer peer-name)

Full Context configure redundancy multi-chassis peer peer-name

Description This command specifies a peer name.

Default no peer-name

Parameters *name* — Specifies the string up to 32 characters. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

20.108 peer-profile

peer-profile

Syntax **peer-profile** *profile-name* [**create**]
no peer-profile *profile-name*

Context [Tree] (config>subscr-mgmt>gtp peer-profile)

Full Context configure subscriber-mgmt gtp peer-profile

Description This command creates a new peer profile.

Parameters *profile-name* — Specifies the profile name, up to 32 characters.

create — Creates an entry.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.109 peer-profile-map

peer-profile-map

Syntax **peer-profile-map**

Context [Tree] (config>router>gtp>s11 peer-profile-map)
[Tree] (config>service>vprn>gtp>s11 peer-profile-map)
[Tree] (config>router>gtp>uplink peer-profile-map)
[Tree] (config>service>vprn>gtp>uplink peer-profile-map)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router gtp s11 peer-profile-map
configure router gtp uplink peer-profile-map
configure service vprn gtp s11 peer-profile-map
configure service vprn gtp uplink peer-profile-map

Description This command configures a mapping of addresses and subnets to GTP peer profiles.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.110 peer-rdi-rx

peer-rdi-rx

Syntax **peer-rdi-rx**

Context **[Tree]** (config>port>ethernet>efm-oam peer-rdi-rx)

Full Context configure port ethernet efm-oam peer-rdi-rx

Description This container allows an action to be configured for the various event conditions that can be received from a peer under the context of the EFM OAM protocol.

Platforms All

20.111 peer-template

peer-template

Syntax [**no**] **peer-template** *template-name*

Context **[Tree]** (config>router>ldp>targeted-session peer-template)

Full Context configure router ldp targeted-session peer-template

Description This command creates a targeted session peer parameter template that can be referenced in the automatic creation of targeted Hello adjacency and LDP session to a discovered peer.

The **no** form of this command deletes the peer template. A peer template cannot be deleted if it is bound to a peer prefix list.

Parameters *template-name* — Specifies the template name to identify targeted peer template. It must be 32 characters maximum.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.112 peer-template-map

peer-template-map

Syntax **peer-template-map** *template-name* **policy** *peer-prefix-policy1* [*peer-prefix-policy2..up to 5*]
no peer-template-map peer-template *template-name*

Context **[Tree]** (config>router>ldp>targeted-session peer-template-map)

Full Context configure router ldp targeted-session peer-template-map

Description This command enables the automatic creation of a targeted Hello adjacency and LDP session to a discovered peer. The user configures a targeted session peer parameter template and binds it to a peer prefix policy.

Each application of a targeted session template to a given prefix in the prefix list will result in the establishment of a targeted Hello adjacency to an LDP peer using the template parameters as long as the prefix corresponds to a router-id for a node in the TE database. As a result of this, the user must enable the traffic-engineering option in ISIS or OSPF. The targeted Hello adjacency will either trigger a new LDP session or will be associated with an existing LDP session to that peer.

Up to 5 peer prefix policies can be associated with a single peer template at all times. Also, the user can associate multiple templates with the same or different peer prefix policies. Thus multiple templates can match with a given peer prefix. In all cases, the targeted session parameters applied to a given peer prefix are taken from the first created template by the user. This provides a more deterministic behavior regardless of the order in which the templates are associated with the prefix policies.

Each time the user executes the above command, with the same or different prefix policy associations, or the user changes a prefix policy associated with a targeted peer template, the system re-evaluates the prefix policy. The outcome of the re-evaluation will tell LDP if an existing targeted Hello adjacency needs to be torn down or if an existing targeted Hello adjacency needs to have its parameters updated on the fly.

If a /32 prefix is added to (removed from) or if a prefix range is expanded (shrunk) in a prefix list associated with a targeted peer template, the same prefix policy re-evaluation described above is performed.

The template comes up in the **no shutdown** state and as such it takes effect immediately. Once a template is in use, the user can change any of the parameters on the fly without shutting down the template. In this case, all targeted Hello adjacencies are updated.

The SR OS supports multiple ways of establishing a targeted Hello adjacency to a peer LSR:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- User configuration of the peer with the targeted session parameters inherited from the **config>router>ldp>targeted-session** in the top level context or explicitly configured for this peer in the **config>router>ldp>targ-session>peer** context and which overrides the top level parameters shared by all targeted peers. Let us refer to the top level configuration context as the global context. Some parameters only exist in the global context; their value will always be inherited by all targeted peers regardless of which event triggered it.
- User configuration of an SDP of any type to a peer with the signaling tldp option enabled (default configuration). In this case the targeted session parameter values are taken from the global context.
- User configuration of a (FEC 129) PW template binding in a BGP-VPLS service. In this case the targeted session parameter values are taken from the global context.
- User configuration of a (FEC 129 type II) PW template binding in a VLL service (dynamic multi-segment PW). In this case the target session parameter values are taken from the global context
- User configuration of a mapping of a targeted session peer parameter template to a prefix policy when the peer address exists in the TE database (this feature). In this case, the targeted session parameter values are taken from the template.

Since the above triggering events can occur simultaneously or in any arbitrary order, the LDP code implements a priority handling mechanism in order to decide which event overrides the active targeted session parameters. The overriding trigger will become the owner of the targeted adjacency to a given peer. The following is the priority order:

- Priority 1: manual configuration of session parameters
- Priority 2: mapping of targeted session template to prefix policy.
- Priority 3: auto-tx parameters
- Priority 4: auto-rx parameters
- Priority 5: manual configuration of SDP, PW template binding in BGP-AD VPLS and in FEC 129 VLL.

Any parameter value change to an active targeted Hello adjacency caused by any of the above triggering events is performed on the fly by having LDP immediately send a Hello message with the new parameters to the peer without waiting for the next scheduled time for the Hello message. This allows the peer to adjust its local state machine immediately and maintains both the Hello adjacency and the LDP session in UP state. The only exceptions are the following:

- The triggering event caused a change to the local-lsr-id parameter value. In this case, the Hello adjacency is brought down which will also cause the LDP session to be brought down if this is the last Hello adjacency associated with the session. A new Hello adjacency and LDP session will then get established to the peer using the new value of the local LSR ID.
- The triggering event caused the targeted peer shutdown option to be enabled. In this case, the Hello adjacency is brought down which will also cause the LDP session to be brought down if this is the last Hello adjacency associated with the session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Finally, the value of any LDP parameter which is specific to the LDP/TCP session to a peer is inherited from the **config>router>ldp>session-params>peer** context. This includes MD5 authentication, LDP prefix per-peer policies, label distribution mode (DU or DOD), and so on.

The **no** form of this command deletes the binding of the template to the peer prefix list and brings down all Hello adjacencies to the discovered LDP peers.

Platforms All

20.113 peer-to-peer

peer-to-peer

Syntax [**no**] **peer-to-peer**

Context **[Tree]** (debug>diameter>node>peer peer-to-peer)

Full Context debug diameter node peer peer-to-peer

Description This command reports only peer level message that are required for bringing up, maintaining and tearing down the peering connection (CER/A, DWR/A, and so on).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.114 peer-tracking-policy

peer-tracking-policy

Syntax **peer-tracking-policy** *policy-name*
no peer-tracking-policy

Context **[Tree]** (config>service>vprn>bgp peer-tracking-policy)

Full Context configure service vprn bgp peer-tracking-policy

Description This command specifies the name of a policy statement to use with the BGP peer-tracking function on the BGP sessions where this is enabled. The policy controls which IP routes in RTM are eligible to indicate reachability of IPv4 and IPv6 BGP neighbor addresses. If the longest matching route in RTM for a BGP neighbor address is an IP route that is rejected by the policy, or it is a BGP route accepted by the policy, or if there is no matching route, the neighbor is considered unreachable and BGP tears down the peering session and holds it in the idle state until a valid route is once again available and accepted by the policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default peer-tracking policy (when the **no peer-tracking-policy** command is configured) is to use the longest matching active route in RTM that is not an LDP shortcut route or an aggregate route.

Note: When **peer-tracking** is configured, the peer-tracking policy should only permit one of **direct-interface** or **direct** routes to be advertised to a BGP peer. Advertising both routes will cause the best route to oscillate.

Default no peer-tracking-policy

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 64 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

peer-tracking-policy

Syntax **peer-tracking-policy** *policy-name*
no peer-tracking-policy

Context **[Tree]** (config>router>bgp peer-tracking-policy)

Full Context configure router bgp peer-tracking-policy

Description This command specifies the name of a policy statement to use with the BGP peer-tracking function on the BGP sessions where this is enabled. The policy controls which IP routes in RTM are eligible to indicate reachability of IPv4 and IPv6 BGP neighbor addresses. If the longest matching route in RTM for a BGP neighbor address is an IP route that is rejected by the policy, or it is a BGP route accepted by the policy, or if there is no matching route, the neighbor is considered unreachable and BGP tears down the peering session and holds it in the idle state until a valid route is once again available and accepted by the policy.

The default peer-tracking policy (when the **no peer-tracking-policy** command is configured) is to use the longest matching active route in RTM that is not an LDP shortcut route or an aggregate route.

Note: When **peer-tracking** is configured, the peer-tracking policy should only permit one of **direct-interface** or **direct** routes to be advertised to a BGP peer. Advertising both routes will cause the best route to oscillate.

Default no peer-tracking-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

20.115 peer-transport

peer-transport

Syntax **peer-transport** *ip-address*
no peer transport

Context **[Tree]** (config>router>ldp>tcp-session-parameters peer-transport)

Full Context configure router ldp tcp-session-parameters peer-transport

Description This command configures the peer transport address, that is, the destination address of the TCP connection, and not the address corresponding to the LDP LSR-ID of the peer.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the TCP connection to the LDP peer in dotted decimal notation.

Platforms All

20.116 peer6

peer6

Syntax **peer6** *ipv6-address*
no peer6

Context **[Tree]** (config>router>nat>inside>redundancy peer6)
[Tree] (config>service>vprn>nat>inside>redundancy peer6)

Full Context configure router nat inside redundancy peer6
configure service vprn nat inside redundancy peer6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used in NAT64 multi-chassis redundancy in conjunction with filters. The configured peer6 address is an IPv6 address configured under an interface on the peering NAT64 node (active or standby). This IPv6 interface address is advertised via routing on the inside in order to attract traffic from the standby to the active NAT64 node.

Under normal circumstances, the NAT64 prefix will be advertised only from the active NAT64 node. Consequently, upstream traffic for NAT64 will be attracted to the active NAT64 node. The nat action in the ipv6-filter on the active NAT64 node will forward traffic to the local MS-ISA where NAT64 function is performed. However, in that case that upstream traffic somehow arrives on the standby NAT64 node, the nat action in the IPv6-filter will forward traffic to the peer6 address (active NAT64 node).

The **no** form of the command removes the peer6 ip-address from the configuration.

Default none

Parameters *ipv6-address* — Specifies the IPv6 address of the NAT redundancy peer.

Values

ipv6-address:	ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.117 peers

peers

Syntax **peers**

Context **[Tree]** (config>li>x-interfaces>x3 peers)

Full Context configure li x-interfaces x3 peers

Description This command enables the configuration of X3 peer LICs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.118 pending-requests-limit

pending-requests-limit

Syntax **pending-request-limit** *limit*
no pending-request-limit

Context **[Tree]** (config>router>radius-server>server pending-requests-limit)
[Tree] (config>service>vprn>radius-server>server pending-requests-limit)

Full Context configure router radius-server server pending-requests-limit
configure service vprn radius-server server pending-requests-limit

Description This command specifies the per-server maximum number of outstanding requests sent to the RADIUS server. If the maximum number is exceeded, the next RADIUS server in the pool is selected.

The **no** form of this command removes the limit value from the configuration.

Default pending-requests-limit 4096

Parameters *limit* — Specifies the maximum number of outstanding requests sent to the RADIUS server.

Values 1 to 4096

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.119 peq

peq

Syntax [**no**] **peq** *peq-slot* [**chassis** *chassis-id*]

Context **[Tree]** (config>system>power-management peq)

Full Context configure system power-management peq

Description This command sets the APEQ slot number. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Parameters *peq-slot* — Identifies the APEQ slot.

Values 1 to 12

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

chassis-id — Specifies chassis ID for the router chassis.

Values 1, 2

Default 1

Platforms 7750 SR-12e, 7950 XRS

20.120 peq-type

peq-type

Syntax **peq-type** *peq-type*
no peq-type

Context **[Tree]** (config>system>pwr-mgmt>peq peq-type)

Full Context configure system power-management peq peq-type

Description This command sets the type of APEQ for the designated APEQ slot. This command is supported in the 7750 SR-S OS and 7950 XRS only.

The **no** form of this command moves the APEQ to an unprovisioned state.

Default no peq-type

Parameters *peq-type* — Identifies the APEQ type.

Values apeq-ac-4400, apeq-ac-3000, apeq-dc-2000, apeq-dc-2200-2800, apeq-dc-4275, apeq-hvdc-3000

Platforms 7750 SR-12e, 7950 XRS

20.121 per-fp-egr-queuing

per-fp-egr-queuing

Syntax [**no**] **per-fp-egr-queuing**

Context **[Tree]** (config>lag>access per-fp-egr-queuing)

Full Context configure lag access per-fp-egr-queuing

Description This command specifies whether a more efficient method of queue allocation for LAG SAPs should be utilized.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the method of queue allocation for LAG SAPs.

Platforms All

20.122 per-fp-ing-queuing

per-fp-ing-queuing

Syntax [**no**] **per-fp-ing-queuing**

Context **[Tree]** (config>lag>access per-fp-ing-queuing)

Full Context configure lag access per-fp-ing-queuing

Description This command provides the ability to reduce the number of hardware queues assigned on each LAG SAP ingress. When the feature is enabled, the queue allocation for SAPs on a LAG will be optimized and only one set of queues per ingress forwarding path (FP) is allocated instead of one per port.

The **no** form of this command disables the method of queue allocation for LAG SAPs.

Platforms All

per-fp-ing-queuing

Syntax [**no**] **per-fp-ing-queuing**

Context **[Tree]** (config>eth-tunnel>lag-emulation>access per-fp-ing-queuing)

Full Context configure eth-tunnel lag-emulation access per-fp-ing-queuing

Description This command provides the ability to reduce the number of hardware queues assigned on each LAG SAP ingress. When the feature is enabled, the queue allocation for SAPs on a LAG will be optimized and only one set of queues per ingress forwarding path (FP) is allocated instead of one per port.

The **no** form of this command reverts the default.

Default no per-fp-ing-queuing

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.123 per-fp-sap-instance

per-fp-sap-instance

Syntax [**no**] **per-fp-sap-instance**

Context **[Tree]** (config>lag>access per-fp-sap-instance)

Full Context configure lag access per-fp-sap-instance

Description This command enables optimized SAP instance allocation on a LAG. When enabled, SAP instance is allocated per each FP the LAG links exits on instead of per each LAG port.

The **no** form of this command disables optimized SAP instance allocation.

Default no per-fp-sap-instance

Platforms All

20.124 per-host-authentication

per-host-authentication

Syntax [**no**] **per-host-authentication**

Context **[Tree]** (config>port>ethernet>dot1x per-host-authentication)

Full Context configure port ethernet dot1x per-host-authentication

Description This command enables dot1x authenticating per host source mac or VLAN. The port does not allow traffic from any hosts or any MAC. When a host is authenticated via RADIUS policy, its source mac is then allowed through the port, while the port is closed for any other mac. Any traffic from the allowed host is forwarded on the port, including untagged and tagged traffic.

Default no per-host-authentication

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.125 per-host-replication

per-host-replication

Syntax **per-host-replication** [**uni-mac** | **mcast-mac**]
no per-host-replication

Context **[Tree]** (config>subscr-mgmt>igmp-policy per-host-replication)

Full Context configure subscriber-mgmt igmp-policy per-host-replication

Description This command enables per-host-replication in IPoE model. For PPPoX, per-host-replication is the only mode of operation. In the per-host-replication mode, multicast traffic is replicated per each host within the subscriber irrespective of the fact that some hosts may be subscribed to the same multicast stream. As a result, in case that multiple hosts within the subscriber are registered for the same multicast group, the multicast streams of that group is generated. The destination MAC address of multicast streams is changed to unicast so that each host receives its own copy of the stream. Multicast traffic in the per-host-replication mode can be classified via the existing QoS CLI structure. As such the multicast traffic will flow through the subscriber queues. HQoS Adjustment is not needed in this case.

The alternative behavior for multicast replication in IPoE environment is per-SAP- replication. In this model, only a single copy of the multicast stream is sent per SAP, irrespective of the number of hosts that are subscribed to the same multicast group. This behavior applies to 1:1 connectivity model as well as on 1:N connectivity model (SAP centric behavior as opposed to subscriber centric behavior).

In the per-SAP-replication model the destination MAC address is multicast (as opposed to unicast in the per-host-replication model). Multicast traffic is flowing via the SAP queue which is outside of the subscriber context. The consequence is that multicast traffic is not accounted in the subscriber HQoS. In addition, HQoS Adaptation is not supported in the per SAP replication model.

Default no per-host-replication — By default there is no per host replication and replication is done per SAP. This mode utilizes the SAP queues. With per-host-replication it will allow the use of the subscriber queues. Per-host-replication uses unicast MAC and multicast IP to deliver multicast content to end hosts. This is useful for multi host per SAP cases. To interoperate with end devices that do not support unicast MAC, there is an option to use per-host-replication with a multicast MAC. The traffic is the same as replication per SAP but the difference of using the subscriber queues.

Parameters **uni-mac** — Specifies that multicast traffic is sent with a unicast MAC and multicast IP.

mcast-mac — Specifies that multicast traffic is sent with a multicast MAC and IP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

per-host-replication

Syntax [**no**] **per-host-replication** [**uni-mac** | **mcast-mac**]

Context **[Tree]** (config>subscr-mgmt>mld-policy per-host-replication)

Full Context configure subscriber-mgmt mld-policy per-host-replication

Description This command enables per-host-replication. In the per-host-replication mode, multicast traffic is replicated per each host within the subscriber irrespective of the fact that some hosts may be subscribed to the same multicast stream. As a result, in case that multiple hosts within the subscriber are registered for the same multicast group, the multicast streams of that group are generated. The destination MAC address of multicast streams is changed to unicast so that each host receives its own copy of the stream. Multicast traffic in the per-host-replication mode can be classified via the existing QoS CLI structure. As such the multicast traffic flows through the subscriber queues. HQoS Adjustment is not needed in this case.

The alternative behavior for multicast replication in IPoE environment is per-SAP- replication. In this model, only a single copy of the multicast stream is sent per SAP, irrespective of the number of hosts that are subscribed to the same multicast group. This behavior applies to 1:1 connectivity model as well as on 1:N connectivity model (SAP centric behavior as opposed to subscriber centric behavior).

In the per-SAP-replication model the destination MAC address is multicast (as opposed to unicast in the per-host-replication model). Multicast traffic is flowing via the SAP queue which is outside of the subscriber context. The consequence is that multicast traffic is not accounted in the subscriber HQoS. In addition, HQoS Adaptation is not supported in the per SAP replication model.

The **no** form of this command reverts to the default.

Parameters **uni-mac** — Specifies that multicast traffic s sent with a unicast MAC and multicast IP.

mcast-mac — Specifies the multicast traffic is sent with a multicast MAC and IP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.126 per-link-hash

per-link-hash

Syntax **per-link-hash**
per-link-hash weighted [**auto-rebalance**]
no per-link-hash

Context **[Tree]** (config>lag per-link-hash)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure lag per-link-hash

Description This command configures per-link-hashing on a LAG. When enabled, SAPs/subscribers/interfaces are hashed on LAG egress to a single LAG link.

The **no** form of this command disables per-link-hashing on a LAG.

Default no per-link-hash

Parameters **weighted** — SAPs/subscribers/interfaces are distributed amongst LAG links based on their preconfigured class and weight. As new links are added to a LAG, existing SAPs/subscribers/interfaces are not impacted.

auto-rebalance — SAPs/subscribers/interfaces are distributed amongst LAG links based on their preconfigured class and weight. As new links are added to a LAG, existing SAPs/subscribers/interfaces are rebalanced automatically.

Platforms All

20.127 per-mcast-plane-capacity

per-mcast-plane-capacity

Syntax [**no**] **per-mcast-plane-capacity**

Context **[Tree]** (config>mcast-mgmt>chassis-level per-mcast-plane-capacity)

Full Context configure mcast-management chassis-level per-mcast-plane-capacity

Description Commands in this context configure multicast plane bandwidth parameters. This CLI node contains the configuration of the overall multicast (primary plus secondary) and specific secondary rate limits for each switch fabric multicast plane.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

20.128 per-peer-queuing

per-peer-queuing

Syntax [**no**] **per-peer-queuing**

Context **[Tree]** (config>system>security per-peer-queuing)

Full Context configure system security per-peer-queuing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables CPM hardware queuing per peer. This means that when a peering session is established, the router will automatically allocate a separate CPM hardware queue for that peer.

The **no** form of this command disables CPM hardware queuing per peer.

Default per-peer-queuing

Platforms All

20.129 per-service-hashing

per-service-hashing

Syntax [**no**] **per-service-hashing**

Context **[Tree]** (config>service>epipe>load-balancing per-service-hashing)

Full Context configure service epipe load-balancing per-service-hashing

Description This command enables on a per service basis, consistent per-service hashing for Ethernet services over LAG, over Ethernet tunnel (eth-tunnel) using loadsharing protection-type or over CCAG. Specifically, it enables the new hashing procedures for Epipe, VPLS, regular or PBB services.

The following algorithm describes the hash-key used for hashing when the new option is enabled:

- If the packet is PBB encapsulated (contains an I-TAG ethertype) at the ingress side, use the ISID value from the I-TAG
- If the packet is not PBB encapsulated at the ingress side
  - For regular (non-PBB) VPLS and Epipe services, use the related service ID
  - If the packet is originated from an ingress IVPLS or PBB Epipe SAP
  - If there is an ISID configured use the related ISID value
  - If there is no ISID yet configured use the related service ID
  - For BVPLS transit traffic use the related flood list id
  - Transit traffic is the traffic going between BVPLS endpoints
  - An example of non-PBB transit traffic in BVPLS is the OAM traffic
  - The preceding rules apply regardless of traffic type
  - Unicast, BUM flooded without MMRP or with MMRP, IGMP snooped

The **no** form of this command implies the use of existing hashing options.

Default no per-service-hashing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

per-service-hashing

Syntax [**no**] **per-service-hashing**

Context **[Tree]** (config>service>vpls>load-balancing per-service-hashing)
[Tree] (config>service>template>vpls-template>load-balancing per-service-hashing)

Full Context configure service template vpls-template load-balancing per-service-hashing
configure service vpls load-balancing per-service-hashing

Description This command enables on a per service basis, consistent per-service hashing for Ethernet services over LAG, over Ethernet tunnel (eth-tunnel) using loadsharing protection-type or over CCAG. Specifically, it enables the new hashing procedures for Epipe, VPLS, regular or PBB services.

The following algorithm describes the hash-key used for hashing when the new option is enabled:

- If the packet is PBB encapsulated (contains an I-TAG ethertype) at the ingress side, use the ISID value from the I-TAG
- If the packet is not PBB encapsulated at the ingress side
  - For regular (non-PBB) VPLS and Epipe services, use the related service ID
  - If the packet is originated from an ingress IVPLS or PBB Epipe SAP
- If there is an ISID configured use the related ISID value
- If there is no ISID yet configured use the related service ID
  - For BVPLS transit traffic use the related flood list id
- Transit traffic is the traffic going between BVPLS endpoints
- An example of non-PBB transit traffic in BVPLS is the OAM traffic
- The above rules apply regardless of traffic type
  - Unicast, BUM flooded without MMRP or with MMRP, IGMP snooped

The **no** form of this command implies the use of existing hashing options.

Default no per-service-hashing

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.130 per-source-rate

per-source-rate

Syntax **per-source-rate** *packet-rate-limit*
no per-source-rate

Context **[Tree]** (config>sys>security>cpu-protection>policy per-source-rate)

Full Context configure system security cpu-protection policy per-source-rate

Description This command configures a per-source packet arrival rate limit. Use this command to apply a packet arrival rate limit on a per source basis. A source is defined as a unique combination of SAP and MAC source address (mac-monitoring) or SAP and source IP address (ip-src-monitoring). The CPU will receive no more than the configured packet rate from each source (only certain protocols are rate limited for ip-src-monitoring as configured under **include-protocols** in the **cpu-protection** policy). The measurement is cleared each second.

This parameter is only applicable if the policy is assigned to an interface (some examples include saps, subscriber-interfaces, and spoke-sdps), and the **mac-monitor** or **ip-src-monitor** keyword is specified in the **cpu-protection** configuration of that interface.

The ip-src-monitoring is useful in subscriber management architectures that have routers between the subscriber and the BNG (router). In layer-3 aggregation scenarios, all packets from all subscribers behind the same aggregation router will arrive with the same source MAC address and as such the mac-monitoring functionality can not differentiate traffic from different subscribers.

Default per-source-rate max

Parameters *packet-rate-limit* — Specifies a per-source packet (per SAP/MAC source address or per SAP/IP source address) arrival rate limit in packets per second.

Values 1 to 65535, **max** (max indicates no limit)

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

20.131 per-spi-replication

per-spi-replication

Syntax [**no**] **per-spi-replication**

Context **[Tree]** (config>subscr-mgmt>igmp-policy per-spi-replication)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt igmp-policy per-spi-replication

Description This command enables per-SLA Profile Instance (SPI) replication. In this mode, a multicast stream is transmitted for the subscriber host SLA profile for each registered multicast group (channel). As a result, multiple copies of the same multicast stream are transmitted over the same SAP. The replication of the multicast packets depends on the number of SLA profile instances configured for the subscriber. For example, if the subscriber hosts use three SLA profiles, the (S,G) is replicated three times, but if the subscriber hosts use the same SLA profile, the (S,G) is only replicated once.

The **no** form of this command disables per-SPI replication.

Default no per-spi-replication

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.132 per-user

per-user

Syntax **per-user user-directory** *dir-url* **file-name** *file-name*
no per-user

Context **[Tree]** (config>system>login-control>login-scripts per-user)

Full Context configure system login-control login-scripts per-user

Description This command allows users to define their own login scripts that can be executed each time they first login to a CLI session. The command executes the script “*file-url* / *username* / *file-name*" when the user *username* logs into a CLI session (authenticated by any means including local user database, TACACS+, or RADIUS).

For example:

per-user user-directory "cf1:/local/users" file-name "login-script.txt"

would search for the following script when user “admin” logs in and authenticates via RADIUS:

cf1:/local/users/admin/login-script.txt

The per user login script is executed after any global script executes and before any login-exec script configured against a local user is executed. This allows users, for example, who are authenticated via TACACS+ or RADIUS to define their own login scripts.

This CLI script executes in the context of the user who opens the CLI session. Any commands in the script that the user is not authorized to execute will fail.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the execution of any per user login-scripts.

Default no per-user

Parameters *dir-url* — Specifies the path or directory name.

file-name — Specifies the name of the file (located in the *dir-url* directory) including the extension.

Platforms All

20.133 percent-rate

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]

Context **[Tree]** (config>port>eth>access>egr>qgrp>qover>q percent-rate)
[Tree] (config>port>ethernet>network>egr>qgrp>qover>q percent-rate)

Full Context configure port ethernet access egress queue-group queue-overrides queue percent-rate
configure port ethernet network egress queue-group queue-overrides queue percent-rate

Description This command specifies percent rates (CIR and PIR).

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **percent-rate** is performed under the **hs-wrr-group** within the egress queue group template.

Parameters *pir-percent* — Specifies the PIR as a percentage.

Values 0.01 to 100.00

cir-percent — Specifies the CIR as a percentage.

Values 0.00 to 100.00

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>service>apipe>sap>egress>policer-over>plcr percent-rate)
[Tree] (config>service>apipe>sap>ingress>policer-over>plcr percent-rate)
[Tree] (config>service>cpipe>sap>egress>policer-over>plcr percent-rate)
[Tree] (config>service>cpipe>sap>ingress>policer-over>plcr percent-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ipipe>sap>egress>policer-over>plcr percent-rate)
[Tree] (config>service>ipipe>sap>ingress>policer-over>plcr percent-rate)
[Tree] (config>service>epipe>sap>egress>policer-over>plcr percent-rate)

Full Context configure service apipe sap egress policer-override policer percent-rate
configure service apipe sap ingress policer-override policer percent-rate
configure service cpipe sap egress policer-override policer percent-rate
configure service cpipe sap ingress policer-override policer percent-rate
configure service epipe sap egress policer-override policer percent-rate
configure service ipipe sap egress policer-override policer percent-rate
configure service ipipe sap ingress policer-override policer percent-rate

Description This command configures the percent rates (CIR and PIR) override.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the policers's parent arbiter rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the policer's CIR as a percentage of the policers's parent arbiter rate.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress policer-override policer percent-rate
- configure service cpipe sap egress policer-override policer percent-rate

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap ingress policer-override policer percent-rate
- configure service epipe sap egress policer-override policer percent-rate
- configure service ipipe sap egress policer-override policer percent-rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap egress policer-override policer percent-rate
- configure service apipe sap ingress policer-override policer percent-rate

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context [Tree] (config>service>apipe>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue percent-rate)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue percent-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>epipe>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue percent-rate)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue percent-rate)

Full Context

configure service apipe sap egress queue-override queue percent-rate
configure service apipe sap ingress queue-override queue percent-rate
configure service cpipe sap egress queue-override queue percent-rate
configure service cpipe sap ingress queue-override queue percent-rate
configure service epipe sap egress queue-override queue percent-rate
configure service fpipe sap egress queue-override queue percent-rate
configure service fpipe sap ingress queue-override queue percent-rate
configure service ipipe sap egress queue-override queue percent-rate
configure service ipipe sap ingress queue-override queue percent-rate

Description

The percent-rate command within the SAP ingress and egress QoS policy enables supports for a queue's PIR and CIR rate to be configured as a percentage of the egress port's line rate or of its parent scheduler's rate.

When the rates are expressed as a port-limit, the actual rates used per instance of the queue will vary based on the port speed. For example, when the same QoS policy is used on a 1-Gb and a 10-Gb Ethernet port, the queue's rates will be 10 times greater on the 10 Gb port due to the difference in port speeds. This enables the same QOS policy to be used on SAPs on different ports without needing to use SAP based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's PIR and CIR rates will be recalculated based on the defined percentage value.

When the rates are expressed as a local-limit, the actual rates used per instance of the queue are relative to the queue's parent scheduler rate. This enables the same QOS policy to be used on SAPs with different parent scheduler rates without needing to use SAP based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the parent scheduler rate changes after the queue is created, the queue's PIR and CIR rates will be recalculated based on the defined percentage value.

Queue rate overrides can only be specified in the form as configured in the QoS policy (a SAP override can only be specified as a percent-rate if the associated QoS policy was also defined as percent-rate). Likewise, a SAP override can only be specified as a rate (kb/s) if the associated QoS policy was also defined as a rate. Queue-overrides are relative to the limit type specified in the QOS policy.

When no percent-rate is defined within a SAP ingress or egress queue-override, the queue reverts to the defined shaping and CIR rates within the SAP ingress and egress QOS policy associated with the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent-of-line-rate* — The percent-of-line-rate parameter is used to express the queue's shaping rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

pir-percent — Specifies the queue's PIR as a percentage dependent on the use of the port-limit or local-limit.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's CIR as a percentage dependent on the use of the port-limit or local-limit.

Values 0.00 to 100.00

Default 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap ingress queue-override queue percent-rate
- configure service cpipe sap egress queue-override queue percent-rate
- configure service cpipe sap ingress queue-override queue percent-rate
- configure service fpipe sap egress queue-override queue percent-rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue percent-rate
- configure service apipe sap ingress queue-override queue percent-rate

All

- configure service ipipe sap ingress queue-override queue percent-rate
- configure service ipipe sap egress queue-override queue percent-rate
- configure service epipe sap egress queue-override queue percent-rate

percent-rate

Syntax **percent-rate** *percent*
no percent-rate

Context **[Tree]** (config>service>epipe>sap>egress>queue-override>hs-wrr-group percent-rate)
[Tree] (config>service>ipipe>sap>egress>queue-override>hs-wrr-group percent-rate)

Full Context configure service epipe sap egress queue-override hs-wrr-group percent-rate
configure service ipipe sap egress queue-override hs-wrr-group percent-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command overrides the scheduling rate applied to the HS WRR group as a percentage of the port rate, including both the port's egress rate and port's HS scheduler policy maximum rate, if configured. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the percent rate override value from the configuration.

Parameters *percent* — Specifies the percent rate of the HS WRR group.

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>service>vpls>sap>egress>policer-override>plcr percent-rate)
[Tree] (config>service>vpls>sap>ingress>policer-override>plcr percent-rate)

Full Context configure service vpls sap egress policer-override policer percent-rate
configure service vpls sap ingress policer-override policer percent-rate

Description This command configures the percent rates (CIR and PIR) override and can only be used when the rate for the associated policer in the applied SAP ingress QoS policy is also configured with the **percent-rate** command.

The **no** form of this command removes the **percent-rate** override so that the **percent-rate** configured for the policer in the applied SAP egress QoS policy is used.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the policers' parent arbiter rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the policer's CIR as a percentage of the policers' parent arbiter rate.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

percent-rate

Syntax **percent-rate** *percent*
no percent-rate

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>hs-wrr-group percent-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls sap egress queue-override hs-wrr-group percent-rate

Description This command overrides the scheduling rate applied to the HS WRR group as a percentage of the port rate, including both the port's egress rate and port's HS scheduler policy max-rate, if configured. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the percent rate override value from the configuration.

Parameters *percent* — Specifies the percent rate of the HS WRR group.

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue percent-rate)

Full Context configure service vpls sap egress queue-override queue percent-rate
configure service vpls sap ingress queue-override queue percent-rate

Description The **percent-rate** command supports a queue's shaping rate and CIR rate as a percentage of the egress port's line rate. When the rates are expressed as a percentage within the template, the actual rate used per instance of the queue group queue-id will vary based on the port speed. For example, when the same template is used to create a queue group on a 1-Gb and a 10-Gb Ethernet port, the queue's rates will be 10 times greater on the 10-Gb port due to the difference in port speeds. This enables the same template to be used on multiple ports without needing to use port based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's shaping and CIR rates will be recalculated based on the defined percentage value.

The **rate** and **percent-rate** commands override one another. If the current rate for a queue is defined using the percent-rate command and the **rate** command is executed, the percent-rate values are deleted. In a similar fashion, the **percent-rate** command causes any **rate** command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

An egress port queue group queue rate override may be expressed as either a percentage or an explicit rate independent on how the queue's template rate is expressed.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case the configuration of the **percent-rate** is performed under the **hs-wrr-group** within the SAP egress QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the queue to its default shaping **rate** and **cir** rate. When **no percent-rate** is defined within a port egress queue group queue override, the queue reverts to the defined shaping and CIR rates within the egress queue group template associated with the queue.

Parameters *pir-percent* — Specifies the queue's shaping rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's committed scheduling rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values 0.00 to 100.00

Default 100.00

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>service>ies>if>sap>egress>policer-override>plcr percent-rate)
[Tree] (config>service>ies>if>sap>ingress>policer-override>plcr percent-rate)

Full Context configure service ies interface sap egress policer-override policer percent-rate
configure service ies interface sap ingress policer-override policer percent-rate

Description This command configures the percent rates (CIR and PIR) override and can only be used when the rate for the associated policer in the applied SAP ingress QoS policy is also configured with the **percent-rate** command.

The **no** form of this command removes the **percent-rate** override so that the **percent-rate** configured for the policer in the applied SAP egress QoS policy is used.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the policers's parent arbiter rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the policer's CIR as a percentage of the policers's parent arbiter rate.

Values 0.00 to 100.00

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

percent-rate

Syntax **percent-rate** *percent*
no percent-rate

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>hs-wrr-group percent-rate)

Full Context configure service ies interface sap egress queue-override hs-wrr-group percent-rate

Description This command overrides the scheduling rate applied to the HS WRR group as a percentage of the port rate, including both the port's egress rate and port's HS scheduler policy max-rate, if configured. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the percent rate override value from the configuration.

Parameters *percent* — Specifies the percent rate of the HS WRR group.

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue percent-rate)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue percent-rate)

Full Context configure service ies interface sap egress queue-override queue percent-rate
configure service ies interface sap ingress queue-override queue percent-rate

Description The **percent-rate** command supports a queue’s shaping rate and CIR rate as a percentage of the egress port’s line rate. When the rates are expressed as a percentage within the template, the actual rate used per instance of the queue group queue-id will vary based on the port speed. For example, when the same template is used to create a queue group on a 1-Gigabit and a 10-Gigabit Ethernet port, the queue’s rates will be 10 times greater on the 10 Gigabit port due to the difference in port speeds. This enables the same template to be used on multiple ports without needing to use port based queue overrides to modify a queue’s rate to get the same relative performance from the queue.

If the port’s speed changes after the queue is created, the queue’s shaping and CIR rates will be recalculated based on the defined percentage value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The rate and percent-rate commands override one another. If the current rate for a queue is defined using the percent-rate command and the rate command is executed, the percent-rate values are deleted. In a similar fashion, the percent-rate command causes any rate command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at anytime.

An egress port queue group queue rate override may be expressed as either a percentage or an explicit rate independent on how the queue's template rate is expressed.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **percent-rate** is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command returns the queue to its default shaping rate and cir rate. When **no percent-rate** is defined within a port egress queue group queue override, the queue reverts to the defined shaping and CIR rates within the egress queue group template associated with the queue.

Parameters *pir-percent* — Specifies the queue's shaping rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's committed scheduling rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values 0.00 to 100.00

Default 100.00

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-override>plcr percent-rate)
[Tree] (config>service>vprn>if>sap>ingress>policer-override>plcr percent-rate)

Full Context configure service vprn interface sap egress policer-override policer percent-rate
configure service vprn interface sap ingress policer-override policer percent-rate

Description This command configures the percent rates (CIR and PIR) override and can only be used when the rate for the associated policer in the applied SAP ingress QoS policy is also configured with the **percent-rate** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the **percent-rate** override so that the **percent-rate** configured for the policer in the applied SAP egress QoS policy is used.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the policers's parent arbiter rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the policer's CIR as a percentage of the policers's parent arbiter rate.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

percent-rate

Syntax **percent-rate** *percent*
no percent-rate

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>hs-wrr-group percent-rate)

Full Context configure service vprn interface sap egress queue-override hs-wrr-group percent-rate

Description This command overrides the scheduling rate applied to the HS WRR group as a percentage of the port rate, including both the port's egress rate and port's HS scheduler policy max-rate, if configured. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the percent rate override value from the configuration.

Parameters *percent* — Specifies the percent rate of the HS WRR group.

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue percent-rate)

Full Context configure service vprn interface sap egress queue-override queue percent-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **percent-rate** command supports a queue's shaping rate and CIR rate as a percentage of the egress port's line rate. When the rates are expressed as a percentage within the template, the actual rate used per instance of the queue group queue-id will vary based on the port speed. For example, when the same template is used to create a queue group on a 1-Gigabit and a 10-Gigabit Ethernet port, the queue's rates will be 10 times greater on the 10 Gigabit port due to the difference in port speeds. This enables the same template to be used on multiple ports without needing to use port based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's shaping and CIR rates will be recalculated based on the defined percentage value.

The rate and percent-rate commands override one another. If the current rate for a queue is defined using the percent-rate command and the rate command is executed, the percent-rate values are deleted. In a similar fashion, the percent-rate command causes any rate command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at anytime.

An egress port queue group queue rate override may be expressed as either a percentage or an explicit rate independent on how the queue's template rate is expressed.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **percent-rate** is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command returns the queue to its default shaping rate and cir rate. When **no percent-rate** is defined within a port egress queue group queue override, the queue reverts to the defined shaping and CIR rates within the egress queue group template associated with the queue.

Parameters *pir-percent* — Specifies the queue's shaping rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's committed scheduling rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values 0.00 to 100.00

Default 100.00

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-rate

Syntax **percent-rate** *percentage* [**local-limit** | **reference-port-limit**]
no percent-rate

Context **[Tree]** (config>qos>plcr-ctrl-plcy>tier>arbiter percent-rate)

Full Context configure qos policer-control-policy tier arbiter percent-rate

Description This command configures the percent rate of this contexts policer policy.

The **no** form of this command removes the configuration.

Parameters *percentage* — Specifies the percentage.

Values 0.01 to 100.00

local-limit — Keyword used to specify the local limit.

reference-port-limit — Keyword used to specify the reference port limit.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*] [**local-limit** | **reference-port-limit**]
no percent-rate

Context **[Tree]** (config>qos>sap-ingress>policer percent-rate)
[Tree] (config>qos>sap-egress>policer percent-rate)

Full Context configure qos sap-egress policer percent-rate
configure qos sap-ingress policer percent-rate

Description The percent-rate command within the SAP ingress and egress QoS policies enables supports for a policer's PIR and CIR rate to be configured as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

This enables the same QoS policy to be used on SAPs on different FPs without needing to use SAP-based policer overrides to modify a policer's rate to get the same relative performance from the policer.

If the parent arbiter rate changes after the policer is created, the policer's PIR and CIR rates will be recalculated based on the defined percentage value.

The rate and percent-rate commands override one another. If the current rate for a policer is defined using the percent-rate command and the rate command is executed, the percent-rate values are deleted. In a similar fashion, the percent-rate command causes any rate command values to be deleted. A policer's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

The **no** form of this command returns the queue to its default shaping rate and CIR rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values Percentage ranging from 0.01 to 100.00

Default 100.00

cir-percent — The **cir** keyword is optional and, when defined, the required cir-percent CIR parameter expresses the policer's CIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values Percentage ranging from 0.00 to 100.00

Default 100.00

local-limit — Keyword used to specify the local limit.

reference-port-limit — Keyword used to specify the reference port limit.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*] [**fir** *fir-percent*] [{**port-limit** | **local-limit** | **reference-port-limit**}]
percent-rate *pir-percent* **police** [{**port-limit** | **local-limit** | **reference-port-limit**}]
no percent-rate

Context **[Tree]** (config>qos>sap-ingress>queue percent-rate)

Full Context configure qos sap-ingress queue percent-rate

Description This command configures a queue's PIR and CIR as a percentage of the ingress port line rate or as a percentage of its parent scheduler rate. When the rates are expressed as a **port-limit**, the actual rates used per instance of the queue will vary based on the port speed. For example, when the same QoS policy is used on a 1 Gb and a 10 Gb Ethernet port, the queue's rates will be 10 times greater on the 10 Gb port due to the difference in port speeds. This enables the same QoS policy to be used on SAPs on different ports without needing to use SAP-based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's PIR, CIR, and FIR rates will be recalculated based on the defined percentage value.

When the rates are expressed as a **local-limit**, the actual rates used per instance of the queue are relative to the queue's parent scheduler rate. This enables the same QoS policy to be used on SAPs with different parent scheduler rates without needing to use SAP-based queue overrides to modify a queue's rate to get the same relative performance from the queue. If the parent scheduler rate changes after the queue is created, the queue's PIR, CIR, and FIR will be recalculated based on the defined percentage value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **rate** and **percent-rate** commands override one another. If the current rate for a queue is defined using the **percent-rate** command and the **rate** command is executed, the **percent-rate** values are deleted. Similarly, the **percent-rate** command causes any **rate** command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

Queue rate overrides can only be specified in the form configured in the QoS policy (for example, a SAP override can only be specified as a **percent-rate** if the associated QoS policy was also defined as percent-rate). Likewise, a SAP override can only be specified as a **rate** (kb/s) if the associated QoS policy was also defined as a rate. Queue-overrides are relative to the limit type specified in the QoS policy.

When no **percent-rate** is defined within a SAP ingress queue-override, the queue uses the defined shaping rate, CIR, and FIR within the SAP ingress QoS policy associated with the queue.

The **no** form of this command returns the queue to its default shaping rate, CIR, and FIR.

Parameters *pir-percent* — Specifies the queue's PIR as a percentage dependent on the use of the **port-limit** or **local-limit**.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's CIR as a percentage dependent on the use of the **port-limit** or **local-limit**.

Values 0.00 to 100.00

Default 100.00

fir-percent — Specifies the queue's FIR as a percentage dependent on the use of the **port-limit** or **local-limit**. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

Values 0.00 to 100.00

Default 100.00

police — Keyword used to specify that traffic feeding into the physical queue instance above the specified PIR rate is dropped. When the **police** keyword is defined, only the PIR rate may be overridden. The **police** keyword is only applicable to SAP ingress.

port-limit — Keyword used to specify that the configured PIR, CIR, and FIR percentages are relative to the rate of the port (including the ingress-rate setting) to which the queue is attached. The **port-limit** is the default.

local-limit — Keyword used to specify that the configured PIR, CIR, and FIR percentages are relative to the queue's parent scheduler rate. If there is no parent scheduler rate, or its rate is **max**, the **port-limit** is used.

reference-port-limit — Keyword used to specify that the configured PIR, CIR, and FIR percentages are relative to the rate of the reference port (including the ingress-rate setting) to which the queue is attached.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*] [{**port-limit** | **local-limit** | **reference-port-limit**}]
no percent-rate

Context **[Tree]** (config>qos>sap-egress>queue percent-rate)

Full Context configure qos sap-egress queue percent-rate

Description This command configures a queue's PIR and CIR as a percentage of the egress port line rate or as a percentage of its parent scheduler rate or **agg-rate** rate. When the rates are expressed as a **port-limit**, the actual rates used per instance of the queue will vary based on the port speed. For example, when the same QoS policy is used on a 1 Gb and a 10 Gb Ethernet port, the queue's rates will be 10 times greater on the 10 Gb port due to the difference in port speeds. This enables the same QoS policy to be used on SAPs on different ports without needing to use SAP-based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's PIR and CIR will be recalculated based on the defined percentage value.

When the rates are expressed as a **local-limit**, the actual rates used per instance of the queue are relative to the queue's parent scheduler rate or **agg-rate** rate. This enables the same QoS policy to be used on SAPs with different parent scheduler rates without needing to use SAP-based queue overrides to modify a queue's rate to get the same relative performance from the queue. If the parent scheduler rate changes after the queue is created, the queue's PIR and CIR will be recalculated based on the defined percentage value.

The **rate** and **percent-rate** commands override one another. If the current rate for a queue is defined using the **percent-rate** command and the **rate** command is executed, the **percent-rate** values are deleted. Similarly, the **percent-rate** command causes any **rate** command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

Queue rate overrides can only be specified in the form as configured in the QoS policy (a SAP override can only be specified as a **percent-rate** if the associated QoS policy was also defined as percent-rate). Likewise, a SAP override can only be specified as a rate (kb/s) if the associated QoS policy was also defined as a rate. Queue-overrides are relative to the limit type specified in the QoS policy.

When configured on an egress HSQ queue group queue, the **cir** keyword is ignored.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **percent-rate** is performed under the **hs-wrr-group** within the SAP egress QoS policy.

When no **percent-rate** is defined within a SAP egress queue-override, the queue uses the defined shaping rate and CIR within the SAP egress QoS policy associated with the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the queue to its default shaping rate and CIR.

Parameters *pir-percent* — Specifies the queue's PIR as a percentage dependent on the use of the **port-limit** or **local-limit**.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's CIR as a percentage dependent on the use of the **port-limit** or **local-limit.**

Values 0.00 to 100.00

Default 100.00

port-limit — Keyword used to specify that the configure PIR and CIR percentages are relative to the rate of the port (including the **egress-rate** setting) to which this queue connects. The **port-limit** is the default.

local-limit — Keyword used to specify that the configure PIR and CIR percentages are relative to the rate of the queue's parent scheduler **rate** or **agg-rate** rate at egress. If there is no parent scheduler rate or **agg-rate** rate, or those rates are **max**, the **port-limit** is used.

reference-port-limit — Keyword used to specify that the configure PIR and CIR percentages are relative to the rate of the reference port (including the **egress-rate** setting) to which this queue connects.

Platforms All

percent-rate

Syntax **percent-rate** *percent*
no percent-rate

Context **[Tree]** (config>qos>sap-egress>hs-wrr-group percent-rate)

Full Context configure qos sap-egress hs-wrr-group percent-rate

Description This command specifies the scheduling rate applied to the HS WRR group as a percentage of the port rate, including both the port's egress rate and port's HS scheduler **policy** *max-rate*, if configured. The **percent-rate** and **rate** commands are mutually exclusive.

The **no** form of the command reverts to the rate **max**.

Parameters *percent* — Specifies the percent rate of the HS WRR group.

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-rate

Syntax **percent-rate** *percent*
no percent-rate

Context **[Tree]** (config>qos>qgrps>egr>qgrp>hs-wrr-group percent-rate)

Full Context configure qos queue-group-templates egress queue-group hs-wrr-group percent-rate

Description This command specifies the scheduling rate applied to the HS WRR group as a percentage of the port rate, including both the port's **egress-rate** and port's HS scheduler policy **max-rate**, if configured. The **percent-rate** and **rate** commands are mutually exclusive.

The **no** form of the command reverts to the rate max.

Parameters *percent* — Specifies the percent rate of the HS WRR group.

Values 0.01 to 100.00

Platforms 7750 SR-7/12/12e

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percentage*] [**local-limit** | **reference-port-limit**]
no percent-rate

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer percent-rate)

Full Context configure qos queue-group-templates egress queue-group policer percent-rate

Description This command configures the percent rate for this contexts policer.

The **no** form of this command removes the configuration.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values 0.01 to 100.00

cir-percent — The **cir** keyword is optional and, when defined, the required cir-percent CIR parameter expresses the policer's CIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values 0.00 to 100.00, sum

local-limit — Keyword used to specify the local limit.

reference-port-limit — Keyword used to specify the reference port limit.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percentage*]
no percent-rate

Context **[Tree]** (config>qos>qgrps>ing>qgrp>policer percent-rate)

Full Context configure qos queue-group-templates ingress queue-group policer percent-rate

Description This command configures the percent rate for this contexts policer.

The **no** form of this command removes the configuration.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values 0.01 to 100.00

cir-percent — The **cir** keyword is optional and, when defined, the required cir-percent CIR parameter expresses the policer's CIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values 0.00 to 100.00, sum

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*] [**fir** *fir-percent*] [{**port-limit** | **local-limit** | **reference-port-limit**}]
percent-rate *pir-percent* **police** [{**port-limit** | **local-limit** | **reference-port-limit**}]
no percent-rate

Context **[Tree]** (config>qos>queue-group-templates>ingress>queue-group>queue percent-rate)

Full Context configure qos queue-group-templates ingress queue-group queue percent-rate

Description This command configures a queue's PIR and CIR as a percentage of the ingress port line rate or as a percentage of its parent scheduler rate. When the rates are expressed as a **port-limit**, the actual rates used per instance of the queue will vary based on the port speed. For example, when the same QoS policy is used on a 1 Gb and a 10 Gb Ethernet port, the queue's rates will be 10 times greater on the 10 Gb port due to the difference in port speeds. This enables the same QoS policy to be used on SAPs on different ports without needing to use SAP-based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's PIR, CIR, and FIR rates will be recalculated based on the defined percentage value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the rates are expressed as a **local-limit**, the actual rates used per instance of the queue are relative to the queue's parent scheduler rate. This enables the same QoS policy to be used on SAPs with different parent scheduler rates without needing to use SAP-based queue overrides to modify a queue's rate to get the same relative performance from the queue. If the parent scheduler rate changes after the queue is created, the queue's PIR, CIR, and FIR will be recalculated based on the defined percentage value.

The **rate** and **percent-rate** commands override one another. If the current rate for a queue is defined using the **percent-rate** command and the **rate** command is executed, the **percent-rate** values are deleted. Similarly, the **percent-rate** command causes any **rate** command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

Queue rate overrides can only be specified in the form configured in the QoS policy (for example, a SAP override can only be specified as a **percent-rate** if the associated QoS policy was also defined as percent-rate). Likewise, a SAP override can only be specified as a **rate** (kb/s) if the associated QoS policy was also defined as a rate. Queue-overrides are relative to the limit type specified in the QoS policy.

When no **percent-rate** is defined within a SAP ingress queue-override, the queue uses the defined shaping rate, CIR, and FIR within the SAP ingress QoS policy associated with the queue.

The **no** form of this command returns the queue to its default shaping rate, CIR, and FIR.

Parameters *pir-percent* — Specifies the queue’s PIR as a percentage dependent on the use of the **port-limit** or **local-limit**.

Values 0.01 to 100.00

Default 100.00

cir-percent — Specifies the queue's CIR as a percentage dependent on the use of the **port-limit** or **local-limit**.

Values 0.00 to 100.00

Default 100.00

fir-percent — Specifies the queue's FIR as a percentage dependent on the use of the **port-limit** or **local-limit**. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

Values 0.00 to 100.00

Default 100.00

police — Keyword used to specify that traffic feeding into the physical queue instance above the specified PIR rate will be dropped. When the **police** keyword is defined, only the PIR rate may be overridden. The **police** keyword is only applicable to SAP ingress.

port-limit — Keyword used to specify that the configured PIR, CIR, and FIR percentages are relative to the rate of the port (including the ingress-rate setting) to which the queue is attached. The **port-limit** is the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-limit — Keyword used to specify that the configured PIR, CIR, and FIR percentages are relative to the queue's parent scheduler rate. If there is no parent scheduler rate, or its rate is **max**, the **port-limit** is used.

reference-port-limit — Keyword used to specify that the configured PIR, CIR, and FIR percentages are relative to the rate of the reference port (including the ingress-rate setting) to which the queue is attached.

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*] [{**port-limit** | **local-limit** | **reference-port-limit**}]
no percent-rate

Context **[Tree]** (config>qos>qgrps>egr>queue-group>queue percent-rate)

Full Context configure qos queue-group-templates egress queue-group queue percent-rate

Description The **percent-rate** command within the egress queue group template enables support for a queue's PIR and CIR rate to be configured as a percentage of the egress port's line rate. When the rates are expressed as a percentage within the template, the actual rate used per instance of the queue group *queue-id* will vary based on the port speed. For example, when the same template is used to create a queue group on a 1-Gb and a 10-Gb Ethernet port, the queue's rates will be 10 times greater on the 10 Gb port due to the difference in port speeds. This enables the same template to be used on multiple ports without needing to use port-based queue overrides to modify a queue's rate to get the same relative performance from the queue.

If the port's speed changes after the queue is created, the queue's shaping and CIR rates will be recalculated based on the defined percentage value.

When configured on an egress HSQ queue group queue, the **cir** keyword is ignored.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case the configuration of the rate is performed under the **hs-wrr-group** within the egress queue group template.

The **rate** and **percent-rate** commands override one another. If the current rate for a queue is defined using the **percent-rate** command and the **rate** command is executed, the **percent-rate** values are deleted. Similarly, the **percent-rate** command causes any **rate** command values to be deleted. A queue's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

The **no** form of this command returns the queue to its default shaping rate and CIR rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *pir-percent* — Expresses the queue's shaping rate as a percentage of line rate. The line rate associated with the queue's port may dynamically change due to configuration or auto-negotiation and the egress rate setting.

Values 0.01 to 100.00 percent

Default 100.0

cir-percent — The **cir** keyword is optional and when defined, the required *pir-percent* parameter expresses the queue's committed scheduling rate as a percentage of line rate. The line rate associated with the queue's port may change dynamically due to configuration or auto-negotiation and the egress rate setting.

Values 0.01 to 100.00 percent

Default 100.0

port-limit — Keyword used to specify that the configure PIR and CIR percentages are relative to the rate of the port (including the **egress-rate** setting) to which this queue connects. The **port-limit** is the default.

local-limit — Keyword used to specify that the configure PIR and CIR percentages are relative to the rate of the queue's parent scheduler **rate** or **agg-rate** rate at egress. If there is no parent scheduler rate or **agg-rate** rate, or those rates are **max**, the **port-limit** is used.

reference-port-limit — Keyword used to specify that the configure PIR and CIR percentages are relative to the rate of the reference port (including the **egress-rate** setting) to which this queue connects.

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percentage*] [**local-limit** | **reference-port-limit**]
no percent-rate

Context **[Tree]** (config>qos>scheduler-policy>tier>scheduler percent-rate)

Full Context configure qos scheduler-policy tier scheduler percent-rate

Description This command configures the percentage rate for the scheduler policy.

The **no** form of this command removes the configuration.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values 0.01 to 100.00

cir-percent — The **cir** keyword is optional and, when defined, the required *cir-percent* CIR parameter expresses the policer's CIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values 0.00 to 100.00, sum

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-limit — Keyword used to specify the local limit.

reference-port-limit — Keyword used to specify the reference port limit.

Platforms All

percent-rate

Syntax **percent-rate** *pir-percent* [**cir** *cir-percent*]
no percent-rate

Context **[Tree]** (config>qos>port-scheduler-policy>group percent-rate)

Full Context configure qos port-scheduler-policy group percent-rate

Description The percent-rate command within the port scheduler policy group enables support for a policer's PIR and CIR rate to be configured as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

If the parent arbiter rate changes after the policer is created, the policer's PIR and CIR rates will be recalculated based on the defined percentage value.

The **rate** and **percent-rate** commands override one another. If the current rate for a policer is defined using the percent-rate command and the rate command is executed, the percent-rate values are deleted. In a similar fashion, the percent-rate command causes any rate command values to be deleted. A policer's rate may dynamically be changed back and forth from a percentage to an explicit rate at any time.

The **no** form of this command returns the queue to its default shaping rate and cir rate.

Parameters *pir-percent* — Specifies the policer's PIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values Percentage ranging from 0.01 to 100.00.

Default 100.00

cir *cir-percent* — The **cir** keyword is optional and, when defined, the required cir-percent CIR parameter expresses the policer's CIR as a percentage of the immediate parent root policer/arbiter rate or the FP capacity.

Values Percentage ranging from 0.00 to 100.00.

Default 100.00

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.134 percent-reduction-from-mbs

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2>prim-path>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>mcast-mgmt>bw-plcy>t2>sec-path>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure mcast-management bandwidth-policy t2-paths primary-path queue-parameters drop-tail low percent-reduction-from-mbs
configure mcast-management bandwidth-policy t2-paths secondary-path queue-parameters drop-tail low percent-reduction-from-mbs

Description This command overrides the default percentage value used to determine the low drop-tail value for the queue. By default, 10 percent of the queue depth is reserved for high congestion priority traffic. When specified, the **percent-reduction-from-mbs** percentage value is applied to the queues' MBS threshold. The resulting value is subtracted from the MBS to derive the low drop-tail threshold maintained by the queue. The low drop-tail threshold defines the point at which all low-congestion priority packets destined for the queue are discarded based on queue depth. Low- and high-congestion priority is derived from the multicast records preference value compared to the record's bundle priority threshold.

The **no** form of this command restores the default value.

Default percent-reduction-from-mbs 10

Parameters *percent* — Specifies the percent of queue depth reserved for high-congestion priority traffic.

Values 0 to 100, default

0 specifies that the MBS and low drop-tail thresholds be set to the same value resulting in high- and low-congestion priority packets being treated equally.

100 specifies that the low drop-tail threshold is set to 0, resulting in all low-congestion priority packets being discarded.

Values between 0 and 100 result in a corresponding differential between the MBS and the low drop-tail threshold values.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>vpls>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure service ies interface sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service ies interface sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
configure service vpls sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service vpls sap ingress queue-override queue drop-tail low percent-reduction-from-mbs

Description This command overrides the low queue drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and this percentage is configured to be 30% for the low drop tail, then the low drop tail is at 420 kbytes and out-of-profile packets are not accepted into the queue if its depth is greater than this value, and discarded.

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover>q>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>port>ethernet>access>ing>qgrp>qover>q>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>port>ethernet>network>egr>qgrp>qover>q>drop-tail>low percent-reduction-from-mbs)

Full Context configure port ethernet access egress queue-group queue-overrides queue drop-tail low percent-reduction-from-mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet access ingress queue-group queue-overrides queue drop-tail low percent-reduction-from-mbs
configure port ethernet network egress queue-group queue-overrides queue drop-tail low percent-reduction-from-mbs

Description This command overrides the low queue drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and this percentage is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes and out-of-profile packets will not be accepted into the queue if its depth is greater than this value, and so will be discarded.

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>epipe>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure service apipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service apipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
configure service cpipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service cpipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
configure service epipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service epipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
configure service fpipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service fpipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
configure service ipipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service ipipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs

Description This command overrides the low queue drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and the percentage reduction is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes. Any out-of-profile packets will not be accepted into the queue if its depth is greater than this value, and so will be discarded.

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs
- configure service fpipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
- configure service cpipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
- configure service cpipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
- configure service apipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs

All

- configure service ipipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
- configure service ipipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap ingress queue-override queue drop-tail low percent-reduction-from-mbs
- configure service epipe sap egress queue-override queue drop-tail low percent-reduction-from-mbs

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure service vprn interface sap egress queue-override queue drop-tail low percent-reduction-from-mbs
configure service vprn interface sap ingress queue-override queue drop-tail low percent-reduction-from-mbs

Description This command overrides the low queue drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and the percentage reduction is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes and out-of-profile packets will not be accepted into the queue if its depth is greater than this value, and so will be discarded.

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>qos>sap-ingress>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure qos sap-ingress queue drop-tail low percent-reduction-from-mbs

Description This command configures the ingress SAP low drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and this percentage is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes and out-of-profile packets will not be accepted into the queue if its depth is greater than this value and will be discarded.

Default percent-reduction-from-mbs 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>qos>sap-egress>queue>drop-tail>exceed percent-reduction-from-mbs)
[Tree] (config>qos>sap-egress>queue>drop-tail>high percent-reduction-from-mbs)
[Tree] (config>qos>sap-egress>queue>drop-tail>highplus percent-reduction-from-mbs)
[Tree] (config>qos>sap-egress>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure qos sap-egress queue drop-tail exceed percent-reduction-from-mbs
configure qos sap-egress queue drop-tail high percent-reduction-from-mbs
configure qos sap-egress queue drop-tail highplus percent-reduction-from-mbs
configure qos sap-egress queue drop-tail low percent-reduction-from-mbs

Description This command configures the egress SAP queue drop tails as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and this percentage is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes and out-of-profile packets will not be accepted into the queue if its depth is greater than this value and will be discarded.

The drop tails apply to packets with the following profile state:

- Exceed drop tail: exceed-profile
- High drop tail: in-profile
- Highplus drop tail: inplus-profile
- Low drop tail: out-of-profile

Default Exceed drop tail: 20%

Low drop tail: 10%

High drop tail: 0%

Highplus drop tail: 0%

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>qos>network-queue>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure qos network-queue queue drop-tail low percent-reduction-from-mbs

Description This command configures the ingress and egress network queue low drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and **percent-reduction-from-mbs** is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes and out-of-profile packets will not be accepted into the queue if its depth is greater than this value and will be discarded.

The exceed drop tail is not configurable for network queues, however, it is set to a value of 10% in addition to low drop tail and capped by the MBS.

Default percent-reduction-from-mbs 10

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>qos>qgrps>ing>qgrp>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure qos queue-group-templates ingress queue-group queue drop-tail low percent-reduction-from-mbs

Description This command configures the ingress queue group queue low drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and the percentage reduction is configured to be 30% for the low drop tail, the low drop tail will be at 420 kbytes. Out-of-profile packets will not be accepted into the queue and will be discarded if the queue depth is greater than this value.

Default 10%

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, **default**

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context [Tree] (config>qos>qgrps>egr>qgrp>queue>drop-tail>exceed percent-reduction-from-mbs)
[Tree] (config>qos>qgrps>egr>qgrp>queue>drop-tail>high percent-reduction-from-mbs)
[Tree] (config>qos>qgrps>egr>qgrp>queue>drop-tail>highplus percent-reduction-from-mbs)
[Tree] (config>qos>qgrps>egr>qgrp>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure qos queue-group-templates egress queue-group queue drop-tail exceed percent-reduction-from-mbs
configure qos queue-group-templates egress queue-group queue drop-tail high percent-reduction-from-mbs
configure qos queue-group-templates egress queue-group queue drop-tail highplus percent-reduction-from-mbs
configure qos queue-group-templates egress queue-group queue drop-tail low percent-reduction-from-mbs

Description This command configures the egress queue group queue drop tails as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and the percentage reduction is configured to be 30% for the low drop tail, the low drop tail will be at 420 kbytes. Out-of-profile packets will not be accepted into the queue and will be discarded if the queue depth is greater than this value.

The drop tails apply to packets with the following profile states:

- exceed drop tail: exceed-profile
- high drop tail: in-profile
- highplus drop tail: inplus-profile
- low drop tail: out-of-profile

Default exceed drop tail: 20%

low drop tail: 10%

high drop tail: 0%

highplus drop tail: 0%

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

percent-reduction-from-mbs

Syntax **percent-reduction-from-mbs** *percent*
no percent-reduction-from-mbs

Context **[Tree]** (config>qos>shared-queue>queue>drop-tail>low percent-reduction-from-mbs)

Full Context configure qos shared-queue queue drop-tail low percent-reduction-from-mbs

Description This command configures the ingress shared queue low drop tail as a percentage reduction from the MBS of the queue. For example, if a queue has an MBS of 600 kbytes and **percent-reduction-from-mbs** is configured to be 30% for the low drop tail, then the low drop tail will be at 420 kbytes and out-of-profile packets will not be accepted into the queue if its depth is greater than this value and will be discarded.

Default percent-reduction-from-mbs 10

Parameters *percent* — Specifies the percentage reduction from the MBS for a queue drop tail.

Values 0 to 100, default

Platforms All

20.135 performance

performance

Syntax **performance**

Context **[Tree]** (config>isa>aa-grp>statistics performance)

Full Context configure isa application-assurance-group statistics performance

Description This command configures the ISA group to enable the aa-performance statistic record. This record contains information on the traffic load and resource consumption for each ISA in the group, to allow tracking of ISA load for long term capacity planning and short term anomalies. The user can configure the accounting policy to be used, and enables the record using the **[no] collect-stats** command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.136 period

period

Syntax **period** *milli-seconds*
no period

Context **[Tree]** (config>router>rsvp>msg-pacing period)

Full Context configure router rsvp msg-pacing period

Description This command specifies the time interval (in ms), when the router can send the specified number of RSVP messages which is specified in the **max-burst** command.

Default period 100

Parameters *milli-seconds* — Specifies the time interval in increments of 10 ms.

Values 100 to 1000

Platforms All

20.137 periodic

periodic

Syntax **periodic**

Context **[Tree]** (config>subscr-mgmt>shcv-policy periodic)

Full Context configure subscriber-mgmt shcv-policy periodic

Description Commands in this context configure periodic SHCV properties for the subscriber management group-interface. This tool periodically scans all known DHCP hosts only and perform unicast ARP/NS requests. The subscriber host connectivity verification maintains state (connected versus not-connected) for all hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.138 periodic-loopback

periodic-loopback

Syntax [**no**] **periodic-loopback**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>atm>oam periodic-loopback)
[Tree] (config>service>vprn>if>sap>atm>oam periodic-loopback)
[Tree] (config>service>vprn>sub-if>grp-if>sap>atm periodic-loopback)

Full Context configure service ies subscriber-interface group-interface sap atm oam periodic-loopback
configure service vprn interface sap atm oam periodic-loopback
configure service vprn subscriber-interface group-interface sap atm periodic-loopback

Description This command enables periodic OAM loopbacks on this SAP. This command is only configurable on IES and VPRN SAPs. When enabled, an ATM OAM loopback cell is transmitted every period as configured in the **config>system>atm>oam>loopback-period** *period* context.

If a response is not received and consecutive retry-down retries also result in failure, the endpoint transitions to an alarm indication signal/loss of clock state. Then, an ATM OAM loopback cell is transmitted every period as configured in the loopback-period *period*. If a response is received for the periodic loopback and consecutive retry-up retries also each receive a response, the endpoint transitions back to the up state.

The **no** form of this command sets the value back to the default.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service ies subscriber-interface group-interface sap atm oam periodic-loopback

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service vprn interface sap atm oam periodic-loopback

periodic-loopback

Syntax [**no**] **periodic-loopback**

Context **[Tree]** (config>service>ies>if>sap>atm>oam periodic-loopback)

Full Context configure service ies interface sap atm oam periodic-loopback

Description This command enables periodic OAM loopbacks on this SAP. This command is only configurable on IES and VPRN SAPs. When enabled, an ATM OAM loopback cell is transmitted every period as configured in the config>system>atm>oam>loopback-period *period* context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a response is not received and consecutive retry-down retries also result in failure, the endpoint will transition to an alarm indication signal/loss of clock state. Then, an ATM OAM loopback cell will be transmitted every period as configured in the loopback-period *period*. If a response is received for the periodic loopback and consecutive retry-up retries also each receive a response, the endpoint will transition back to the up state.

The **no** form of this command sets the value back to the default.

Default no periodic-loopback

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

20.139 periodic-sm

periodic-sm

Syntax [**no**] **periodic-sm**

Context **[Tree]** (debug>service>id>mrp periodic-sm)

Full Context debug service id mrp periodic-sm

Description This command enables debugging of the periodic state machine.

The **no** form of this command disables debugging of the periodic state machine.

Platforms All

20.140 periodic-time

periodic-time

Syntax **periodic-time** *value*
no periodic-time

Context **[Tree]** (config>service>vpls>sap>mrp periodic-time)
[Tree] (config>service>vpls>spoke-sdp>mrp periodic-time)
[Tree] (config>service>vpls>mesh-sdp>mrp periodic-time)

Full Context configure service vpls mesh-sdp mrp periodic-time
configure service vpls sap mrp periodic-time
configure service vpls spoke-sdp mrp periodic-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls the frequency the Periodic Transmission state machine generates periodic events if the Periodic Transmission Timer is enabled. The timer is required on a per-Port basis. The Periodic Transmission Timer is set to one second when it is started.

Default periodic-time 10

Parameters *value* — The frequency with which the Periodic Transmission state machine generates periodic events, in tenths of a second.

Values 10 to 100

Platforms All

20.141 periodic-timer

periodic-timer

Syntax [**no**] **periodic-timer**

Context **[Tree]** (config>service>vpls>sap>mrp periodic-timer)
[Tree] (config>service>vpls>spoke-sdp>mrp periodic-timer)
[Tree] (config>service>vpls>mesh-sdp>mrp periodic-timer)

Full Context configure service vpls mesh-sdp mrp periodic-timer
configure service vpls sap mrp periodic-timer
configure service vpls spoke-sdp mrp periodic-timer

Description This command enables or disables the Periodic Transmission Timer.

Default no periodic-timer

Platforms All

20.142 periodic-update

periodic-update

Syntax **periodic-update interval** *hours* [**rate-limit** *rate*]
no periodic-update

Context **[Tree]** (config>aaa>isa-radius-plcy periodic-update)

Full Context configure aaa isa-radius-policy periodic-update

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables periodic RADIUS logging of currently allocated port blocks for a NAT subscriber (NAT binding).

Default no periodic-update (no Interim Update messages are sent)

Parameters **interval** *hours* — Specifies the interval at which RADIUS logging is refreshed. The log generation might delayed past the configured interval value if the message pacing (rate-limit) is enabled or when the number of un-acknowledged (pending) messages in SR OS has reached its upper limit. An increased number of pending Interim Update messages in SR OS is due to lack of adequate responsiveness of the RADIUS server.

Values 1 to 72

rate-limit *rate* — Specifies the pacing of the Interim Update messages related to refreshment of the currently allocated port blocks. By default, when this command is disabled, the messages are sent at a high rate determined by the processing capability of the SR OS. Such a high message rate can exceed the processing power of the logging server which can result in the loss of logging information. To overcome this, the Interim Update messages can be generated in a staggered manner at a configured interval that is accommodating toward the processing capabilities of the logging server.

Default 1 to 100000 messages per second

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.143 periodic-update-interval

periodic-update-interval

Syntax **periodic-update-interval** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update periodic-update-interval)

Full Context configure system security pki ca-profile auto-crl-update periodic-update-interval

Description This command specifies the interval for periodic updates. The minimal interval is 1 hour. The maximum interval is 366 days.

Default periodic-update-interval days 1

Parameters **days** *days* — Specifies the number of days for periodic updates.

Values 0 to 366

hours — Specifies the number of hours for periodic updates.

Values 0 to 23

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

minutes — Specifies the number of minutes for periodic updates.

Values 0 to 59

seconds — Specifies the number of seconds for periodic updates.

Values 0 to 59

Platforms All

20.144 persist

persist

Syntax **persist** {**on** | **off**}

Context **[Tree]** (bof persist)

Full Context bof persist

Description This command specifies whether the system will preserve system indexes when a **save** command is executed. During a subsequent boot, the index file is read along with the configuration file. As a result, a number of system indexes are preserved between reboots, including the interface index, LSP IDs, path IDs, and so on. This reduces resynchronizations of the Network Management System (NMS) with the affected network element.

In the event that persist is **on** and the reboot with the appropriate index file fails, SNMP is operationally shut down to prevent the management system from accessing and possibly synchronizing with a partially booted or incomplete network element. To enable SNMP access, enter the **config>system>snmp>no shutdown** command.

If **persist** is enabled and the **admin save** *url* command is executed with an FTP path used as the *url* parameter, two FTP sessions simultaneously open to the FTP server. The FTP server must be configured to allow multiple sessions from the same login, otherwise, the configuration and index files will not be saved correctly.

Note:

- Persistency files (.ndx) are saved on the same disk as the configuration files and the image files.
- When an operator sets the location for the persistency file, the system will check to ensure that the disk has enough free space. If this there is not enough free space, the persistency will not become active and a trap will be generated. Then, it is up to the operator to free adequate disk space. In the meantime, the system will perform a space availability check every 30 seconds. As soon as the space is available the persistency will become active on the next (30 second) check.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default persist off

Parameters **on** — Enables the system index saves between reboots.

off — Disables the system index saves between reboots.

Platforms All

20.145 persistence

persistence

Syntax **persistence** *seconds*
no persistence

Context **[Tree]** (config>python>py-pol>cache>minimum-lifetimes persistence)

Full Context configure python python-policy cache minimum-lifetimes persistence

Description This command configures the minimum lifetime for a cache entry to be made persistent.

The **no** form of this command reverts to the default.

Parameters *persistence* — The minimum lifetime, in seconds.

Values 1 to 600

Platforms All

persistence

Syntax [**no**] **persistence**

Context **[Tree]** (config>python>py-pol>cache persistence)

Full Context configure python python-policy cache persistence

Description This command enables persistency support for the cached entries of the python-policy.

The **no** form of this command reverts to the default.

Platforms All

persistence

Syntax **persistence**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system persistence)

Full Context configure system persistence

Description Commands in this context configure persistence parameters on the system.

The persistence feature enables state information learned through applications such as subscriber management, DHCP server, or application assurance to be retained across reboots.

Platforms All

persistence

Syntax **persistence** [*persistence-client*]
no persistence

Context [Tree] (debug>system persistence)

Full Context debug system persistence

Description This command displays persistence debug information.

Parameters *persistence-client* — Displays persistence debug information.

Values

ancp	ANCP
application-assurance	application-assurance
dhcp-server	local DHCP server
nat-fwds	NAT port forwarding
python-policy-cache	Python Cache
submgt	subscriber management

Platforms All

20.146 persistency-database

persistency-database

Syntax [**no**] **persistency-**database

Context [Tree] (config>service>vpls>gsmp>group persistency-database)
[Tree] (config>service>vprn>gsmp>group persistency-database)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls gsmp group persistency-database
configure service vprn gsmp group persistency-database

Description This command enables the system to store DSL line information in memory. If the GSMP connection terminates, the DSL line information will remain in memory and accessible for RADIUS authentication and accounting.

The **no** form of this command reverts to the default.

Platforms All

persistency-database

Syntax [**no**] **persistency-database**

Context **[Tree]** (config>service>vpls>gsmp persistency-database)

Full Context configure service vpls gsmp persistency-database

Description This command enables the system to store DSL line information in memory. If the GSMP connection terminates, the DSL line information will remain in memory and accessible for Radius authentication and accounting.

Default no persistency-database

persistency-database

Syntax [**no**] **persistency-database**

Context **[Tree]** (config>service>vprn>gsmp persistency-database)

Full Context configure service vprn gsmp persistency-database

Description This command enables the system to store DSL line information in memory. If the GSMP connection terminates, the DSL line information remains in memory and accessible for RADIUS authentication and accounting.

The **no** form of this command reverts to the default.

Default no persistency-database

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.147 persistent-subscriptions

persistent-subscriptions

Syntax **persistent-subscriptions**

Context **[Tree]** (config>system>telemetry persistent-subscriptions)

Full Context configure system telemetry persistent-subscriptions

Description Commands in this context configure persistent subscriptions.

Platforms All

20.148 pfcp

pfcp

Syntax **pfcp**

Context **[Tree]** (config>service>vpls>sap pfcp)

Full Context configure service vpls sap pfcp

Description Commands in this context configure an active PFCP association for the VPLS capture SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pfcp

Syntax **pfcp**

Context **[Tree]** (debug>subscr-mgmt pfcp)

Full Context debug subscriber-mgmt pfcp

Description Commands in this context use debug commands associated with the PFCP protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.149 pfcp-association

pfcp-association

Syntax **pfcp-association** *name* [**create**]
no pfcp-association *name*

Context **[Tree]** (config>subscr-mgmt pfcp-association)

Full Context configure subscriber-mgmt pfcp-association

Description This command creates a PFCP association towards a BNG CUPS CPF.

The **no** form of this command removes the association.

Parameters *name* — Specifies the name of the PFCP association, up to 32 characters.

create — Keyword used to create the PFCP association.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.150 pfcp-mappings

pfcp-mappings

Syntax **pfcp-mappings**

Context **[Tree]** (config>subscr-mgmt>sla-prof pfcp-mappings)

Full Context configure subscriber-mgmt sla-profile pfcp-mappings

Description Commands in this context configure the mapping of PFCP QoS IEs (such as QER GBR/MBR IEs), to local QoS overrides (such as queue and policer rates).

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.151 pfs

pfs

Syntax **pfs** [**dh-group** {**1** | **2** | **5** | **14** | **15** | **19** | **20** | **21**}]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no pfs

Context [Tree] (config>ipsec>ike-policy pfs)

Full Context configure ipsec ike-policy pfs

Description This command enables perfect forward secrecy on the IPsec tunnel using this policy. PFS provides for a new Diffie-Hellman key exchange each time the SA key is renegotiated. After that SA expires, the key is forgotten and another key is generated (if the SA remains up). This means that an attacker who cracks part of the exchange can only read the part that used the key before the key changed. There is no advantage in cracking the other parts if they attacker has already cracked one.

The **no** form of this command disables PFS. If this it turned off during an active SA, when the SA expires and it is time to re-key the session, the original Diffie-Hellman primes will be used to generate the new keys.

Default no pfs

Parameters **dh-group {1 | 2 | 5 | 14 | 15 | 19 | 20 | 21}** — Specifies which Diffie-Hellman group to use for calculating session keys. More bits provide a higher level of security, but require more processing. Three groups are supported with IKE-v1:

Group 1: 768 bits
Group 2: 1024 bits
Group 5: 1536 bits
Group 14: 2048 bits
Group 15: 3072 bits
Group 19: P-256 ECC Curve, 256 bits
Group 20: P-384 ECC Curve, 384 bits
Group 21: P-512 ECC Curve, 512 bits

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.152 pfs-dh-group

pfs-dh-group

Syntax **pfs-dh-group** {**1** | **2** | **5** | **14** | **15** | **19** | **20** | **21**}
pfs-dh-group inherit
no pfs-dh-group

Context [Tree] (config>ipsec>ipsec-transform pfs-dh-group)

Full Context configure ipsec ipsec-transform pfs-dh-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the Diffie-Hellman group to be used for Perfect Forward Secrecy (PFS) computation during CHILD_SA rekeying.

The **no** form of this command reverts to the default.

Default pfs-dh-group inherit

Parameters {**1** | **2** | **5** | **14** | **15** | **19** | **20** | **21**} — Specifies the Diffie-Hellman group to achieve PFS.

inherit — Specifies that the value of the DH group used by the system is inherited from the IPsec gateway or IPsec tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.153 pgw

pgw

Syntax **pgw**

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile pgw)

Full Context configure subscriber-mgmt gtp peer-profile pgw

Description Commands in this context configure communication with a Packet Data Network Gateway.

Default none

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.154 phone

phone

Syntax [**no**] **phone** *phone-number*

Context **[Tree]** (config>service>cust phone)

Full Context configure service customer phone

Description This command adds telephone number information for a customer ID. The **no** form of this command removes the phone number value from the customer ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *string* — Specifies the customer phone number entered as an ASCII string up to 80 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.

Platforms All

20.155 physical-access-id

physical-access-id

Syntax [**no**] **physical-access-id**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp physical-access-id)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp physical-access-id

Description This command includes the physical access ID.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.156 pid-pmt-unref

pid-pmt-unref

Syntax [**no**] **pat-syntax**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms pid-pmt-unref)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms pid-pmt-unref)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms pid-pmt-unref)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms pid-pmt-unref
configure mcast-management multicast-info-policy bundle channel video analyzer alarms pid-pmt-unref
configure mcast-management multicast-info-policy bundle video analyzer alarms pid-pmt-unref

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the analyzer to check for unreferenced PIDs that have not been referred in the PMT.

Default no pid-pmt-unref

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.157 pim

pim

Syntax **pim** {**asm** | **ssm**} *grp-ip-address*
no pim

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive pim)

Full Context configure service vprn mvpn provider-tunnel inclusive pim

Description This command specifies the PIM mode to use, ASM or SSM, for PIM-based inclusive provider tunnels and the multicast group address to use. Also enables the context for specifying parameters for PIM peering on the inclusive provider tunnel.

Auto-discovery must be enabled in order for SSM to operate.

The **no** form of this command removes the pim context including the statements under the context.

Default no pim

Parameters **asm** — Specifies to use PIM ASM for inclusive provider tunnels.

ssm — Specifies to u PIM SSM for inclusive provider tunnels.

group-address — Specifies the multicast group address to use.

Platforms All

pim

Syntax [**no**] **pim**

Context **[Tree]** (config>service>vprn pim)

Full Context configure service vprn pim

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a Protocol Independent Multicast (PIM) instance in the VPRN service. When an PIM instance is created, the protocol is enabled. PIM is used for multicast routing within the network. Devices in the network can receive the multicast feed requested and non-participating routers can be pruned. The router supports PIM sparse mode (PIM-SM).

The **no** form of this command deletes the PIM protocol instance removing all associated configuration parameters.

Platforms All

pim

Syntax [**no**] **pim**

Context **[Tree]** (config>router pim)

Full Context configure router pim

Description This command enables a Protocol Independent Multicast (PIM) instance.

PIM is used for multicast routing within the network. Devices in the network can receive the multicast feed requested and non-participating routers can be pruned. The router OS supports PIM sparse mode (PIM-SM).

The **no** form of this command disables the PIM instance.

Default no pim

Platforms All

pim

Syntax **pim** [*grp-address*]
no pim

Context **[Tree]** (debug>router>msdp pim)

Full Context debug router msdp pim

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) PIM.

The **no** form of the command disables MSDP PIM debugging.

Parameters *grp-address* — Debugs the IP multicast group address for which this entry contains information.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.158 pim-asm

pim-asm

Syntax **pim-asm** {*grp-ip-address/mask* | *grp-ip-address netmask*}
no pim-asm

Context **[Tree]** (config>service>vprn>mvpn>pt>selective pim-asm)

Full Context configure service vprn mvpn provider-tunnel selective pim-asm

Description This command specifies the range of PIM-ASM groups to use on the sender PE to setup ASM multicast tree for draft Rosen based Data MDT.

Parameters *grp-ip-address* — Specifies the multicast group address.

mask — Specifies the mask of the multicast-ip-address.

Values 4 to 32

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

Platforms All

20.159 pim-policy

pim-policy

Syntax **pim-policy** *pim-policy-name* [**create**]
no pim-policy *pim-policy-name*

Context **[Tree]** (config>subscr-mgmt pim-policy)

Full Context configure subscriber-mgmt pim-policy

Description This command creates a PIM policy or enters the context to configure a PIM policy.

The **no** form of this command deletes the specified PIM policy.

Parameters *pim-policy-name* — Specifies the PIM policy name, up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — Specifies the keyword used to create the PIM policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pim-policy

Syntax **pim-policy** *policy-name*
no pim-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt>sub-prof pim-policy)

Full Context configure subscriber-mgmt sub-profile pim-policy

Description This command adds an existing PIM policy to this subscriber profile.

The **no** form of this command removes the specified PIM policy from this subscriber profile.

Parameters *policy-name* — Specifies the name of the PIM policy name, up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.160 pim-snooping

pim-snooping

Syntax **pim-snooping** [**saps**] [**spoke-sdps**]
no pim-snooping

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync pim-snooping)

Full Context configure redundancy multi-chassis peer sync pim-snooping

Description This command specifies whether PIM snooping for IPv4 information should be synchronized with a multi-chassis peer. Entering **pim-snooping** without any parameters results in the synchronization being applied only to SAPs.

Specifying the **spoke-sdps** parameter results in the synchronization being applied to manually configured spoke SDPs. Specifying both the **saps** and **spoke-sdps** parameters results in the synchronization being applied to both SAPs and manually configured spoke SDPs.

The synchronization of PIM snooping is only supported for manually configured spoke SDPs but is not supported for spoke SDPs configured within an endpoint. See PIM Snooping for IPv4 Synchronization for service support.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no pim-snooping

Parameters **saps** — Specifies that SAPs are to be synchronized with the multi-chassis peer according to the synchronization tags configured on the port. This is the default when no parameters are specified.

spoke-sdps — Specifies that spoke SDPs are to be synchronized with the multi-chassis peer according to the synchronization tags configured on spoke SDPs.

Platforms All

pim-snooping

Syntax **pim-snooping**

Context **[Tree]** (config>service>vpls pim-snooping)
[Tree] (config>service>vpls>spoke-sdp pim-snooping)
[Tree] (config>service>vpls>sap pim-snooping)

Full Context configure service vpls pim-snooping
configure service vpls sap pim-snooping
configure service vpls spoke-sdp pim-snooping

Description This command enables PIM snooping for the VPLS service. When enabled, it is enabled for all SAPs except default SAPs. A default SAP is a SAP that has a wild card VLAN ID, such as sap 1/1/1:*.

The **no** form of this command removes the PIM snooping configuration.

Platforms All

pim-snooping

Syntax [**no**] **pim-snooping**

Context **[Tree]** (debug>service>id pim-snooping)

Full Context debug service id pim-snooping

Description This command enables PIM-snooping debugging.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.161 pim-ssm

pim-ssm

Syntax **pim-ssm** {*grp-ip-address/mask* | *grp-ip-address netmask*}
no pim-ssm

Context **[Tree]** (config>service>vprn>mvpn>pt>selective pim-ssm)

Full Context configure service vprn mvpn provider-tunnel selective pim-ssm

Description This command specifies the PIM SSM groups to use for the selective provider tunnel.

Parameters *group-address/mask* — Specifies a multicast group address and netmask length.

Platforms All

20.162 pim-ssm-scaling

pim-ssm-scaling

Syntax [**no**] **pim-ssm-scaling**

Context **[Tree]** (config>router>pim pim-ssm-scaling)

Full Context configure router pim pim-ssm-scaling

Description This command enables an increase of PIM SSM (S,G) scaling to a maximum of 256kper system. The per-complex (FP) multicast scaling limit is still in place, but multiple complexes can be used to achieve the 256k per-system (S,G) scaling.

The **no** form of this command disables the increase in PIM SSM scaling.

Default no pim-ssm-scaling

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.163 ping

ping

Syntax **ping** {*ip-address* | *dns-name*} [**bypass-routing** | {**interface** *interface-name*} | {**next-hop** *ip-address*}] [**count** *requests*] [**detail** | **rapid**] [**do-not-fragment**] [**fc** *fc-name*] [**interval** {**centisecs** | **secs**}] [**pattern** *pattern*] [{**router** *router-or-service*} | {**router-instance** *router-instance*} | {**service-name** *service-name*}] [**size** *bytes*] [**source** *ip-address*] [**timeout** *timeout*] [**tos** *type-of-service*] [**ttl** *time-to-live*]

ping *ipv4-address* **subscriber-id** *sub-dent-string* [**count** *requests*] [**detail** | **rapid**] [**do-not-fragment**] [**fc** *fc-name*] [**interval** {**centisecs** | **secs**}] [**pattern** *pattern*] [{**router** *router-or-service*} | {**router-instance** *router-instance*} | {**service-name** *service-name*}] [**size** *bytes*] [**source** *ip-address*] [**timeout** *timeout*] [**tos** *type-of-service*] [**ttl** *time-to-live*]

Context **[Tree]** (global ping)

Full Context global ping

Description **Generic ping to verify IP reachability**

The **ping** {*ip-address* |*dns-name*} [{**bypass-routing** |{**interface** *interface-name*} |{**next-hop** *ip-address*}}] command is the TCP/IP utility that is used to verify IP reachability.

Ping to verify L2-aware remote host reachability

The **ping** *ipv4-address* **subscriber-id** *sub-dent-string* command can be initiated from the gateway IPv4 address in the inside routing context or from any IPv4 address in the outside routing context. If the gateway IPv4 address is used as the source address, it must be explicitly configured in the L2-Aware **ping** command.

To test the relevant NAT policy, any source address can be used for the ping. If the given source address refers to a policy that does not reside on the given router, the message “MINOR: OAM #2160 router ID is not an outside router for this subscriber” is displayed to the operator. The source address does not have to belong to the system.

If the outside routing context is not specified, by default, the Base router is selected. If the specified or the default Base router instance is not the outside routing context for the subscriber, the L2-Aware **ping** command execution fails and the message “MINOR: OAM #2160 router ID is not an outside router for this subscriber” is displayed to the operator.

The NAT application shares query IDs between L2-Aware pings and ICMP or GRE traffic that has undergone NAT and is destined to a DMZ host. If there is query ID space exhaustion, ICMP/GRE flows destined to DMZs hosts are deleted so their query IDs can be reused for the requested L2-Aware pings.

Parameters **bypass-routing** — Specifies whether to send the ping request to a host on a directly attached network, bypassing the routing table.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bytes — Specifies the request packet size in bytes, expressed as a decimal integer.

Values 0 to 16384

Default 56

centiseconds | *secs* — Sets the interval.

Values 1 to 10000 centiseconds, if **rapid** is selected.
1 to 1000 seconds, if **secs** is selected.

Default 1 centisecond if **rapid** is selected.
1 second if **secs** is selected.

detail — Displays detailed information.

do-not-fragment — Sets the DF (Do Not Fragment) bit in the ICMP ping packet (does not apply to ICMPv6).

dns-name — Specifies the DNS name of the far-end device to which to send the **svc-ping** request message, expressed as a character string.

fc-name — Specifies the forwarding class of the MPLS echo request packets.

Values be, l2, af, l1, h2, ef, h1, nc

Default nc

interface-name — Specifies the name of an IP interface. The name must already exist in the **config>router>interface** context.

ip-address — Specifies the far-end IP address, in dotted decimal notation, to which to send the **svc-ping** request message.

Values

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x[-*interface*]	
	x:x:x:x:x:x:d.d.d.d[-*interface*]	
	x:	[0 to FFFF]H
	d:	[0 to 255]D
	interface:	up to 32 characters, mandatory for link local addresses

next-hop *ip-address* — Displays only static routes with the specified next hop IP address.

Values

ipv4-address:	a.b.c.d (host bits must be 0)	
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pattern — Specifies that the date portion in a ping packet that is filled with the pattern value specified. If not specified, position information is filled instead.

Values 0 to 65535

Default system-generated sequential pattern

rapid — Specifies that packets be generated as fast as possible instead of the default 1 per second.

requests — Specifies the number of times to perform an OAM ping probe operation. Each OAM echo message request must either time out or receive a reply before the next message request is sent.

Values 1 to 100000

Default 5

router-instance — Specifies the preferred method for entering a service name. Stored as the service name. This is the only service-linking function allowed for both mixed-mode and model-driven configuration modes.

Values router-name: Base, management, *cpm-vr-name*, vpls-management
vprn-svc-name: The service name, up to 64 characters
cpm-vr-name: The CPM VR name, up to 32 characters

router-or-service — Specifies the routing instance or service, by number. The *router-instance* parameter is preferred for specifying the router or service.

Values router-name: Base, management, vpls-management
vprn-svc-id: 1 to 2147483647

Default Base

seconds — Overrides the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

Default 5

Values 1 to 10

service-name — Specifies the alias function that allows the service-name to be used, converted, and stored as a service ID.

sub-ident-string — Specifies the L2-Aware NAT subscriber to which ICMP-ping is sent, up to 32 characters. The **subscriber-id** keyword serves as a differentiator between the subscribers with the same IP address in the same routing context (which is allowed in L2-Aware NAT). The **subscriber-id** keyword is mandatory for L2-Aware IPv4 ping, but optional in generic ping framework.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

source *ip-address* — Specifies the IP address to be used.

Values

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

timeout — Specifies the time out, in seconds.

Values 1 to 10

Default 5

type-of-service — Specifies the service type.

Values 0 to 255

Default 0

time-to-live — Specifies the TTL value for the MPLS label, expressed as a decimal integer.

Values 1 to 128

Default 64

20.164 ping-reply

ping-reply

Syntax [**no**] **ping-reply**

Context **[Tree]** (config>service>ies>if>ipv6>vrrp ping-reply)

Full Context configure service ies interface ipv6 vrrp ping-reply

Description This command enables the non-owner master to reply to ICMP echo requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental Ip interface or based on the ping source host address). when ping-reply is not enabled, icmp Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP echo requests regardless of the setting of ping-reply configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The ping-reply command is only available in non-owner **vrrp** *virtual-router-id* nodal context. If the ping-reply command is not executed, ICMP echo requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all ICMP echo request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply

Platforms All

ping-reply

Syntax [**no**] **ping-reply**

Context **[Tree]** (config>service>ies>if>vrrp ping-reply)

Full Context configure service ies interface vrrp ping-reply

Description This command enables the non-owner master to reply to ICMP Echo Requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address). When ping-reply is not enabled, ICMP Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP Echo Requests regardless of the setting of ping-reply configuration.

The ping-reply command is only available in non-owner **vrrp** *virtual-router-id* nodal context. If the ping-reply command is not executed, ICMP Echo Requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all ICMP Echo Request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply

Platforms All

ping-reply

Syntax [**no**] **ping-reply**

Context **[Tree]** (config>service>vprn>if>vrrp ping-reply)
[Tree] (config>service>vprn>if>ipv6>vrrp ping-reply)

Full Context configure service vprn interface ipv6 vrrp ping-reply

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface vrrp ping-reply

Description This command enables the non-owner master to reply to ICMP Echo Requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address). When ping-reply is not enabled, ICMP Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP Echo Requests regardless of the setting of ping-reply configuration.

The ping-reply command is only available in non-owner **vrrp** *virtual-router-id* nodal context. If the ping-reply command is not executed, ICMP Echo Requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all ICMP Echo Request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply

Platforms All

ping-reply

Syntax [**no**] **ping-reply**

Context **[Tree]** (config>router>if>vrrp ping-reply)
[Tree] (config>router>if>ipv6>vrrp ping-reply)

Full Context configure router interface ipv6 vrrp ping-reply
configure router interface vrrp ping-reply

Description This command enables the non-owner master to reply to ICMP echo requests directed at the virtual router instances IP addresses.

Non-owner virtual router instances are limited by the VRRP specifications to responding to ARP requests destined to the virtual router IP addresses and routing IP packets not addressed to the virtual router IP addresses. Many network administrators find this limitation frustrating when troubleshooting VRRP connectivity issues.

SR OS allows this access limitation to be selectively lifted for certain applications. Ping, Telnet and SSH can be individually enabled or disabled on a per-virtual-router-instance basis.

The **ping-reply** command enables the non-owner master to reply to ICMP echo requests directed at the virtual router instances IP addresses. The Ping request can be received on any routed interface. Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When **ping-reply** is not enabled, ICMP echo requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP echo requests regardless of the **ping-reply** setting.

The **ping-reply** command is only available in non-owner **vrrp** nodal context.

By default, ICMP echo requests to the virtual router instance IP addresses are silently discarded.

The **no** form of the command configures discarding all ICMP echo request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply — ICMP echo requests to the virtual router instance IP addresses are discarded.

Platforms All

20.165 ping-template

ping-template

Syntax **ping-template** *template-name* [**create**]
no ping-template *template-name*

Context **[Tree]** (config>test-oam>icmp ping-template)

Full Context configure test-oam icmp ping-template

Description This command creates a ping-template that can be assigned to a VPRN or IES service IP interface.

The **no** form of this command removes the template name from the configuration.

Parameters *template-name* — Specifies the name of the ping template, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ping-template

Syntax **ping-template** *template-name*
no ping-template

Context **[Tree]** (config>service>ies>if ping-template)
[Tree] (config>service>vprn>if ping-template)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface ping-template
configure service vprn interface ping-template

Description This command maps a **ping-template** name to the service IP interface. The **ping-template** *template-name* is configured in the **config>test-oam>icmp** context and assigned to the service IP interface using this command.

The **config>service>ies|vprn**>if>ping-template must be shut down to remove or change the **destination-address** value.

The **no** form of this command removes the template name from the configuration.

Parameters *template-name* — Specifies the name of the ping template to be assigned to the IP interface, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.166 ping-test

ping-test

Syntax [**no**] **ping-test**

Context **[Tree]** (config>filter>redirect-policy>dest ping-test)

Full Context configure filter redirect-policy destination ping-test

Description This command configures parameters to perform connectivity ping tests to validate the ability for the destination to receive redirected traffic.

Default no ping-test

Platforms All

20.167 pip

pip

Syntax **pip**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if pip)

Full Context configure mcast-management multicast-info-policy video-policy video-interface pip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure within a video interface policy the properties relating to requests received by the video interface for Picture-in-Picture (PIP) channel requests.

Default none

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.168 pir

pir

Syntax **pir** *pir-rate*
pir max
no pir

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl pir)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level pir

Description This command configures the PIR which is enforced for all queues pertaining to this category.

The **no** form of this command reverts to the default.

Parameters *pir-rate* — Specifies the amount of bandwidth in kilobits per second.

Values 1 to 100000000

max — Specifies to use the maximum amount of bandwidth.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pir

Syntax **pir** *congested-pir*
no pir

Context **[Tree]** (config>app-assure>group>policer>congestion-override pir)

Full Context configure application-assurance group policer congestion-override pir

Description This command provides a mechanism to configure the PIR for the congestion override policer. It is recommended that the PIR is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic.

The **no** form of this command resets the PIR value to its default.

Default pir max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *congested-pir* — Specifies an integer value defining size, in kbytes, for the PIR of the policer.

Values 0 to 100000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pir

Syntax **pir** *pir-rate*
no pir

Context **[Tree]** (config>app-assure>group>pol>cng-ovrd-stg2 pir)

Full Context configure application-assurance group policer congestion-override-stage2 pir

Description This command provides a mechanism to configure the PIR for the congestion override policer. It is recommended that the PIR is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic.

The **no** form of this command resets the PIR value to its default.

Default pir max

Parameters *congested-pir* — Specifies an integer value defining size, in kbytes, for the PIR of the policer.

Values 0 to 100000000, max

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.169 pki

pki

Syntax **pki**

Context **[Tree]** (config>system>security pki)

Full Context configure system security pki

Description Commands in this context configure PKI related parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.170 pkt-too-big

pkt-too-big

Syntax [**no**] **pkt-too-big**

Context **[Tree]** (config>ipsec>tnl-temp>icmp6-gen pkt-too-big)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>icmp6-gen pkt-too-big)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>icmp6-gen pkt-too-big)
[Tree] (config>service>vprn>if>sap>ipsec-tun>icmp6-gen pkt-too-big)
[Tree] (config>router>if>ipsec-tunnel>icmp-gen pkt-too-big)

Full Context configure ipsec tunnel-template icmp6-generation pkt-too-big
configure router interface ipsec-tunnel icmp-gen pkt-too-big
configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big
configure service vprn interface ipsec ipsec-tunnel icmp6-generation pkt-too-big
configure service vprn interface sap ipsec-tunnel icmp6-generation pkt-too-big

Description This command enables the system to send ICMPv6 PTB (Packet Too Big) messages on the private side and optionally specifies the rate.

With this command configured, the system sends PTB back if it received an IPv6 packet on the private side that is bigger than 1280 bytes and also exceeds the private MTU of the tunnel.

The **ip-mtu** command (under **ipsec-tunnel** or **tunnel-template**) specifies the private MTU for the ipsec-tunnel or dynamic tunnel.

The **no** form of this command reverts **interval** and **message-count** values to their default values.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec tunnel-template icmp6-generation pkt-too-big
- configure service vprn interface sap ipsec-tunnel icmp6-generation pkt-too-big

VSR

- configure service ies interface ipsec ipsec-tunnel icmp6-generation pkt-too-big
- configure service vprn interface ipsec ipsec-tunnel icmp6-generation pkt-too-big

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.171 platform-type

platform-type

Syntax **platform-type** *type*
no platform type

Context **[Tree]** (config>system>ned>profile platform-type)

Full Context configure system network-element-discovery profile platform-type

Description This command configures the platform name and chassis type to be advertised.

The **no** form of this command removes any explicitly defined type and the default type of "chassis-name, chassis-type" is used.

Default no platform-type

Parameters *type* — Specifies the platform type to be associates with the profile, up to 255 characters.

Platforms All

20.172 pm-tti

pm-tti

Syntax **pm-tti**

Context **[Tree]** (config>port>otu pm-tti)

Full Context configure port otu pm-tti

Description Commands in this context configure path monitoring trail trace identifier parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.173 pmt-repetition

pmt-repetition

Syntax **pcr-repetition** [**tnc** *tnc-milli-seconds* **qos** *qos-milli-seconds* **poa** *poa-milli-seconds*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no pcr-repetition

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms pmt-repetition)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms pmt-repetition)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms pmt-repetition)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms pmt-repetition
configure mcast-management multicast-info-policy bundle channel video analyzer alarms pmt-repetition
configure mcast-management multicast-info-policy bundle video analyzer alarms pmt-repetition

Description This command configures the analyzer to check for the program map table (PMT). It is expected that the PMT arrives periodically within a certain interval range. It is possible to configure the type of alarm that is raised when the PMT fails to arrive within the specified interval. As the delay increases between two consecutive PMTs, the type of alarm raised becomes more critical, from TNC to POA.

Default no pmt-repetition

Parameters *tnc-milli-seconds* — Specifies the time, in milliseconds, for which a TNC alarm is raised if the interval between two consecutive PMTs is greater than or equal to this configured value.

Values 100 to 4800 in multiples of 100 only

Default 400

qos-milli-seconds — Specifies the time, in milliseconds, for which a QoS alarm is raised if the interval between two consecutive PMTs is greater than or equal to this configured value.

Values 200 to 4900 in multiples of 100 only and higher than the *tnc-milli-seconds* value

Default 800

poa-milli-seconds — Specifies the time, in milliseconds, for which a POA alarm is raised if the interval between two consecutive PMTs is greater than or equal to this configured value.

Values 300 to 5000 in multiples of 100 only and higher than the *qos-milli-seconds* value

Default 2000

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.174 pmt-syntax

pmt-syntax

Syntax [**no**] **pat-syntax**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms pmt-syntax)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms pmt-syntax)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms pmt-syntax)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms pmt-syntax
configure mcast-management multicast-info-policy bundle channel video analyzer alarms pmt-syntax
configure mcast-management multicast-info-policy bundle video analyzer alarms pmt-syntax

Description This command configures the analyzer to check for PMT syntax errors.

Default no pmt-syntax

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.175 pmtu-discovery-aging

pmtu-discovery-aging

Syntax **pmtu-discovery-aging** *seconds*
no pmtu-discovery-aging

Context **[Tree]** (config>ipsec>tnl-temp pmtu-discovery-aging)
[Tree] (config>router>if>ipsec>ipsec-tunnel pmtu-discovery-aging)
[Tree] (config>service>ies>if>sap>ip-tunnel pmtu-discovery-aging)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel pmtu-discovery-aging)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel pmtu-discovery-aging)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel pmtu-discovery-aging)
[Tree] (config>service>vprn>if>sap>ip-tunnel pmtu-discovery-aging)

Full Context configure ipsec tunnel-template pmtu-discovery-aging
configure router interface ipsec ipsec-tunnel pmtu-discovery-aging
configure service ies interface ipsec ipsec-tunnel pmtu-discovery-aging
configure service ies interface sap ip-tunnel pmtu-discovery-aging

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface ipsec ipsec-tunnel pmtu-discovery-aging
configure service vprn interface sap ip-tunnel pmtu-discovery-aging
configure service vprn interface sap ipsec-tunnel pmtu-discovery-aging

Description This command configures the time used to age out the learned temporary MTU which is from the public network. The temporary MTU is used for MTU propagation.

The **no** form of of this command reverts to the default value.

Default pmtu-discovery-aging 900

Parameters *seconds* — specifies the time, in seconds, used to age out the learned MTU

Values 900 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel pmtu-discovery-aging
- configure service vprn interface sap ip-tunnel pmtu-discovery-aging
- configure service ies interface sap ip-tunnel pmtu-discovery-aging
- configure ipsec tunnel-template pmtu-discovery-aging

VSR

- configure service ies interface ipsec ipsec-tunnel pmtu-discovery-aging
- configure service vprn interface ipsec ipsec-tunnel pmtu-discovery-aging
- configure router interface ipsec ipsec-tunnel pmtu-discovery-aging

20.176 poi-tlv-enable

poi-tlv-enable

Syntax **[no] poi-tlv-enable**

Context **[Tree]** (config>service>vprn>isis poi-tlv-enable)

Full Context configure service vprn isis poi-tlv-enable

Description Enable use of Purge Originator Identification (POI) TLV for this IS-IS instance. The POI is added to purges and contains the system ID of the router that generated the purge, which simplifies troubleshooting and determining what caused the purge.

The **no** form of this command removes the POI functionality from the configuration.

Default no poi-tlv-enable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

poi-tlv-enable

Syntax **[no] poi-tlv-enable**

Context **[Tree]** (config>router>isis poi-tlv-enable)

Full Context configure router isis poi-tlv-enable

Description Enable use of Purge Originator Identification (POI) TLV for this IS-IS instance. The POI is added to purges and contains the system ID of the router that generated the purge, which simplifies troubleshooting and determining what caused the purge.

The **no** form of this command removes the POI functionality from the configuration.

Default no poi-tlv-enable

Platforms All

20.177 policer

policer

Syntax **policer** *policer-id* {**ingress-only** | **egress-only** | **ingress-egress**}
no policer *policer-id*

Context **[Tree]** (config>subscr-mgmt>cat-map>category policer)

Full Context configure subscriber-mgmt category-map category policer

Description This command configures a policer in this category.

The **no** form of this command reverts to the default.

Parameters *policer-id* — Specifies an existing policer identifier.

Values 1 to 63

ingress-only — Specifies that ingress policers are defined in this category.

egress-only — Specifies that egress policers are defined in this category.

ingress-egress — Specifies that ingress and egress policers are defined in this category.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer

Syntax [**no**] **policer** *policer-id*

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos policer)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos policer)

Full Context configure subscriber-mgmt sla-profile egress qos policer
configure subscriber-mgmt sla-profile ingress qos policer

Description This command is used in the sap-ingress and sap-egress QoS policies to create, modify or delete a policer. Policers are created and used in a similar manner to queues. The policer ID space is separate from the queue ID space, allowing both a queue and a policer to share the same ID. The sap-ingress policy may have up to 32 policers (numbered 1 through 32) may be defined while the sap-egress QoS policy supports a maximum of 8 (numbered 1 through 8). While a policer may be defined within a QoS policy, it is not actually created on SAPs or subscribers associated with the policy until a forwarding class is mapped to the policer's ID.

All policers must be created within the QoS policies. A default policer is not created when a sap-ingress or sap-egress QoS policy is created.

Once a policer is created, the policer's metering rate and profiling rates may be defined as well as the policer's maximum and committed burst sizes (MBS and CBS respectively). Unlike queues which have dedicated counters, policers allow various stat-mode settings that define the counters that is associated with the policer. Another supported feature—packet-byte-offset—provides a policer with the ability to modify the size of each packet based on a defined number of bytes.

Once a policer is created, it cannot be deleted from the QoS policy unless any forwarding classes that are mapped to the policer are first moved to other policers or queues.

The system will allow a policer to be created on a SAP QoS policy regardless of the ability to support policers on objects where the policy is currently applied. The system only scans the current objects for policer support and sufficient resources to create the policer when a forwarding class is first mapped to the policer ID. If the policer cannot be created due to one or more instances of the policy not supporting policing or having insufficient resources to create the policer, the forwarding class mapping will fail.

The **no** form of this command is used to delete a policer from a sap-ingress or sap-egress QoS policy. The specified policer cannot currently have any forwarding class mappings for the removal of the policer to succeed. It is not necessary to actually delete the policer ID for the policer instances to be removed from SAPs or subscribers associated with the QoS policy once all forwarding classes have been moved away from the policer. It is automatically deleted from each policing instance although it still appears in the QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policer-id* — Specifies the policer ID. The policer-id must be specified when executing the policer command. If the specified ID already exists, the system enters that policer's context to allow the policer's parameters to be modified. If the ID does not exist and is within the allowed range for the QoS policy type, a context for the policer ID is created (depending on the system's current create keyword requirements which may require the create keyword to actually add the new policer ID to the QoS policy) and the system will enter that new policer's context for possible parameter modification.

Values 1 to 63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer

Syntax **policer** *policer-name*
no policer

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>xconnect policer)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>xconnect policer)

Full Context configure service ies subscriber-interface group-interface wlan-gw ranges range vrgw lanext xconnect policer
configure service vprn subscriber-interface group-interface wlan-gw ranges range vrgw lanext xconnect policer

Description This command configures an ISA policer for cross-connect traffic.

The **no** form of this command removes the policer name from the configuration.

Default no policer

Parameters *policer-name* — Specifies the name of the policer, up to 32 characters.

policer

Syntax **policer** *policer-name*
no policer

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network policer)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>network policer)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext network policer
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext network policer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an ISA policer for HLE network (such as DC) access facing connection traffic, per tunnel.

The **no** form of this command removes the policer name from the configuration.

Default no policer

Parameters *policer-name* — Specifies the name of the policer, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer

Syntax **policer** *policer-name*
no policer

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>access policer)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>vrgw>lanext>access policer)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access policer
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw lanext access policer

Description This command configures an ISA policer for HLE ingress (such as home) access facing connection traffic, per tunnel

The **no** form of this command removes the policer name from the configuration.

Default no policer

Parameters *policer-name* — Specifies the name of the policer, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

Context **[Tree]** (config>card>fp>ingress>access>qgrp>policer-over policer)
[Tree] (config>card>fp>ingress>network>qgrp>policer-over policer)

Full Context configure card fp ingress access queue-group policer-override policer
configure card fp ingress network queue-group policer-override policer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates, modifies or deletes a policer. Policers are created and used in a similar manner to queues. The policer ID space is separate from the queue ID space, allowing both a queue and a policer to share the same ID. The sap-ingress policy may have up to 32 policers (numbered 1 through 32) may be defined while the sap-egress QoS policy supports a maximum of 8 (numbered 1 through 8). While a policer may be defined within a QoS policy, it is not actually created on SAPs or subscribers associated with the policy until a forwarding class is mapped to the policer's ID.

All policers must be created within the QoS policies. A default policer is not created when a sap-ingress or sap-egress QoS policy is created.

Once a policer is created, the policer's metering rate and profiling rates may be defined as well as the policer's maximum and committed burst sizes (MBS and CBS respectively). Unlike queues which have dedicated counters, policers allow various stat-mode settings that define the counters that will be associated with the policer. Another supported feature—packet-byte-offset—provides a policer with the ability to modify the size of each packet based on a defined number of bytes.

Once a policer is created, it cannot be deleted from the QoS policy unless any forwarding classes that are mapped to the policer are first moved to other policers or queues.

The system will allow a policer to be created on a SAP QoS policy regardless of the ability to support policers on objects where the policy is currently applied. The system only scans the current objects for policer support and sufficient resources to create the policer when a forwarding class is first mapped to the policer ID. If the policer cannot be created due to one or more instances of the policy not supporting policing or having insufficient resources to create the policer, the forwarding class mapping fails.

The **no** form of this command deletes a policer from a sap-ingress or sap-egress QoS policy. The specified policer cannot currently have any forwarding class mappings for the removal of the policer to succeed. It is not necessary to actually delete the policer ID for the policer instances to be removed from SAPs or subscribers associated with the QoS policy once all forwarding classes have been moved away from the policer. It is automatically deleted from each policing instance although it still appears in the QoS policy.

Parameters *policer-id* — Specifies that the *policer-id* must be specified when executing the policer command. If the specified ID already exists, the system enters that policer's context to allow the policer's parameters to be modified. If the ID does not exist and is within the allowed range for the QoS policy type, a context for the policer ID will be created (depending on the system's current create keyword requirements which may require the create keyword to actually add the new policer ID to the QoS policy) and the system will enter that new policer's context for possible parameter modification.

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

Context **[Tree]** (config>service>apipe>sap>egress>policer-over policer)
[Tree] (config>service>apipe>sap>ingress>policer-over policer)
[Tree] (config>service>cpipe>sap>egress>policer-over policer)
[Tree] (config>service>cpipe>sap>ingress>policer-over policer)
[Tree] (config>service>epipe>sap>egress>policer-over policer)
[Tree] (config>service>fpipe>sap>egress>policer-over policer)
[Tree] (config>service>fpipe>sap>ingress>policer-over policer)
[Tree] (config>service>ipipe>sap>egress>policer-over policer)
[Tree] (config>service>ipipe>sap>ingress>policer-over policer)

Full Context configure service apipe sap egress policer-override policer
configure service apipe sap ingress policer-override policer
configure service cpipe sap egress policer-override policer
configure service cpipe sap ingress policer-override policer
configure service epipe sap egress policer-override policer
configure service fpipe sap egress policer-override policer
configure service fpipe sap ingress policer-override policer
configure service ipipe sap egress policer-override policer
configure service ipipe sap ingress policer-override policer

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to a specific policer created on the SAP through a sap-ingress or sap-egress QoS policy.

The **no** form of this command is used to remove any existing overrides for the specified policer-id.

Parameters *policer-id* — The *policer-id* parameter is required when executing the policer command within the policer-overrides context. The specified *policer-id* must exist within the sap-ingress or sap-egress QoS policy applied to the SAP. If the policer is not currently used by any forwarding class or forwarding type mappings, the policer will not actually exist on the SAP. This does not preclude creating an override context for the policer-id.

create — The create keyword is required when a **policer** policer-id override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress policer-override policer
- configure service cpipe sap ingress policer-override policer
- configure service fpipe sap ingress policer-override policer
- configure service cpipe sap egress policer-override policer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap ingress policer-override policer
- configure service ipipe sap egress policer-override policer
- configure service epipe sap egress policer-override policer

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-override policer
- configure service apipe sap egress policer-override policer

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

Context **[Tree]** (config>service>vpls>sap>egress>policer-override policer)
[Tree] (config>service>vpls>sap>ingress>policer-override policer)

Full Context configure service vpls sap egress policer-override policer
configure service vpls sap ingress policer-override policer

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to a specific policer created on the SAP through a sap-ingress or sap-egress QoS policy.

The **no** form of this command is used to remove any existing overrides for the specified policer-id.

Parameters *policer-id* — The policer-id parameter is required when executing the policer command within the policer-overrides context. The specified policer-id must exist within the sap-ingress or sap-egress QoS policy applied to the SAP. If the policer is not currently used by any forwarding class or forwarding type mappings, the policer will not actually exist on the SAP. This does not preclude creating an override context for the policer-id.

create — The create keyword is required when a policer policer-id override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>egress>policer-override policer)
[Tree] (config>service>ies>if>sap>ingress>policer-override policer)

Full Context configure service ies interface sap egress policer-override policer
configure service ies interface sap ingress policer-override policer

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to a specific policer created on the SAP through a sap-ingress or sap-egress QoS policy.

The **no** form of this command is used to remove any existing overrides for the specified policer-id.

Parameters *policer-id* — This parameter is required when executing the policer command within the policer-override context. The specified *policer-id* must exist within the sap-ingress or sap-egress QoS policy applied to the SAP. If the policer is not currently used by any forwarding class or forwarding type mappings, the policer will not actually exist on the SAP. This does not preclude creating an override context for the *policer-id*.

create — The create keyword is required when a policer override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit configuration, the **create** keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

Context [Tree] (config>service>vprn>if>sap>egress>policer-override policer)
[Tree] (config>service>vprn>if>sap>ingress>policer-override policer)

Full Context configure service vprn interface sap egress policer-override policer
configure service vprn interface sap ingress policer-override policer

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to a specific policer created on the SAP through a sap-ingress or sap-egress QoS policy.

The **no** form of this command is used to remove any existing overrides for the specified policer-id.

Parameters *policer-id* — This parameter is required when executing the policer command within the policer-override context. The specified *policer-id* must exist within the sap-ingress or sap-egress QoS policy applied to the SAP. If the policer is not currently used by any forwarding class or forwarding type mappings, the policer will not actually exist on the SAP. This does not preclude creating an override context for the *policer-id*.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — The create keyword is required when a policer override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit configuration, the **create** keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer

Syntax **policer** *policer-name* **type** *type* **granularity** *granularity* [**create**]
policer *policer-name*
no policer *policer-name*

Context **[Tree]** (config>app-assure>group policer)

Full Context configure application-assurance group policer

Description This command creates application assurance policer profile of a specified type. Policers can be bandwidth or flow limiting and can have a system scope (limits traffic entering AA ISA for all or a subset of AA subscribers), subscriber scope or granularity (limits apply to each AA subscriber traffic).

The policer type and granularity can only be configured during creation. They cannot be modified. The policer profile must be removed from all AQPs in order to be removed. Changes to policer profile parameters take effect immediately for policers instantiated as result of AQP actions using this profile.

The **no** form of this command deletes the specified policer from the configuration.

Parameters *policer-name* — Specifies a string of up to 32 characters that identifies the policer.

type — Specifies the policer type.

Values **single-bucket-bandwidth** — Creates a profile for a single bucket (PIR) bandwidth limiting policer.

dual-bucket-bandwidth — Creates profile for a dual bucket (PIR, CIR) bandwidth limiting policer.

flow-rate-limit — Creates profile for a policer limiting rate of flow set-ups.

flow-count-limit — Creates profile for a policer limiting total flow count.

granularity — Specifies the granularity type.

Values **system** — Creates a system policer profile for a policer that limits the traffic in the scope of all or a subset of AA subscribers on a given AA ISA.

subscriber — Creates a policer profile for a policer for each AA subscriber that limits the traffic in the scope of that subscriber.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

access-network-location — Creates a policer profile for a policer instance for each ANL that limits traffic bandwidth in the scope of that ANL. For ANL, only single-bucket bandwidth policers can be configured.

create — Keyword used to create the policer name and parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer

Syntax **policer** *policer-name* **direction** *direction* [**create**]
no policer *policer-name* **direction** *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca policer)

Full Context configure application-assurance group statistics threshold-crossing-alert policer

Description This command configures a TCA for the counter capturing drops or admit events due to the specified flow policer. A policer TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a policer TCA.

Parameters *policer-name* — Specifies the name of the flow policer, up to 32 characters

direction — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer

Syntax **policer** *policer-id* [**fp-redirect-group**]
no policer

Context **[Tree]** (config>qos>sap-ingress>fc policer)

Full Context configure qos sap-ingress fc policer

Description Within a sap-ingress QoS policy forwarding class context, the **policer** command is used to map packets that match the forwarding class and are considered unicast in nature to the specified policer-id. The specified policer-id must already exist within the **sap-ingress** QoS policy. While the system is determining the forwarding class of a packet, it is also looking up its forwarding destination. If ingress forwarding logic has resolved a unicast destination (the packet does not need to be sent to multiple destinations), it is considered to be a unicast packet and will be mapped to either an ingress queue (using the **queue** *queue-id* or **queue** *queue-id* **group** *ingress-queue-group* commands) or an ingress policer (**policer** *policer-id*).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **queue** and **policer** commands within the forwarding class context are mutually exclusive. By default, the unicast forwarding type is mapped to the SAP ingress default queue (queue 1). If the **policer** *policer-id* command is executed, any previous policer mapping or queue mapping for the unicast forwarding type within the forwarding class is overridden if the policer mapping is successful.

A policer defined within the **sap-ingress** policy is not actually created on an ingress SAP or a subscriber using an **sla-profile** where the policy is applied until at least one forwarding type (unicast, broadcast, unknown, or multicast) from one of the forwarding classes is mapped to the policer. If insufficient policer resources exist to create the policer for a SAP or subscriber or multiservice site or ingress policing is not supported on the port associated with the SAP or subscriber or multiservice site, the initial forwarding class forwarding type mapping will fail.

When the unicast forwarding type within a forwarding class is mapped to a policer, the unicast packets classified to the subclasses within the forwarding class are also mapped to the policer.

The **no** form of this command is used to restore the mapping of the unicast forwarding type within the forwarding class to the default queue. If all forwarding class forwarding types had been removed from the default queue, the queue will not exist on the SAPs or subscriber or multiservice sites associated with the QoS policy and the **no policer** command will cause the system to attempt to create the default queue on each object. If the system cannot create the default queue in each instance, the **no policer** command will fail and the unicast forwarding type within the forwarding class will continue its mapping to the existing *policer-id*. If the **no policer** command results in a policer without any current mappings, the policer will be removed from the SAPs and subscribers associated with the QoS policy. All statistics associated with the policer on each SAP and subscriber will be lost.

Parameters *policer-id* — When the forwarding class **policer** command is executed, a valid *policer-id* must be specified. The parameter *policer-id* references a *policer-id* that has already been created within the **sap-ingress** QoS policy.

Values 1 to 63

fp-redirect-group — Redirects a forwarding class to a forwarding plane queue-group as specified in a SAP QoS policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

Context **[Tree]** (config>qos>sap-ingress policer)

Full Context configure qos sap-ingress policer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used in the sap-ingress and sap-egress QoS policies to create, modify, or delete a policer. Policers are created and used in a similar manner to queues. The policer ID space is separate from the queue ID space, allowing both a queue and a policer to share the same ID. The sap-ingress policy may be defined to have up to 63 policers (numbered 1 through 63) while the sap-egress QoS policy supports a maximum of 8 (numbered 1 through 8). While a policer may be defined within a QoS policy, it is not actually created on SAPs or subscribers or multiservice sites associated with the policy until a forwarding class is mapped to the policer's ID.

All policers must be created within the QoS policies. A default policer is not created when a sap-ingress or sap-egress QoS policy is created.

When a policer is created, the policer's metering rate and profiling rates may be defined as well as the policer's maximum and committed burst sizes (MBS and CBS, respectively). Unlike queues that have dedicated counters, policers allow various stat-mode settings that define the counters that will be associated with the policer. Another supported feature—packet-byte-offset—provides a policer with the ability to modify the size of each packet, based on a defined number of bytes.

When a policer is created, it cannot be deleted from the QoS policy unless any forwarding classes that are mapped to the policer are first moved to other policers or queues.

The system will allow a policer to be created on a SAP QoS policy regardless of the ability to support policers on objects where the policy is currently applied. The system only scans the current objects for policer support and sufficient resources to create the policer when a forwarding class is first mapped to the policer ID. If the policer cannot be created due to one or more instances of the policy not supporting policing or having insufficient resources to create the policer, the forwarding class mapping will fail.

The **no** form of this command is used to delete a policer from a sap-ingress or sap-egress QoS policy. The specified policer cannot currently have any forwarding class mappings for the removal of the policer to succeed. It is not necessary to actually delete the policer ID for the policer instances to be removed from SAPs or subscriber or multiservice sites associated with the QoS policy when all forwarding classes have been moved away from the policer. It is automatically deleted from each policing instance although it still appears in the QoS policy.

Parameters *policer-id* — The *policer-id* must be specified when executing the policer command. If the specified ID already exists, the system enters that policer's context to allow the policer's parameters to be modified. If the ID does not exist and is within the allowed range for the QoS policy type, a context for the policer ID will be created (depending on the system's current create keyword requirements, which may require the create keyword to actually add the new policer ID to the QoS policy) and the system will enter that new policer's context for possible parameter modification.

Values 1 to 63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer

Syntax **policer** *policer-id* [{[**port-redirect-group-queue**] [**queue** *queue-id*] | **group** *group-name* [**instance** *instance-id*] [**queue** *queue-id*]}]
no policer

Context **[Tree]** (config>qos>sap-egress>fc policer)

Full Context configure qos sap-egress fc policer

Description Within a sap-egress QoS policy forwarding class context, the policer command is used to map packets that match the forwarding class to the specified policer-id. The specified policer-id must already exist within the sap-egress QoS policy. The forwarding class of the packet is first discovered at ingress, based on the ingress classification rules. When the packet arrives at egress, the sap-egress QoS policy may match a forwarding class reclassification rule that overrides the ingress derived forwarding class. The forwarding class context within the sap-egress QoS policy is then used to map the packet to an egress queue (using the queue queue-id, or port-redirect-group queue queue-id, or group queue-group-name instance instance-id queue queue-id commands) or an egress policer (policer policer-id). The queue and policer commands within the forwarding class context are mutually exclusive. By default, the forwarding class is mapped to the SAP egress default queue (queue 1). If the **policer** *policer- id* command is executed, any previous policer mapping or queue mapping for the forwarding class is overridden if the policer mapping is successful.

A policer defined within the sap-egress policy is not actually created on an egress SAP, or a subscriber using an SLA profile where the policy is applied, until at least one forwarding class is mapped to the policer. If insufficient policer resources exist to create the policer for a SAP or subscriber, or egress policing is not supported on the port associated with the SAP or subscriber, the initial forwarding class mapping will fail.

Packets that are mapped to an egress policer that are not discarded by the policer must be placed into a default queue on the packet's destination port. The system uses egress port queue groups for this purpose. An egress queue group named policer-output-queues is automatically created on each port that supports egress policers. By default, the system uses the forwarding class mappings within this queue group to decide which queue within the group will receive each packet output from the policer. This default policer output queuing behavior may be overridden for non-subscriber packets by redirection to a queue group. The name and instance of the queue group to redirect to is either specified in the QoS policy, or the fact that a forwarding class must be redirected is identified in the QoS policy and the specific queue group instance is only identified at the time the QoS policy is applied:

- If the **policer** *policer-id* command is successfully executed, the default egress queuing is performed for the forwarding class using the policer-output-queues queue group and the *queue-id* within the group based on the forwarding class map from the group template.
- If the **policer** *policer-id* **queue** *queue-id* command is successfully executed, the specified SAP *queue-id* within the egress QoS policy is used instead of the default policer output queues.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If the **policer** *policer-id* **port-redirect-group-queue** keyword is successfully executed, the system will map the forwarding class to the queue within the egress queue group instance specified at the time the QoS policy is applied to the SAP, using the forwarding class map from the queue group template.
- If the **policer** *policer-id* **port-redirect-group queue** *queue-id* command is successfully executed, the system will map the forwarding class to the configured *queue-id* within the egress queue group instance that is specified at the time the QoS policy is applied to the SAP (ignoring using the forwarding class map from the queue group template).
- If the **policer** *policer-id* **group** *queue-group-name* **instance** *instance-id* command is successfully executed, the system will map the forwarding class to the queue within the specified egress queue group instance using the forwarding class map from the group template.
- If the **policer** *policer-id* **group** *queue-group-name* **instance** *instance-id* **queue** *queue-id* command is successfully executed, the system will map the forwarding class to the specified *queue-id* within the specified egress queue group instance (ignoring the forwarding class map in the group template).

If the specified **group** *group-name* is not defined as an egress queue-group-template, the **policer** command will fail. Also, if the specified group does not exist on the port for the SAPs or subscribers associated with the **sap-egress** QoS policy, the policer command will fail. While a group queue-group-name is specified in a **sap-egress** QoS policy, the groups corresponding egress template cannot be deleted. While a port egress queue group is associated with a policer instance, the port queue group cannot be deleted.

If the specified **queue** *queue-id* is not defined in the egress queue-group-template queue-group- name, the policer command will fail. While a *queue-id* within an egress queue group template is referenced by a **sap-egress** QoS policy forwarding class policer command, the queue cannot be deleted from the queue group template.

If an egress policed packet is discarded by the egress port queue group queue, the source policer discard stats are incremented. This means that the discard counters for the policer represent both the policer discard events and the destination queue drop tail events associated with the policer.

The **no** form of this command is used to restore the mapping of the forwarding class to the default queue. If all forwarding classes have been removed from the default queue, the queue will not exist on the SAPs or subscribers associated with the QoS policy and the **no policer** command will cause the system to attempt to create the default queue on each object. If the system cannot create the default queue in each instance, the **no policer** command will fail and the forwarding class will continue its mapping to the existing *policer-id*. If the **no policer** command results in a policer without any current mappings, the policer will be removed from the SAPs and subscribers associated with the QoS policy. All statistics associated with the policer on each SAP and subscribers will be lost.

Default no policer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policer-id* — When the forwarding class **policer** command is executed, a valid *policer-id* must be specified. The parameter *policer-id* references a *policer-id* that has already been created within the **sap-egress** QoS policy.

Values 1 to 63

port-redirect-group-queue — Used to override the forwarding class default egress queue destination to an egress port queue group. The specific egress queue group instance to use is specified at the time the QoS policy is applied to the SAP. Therefore, this parameter is only valid if SAP-based redirection is required.

queue *queue-id* — This parameter overrides the forwarding class default egress queue destination to a specified *queue-id*. If port-redirect-group is not configured, this will be a local SAP queue of that *queue-id*. A queue of ID *queue-id* must exist within the egress QoS policy. If **port-redirect-group-queue** is configured, the **queue** *queue-id* in the egress port queue group instance is used.

Values 1 to 8

Default Derived from forwarding class assignment in queue-group definition.

group *group-name* — The **group** *queue-group-name* is optional and is used to override the forwarding class's default egress queue destination. If the queue group-queue-id parameter is not specified, the forwarding class map within the specified group's template is used to derive which queue within the group will receive the forwarding class's packets. An egress queue group template must exist for the specified queue-group-name or the policer command will fail. The specified queue-group-name must also exist as an egress queue group on the ports where SAPs and subscribers associated with the sap-egress policy are applied or the policer command will fail.

Values Any qualifying egress queue group name

Default policer-output-queues

queue *queue-id* — The **queue** *group-queue-id* is optional when the group queue-group-name parameter is specified and is used to override the forwarding class mapping within the group's egress queue group template. The specified group-queue-id must exist within the group's egress queue group template or the policer command will fail.

Values 1 to 8

Default Derived from forwarding class assignment in queue-group definition

instance *instance-id* — This parameter is used to specify the specific instance of a queue group with template queue-group-name to which this queue should be redirected. This parameter is only valid for queue groups on egress ports where policy-based redirection is required.

Values 1 to 40960

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer

Syntax **policer** *policer-id* [**create**]
no policer

Context **[Tree]** (config>qos>sap-egress policer)

Full Context configure qos sap-egress policer

Description A policer defined within the sap-egress policy is not actually created on an egress SAP, or a subscriber using an SLA profile where the policy is applied, until at least one forwarding class is mapped to the policer. If insufficient policer resources exist to create the policer for a SAP or subscriber, or egress policing is not supported on the port associated with the SAP or subscriber, the initial forwarding class mapping will fail.

Packets that are mapped to an egress policer that are not discarded by the policer must be placed into a default queue on the packet's destination port. The system uses egress port queue groups for this purpose. An egress queue group named policer-output-queues is automatically created on each port that supports egress policers. By default, the system uses the forwarding class mappings within this queue group to decide which queue within the group will receive each packet output from the policer. This default policer output queuing behavior may be overridden for non-subscriber packets by redirection to a queue group. The name and instance of the queue group to redirect to is either specified in the QoS policy, or the fact that a forwarding class must be redirected is identified in the QoS policy and the specific queue group instance is only identified at the time the QoS policy is applied:

- If the **policer** *policer-id* command is successfully executed, the default egress queuing is performed for the forwarding class using the policer-output-queues queue group and the *queue-id* within the group based on the forwarding class map from the group template.
- If the **policer** *policer-id* **queue** *queue-id* command is successfully executed, the specified SAP *queue-id* within the egress QoS policy is used instead of the default policer output queues.
- If the **policer** *policer-id* **port-redirect-group-queue** keyword is successfully executed, the system will map the forwarding class to the queue within the egress queue group instance specified at the time the QoS policy is applied to the SAP, using the forwarding class map from the queue group template.
- If the **policer** *policer-id* **port-redirect-group queue** *queue-id* command is successfully executed, the system will map the forwarding class to the configured *queue-id* within the egress queue group instance that is specified at the time the QoS policy is applied to the SAP (ignoring using the forwarding class map from the queue group template).
- If the **policer** *policer-id* **group** *queue-group-name* **instance** *instance-id* command is successfully executed, the system will map the forwarding class to the queue within the specified egress queue group instance using the forwarding class map from the group template.
- If the **policer** *policer-id* **group** *queue-group-name* **instance** *instance-id* **queue** *queue-id* command is successfully executed, the system will map the forwarding class to the specified *queue-id* within the specified egress queue group instance (ignoring the forwarding class map in the group template).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the specified **group** *group-name* is not defined as an egress queue-group-template, the **policer** command will fail. Also, if the specified group does not exist on the port for the SAPs or subscribers associated with the **sap-egress** QoS policy, the policer command will fail. While a group queue-group-name is specified in a **sap-egress** QoS policy, the groups corresponding egress template cannot be deleted. While a port egress queue group is associated with a policer instance, the port queue group cannot be deleted.

If the specified **queue** *queue-id* is not defined in the egress queue-group-template queue-group- name, the policer command will fail. While a *queue-id* within an egress queue group template is referenced by a **sap-egress** QoS policy forwarding class policer command, the queue cannot be deleted from the queue group template.

If an egress policed packet is discarded by the egress port queue group queue, the source policer discard stats are incremented. This means that the discard counters for the policer represent both the policer discard events and the destination queue drop tail events associated with the policer.

The **no** form of this command is used to restore the mapping of the forwarding class to the default queue. If all forwarding classes have been removed from the default queue, the queue will not exist on the SAPs or subscribers associated with the QoS policy and the **no policer** command will cause the system to attempt to create the default queue on each object. If the system cannot create the default queue in each instance, the **no policer** command will fail and the forwarding class will continue its mapping to the existing *policer-id*. If the **no policer** command results in a policer without any current mappings, the policer will be removed from the SAPs and subscribers associated with the QoS policy. All statistics associated with the policer on each SAP and subscribers will be lost.

Default no policer

Parameters *policer-id* — When the forwarding class **policer** command is executed, a valid *policer-id* must be specified. The parameter *policer-id* references a *policer-id* that has already been created within the **sap-egress** QoS policy.

Values 1 to 63

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer

Syntax **policer** *policer-id* [**create**]
no policer *policer-id*

Context **[Tree]** (config>qos>qgrps>ing>queue-group policer)
[Tree] (cfg>qos>qgrps>egr>queue-group policer)

Full Context configure qos queue-group-templates egress queue-group policer
configure qos queue-group-templates ingress queue-group policer

Description This command is used in ingress and egress queue-group templates to create, modify, or delete a policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Policers are created and used in a similar manner to queues. The policer ID space is separate from the queue ID space, allowing both a queue and a policer to share the same ID. While a policer may be defined in a queue-group template, it is not actually created until the queue-group template is instantiated on the ingress context of a forwarding plane or on the egress context of a port.

When a policer is created, the policer's metering rate and profiling rates may be defined, as well as the policer's maximum and committed burst sizes (MBS and CBS, respectively). Unlike queues that have dedicated counters, policers allow various stat-mode settings that define the counters that will be associated with the policer. Another supported feature—packet-byte-offset—provides a policer with the ability to modify the size of each packet based on a defined number of bytes.

When a policer is created, it cannot be deleted from the queue-group template unless any forwarding classes that are redirected to the policer are first removed.

The **no** version of this command deletes the policer.

Parameters *policer-id* — The *policer-id* must be specified when executing the policer command. If the specified ID already exists, the system enters that policer's context to allow the policer's parameters to be modified. If the ID does not exist and is within the allowed range for the QoS policy type, a context for the policer ID will be created (depending on the system's current create keyword requirements, which may require the **create** keyword to actually add the new policer ID to the QoS policy) and the system enters that new policer's context for possible parameter modification.

Values

ingress	all platforms	1 to 32
egress	VSR	1 to 8
egress	all other platforms	1 to 16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer

Syntax [**no**] **policer** *policer-id*

Context **[Tree]** (config>log>acct-policy>cr policer)

Full Context configure log accounting-policy custom-record policer

Description This command creates a policer context for which counters should be included in the custom-record.

The **no** form of this command deletes the policer and its counters from the custom-record.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policer-id* — Specifies the policer for which counters should be included in or deleted from the custom-record.

Values 1 to 63

Platforms All

policer

Syntax [**no**] **policer** *policer-id*

Context **[Tree]** (config>router>policy-acct-template policer)

Full Context configure router policy-acct-template policer

Description Commands in this context configure policer index information. Each policy accounting template supports up to 63 policers.

Policing by action of a policy accounting template is only supported by FP4 cards and systems.

The **no** form of this command deletes the policer ID from the configuration.

Parameters *policer-id* — Specifies the policer index.

Values 1 to 63

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

20.178 policer-control-override

policer-control-override

Syntax **policer-control-override** [**create**]
no policer-control-override

Context **[Tree]** (config>card>fp>ingress>access>queue-group policer-control-override)
[Tree] (config>card>fp>ingress>network>queue-group policer-control-override)

Full Context configure card fp ingress access queue-group policer-control-override
configure card fp ingress network queue-group policer-control-override

Description This command configures policer control overrides.

Parameters **create** — Keyword required to create a new policer control override instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer-control-override

Syntax **policer-control-override** [**create**]
no policer-control-override

Context **[Tree]** (config>service>apipe>sap>egress policer-control-override)
[Tree] (config>service>apipe>sap>ingress policer-control-override)
[Tree] (config>service>cpipe>sap>egress policer-control-override)
[Tree] (config>service>cpipe>sap>ingress policer-control-override)
[Tree] (config>service>epipe>sap>egress policer-control-override)
[Tree] (config>service>epipe>sap>ingress policer-control-override)
[Tree] (config>service>fpipe>sap>egress policer-control-override)
[Tree] (config>service>fpipe>sap>ingress policer-control-override)
[Tree] (config>service>ipipe>sap>egress policer-control-override)
[Tree] (config>service>ipipe>sap>ingress policer-control-override)

Full Context configure service apipe sap egress policer-control-override
configure service apipe sap ingress policer-control-override
configure service cpipe sap egress policer-control-override
configure service cpipe sap ingress policer-control-override
configure service epipe sap egress policer-control-override
configure service epipe sap ingress policer-control-override
configure service fpipe sap egress policer-control-override
configure service fpipe sap ingress policer-control-override
configure service ipipe sap egress policer-control-override
configure service ipipe sap ingress policer-control-override

Description This command, within the SAP ingress or egress contexts, creates a CLI node for specific overrides to the applied policer-control-policy. A policy must be applied for a policer-control-overrides node to be created. If the policer-control-policy is removed or changed, the policer-control-overrides node is automatically deleted from the SAP.

The **no** form of this command removes any existing policer-control-policy overrides and the policer-control-overrides node from the SAP.

Default no policer-control-override

Parameters **create** — The create keyword is required when the policer-control-overrides node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress policer-control-override
- configure service fpipe sap ingress policer-control-override
- configure service cpipe sap ingress policer-control-override
- configure service fpipe sap egress policer-control-override

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap ingress policer-control-override
- configure service epipe sap egress policer-control-override
- configure service ipipe sap ingress policer-control-override
- configure service ipipe sap egress policer-control-override

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-control-override
- configure service apipe sap egress policer-control-override

policer-control-override

Syntax **policer-control-override** [**create**]
no policer-control-override

Context **[Tree]** (config>service>vpls>sap>egress policer-control-override)
[Tree] (config>service>vpls>sap>ingress policer-control-override)

Full Context configure service vpls sap egress policer-control-override
configure service vpls sap ingress policer-control-override

Description This command, within the SAP ingress or egress contexts, creates a CLI node for specific overrides to the applied policer-control-policy. A policy must be applied for a policer-control-overrides node to be created. If the policer-control-policy is removed or changed, the policer-control-overrides node is automatically deleted from the SAP.

The **no** form of this command removes any existing policer-control-policy overrides and the policer-control-overrides node from the SAP.

Default no policer-control-override

Parameters **create** — The create keyword is required when the policer-control-overrides node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-override

Syntax **policer-control-override** [**create**]
no policer-control-override

Context **[Tree]** (config>service>ies>if>sap>egress policer-control-override)
[Tree] (config>service>ies>if>sap>ingress policer-control-override)

Full Context configure service ies interface sap egress policer-control-override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap ingress policer-control-override

Description This command, within the SAP ingress or egress contexts, creates a CLI node for specific overrides to the applied policer-control-policy. A policy must be applied for a policer-control-overrides node to be created. If the policer-control-policy is removed or changed, the policer-control-overrides node is automatically deleted from the SAP.

The **no** form of this command removes any existing policer-control-policy overrides and the policer-control-overrides node from the SAP.

Default no policer-control-override

Parameters **create** — The create keyword is required when the policer-control-overrides node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-override

Syntax **policer-control-override** [**create**]
no policer-control-override

Context **[Tree]** (config>service>vprn>if>sap>egress policer-control-override)
[Tree] (config>service>vprn>if>sap>ingress policer-control-override)

Full Context configure service vprn interface sap egress policer-control-override
configure service vprn interface sap ingress policer-control-override

Description This command, within the SAP ingress or egress contexts, creates a CLI node for specific overrides to the applied policer-control-policy. A policy must be applied for a policer-control-overrides node to be created. If the policer-control-policy is removed or changed, the policer-control-overrides node is automatically deleted from the SAP.

The **no** form of this command removes any existing policer-control-policy overrides and the policer-control-overrides node from the SAP.

Default no policer-control-override

Parameters **create** — The create keyword is required when the policer-control-overrides node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.179 policer-control-policy

policer-control-policy

Syntax **policer-control-policy** *policy-name* [**create**]
no policer-control-policy

Context **[Tree]** (config>subscr-mgmt>sub-prof>ingress policer-control-policy)
[Tree] (config>subscr-mgmt>sub-prof>egress policer-control-policy)

Full Context configure subscriber-mgmt sub-profile egress policer-control-policy
configure subscriber-mgmt sub-profile ingress policer-control-policy

Description This command is used to create, delete, or modify policer control policies. The **policer-control-policy** controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy can also be applied to the ingress or egress context of a sub-profile.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the policer control policy name. Each policer-control-policy must be created with a unique policy name. The name given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy's context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

create — The **create** keyword is required when a new policy is being created and the system is configured for explicit object creation mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress policer-control-policy)
[Tree] (config>service>ies>sub-if>grp-if>sap>ingress policer-control-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress policer-control-policy)

Full Context configure service ies subscriber-interface group-interface sap egress policer-control-policy
configure service ies subscriber-interface group-interface sap ingress policer-control-policy
configure service vprn subscriber-interface group-interface sap egress policer-control-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to create, delete, or modify policer control policies. The **policer-control-policy** controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy can also be applied to the ingress or egress context of a sub-profile.

The **no** form of this command resets the command to the default setting.

Parameters *policy-name* — Specifies the policer control policy name. Each policer control policy name must be unique and adhere to the system policy ASCII naming requirements. If the defined policy name already exists, the system enters that policy's context for editing purposes. If policy-name does not exist, the system attempts to create a policy with the specified name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policer-control-policy

Syntax **policer-control-policy** *policer-control-policy-name*
no policer-control-policy

Context **[Tree]** (config>card>fp>ingress>access>queue-group policer-control-policy)
[Tree] (config>card>fp>ingress>network>queue-group policer-control-policy)

Full Context configure card fp ingress access queue-group policer-control-policy
configure card fp ingress network queue-group policer-control-policy

Description This command configures an policer-control policy that can apply to a queue-group on the forwarding plane.

The **no** form of this command removes the policer-control policy association from the queue-group.

Default no policer-control-policy

Parameters *policer-control-policy-name* — Specifies the name of the policer-control policy to use for the queue-group. The name can be up to 32 characters long.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>port>ethernet>network>egress>queue-group>policer-control-policy policer-control-policy)

Full Context configure port ethernet network egress queue-group policer-control-policy policer-control-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the policer control policy for the QoS egress queue-group.

Parameters *policy-name* — Specifies the name of the policer control policy, up to 32 characters.

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>service>apipe>sap>egress policer-control-policy)
[Tree] (config>service>apipe>sap>ingress policer-control-policy)
[Tree] (config>service>cpipe>sap>egress policer-control-policy)
[Tree] (config>service>cpipe>sap>ingress policer-control-policy)
[Tree] (config>service>epipe>sap>egress policer-control-policy)
[Tree] (config>service>epipe>sap>ingress policer-control-policy)
[Tree] (config>service>fpipe>sap>egress policer-control-policy)
[Tree] (config>service>fpipe>sap>ingress policer-control-policy)
[Tree] (config>service>ipipe>sap>egress policer-control-policy)
[Tree] (config>service>ipipe>sap>ingress policer-control-policy)

Full Context configure service apipe sap egress policer-control-policy
configure service apipe sap ingress policer-control-policy
configure service cpipe sap egress policer-control-policy
configure service cpipe sap ingress policer-control-policy
configure service epipe sap egress policer-control-policy
configure service epipe sap ingress policer-control-policy
configure service fpipe sap egress policer-control-policy
configure service fpipe sap ingress policer-control-policy
configure service ipipe sap egress policer-control-policy
configure service ipipe sap ingress policer-control-policy

Description This command, within the QoS CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied.

When applied to a sub-profile on a 7450 ESS and 7750 SR, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis.

For subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and therefore the root arbiter's parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet's child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

As previously stated, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either to an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child's weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child's required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer's peak rate and maximum burst size, the CIR leaky bucket manages the policer's committed rate and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer's fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child's FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child's FIR rate is set according to the child's weight divided by the sum of the active children's weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair-based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child's PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer's discarded packets do not consume depth in the child policer's CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policer Priority Level Thresholds

As stated in the Tier 1 and Tier 2 Arbiter subsection, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer's priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority's thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority's discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority's discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

Each child's rate feeding into the parent policer is governed by the child policer's PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer's configured maximum rate.

Root Arbiter's Parent Policer's Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

To derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level's shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority's mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level's discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level's own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level's shared-portions and fair-portions. The discard-unfair threshold is the priority level's base threshold plus the priority level's shared-portion. The discard-all threshold for the priority level is the priority level's base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level's thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The **no** form of this command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP context.

Parameters *policy-name* — Each policer-control-policy must be created with a unique policy name. The name given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy's context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — The keyword is required when a new policy is being created and the system is configured for explicit object creation mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap ingress policer-control-policy
- configure service fpipe sap egress policer-control-policy
- configure service cpipe sap egress policer-control-policy
- configure service cpipe sap ingress policer-control-policy

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service epipe sap egress policer-control-policy
- configure service epipe sap ingress policer-control-policy
- configure service ipipe sap egress policer-control-policy
- configure service ipipe sap ingress policer-control-policy

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-control-policy
- configure service apipe sap egress policer-control-policy

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>service>vpls>sap>egress policer-control-policy)
[Tree] (config>service>vpls>sap>ingress policer-control-policy)
[Tree] (config>service>template>vpls-sap-template>egress policer-control-policy)
[Tree] (config>service>template>vpls-sap-template>ingress policer-control-policy)

Full Context configure service template vpls-sap-template egress policer-control-policy
configure service template vpls-sap-template ingress policer-control-policy
configure service vpls sap egress policer-control-policy
configure service vpls sap ingress policer-control-policy

Description This command, within the qos CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy may also be applied to the ingress or egress context of a sub-profile.

Policer Control Policy Instances

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

On the SAP side, an instance of a policy is created each time a policy is applied. When applied to a sub-profile, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis. For subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and therefore the root arbiter's parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet's child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either to an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child's weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child's required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer's peak rate and maximum burst size, the CIR leaky bucket manages the policer's committed rate and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer's fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child's FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child's FIR rate is set according to the child's weight divided by the sum of the active children's weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair-based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child's PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer's discarded packets do not consume depth in the child policer's CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policer Priority Level Thresholds

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer's priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority's thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority's discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority's discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child's rate feeding into the parent policer is governed by the child policer's PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer's configured maximum rate.

Root Arbiter's Parent Policer's Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

To derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level's shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority's mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level's discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level's own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level's shared-portions and fair-portions. The discard-unfair threshold is the priority level's base threshold plus the priority level's shared-portion. The discard-all threshold for the priority level is the priority level's base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level's thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The **no** form of this command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP or subscriber management sub-profile context.

Parameters *policy-name* — Specifies the policy name. Each policer-control-policy must be created with a unique policy name. The name must be given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy's context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — The keyword is required when a new policy is being created and the system is configured for explicit object creation mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>service>ies>if>sap>egress policer-control-policy)
[Tree] (config>service>ies>if>sap>ingress policer-control-policy)

Full Context configure service ies interface sap egress policer-control-policy
configure service ies interface sap ingress policer-control-policy

Description This command, within the qos CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy may also be applied to the ingress or egress context of a sub-profile.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied. When applied to a sub-profile, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis. For subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and therefore the root arbiter's parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet's child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either to an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child's weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child's required bandwidth.

Fair and Unfair Bandwidth Control

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each child policer supports three leaky buckets. The PIR bucket manages the policer's peak rate and maximum burst size, the CIR leaky bucket manages the policer's committed rate and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer's fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child's FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child's FIR rate is set according to the child's weight divided by the sum of the active children's weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair-based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child's PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer's discarded packets do not consume depth in the child policer's CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policer Priority Level Thresholds

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer's priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority's thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority's discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority's discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child's rate feeding into the parent policer is governed by the child policer's PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer's configured maximum rate.

Root Arbiter's Parent Policer's Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

To derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level's shared-portion is zero since all packets from the child will be marked fair and the

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority's mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level's discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level's own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level's shared-portions and fair-portions. The discard-unfair threshold is the priority level's base threshold plus the priority level's shared-portion. The discard-all threshold for the priority level is the priority level's base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level's thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The **no** form of this command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP or subscriber management sub-profile context.

Parameters *policy-name* — Specifies the policy name. Each policer-control-policy must be created with a unique policy name. The name must be given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy's context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>service>vprn>if>sap>egress policer-control-policy)
[Tree] (config>service>vprn>if>sap>ingress policer-control-policy)

Full Context configure service vprn interface sap egress policer-control-policy
configure service vprn interface sap ingress policer-control-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command, within the qos CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy may also be applied to the ingress or egress context of a sub-profile.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied. When applied to a sub-profile, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis. For subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and therefore the root arbiter's parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet's child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either to an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child's weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child's required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer's peak rate and maximum burst size, the CIR leaky bucket manages the policer's committed rate and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer's fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child's FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child's FIR rate is set according to the child's weight divided by the sum of the active children's weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair-based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child's PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer's discarded packets do not consume depth in the child policer's CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policer Priority Level Thresholds

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer's priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority's thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority's discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority's discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child's rate feeding into the parent policer is governed by the child policer's PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer's configured maximum rate.

Root Arbiter's Parent Policer's Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

To derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level's shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority's mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level's discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level's own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level's shared-portions and fair-portions. The discard-unfair threshold is the priority level's base threshold plus the priority level's shared-portion. The discard-all threshold for the priority level is the priority level's base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level's thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The **no** form of this command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP or subscriber management sub-profile context.

Parameters *policy-name* — Specifies the policy name. Each policer-control-policy must be created with a unique policy name. The name must be given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy's context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer-control-policy

Syntax **policer-control-policy** *policy-name* [**create**]
no policer-control-policy *policy-name*

Context **[Tree]** (config>qos policer-control-policy)

Full Context configure qos policer-control-policy

Description This command is used to create, delete, or modify policer control policies. The **policer-control-policy** controls the aggregate bandwidth available to a set of child policers. When created, the policy can be applied to ingress or egress SAPs. The policy can also be applied to the ingress or egress context of a sub-profile.

Parameters *policy-name* — Each policer-control-policy must be created with a unique policy name. The *policy-name* must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy's context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

Default None

create — The **create** keyword is required when a new policy is being created and the system is configured for explicit object creation mode.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-policy

Syntax **policer-control-policy** *policy-name*
no policer-control-policy

Context **[Tree]** (config>service>cust>multi-service-site>egress policer-control-policy)
[Tree] (config>service>cust>multi-service-site>ingress policer-control-policy)

Full Context configure service customer multi-service-site egress policer-control-policy
configure service customer multi-service-site ingress policer-control-policy

Description This command, within the QoS CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied. When applied to a 7750 SR or 7450 ESS sub-profile, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and not subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis. For 7750 SR or 7450 ESS subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and thus the root arbiter's parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet's child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either to an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child's weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child's required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer's peak rate and maximum burst size, the CIR leaky bucket manages the policer's committed rate and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer's fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child's FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child's FIR rate is set according to the child's weight divided by the sum of the active children's weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child's PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer's discarded packets do not consume depth in the child policer's CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policer Priority Level Thresholds

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer's priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority's thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority's discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority's discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child's rate feeding into the parent policer is governed by the child policer's PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer's configured maximum rate.

Root Arbiter's Parent Policer's Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In order to derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level's shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority's mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level's discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level's own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level's shared-portions and fair-portions. The discard-unfair threshold is the priority level's base threshold plus the priority level's shared-portion. The discard-all threshold for the priority level is the priority level's base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level's thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The **no** form of the command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP context.

Parameters *policy-name* — Specifies the policy name up to 32 characters in length. Each policer-control-policy must be created with a unique policy name. The name must adhere to the system policy ASCII naming requirements. If the defined policy name already exists, the system will enter that policy's context for editing purposes. If policy name does not exist, the system will attempt to create a policy with the specified name.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-control-policy

Syntax **policer-control-policy** *src-name dst-name* [**overwrite**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>copy policer-control-policy)

Full Context configure qos copy policer-control-policy

Description This command copies an existing **policer-control-policy** to another **policer-control-policy**. The **copy** command is a configuration level maintenance tool used to create new entries using an existing profile ID. If **overwrite** is not specified, an error occurs if the destination policy exists.

Parameters *src-name* — Specifies the existing source **policer-control-policy**, up to 32 characters, from which the **copy** command attempts to copy.

dst-name — Specifies the destination **policer-control-policy** *dst-name*, up to 32 characters, to which the copy command attempts to copy.

overwrite — Use this parameter when the **policer-control-policy** *dst-name* already exists. If it does, everything in the existing destination **policer-control-policy** *dst-name* is completely overwritten with the contents of the **policer-control-policy** *src-name*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI Destination "pcp-name2" exists - use {overwrite}.
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.180 policer-override

policer-override

Syntax [**no**] **policer-override**

Context [Tree] (config>card>fp>ingress>access>queue-group policer-override)
[Tree] (config>card>fp>ingress>network>queue-group policer-override)

Full Context configure card fp ingress access queue-group policer-override
configure card fp ingress network queue-group policer-override

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The **no** form of this command removes any existing policer overrides.

Default no policer-override

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policer-override

Syntax [**no**] **policer-override**

Context **[Tree]** (config>service>apipe>sap>egress policer-override)
[Tree] (config>service>apipe>sap>ingress policer-override)
[Tree] (config>service>cpipe>sap>egress policer-override)
[Tree] (config>service>cpipe>sap>ingress policer-override)
[Tree] (config>service>epipe>sap>egress policer-override)
[Tree] (config>service>epipe>sap>ingress policer-override)
[Tree] (config>service>fpipe>sap>egress policer-override)
[Tree] (config>service>fpipe>sap>ingress policer-override)
[Tree] (config>service>ipipe>sap>egress policer-override)
[Tree] (config>service>ipipe>sap>ingress policer-override)

Full Context configure service apipe sap egress policer-override
configure service apipe sap ingress policer-override
configure service cpipe sap egress policer-override
configure service cpipe sap ingress policer-override
configure service epipe sap egress policer-override
configure service epipe sap ingress policer-override
configure service fpipe sap egress policer-override
configure service fpipe sap ingress policer-override
configure service ipipe sap egress policer-override
configure service ipipe sap ingress policer-override

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The **no** form of this command is used to remove any existing policer overrides.

Default no policer-overrides

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress policer-override
- configure service cpipe sap egress policer-override
- configure service fpipe sap ingress policer-override
- configure service fpipe sap egress policer-override

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service epipe sap egress policer-override
- configure service epipe sap ingress policer-override
- configure service ipipe sap egress policer-override
- configure service ipipe sap ingress policer-override

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe sap egress policer-override
- configure service apipe sap ingress policer-override

policer-override

Syntax [**no**] **policer-override**

Context **[Tree]** (config>service>vpls>sap>egress policer-override)
[Tree] (config>service>vpls>sap>ingress policer-override)

Full Context configure service vpls sap egress policer-override
configure service vpls sap ingress policer-override

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The **no** form of this command is used to remove any existing policer overrides.

Default no policer-overrides

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-override

Syntax [**no**] **policer-override**

Context **[Tree]** (config>service>ies>if>sap>egress policer-override)
[Tree] (config>service>ies>if>sap>ingress policer-override)

Full Context configure service ies interface sap egress policer-override
configure service ies interface sap ingress policer-override

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The **no** form of this command is used to remove any existing policer overrides.

Default no policer-override

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

policer-override

Syntax [**no**] **policer-override**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>if>sap>egress policer-override)
[Tree] (config>service>vprn>if>sap>ingress policer-override)

Full Context configure service vprn interface sap egress policer-override
configure service vprn interface sap ingress policer-override

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The **no** form of this command is used to remove any existing policer overrides.

Default no policer-override

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.181 policer-stats

policer-stats

Syntax [**no**] **policer-stats**

Context [Tree] (config>app-assure>group>statistics>aa-admit-deny policer-stats)

Full Context configure application-assurance group statistics aa-admit-deny policer-stats

Description This command configures whether to include or exclude system and subscriber-level flow count and flow-setup rate policer admit-deny statistics in accounting records.

Default no policer-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.182 policer-stats-resources

policer-stats-resources

Syntax [**no**] **policer-stats-resources**

Context [Tree] (config>app-assure>group>statistics>aa-admit-deny policer-stats-resources)

Full Context configure application-assurance group statistics aa-admit-deny policer-stats-resources

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the operator to allocate or deallocate AA partition resources for policer admit-deny statistics.

Default no policer-stats-resources

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.183 policers

policers

Syntax **policers** *policy-limit*
no policers

Context **[Tree]** (config>card>fp>ingress>policy-accounting policers)

Full Context configure card fp ingress policy-accounting policers

Description This command configures the number of policer resources for an policy accounting. Policy accounting can be used to collect statistics about the amount of traffic matching particular routes and, on FP4 cards and systems only, it can also be used to police traffic associated with certain routes as destinations of the traffic.

Using only statistics (policing is not performed) requires the reservation of policer statistics index resources on each FP receiving the traffic to be counted. Every **policy-accounting** interface on a card or FP uses one of these resources for every source and destination class index listed in the template referenced by the interface. The total reservation at the FP level is set using the **configure card** *slot-number* **fp** *fp-number* **policy-accounting** command.

Using FP4 policing requires the above resource, and in addition, policer index resources. Every **policy-accounting** interface on a card or FP uses one of these resources for every destination class associated with a policer in the template referenced by the interface. The total reservation of this second resource at the FP level is set using the **configure card** *slot-number* **fp** *fp-number* **ingress policy-accounting policers** command.

The total number of the above resources, per FP, must be less than or equal to 128000. In addition, the second resource pool size must be less than or equal to the size of the first resource pool.

It is possible to increase or decrease the size of either resource sub pool at any time. A decrease can cause some interfaces (randomly selected) to immediately lose their resources and stop counting or policing some traffic that was previously being counted or policed.

If the policy accounting is enabled on a spoke SDP or R-VPLS interface all FPs in the system should have a reservation for each of the above resources, otherwise the **show router interface policy-accounting** command output reports that statistics are possibly incomplete.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no policers

Parameters *policy-limit* — Specifies the number of policer resources for policy accounting.

Values 1 to 64000

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

20.184 policers-hqos-manageable

policers-hqos-manageable

Syntax [**no**] **policers-hqos-manageable**

Context **[Tree]** (config>qos>sap-egress policers-hqos-manageable)

Full Context configure qos sap-egress policers-hqos-manageable

Description This command enables Hierarchical QoS (HQoS) management of the policiers within the SAP egress policy, when the policy is applied to either the egress SAP configuration or the egress SLA profile, with multiservice sites (MSS) supported for SAPs. When enabled, the system can manage egress policers and queues together in the same HQoS hierarchy.

To be managed by HQoS, egress policers within a SAP egress QoS policy must be configured with either a **scheduler-parent** or **port-parent** command or be orphaned to an egress port scheduler applied on a Vport or port.

The **policers-hqos-manageable** command and **parent-location sla** or policers with **enable-exceed-pir** or **stat-mode no-stats** within a SAP egress QoS policy are mutually exclusive.

To prevent HQoS from measuring the traffic through both a policer managed by HQoS, then again through a post-policer access egress queue group queue, configure post-policer access egress queue groups with **no queues-hqos-manageable** so their queues are not managed by HQoS.

A post-policer local queue is not supported with HQoS managed policers, nor are those mapped by the **use-fc-mapped-queue** parameter in a criteria action statement. The **policers-hqos-manageable** command is not supported for SAP egress dynamic policers or on a 7950 XRS.

The **no** form of this command rdisables HQoS management of policers within the SAP QoS egress policy.

Default no policers-hqos-manageable

Platforms 7450 ESS, 7750 SR, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-e, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policers-hqos-manageable

Syntax [**no**] **policers-hqos-manageable**

Context **[Tree]** (config>qos>sap-ingress policers-hqos-manageable)

Full Context configure qos sap-ingress policers-hqos-manageable

Description This command specifies that the policers within this SAP ingress policy are to be managed by the Hierarchical QoS (HQoS) process when the policy is applied to either the ingress part of a SAP configuration or the ingress part of an SLA profile, with multiservice sites (MSS) supported for SAPs. When enabled, ingress policers and queues can be managed together in the same HQoS hierarchy.

To be managed by HQoS, ingress policers within a SAP ingress QoS policy must be configured with either a **scheduler-parent** or **parent** command or be orphaned to an ingress port scheduler applied on a Vport or port. The **scheduler-parent** and **parent** commands are mutually exclusive.

The **policers-hqos-manageable** command and the **stat-mode no-stats** command within a SAP ingress QoS policy are mutually exclusive.

The **no** form of this command results in policers within this SAP QoS ingress policy being non-HQoS-manageable.

Default no policers-hqos-manageable

Platforms 7450 ESS, 7750 SR, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-e

20.185 policing

policing

Syntax [**no**] **policing**

Context **[Tree]** (config>qos>atm-td-profile policing)

Full Context configure qos atm-td-profile policing

Description This command determines whether ingress traffic is policed. Policing is valid for CBR (PIR), RT-VBR (PIR and SIR), NRT-VBR, and UBR/UBR+MIR (PIR). This is cell-based policing.

Default no policing

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.186 policy

policy

Syntax **policy** *msap-policy-name*
no policy

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>msap-defaults policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>msap-defaults policy)

Full Context configure subscriber-mgmt local-user-db ipoe host msap-defaults policy
configure subscriber-mgmt local-user-db ppp host msap-defaults policy

Description This command configures the MSAP policy.

The **no** form of this command removes the MSAP policy name from the configuration.

Parameters *msap-policy-name* — Specifies the policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

policy

Syntax **policy** *ppp-policy-name*
no policy

Context [Tree] (config>service>vprn>sub-if>grp-if>pppoe policy)
[Tree] (config>service>vprn>sub-if>grp-if>ppp policy)
[Tree] (config>service>ies>sub-if>grp-if>pppoe policy)
[Tree] (config>service>ies>sub-if>grp-if>ppp policy)

Full Context configure service ies subscriber-interface group-interface ppp policy
configure service ies subscriber-interface group-interface pppoe policy
configure service vprn subscriber-interface group-interface ppp policy
configure service vprn subscriber-interface group-interface pppoe policy

Description This command specifies the PPPoE policy on this interface.

The **no** form of this command reverts to the default.

Default policy “default”

Parameters *ppp-policy-name* — Specifies the PPP policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy

Syntax **policy** *policy-name*
no policy

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac policy)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac policy

Description This command configures the multicast CAC policy name.

The **no** form of this command reverts to the default.

Parameters *policy-name* — The multicast CAC policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

policy

Syntax **policy** *name1* [*name2*] [*name3*] [*name4*] [*name5*]
no policy

Context **[Tree]** (config>subscr-mgmt>sub-prof>rad-acct policy)

Full Context configure subscriber-mgmt sub-profile radius-accounting policy

Description This command specifies the RADIUS accounting policy for the subscriber that is using this subscriber profile. This command allows the configuration of up to five RADIUS accounting policies. The RADIUS accounting policies function according to their respective configuration, including the individual accounting mode, their own included attributes, and the update interval.

Parameters *name1* — Specifies the name of the RADIUS accounting policy, up to 32 characters, to be used for the subscriber profile.

name2 — Specifies the name of the second RADIUS accounting policy, up to 32 characters, to be used for the subscriber profile.

name3 — Specifies the name of the third RADIUS accounting policy, up to 32 characters, to be used for the subscriber profile.

name4 — Specifies the name of the fourth RADIUS accounting policy, up to 32 characters, to be used for the subscriber profile.

name5 — Specifies the name of the fifth RADIUS accounting policy, up to 32 characters, to be used for the subscriber profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy

Syntax **policy** *vrrp-policy-id*
no policy[*vrrp-policy-id*]

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp policy)
[Tree] (config>service>vprn>sub-if>grp-if>srrp policy)

Full Context configure service ies subscriber-interface group-interface srrp policy
configure service vprn subscriber-interface group-interface srrp policy

Description This command associates one or more VRRP policies with the SRRP instance. A VRRP policy is a collection of connectivity and verification tests used to manipulate the in-use priorities of VRRP and SRRP instances. A VRRP policy can test the link state of ports, ping IP hosts, discover the existence of routes in the routing table or the ability to reach Layer 2 hosts. When one or more of these tests fail, the VRRP policy has the option of decrementing or setting an explicit value for the in-use priority of an SRRP instance.

More than one VRRP policy may be associated with an SRRP instance. When more than one VRRP policy is associated with an SRRP instance the delta decrement of the in-use priority is cumulative unless one or more test fail that have explicit priority values. When one or more explicit tests fail, the lowest priority value event takes effect for the SRRP instance. When the highest delta-in-use-limit is used to manage the lowest delta derived in-use priority for the SRRP instance.

VRRP policy associations may be added and removed at any time. A maximum of two VRRP policies can be associated with a single SRRP instance.

The **no** form of this command removes the association with the *vrrp-policy-id* from the SRRP instance.

Parameters *vrrp-policy-id* — Specifies one or more VRRP policies with the SRRP instance.

Values 1 to 9999

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

policy

Syntax [**no**] **policy** *policy-name*

Context **[Tree]** (debug>diam>application policy)

Full Context debug diameter application policy

Description This command debugs Diameter applications for a particular application policy.

Parameters *policy-name* — Specifies the policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy

Syntax **policy** *msap-policy-name*
no policy

Context **[Tree]** (config>service>vpls>sap>msap-defaults policy)

Full Context configure service vpls sap msap-defaults policy

Description This command sets default msap-policy for all subscribers created based on trigger packets received on the specified capture-sap in case the corresponding VSA is not included in the RADIUS authentication response. This command is applicable to capture SAP only.

Default no policy

Platforms All

policy

Syntax **policy** *policy-name*
no policy

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping>mcac policy)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping>mcac policy)
[Tree] (config>service>vpls>sap>mld-snooping>mcac policy)
[Tree] (config>service>vpls>sap>igmp-snooping>mcac policy)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping>mcac policy)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping>mcac policy)
[Tree] (config>service>pw-template>igmp-snooping>mcac policy)

Full Context configure service pw-template igmp-snooping mcac policy
configure service vpls mesh-sdp igmp-snooping mcac policy
configure service vpls mesh-sdp mld-snooping mcac policy
configure service vpls sap igmp-snooping mcac policy
configure service vpls sap mld-snooping mcac policy
configure service vpls spoke-sdp igmp-snooping mcac policy
configure service vpls spoke-sdp mld-snooping mcac policy

Description This command configures the multicast CAC policy name. MCAC policy is not supported with MLD-snooping, therefore executing the command in the mld-snooping contexts will return an error.

Parameters *policy-name* — Specifies the multicast CAC policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy

Syntax **policy** *vrrp-policy-id*
no policy

Context **[Tree]** (config>service>ies>if>ipv6>vrrp policy)

Full Context configure service ies interface ipv6 vrrp policy

Description This command creates VRRP control policies. The VRRP policy ID must be created by the policy command prior to association with the virtual router instance.

The policy command provides the ability to associate a VRRP priority control policy to a virtual router instance. The policy may be associated with more than one virtual router instance. The priority events within the policy either override or diminish the base-priority dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority may eventually be restored to the base-priority value.

The policy command is only available in the non-owner **vrrp** *virtual-router-id* nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed by VRRP priority control policies. For non-owner virtual router instances, if the policy command is not executed, the base-priority will be used as the in-use priority.

The **no** form of this command removes any existing VRRP priority control policy association from the virtual router instance. All such associations must be removed prior to the policy being deleted from the system.

Parameters *vrrp-policy-id* — The vrrp-policy-id parameter associated the corresponding VRRP priority control policy-id with the virtual router instance. The vrrp-policy-id must already exist in the system for the policy command to be successful.

Values 1 to 9999

Platforms All

policy

Syntax **policy** *vrrp-policy-id*
no policy

Context **[Tree]** (config>service>ies>if>vrrp policy)

Full Context configure service ies interface vrrp policy

Description This command creates VRRP control policies. The VRRP policy ID must be created by the policy command prior to association with the virtual router instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The policy command provides the ability to associate a VRRP priority control policy to a virtual router instance. The policy may be associated with more than one virtual router instance. The priority events within the policy either override or diminish the base-priority dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority may eventually be restored to the base-priority value.

The policy command is only available in the non-owner **vrrp** *virtual-router-id* nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed by VRRP priority control policies. For non-owner virtual router instances, if the policy command is not executed, the base-priority will be used as the in-use priority.

The **no** form of this command removes any existing VRRP priority control policy association from the virtual router instance. All such associations must be removed prior to the policy being deleted from the system.

Parameters *vrrp-policy-id* — The vrrp-policy-id parameter associated the corresponding VRRP priority control policy-id with the virtual router instance. The vrrp-policy-id must already exist in the system for the policy command to be successful.

Values 1 to 9999

Platforms All

policy

Syntax **policy** *policy-name*
no policy

Context **[Tree]** (config>service>vprn>bgp>next-hop-res policy)

Full Context configure service vprn bgp next-hop-resolution policy

Description This command specifies the name of a policy statement to use with the BGP next-hop resolution process. The policy controls which IP routes in RTM are eligible to resolve the BGP next-hop addresses of IPv4 and IPv6 routes. The policy has no effect on the resolution of BGP next-hops to MPLS tunnels. If a BGP next-hop of an IPv4 or IPv6 route R is resolved in RTM and the longest matching route for the next-hop address is an IP route N that is rejected by the policy then route R is unresolved; if the route N is accepted by the policy then it becomes the resolving route for R.

The default next-hop resolution policy (when the **no policy** command is configured) is to use the longest matching active route in RTM that is not a BGP route (unless **use-bgp-routes** is configured), an aggregate route or a subscriber management route.

Default no policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

policy

Syntax **policy** *policy-name*
no policy

Context **[Tree]** (config>service>vprn>igmp>grp-if>mcac policy)
[Tree] (config>service>vprn>igmp>if>mcac policy)
[Tree] (config>service>vprn>mld>grp-if>mcac policy)
[Tree] (config>service>vprn>pim>if>mcac policy)

Full Context configure service vprn igmp group-interface mcac policy
configure service vprn igmp interface mcac policy
configure service vprn mld group-interface mcac policy
configure service vprn pim interface mcac policy

Description This command references the global channel bandwidth definition policy that is used for HMCAC and HQoS Adjust.

HQoS Adjustment is supported with redirection enabled or per-host-replication disabled. In other words, the policy from the redirected interface is used for HQoS Adjustment.

Hierarchical MCAC (HMCAC) is supported with redirection enabled or per-host-replication disabled. In HMCAC, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface against the bandwidth limits defined under the redirected interface. In the HMCAC case, the channel definition policy must be referenced under the redirected interface level.

Parameters *policy-name* — Specifies the name of the global MCAC channel definition policy defined under the hierarchy **config>router>mcac>policy**. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface mcac policy
- configure service vprn mld group-interface mcac policy

All

- configure service vprn pim interface mcac policy
- configure service vprn igmp interface mcac policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy

Syntax **policy** *vrrp-policy-id*
no policy

Context **[Tree]** (config>service>vprn>if>vrrp policy)
[Tree] (config>service>vprn>if>ipv6>vrrp policy)

Full Context configure service vprn interface ipv6 vrrp policy
configure service vprn interface vrrp policy

Description This command associates a VRRP priority control policy with the virtual router instance (non-owner context only).

Parameters *vrrp-policy-id* — Specifies a VRRP priority control policy.

Values 1 to 9999

Platforms All

policy

Syntax **policy**

Context **[Tree]** (config>app-assure>group policy)

Full Context configure application-assurance group policy

Description Commands in this context configure parameters for application assurance policy. To edit any policy content begin command must be executed first to enter editing mode. The editing mode is left when the abort or commit commands are issued.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policy

Syntax **policy aa-sub** {**sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id* | **transit** *transit-aasub-name*} [**create**]
no policy aa-sub {**sap** *sap-id* | **spoke-sdp** *sdp-id:vc-id* | **transit** *transit-aasub-name*}

Context **[Tree]** (config>app-assure>group>policy-override policy)

Full Context configure application-assurance group policy-override policy

Description This command specifies a given SAP or SDP to be used for a static policy override.

The **no** form of this command removes the policy override.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 to 32767
1 to 4294967295

transit-aasub-name — Specifies an existing transit subscriber name, up to 32 characters.

create — Keyword used to create the policy override.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

policy

Syntax **policy** *policy-name*
no policy

Context **[Tree]** (config>router>igmp>grp-if>mcac policy)
[Tree] (config>router>igmp>interface>mcac policy)
[Tree] (config>router>mcac policy)
[Tree] (config>router>mld>group-interface policy)
[Tree] (config>router>mld>interface policy)
[Tree] (config>router>pim>interface policy)

Full Context configure router igmp group-interface mcac policy
configure router igmp interface mcac policy
configure router mcac policy
configure router mld group-interface policy
configure router mld interface policy
configure router pim interface policy

Description This command references the global channel bandwidth definition policy that is used for (H)MCAC and HQoS adjustment.

Within the scope of HQoS adjustment, the channel definition policy under the group-interface is used if redirection is disabled. In this case, the HQoS adjustment can be applied to IPoE subscribers in per-SAP replication mode.

If redirection is enabled, the channel bandwidth definition policy applied under the Layer 3 redirected interface is in effect.

Hierarchical MCAC (HMCAC) is supported on two levels simultaneously:

- subscriber level and redirected interface in case that redirection is enabled
- subscriber level and group-interface level in case that redirection is disabled

In HMCAC, the subscriber is first checked against its bandwidth limits followed by the check on the redirected interface (or group-interface) against the bandwidth limits there.

In the case that the redirection is enabled but the policy is referenced only under the group-interface, no admission control will be executed (HMCAC or MCAC).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the name of the global MCAC channel definition policy, up to 32 characters, defined under the hierarchy **config**>**router**>**mcac**>**policy**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface mcac policy

All

- configure router igmp interface mcac policy
- configure router mcac policy

policy

Syntax **policy** *vrrp-policy-id*
no policy

Context **[Tree]** (config>router>if>vrrp policy)
[Tree] (config>router>if>ipv6>vrrp policy)

Full Context configure router interface ipv6 vrrp policy
configure router interface vrrp policy

Description This command adds a VRRP priority control policy association with the virtual router instance.

To further augment the virtual router instance base priority, VRRP priority control policies can be used to override or adjust the base priority value depending on events or conditions within the chassis.

The policy can be associated with more than one virtual router instance. The priority events within the policy either override or diminish the base priority set with the **priority** command dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority can eventually be restored to the base **priority** value.

The **policy** command is only available in the non-owner **vrrp** nodal context. The priority of **owner** virtual router instances is permanently set to 255 and cannot be changed by VRRP priority control policies. For non-owner virtual router instances, if the **policy** command is not executed, the base **priority** is used as the in-use priority.

The **no** form of the command removes existing VRRP priority control policy associations from the virtual router instance. All associations must be removed prior to deleting the policy from the system.

Default no policy — No VRRP priority control policy is associated with the virtual router instance.

Parameters *vrrp-policy-id* — The policy ID of the VRRP priority control expressed as a decimal integer. The *vrrp-policy-id* must already exist for the command to function.

Values 1 to 9999

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy

Syntax **policy** *policy-id* **context** *context-value*
policy *policy-id* **context name** *name*
no policy *policy-id*

Context **[Tree]** (config>vrrp policy)

Full Context configure vrrp policy

Description This command creates the context to configure a VRRP priority control policy which is used to control the VRRP in-use priority based on priority control events. It is a parental node for the various VRRP priority control policy commands that define the policy parameters and priority event conditions.

The virtual router instance **priority** command defines the initial or base value to be used by non-owner virtual routers. This value can be modified by assigning a VRRP priority control policy to the virtual router instance. The VRRP priority control policy can override or diminish the base priority setting to establish the actual in-use priority of the virtual router instance.

The **policy** *policy-id* command must be created first, before it can be associated with a virtual router instance.

Because VRRP priority control policies define conditions and events that must be maintained, they can be resource intensive. The number of policies is limited to 1000.

The *policy-id* do not have to be consecutive integers. The range of available policy identifiers is from 1 to 9999.

The **no** form of the command deletes the specific *policy-id* from the system. The *policy-id* must be removed first from all virtual router instances before the **no policy** command can be issued. If the *policy-id* is associated with a virtual router instance, the command will fail.

Parameters *policy-id* — The VRRP priority control ID expressed as a decimal integer that uniquely identifies this policy from any other VRRP priority control policy defined on the system. Up to 1000 policies can be defined.

Values 1 to 9999

context-value — Specifies the service ID to which this policy applies. A value of zero (0) means that this policy does not apply to a service but applies to the base router instance.

Values 1 to 2147483647

Platforms All

policy

Syntax **policy** *cpu-protection-policy-id* [**create**]
no policy *cpu-protection-policy-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>sys>security>cpu-protection policy)

Full Context configure system security cpu-protection policy

Description This command configures CPU protection policies.

The **no** form of this command deletes the specified policy from the configuration.

Policies 254 and 255 are reserved as the default access and network interface policies, and cannot de deleted. The parameters within these policies can be modified. An event will be logged (warning) when the default policies are modified.

Default Policy 254 (default access interface policy):

- per-source-rate: max (no limit)
- overall-rate: 6000
- out-profile–rate: 6000
- alarm

Policy 255 (default network interface policy):

- per-source-rate: max (no limit)
- overall-rate: max (no limit)
- out-profile-rate: 3000
- alarm

Parameters *cpu-protection-policy-id* — Assigns a policy ID to the specific CPU protection policy.

Values 1 to 255

create — Keyword used to create CPU protection policy. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

policy

Syntax **policy** *policy-name* [**create**] [**type** {**access-network | port**}]
no policy *policy-name*

Context [Tree] (config>sys>security>dist-cpu-protection policy)

Full Context configure system security dist-cpu-protection policy

Description This command configures one of the maximum 18 Distributed CPU Protection (DCP) policies. These policies can be applied to objects such as SAPs, network interfaces or ports.

Parameters *policy-name* — Specifies the name of the policy, up to 32 characters.

create — Keyword used to create a new policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type — Specifies the Distributed CPU protection type for the policy.

Values access-network — Specifies this is a distributed CPU protection policy for access or network interfaces.
port — Specifies this is a distributed CPU protection policy for ports.

Default access-network

Platforms All

policy

Syntax **policy** *policy-name*
no policy

Context **[Tree]** (config>router>bgp>next-hop-resolution policy)

Full Context configure router bgp next-hop-resolution policy

Description This command specifies the policy statement name to use with the BGP next-hop resolution process. The policy determines the eligibility of IP routes in the RTM to resolve the BGP next-hop addresses of IPv4 and IPv6 routes. The policy has no effect on the resolution of BGP next hops to MPLS tunnels.

For example, if a BGP next hop of an IPv4 or IPv6 route R is resolved in RTM and the longest matching route for the next-hop address is an IP route N that is rejected by the policy then route R is unresolved. If the route N is accepted by the policy, it becomes the resolving route for R.

The **no** form of this command reverts to the default next-hop resolution policy, which uses the longest matching active route in RTM that is not a BGP route (unless **use-bgp-routes** is configured), an aggregate route or a subscriber management route.

Default no policy

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

policy

Syntax **policy** *plcy-or-long-expr*
no policy

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router policy-options policy-statement entry from policy

Description This command is used to call another policy by name and evaluate it as a subroutine, or to evaluate a logical expression of subroutine policies.

If the result of the subroutine evaluation is an 'accept', then the route is considered to match the entry in the parent policy that called the subroutine. If the result of the subroutine evaluation is a 'reject', then the route is considered a non-match of the entry in the parent policy that called the subroutine.

Up to 3 levels of subroutine calls are supported. If a subroutine at maximum depth has this command, it is automatically considered a non-match of all routes.

The **no** form of this command removes the policy statement as a match criterion.

Default no policy

Parameters *plcy-or-long-expr* — Specifies the name of a single **policy-statement** (up to 64 characters in length) or a policy logical expression (up to 255 characters in length) consisting of **policy-statement** names (enclosed in square brackets), logical operations ('and', 'or', 'not'), and parentheses for grouping.

Platforms All

policy

Syntax **policy** *plcy-or-long-expr*
no policy

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action policy)

Full Context configure router policy-options policy-statement entry action policy

Description This command configures a nested policy statement as a match criterion for the route policy entry.

Policy statements are configured at the global route policy level (**config>router>policy-options policy-statement**).

The command is used to call another policy by name and evaluate it as a subroutine. If the result of the subroutine evaluation is an 'accept', then the route is considered to match the entry in the parent policy that called the subroutine. If the result of the subroutine evaluation is a 'reject', then the route is considered a non-match of the entry in the parent policy that called the subroutine. Up to 3 levels of subroutine calls are supported. If a subroutine at maximum depth has this command, it is automatically considered a non-match of all routes.

The **no** form of this command removes the policy statement as a match criterion.

Default no policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters long) or a policy logical expression (up to 255 characters). Allowed values are any string up to 255 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

20.187 policy-accounting

policy-accounting

Syntax **policy-accounting**

Context **[Tree]** (config>card>fp>ingress policy-accounting)

Full Context configure card fp ingress policy-accounting

Description Commands in this context configure policy accounting FP information.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

policy-accounting

Syntax **policy-accounting** *template-name*
no policy-accounting

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ingress policy-accounting)

Full Context configure service vprn subscriber-interface group-interface ingress policy-accounting

Description This command configures the specified policy accounting template.

The **no** form of this command disables the policy accounting template.

Parameters *template-name* — Specifies the template name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s

policy-accounting

Syntax **policy-accounting** <*template-name*>
no policy-accounting

Context **[Tree]** (config>service>vprn>if>ingress policy-accounting)

Full Context configure service vprn interface ingress policy-accounting

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the service VPRN interface ingress policy accounting

Parameters *template-name* — Specifies the template name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

policy-accounting

Syntax **policy-accounting** <*template-name*>
no policy-accounting

Context **[Tree]** (config>service>ies>if>ingress policy-accounting)

Full Context configure service ies interface ingress policy-accounting

Description This command configures the service IES interface ingress policy accounting

Parameters *template-name* — Specifies the template name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

policy-accounting

Syntax **policy-accounting** *template-name*
no policy-accounting

Context **[Tree]** (config>router>if>ingress policy-accounting)

Full Context configure router interface ingress policy-accounting

Description This command applies a policy accounting template to the associated interface.

The **no** form of this command removes the policy accounting template.

Parameters *template-name* — Specifies the template name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

20.188 policy-acct-template

policy-acct-template

Syntax [**no**] **policy-acct-template** *template-name*

Context **[Tree]** (config>router policy-acct-template)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router policy-acct-template

Description This command configures a policy accounting template.

The **no** form of this command deletes the specified policy accounting template.

Parameters *template-name* — Specifies the template name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

20.189 policy-control

policy-control

Syntax **policy-control** *diameter-policy-name*
no policy-control

Context **[Tree]** (config>service>ies>sub-if>grp-if policy-control)
[Tree] (config>service>vprn>sub-if>grp-if policy-control)

Full Context configure service ies subscriber-interface group-interface policy-control
configure service vprn subscriber-interface group-interface policy-control

Description This command configures a policy-control policy for the interface.

The **no** form of this command reverts to the default.

Parameters *diameter-policy-name* — Specifies the name of an existing diameter policy, up to 32 characters.

20.190 policy-options

policy-options

Syntax [**no**] **policy-options**

Context **[Tree]** (config>router policy-options)

Full Context configure router policy-options

Description Commands in this context configure route policies. Route policies are applied to the routing protocol.

The **no** form of this command deletes the route policy configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

20.191 policy-override

policy-override

Syntax **policy-override**

Context **[Tree]** (config>app-assure>group policy-override)

Full Context configure application-assurance group policy-override

Description Commands in this context configure policy override parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.192 policy-reference-checks

policy-reference-checks

Syntax [**no**] **policy-reference-checks**

Context **[Tree]** (config>router policy-reference-checks)

Full Context configure router policy-reference-checks

Description This command checks policy references to ensure that a policy exists and displays a CLI error if the policy does not exist. Enabling this option protects against accidentally referencing a missing or misspelled policy, that can lead to unexpected results when the policy is evaluated.

The **no** version of this command disables policy reference checks and allows policies that do not exist to be referenced.

Default no policy-reference-checks

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.193 policy-statement

policy-statement

Syntax **policy-statement** *policy-name* [*policy-name*]
no policy-statement

Context **[Tree]** (config>test-oam>ldp-treetrace>path-discovery policy-statement)

Full Context configure test-oam ldp-treetrace path-discovery policy-statement

Description This command configures the FEC policy to determine which routes are imported from the LDP FEC database to discover its paths and probing them.

If no policy is specified, the ingress LER imports the full list of FECs from the LDP FEC database. New FECs are added to the discovery list at the next path discovery and not when they are learned and added into the FEC database. The maximum number of FECs to be discovered with path discovery is limited to 500.

The user can configure FECs to **include** or **exclude**.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified.

The **no** form of this command removes the policy from the configuration.

Default no policy-statement

Parameters *policy-name* — Specifies up to five route policy names to filter LDP imported address FECs. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified policy name(s) must already be defined.

Platforms All

policy-statement

Syntax [**no**] **policy-statement** *name*

Context **[Tree]** (config>router>policy-options policy-statement)

Full Context configure router policy-options policy-statement

Description This command creates the context to configure a route policy statement.

Route policy statements control the flow of routing information to and from a specific protocol, set of protocols, or to a specific BGP neighbor.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **policy-statement** is a logical grouping of match and action criteria. A single **policy-statement** can affect routing in one or more protocols and/or one or more protocols peers/neighbors. A single **policy-statement** can also affect both the import and export of routing information.

The **no** form of this command deletes the policy statement.

Default no policy-statement

Parameters *name* — Specifies the route policy statement name. Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

20.194 policy-variables

policy-variables

Syntax **policy-variables**

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from policy-variables)

Full Context configure router policy-options policy-statement entry from policy-variables

Description Commands in this context configure **policy-variables** parameters.

The **no** form of this command removes all policy variables.

Platforms All

20.195 poll

poll

Syntax **poll ca** *ca-profile-name*

Context **[Tree]** (admin>certificate>cmpv2 poll)

Full Context admin certificate cmpv2 poll

Description This command polls the status of the pending CMPv2 request toward the specified CA.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the response is ready, this command will resume the CMPv2 protocol exchange with server as the original command would do. The requests could be also still be pending as a result, then this command could be used again to poll the status.

SR OS allows only one pending CMP request per CA, which means no new request is allowed when a pending request is present.

Parameters *ca-profile-name* — Specifies a ca-profile name up to 32 characters.

Platforms All

20.196 poll-interval

poll-interval

Syntax **poll-interval** *seconds*
no poll-interval

Context **[Tree]** (config>service>vprn>ospf>area>if poll-interval)
[Tree] (config>service>vprn>ospf3>area>if poll-interval)

Full Context configure service vprn ospf area interface poll-interval
configure service vprn ospf3 area interface poll-interval

Description This command configures the poll interval, in seconds. The poll interval is the time between two Hello packets to a dead (non-adjacent) OSPF NBMA neighbor. The default value of the poll interval timer is higher than the hello interval timer to avoid wasting bandwidth on non-broadcast networks, since OSPF messages are unicast to each configured neighbor. The poll interval timer is used only on **non-broadcast** interface types and has no effect if configured on other interface types.

The **no** form of this command removes the **poll-interval** configuration.

Default 120

Parameters *seconds* — Specifies the poll interval, in seconds.

Values 0 to 4294967295

Platforms All

poll-interval

Syntax **poll-interval** *seconds*
no poll-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>ospf>area>interface poll-interval)
[Tree] (config>router>ospf3>area>interface poll-interval)

Full Context configure router ospf area interface poll-interval
configure router ospf3 area interface poll-interval

Description This command configures the poll interval, in seconds. The poll interval is the time between two Hello packets to a dead (non-adjacent) OSPF NBMA neighbor. The default value of the poll interval timer is higher than the hello interval timer to avoid wasting bandwidth on non-broadcast networks, since OSPF messages are unicast to each configured neighbor. The poll interval timer is used only on **non-broadcast** interface types and has no effect if configured on other interface types.

The **no** form of this command removes the **poll-interval** configuration.

Default 120

Parameters *seconds* — Specifies the poll interval, in seconds.

Values 0 to 4294967295

Platforms All

20.197 pool

pool

Syntax **pool** *pool-name* [**create**]
no pool *pool-name*

Context [Tree] (config>router>dhcp>server pool)
[Tree] (config>router>dhcp6>server pool)
[Tree] (config>service>vprn>dhcp>server pool)
[Tree] (config>service>vprn>dhcp6>server pool)

Full Context configure router dhcp local-dhcp-server pool
configure router dhcp6 local-dhcp-server pool
configure service vprn dhcp local-dhcp-server pool
configure service vprn dhcp6 local-dhcp-server pool

Description This command configures a DHCP address pool on the router.

The **no** form of this command removes the pool name from the configuration.

Parameters *pool name* — Specifies the name of this IP address pool. Allowed values are any string, up to 32 characters.

create — Keyword used to create the pool. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pool

Syntax **pool** *pool-name* **router** *router-instance* [**create**]
no pool *pool-name* **router** *router-instance*

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>evpn>export>ip-advertise-routes pool)

Full Context configure subscriber-mgmt isa-service-chaining evpn export ip-advertise-routes pool

Description This command configures NAT pools that are advertised in EVPN type 5 routes to the peer participating in service chaining.

The **no** form of this command removes the parameters from the configuration.

Parameters *pool-name* — Specifies the name of the NAT pool up, to 32 characters.

router-instance — Specifies the router instance belonging to the pool.

Values *router-name* | *vprn-svc-id*
router-name: Base, management, *cpm-vr-name,* vpls-management
Default - Base
vprn-svc-id: [1 to 2147483647]
cpm-vr-name: [up to 32 characters]
service-name: [up to 64 characters]

create — Keyword used to create a pool instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pool

Syntax **pool** [*name*]

Context **[Tree]** (config>port>access>egress pool)
[Tree] (config>port>access>ingress pool)
[Tree] (config>port>network>egress pool)

Full Context configure port access egress pool
configure port access ingress pool
configure port network egress pool

Description This command configures pool policies.

On the MDA level, access and network egress and access ingress pools are only allocated on channelized MDAs. Network ingress pools are allocated on the FP level for non-channelized MDAs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default pool default

Parameters *name* — If specified, the name must be **default**.

Platforms All

pool

Syntax **pool** [*name*]

Context **[Tree]** (config>card>fp>ingress>network pool)

Full Context configure card fp ingress network pool

Description This command configures the per-FP network ingress pool.

Default pool default

Parameters *name* — If specified, the name must be **default**.

Platforms All

pool

Syntax **pool** *nat-pool-name* [**nat-group** *nat-group-id* **type** *pool-type* [**applications** *applications*] [**create**]
no pool *nat-pool-name*

Context **[Tree]** (config>service>vprn>nat>outside pool)

Full Context configure service vprn nat outside pool

Description This command configures a NAT pool.

Parameters *nat-pool-name* — Specifies the NAT pool name.

Values 32 chars max

nat-group-id — Specifies the NAT group ID.

Values 1 to 4

create — This parameter must be specified to create the instance.

pool-type — Specifies the pool type.

Values large-scale, l2-aware, wlan-gw-anchor

applications — Specifies the application.

Values agnostic

create — Keyword used to create the pool.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pool

Syntax **pool** *nat-pool-name* **nat-group** *nat-group-id* **type** *pool-type* [**applications** *applications*] [**create**]
no pool *nat-pool-name*

Context **[Tree]** (config>router>nat>outside pool)

Full Context configure router nat outside pool

Description This command creates a NAT pool in the outside routing context. The NAT pool defines the parameters that will be used for IP address and port translation within the pool.

Parameters *nat-pool-name* — Specifies the NAT pool name, up to 32 characters.

nat-group-id — Specifies the NAT group ID.

Values 1 to 4

create — Creates the instance.

pool-type — Species the pool type.

Values large-scale, l2-aware, wlan-gw-anchor

applications — This creation-time parameter configures the NAT pool for protocol agnostic operation. The IP addresses are translated in 1:1 fashion regardless of the protocol. No ports are translated for TCP or UDP traffic. Traffic through the pool can be initiated from inside or outside. When nat-pool is configured in agnostic mode, certain parameters in the pool are pre-set and cannot be changed:

- mode one-to-one
- port-forwarding-range 0
- port-reservation blocks 1
- subscriber-limit 1
- deterministic port-reservation 65536.

This pool is used to configure static 1:1 NAT, where the operator have the control of the mapping between the inside and outside IP addresses. The static IP address mapping is using CLI constructs used in deterministic NAT (prefix and map deterministic NAT commands in the inside routing context).

ALG for TCP/UDP is supported in the protocol agnostic pool.

Values agnostic

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pool

Syntax **pool** [*name*]
no pool

Context **[Tree]** (config>isa>aa-grp>qos>egress>from-subscriber pool)
[Tree] (config>isa>aa-grp>qos>egress>to-subscriber pool)

Full Context configure isa application-assurance-group qos egress from-subscriber pool
configure isa application-assurance-group qos egress to-subscriber pool

Description Commands in this context configure an IOM pool as applicable to the specific application assurance group traffic. The user can configure resv-cbs (as percentage) values and slope-policy similarly to other IOM pool commands.

Default pool default

Parameters *name* — If specified, the name must be **default**.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pool

Syntax **pool** *nat-pool-name* **service-name** *service-name*
pool *nat-pool-name* **router** *router-instance*
no pool

Context **[Tree]** (config>service>nat>nat-policy pool)

Full Context configure service nat nat-policy pool

Description This command configures the NAT pool of this policy.

Parameters *nat-pool-name* — Specifies the name of the NAT pool, up to 32 characters.

router-instance — Specifies the router instance the pool belongs to, either by router name or service ID.

Values 1 to 2147483647 svc-name — a string up to 64 characters.

Values *router-name*: “Base” | “management”

Default Base

service-name — Specifies the name of the service, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.198 pool-manager

pool-manager

Syntax **pool-manager**

Context [Tree] (config>service>ies>sub-if>wlan-gw pool-manager)
[Tree] (config>service>vprn>sub-if>wlan-gw pool-manager)

Full Context configure service ies subscriber-interface wlan-gw pool-manager
configure service vprn subscriber-interface wlan-gw pool-manager

Description Commands in this context configure pool manager data for a WLAN GW subscriber interface.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.199 pool-name

pool-name

Syntax [**no**] **pool-name**

Context [Tree] (config>service>vprn>if>dhcp>option>vendor pool-name)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option>vendor pool-name)
[Tree] (config>service>ies>if>dhcp>option>vendor pool-name)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option>vendor pool-name)

Full Context configure service ies interface dhcp option vendor-specific-option pool-name
configure service ies subscriber-interface group-interface dhcp option vendor-specific-option pool-name
configure service vprn interface dhcp option vendor-specific-option pool-name
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option pool-name

Description This command sends the pool name in the Nokia vendor specific sub-option of the DHCP relay packet.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option pool-name
- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option pool-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service ies interface dhcp option vendor-specific-option pool-name
- configure service vprn interface dhcp option vendor-specific-option pool-name

pool-name

Syntax **pool-name** *name*
no pool-name

Context **[Tree]** (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client>slaac pool-name)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client>slaac pool-name)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client>ia-na pool-name)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client>ia-na pool-name)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client>dhcpv4-nat pool-name)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client>dhcpv4-nat pool-name)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client dhcpv4-nat pool-name
configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client ia-na pool-name
configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client slaac pool-name
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client dhcpv4-nat pool-name
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client ia-na pool-name
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client slaac pool-name

Description This command specifies the pool name that should be sent in the DHCPv6 messages. This is reflected in the Nokia vendor specific pool option (vendor-id 6527, option-id 0x02).

The **no** form of this command removes pool-name and the option will not be sent in DHCPv6.

Parameters *name* — Specifies the pool name up with 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pool-name

Syntax [**no**] **pool-name**

Context **[Tree]** (config>router>if>dhcp>option>vendor-specific-option pool-name)

Full Context configure router interface dhcp option vendor-specific-option pool-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the sending of the pool name in the Nokia vendor-specific suboption of the DHCP relay packet.

The **no** form of this command disables the feature.

Default no pool-name

Platforms All

20.200 pop

pop

Syntax [**no**] **pop**

Context **[Tree]** (config>router>mpls>if>label-map pop)

Full Context configure router mpls interface label-map pop

Description This command specifies that the incoming label must be popped (removed). No label stacking is supported for a static LSP. The service header follows the top label. Once the label is popped, the packet is forwarded based on the service header.

The **no** form of this command removes the **pop** action for the *in-label*.

Platforms All

20.201 populate

populate

Syntax **populate** {**static** | **dynamic** | **evpn**} [**route-tag** [*1..255*]]
no populate {**static** | **dynamic** | **evpn**}

Context **[Tree]** (config>service>ies>if>arp-host-route populate)
[Tree] (config>service>vprn>if>arp-host-route populate)
[Tree] (config>service>vprn>if>ipv6>nd-host-route populate)

Full Context configure service ies interface arp-host-route populate
configure service vprn interface arp-host-route populate
configure service vprn interface ipv6 nd-host-route populate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the creation of ARP/ND host-route entries in the route-table out of a certain ARP/ND entry type.

The **no** form of this command reverts to the default.

Default no populate

Parameters **evpn** — Enables the creation of ARP-ND host routes in the route table out of EVPN ARP/ND entries (entries learned from EVPN MAC/IP routes).

dynamic — Enables the creation of ARP-ND host routes in the route table out of dynamic ARP/ND entries (learned from received ARP/ND messages from the hosts).

static — Enables the creation of ARP-ND host routes in the route table out of configured static ARP/ND entries.

route-tag [*1..255*] — Specifies the route tag that is added in the route table for ARP-ND host routes of type **evpn**, **dynamic**, or **static**. This tag can be matched on BGP VRF export and BGP peer export policies.

Platforms All

20.202 port

port

Syntax **port** *port-id* [**sync-tag** *sync-tag*] [**create**]
no port *port-id*]

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync port)

Full Context configure redundancy multi-chassis peer sync port

Description This command specifies the port to be synchronized with the multi-chassis peer and a synchronization tag to be used while synchronizing this port with the multi-chassis peer.

Parameters *port-id* — Specifies the port to be synchronized with the multi-chassis peer.

Values

port-id	slot/mda/port	
lag-id	lag-id	
	lag	keyword
	id	1 to 200
pw-id	pw-*id*	
	pw	keyword
	id	1 to 10239

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sync-tag — Specifies a synchronization tag, up to 32 characters in length, to be used while synchronizing this port with the multi-chassis peer.

create — Creates an entry; mandatory while creating an entry.

Platforms All

port

Syntax [**no**] **port** {*port-id* | *bundle-id* | *bpgrp-id* | *aps-id* | *connector-port-id*}

Context **[Tree]** (config port)

Full Context configure port

Description This command enables access to the context to configure ports, multilink bundles, and bundle protection groups (BPGs). Before a port can be configured, the chassis slot must be provisioned with a valid card type and the MDA parameter must be provisioned with a valid MDA type.

Default No ports are configured. All ports must be explicitly configured and enabled.

Parameters *port-id* — Specifies the physical port ID in the following format:

Values *slot*/*mda*/*port* [.*channel*]

eth-sat-id — Specifies the Ethernet satellite ID to be associated with this IP interface. This parameter applies to the 7950 XRS only.

Values

eth-sat-id	esat-*id*/*slot*/*port*	
	esat	keyword
	id	1 to 20

pxc-id — Specifies the PXC ID to be associated with this IP interface. This parameter applies to the 7950 XRS only.

Values

pxc-id	pxc-*id*.*sub-port*	
	pxc	keyword
	id	1 to 64
	sub-port	a, b

bundle-id — Specifies the multilink bundle to be associated with this IP interface. The command syntax must be configured as follows:

Values bundle-*type*-*slot/mda.bundle-num*

bundle-ppp-*slot/mda.bundle-num*	Creates a multilink PPP bundle.
bundle-ima-*slot/mda.bundle-num*	Creates an IMA bundle.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

bundle-fr-*slot/mda.bundle-num*	Creates an MLFR bundle.
where:	**bundle**: keyword
	slot: IOM/MDA slot numbers
	bundle-num: 1 to 336

For example:
router1>config# port bundle-ppp-5/1.1 (multilink PPP bundle)
router1>config# port bundle-ima-5/1.2 (IMA bundle)

aps-id — This option configures APS on unbundled SONET/SDH ports. All SONET-SDH port parameters, with certain exceptions, for the working and protection circuit ports must be configured in the **config>port>aps-id** context. The working and protection circuit ports inherit all those parameters configured. The exception parameters for the working and protect circuits can be configured in the **config>port>sonet-sdh** context. Exception list commands include:

- clock-source
- [no] loopback
- [no] report-alarm
- section-trace
- [no] threshold

When an **aps-id** is created all applicable parameters under the port CLI tree (including parameters under any submenus) assume **aps-id** defaults, or when those are not explicitly specified, default to SONET/SDH port defaults for any SONET port.

All but a few exception SONET/SDH parameters for the working channel port must be configured in the **config>port>aps>sonet-sdh** context. The protection channel inherits all the configured parameters. The exception parameters for the protection channel can be configured in the **config>port>aps>sonet-sdh** context.

Signal failure (SF) and signal degrade (SD) alarms are not enabled by default on POS interfaces. It is recommended to change the default alarm notification configuration for POS ports that belong to APS groups in order to be notified of SF/SD occurrences to be able to interpret the cause for an APS group to switch the active line.

For path alarms, modify the logical line aps-id in the **config>port aps-***id* **<sonet-sdh>path report-alarm** context. For example:

configure port **aps-1** sonet-sdh path report-alarm p-ais

For line alarms, separately, modify the 2 physical ports that are members of the logical aps-id port (the working and protect lines). APS reacts only to line alarms, not path alarms. For example:

configure port **1/2/3** sonet-sdh report-alarm lb2er-sd
configure port **4/5/6** sonet-sdh report-alarm lb2er-sd

If the SD and SF threshold rates must be modified, the changes must be performed at the line level on both the working and protect APS port member.

The **no** form of this command deletes an aps-*group-id* or bundle-aps-group-id. In order for an aps-*group-id* to be deleted,

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The same rules apply for physical ports, bundles deletions apply to APS ports/ bundles deletions (for example an aps-group-id must be shutdown, have no service configuration on it, and no path configuration on it). In addition working and protection circuits must be removed before an aps-group-id may be removed.

Values **port aps**-*group-id* **aps**:keyword where *group-id*: 1 to 64

Example: **port aps**-64

bpgrp-id — Creates a bundle protection group (BPG). The BPGrp consists of a working and protection bundles that provide APS protection to each other using bi-directional APS as supported on the 7750 SR family of products. All members of a working/ protection bundle must be on the same working/protection circuit respectively of the same, already provisioned APS group. The working bundle must have already been created in the **config>port** context before services can be created on a BPGrp.

Values **bpgrp**-*type*-*bpgrp-num*

bpgrp: keyword
type: **ppp** — Provides protection of one PPP bundle by another.
ima — Provides protection of one IMA bundle by another IMA bundle.
bpgrp-num: 1 to 1600

connector-port-id — Specifies the physical port of a connector in the following format.

Values *slot*/*mda*/*connector*/*port*

Platforms All

port

Syntax **port** *port-id*
no port

Context **[Tree]** (config>port-xc>pxc port)

Full Context configure port-xc pxc port

Description This command configures the referenced Ethernet port as a loopback or a cross-connect port (PXC). When this command is executed, the system automatically creates two PXC subports under this Ethernet port.

The physical PXC port does not require any external connectivity or optical transceivers to function properly. Consequently, all optic-related alarms are disabled on the port.

The physical PXC port is automatically configured as a hybrid port. The MTU is preset to 9212 bytes, the encapsulation type is set to dot1q, and dot1x tunneling is turned on.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A single physical port can be associated with more than one PXC. In other words, multiple PXCs are supported per physical port. Because PXC subports use a single physical port to transmit traffic in both directions, the nominal port bandwidth is asymmetrically divided between the two directions. For example, a 10 Gb/s Ethernet port in PXC mode can accommodate 9 Gb/s of traffic in one direction and 1 Gb/s in the other. Any other ratio can be achieved as long as the sum of the bandwidth of the two PXC subports does not exceed the bandwidth capacity of the physical port (10 Gb/s in this case).

Since the PXC uses a single physical port to transmit traffic in both directions, the nominal port bandwidth is asymmetrically divided between the two directions. For example, a 10 Gb/s Ethernet port in PXC mode can accommodate 9 Gb/s of traffic in one direction and 1 Gb/s in the other. Any other ratio can be achieved as long as the sum of the bandwidth of the two PXC subports does not exceed the bandwidth capacity of the physical port (10 Gb/s in this case).

The following rules apply to PXC port configurations:

- Only unused physical ports (not associated with an interface or SAP) can be referenced inside of a PXC ID configuration.
- The physical port cannot be removed from a PXC ID configuration if the corresponding PXC subports are currently in use.
- A physical port cannot be used outside the configured PXC context. For example, a regular IP interface cannot use this physical port, or a SAP on that port cannot be associated with a service.

The **no** form of this command removes the port ID from the configuration.

Parameters *port-id* — Specifies the physical port in the *slot*/*mda*/*port* format.

Platforms All

port

Syntax **port** *port-id* [*port-id*] [**priority** *priority*] [**sub-group** *sub-group-id*] [**hash-weight** *weight*]
no port *port-id* [*port-id*]

Context **[Tree]** (config>lag port)

Full Context configure lag port

Description This command adds ports to a Link Aggregation Group (LAG).

The port configuration of the first port added to the LAG is used as a basis to compare to subsequently added ports. If a discrepancy is found with a newly added port, that port will not be added to the LAG.

Multiple (space separated) ports can be added or removed from the LAG link assuming the maximum of number of ports is not exceeded.

Ports that are part of a LAG must be configured with auto-negotiate limited or disabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes ports from the LAG.

Default No ports are defined as members of a LAG.

Parameters *port-id* — Specifies the port ID.

The maximum number of ports in a LAG depends on the platform type, the hardware deployment, and the SR OS software release. Adding a port over the maximum allowed per given router or switch is blocked. Some platforms support double port scale for specific port types on LAGs with LAG ID in the range of 1 to 64 inclusive. Up to 16 ports can be specified in a single statement, up to 64 ports total.

Values These values apply to the 7950 XRS only.

slot/*mda*/*port*		
eth-sat-id	esat-*id*/*slot*/*port*	
	esat	keyword
	id	1 to 20
pxc-id	pxc-*id*.*sub-port*	
	pxc	keyword
	id	1 to 64
	sub-port	a to b

priority — Specifies the port priority used by LACP. The port priority is also used to determine the primary port. The port with the lowest priority is the primary port. In the event of a tie, the smallest port ID becomes the primary port.

Values 1 to 65535

sub-group-id — Identifies a LAG subgroup. When using subgroups in a LAG, they should only be configured on one side of the LAG, not both. Only having one side perform the active/standby selection guarantees a consistent selection and fast convergence. The active or standby selection is signaled through LACP to the other side. The hold time should be configured when using subgroups to prevent the LAG going down when switching between active and standby subgroup since momentarily all ports are down in a LAG (break-before-make).

Values 1 to 8 identifies a LAG subgroup The **auto-iom** subgroup is defined based on the IOM (all ports of the same IOM are assigned to the same subgroup). The **auto-mda** subgroup is defined based on the MDA. (all ports of the same MDA are assigned to the same subgroup).

weight — Specifies the flow hashing distribution between LAG ports.

Values 1 to 100000, port-speed

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** *port-id*
no port

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg port)

Full Context configure service system bgp-evpn ethernet-segment port

Description This command configures a port-id associated with the Ethernet-Segment. If the Ethernet-Segment is configured as **all-active**, then only a lag or a PW port can be associated to the Ethernet-Segment. If the Ethernet-Segment is configured as **single-active**, then a lag, port or sdp can be associated to the Ethernet-Segment. In any case, only one of the four objects can be configured in the Ethernet-Segment. A specified port can be part of only one Ethernet-Segment. Only Ethernet ports can be added to an Ethernet-Segment.

Default no port

Parameters *port-id* — Specifies the port ID associated to the Ethernet-Segment.

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

Platforms All

port

Syntax **port** [*port-id* | *lag-id*]
no port

Context **[Tree]** (config>service>sdp>binding port)

Full Context configure service sdp binding port

Description This command specifies the port or lag identifier, to which the pseudowire ports associated with the underlying SDP are bound. If the underlying SDP is re-routed to a port or lag other than the specified one, the pseudowire ports on the SDP are operationally brought down.

The **no** form of the command removes the value from the configuration.

Default no port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id* — Specifies the identifier of the port in the slot/mda/port format.

port-id	*slot*/*mda*/*port*[.*channel*]		
	pxc-id	psc-id.sub-port	
		pxc psc-id.sub-port	
		pxc: keyword	
		id: 1 to 64	
		sub-port: a, b	
	aps-id	aps-*group-id*[.*channel*]	
		aps keyword	
		group-id	1 to 64
		group-id	1 to 16
	bundle-*type*-*slot/mda*.*bundle-num*		
		bundle	keyword
		type	ima, ppp
		bundle-num	1 to 256
	bpgrp-id:	bpgrp-*type*-*bpgrp-num*	
		bpgrp	keyword
		type	ima
		bpgrp-num	1 to 1280
	ccag-id	- ccag-<id>.<path-id>[cc-type]	
		ccag	keyword
		id	1 to 8
		path-id	a, b
		cc-type[.sap-net | .net-sap]	
	lag-id	lag-*id*	
		lag	keyword
		id	1 to 800

lag-id — Specifies the LAG identifier.

Platforms All

port

Syntax **port** [**evpn-mpls** | **sap** *sap-id* | **sdp** *sdp-id:vc-id* | **vxlan vtep** *ip-address* **vni** *vni-id*] [**detail**]
no port

Context **[Tree]** (debug>service>id>pim-snooping port)

Full Context debug service id pim-snooping port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables or disables debugging for PIM ports.

Parameters *sap-id* — Only debugs packets associated with the specified SAP

sdp-id:vc-id — Only debugs packets associated with the specified SDP

detail — Provides detailed debugging information

evpn-mpls — Debugs PIM snooping statistics for EVPN-MPLS destinations

Platforms All

port

Syntax [**no**] **port** *port-id*

Context **[Tree]** (config>service>pw-port-list port)

Full Context configure service pw-port-list port

Description This command is only applicable for VSR configurations. This command is used to select ports eligible for use with Flex PW port. Physical ports used by Flex PW port can be shared with any other Layer 2 or Layer 3 service. In other words, a Layer 3 interface using a regular SAP can be associated with a VPRN service, while the port is used by a Flex PW port. Another regular SAP from the same port can be associated with a VPLS or Epipe service at the same time.

The following rules should be followed when populating a pw-port-list:

- A port must be in hybrid mode before it is added to a pw-port-list.
- Before a port is removed from or added to a pw-port-list, all PW ports must be dissociated from the corresponding Epipe services (PW ports must be unconfigured). This implies that all PW SAPs must be deleted.
- Network interfaces (configured in the Base routing context) can be configured only on ports that are in the pw-port-list.
- A port mode (access, network, or hybrid) cannot be changed while the port is in the pw-port-list.

From this, the operator can consider adding all ports that are in hybrid mode to a pw-port-list at the beginning of the system configuration. This ensures that those ports can be used by a Flex PW port at any later time, independently of their current use.

The **no** form of this command removes the port ID from the configuration.

Parameters *port-id* — Specifies the IP of the port.

Values slot/mda/port: 1 to 16

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** *port*
no port

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius port)

Full Context configure service vprn aaa remote-servers radius port

Description This command configures the UDP port number to contact the RADIUS server.

The **no** form of this command reverts to the default value.

Default port 1812 (as specified in RFC 2865, *Remote Authentication Dial In User Service* (*RADIUS*))

Parameters *port* — Specifies the UDP port number to contact the RADIUS server.

Values 1 to 65535

Platforms All

port

Syntax **port** *value*
no port

Context **[Tree]** (config>service>vprn>log>syslog port)

Full Context configure service vprn log syslog port

Description This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

The **no** form of this command reverts to default value.

Default no port

Parameters *value* — The value is the configured UDP port number used when sending syslog messages.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax [**no**] **port** *port-id*

Context **[Tree]** (config>router>lmp>te-link>data-bearer port)

Full Context configure router lmp te-link data-bearer port

Description This command configures the port associated with the data bearer. The port must be a physical black and white Ethernet port.

Default no port

Parameters *port-id* — Specifies the ID of the port.

Values			
port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

port

Syntax **port** *port*

Context **[Tree]** (config>app-assure>group>event-log>syslog port)

Full Context configure application-assurance group event-log syslog port

Description This command specifies the UDP port used by application assurance to inject the syslog events inband.

Default port 514

Parameters *port* — Specifies the UDP port number.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax [**no**] **port** *port-number*
[**no**] **port range** *start-port-num end-port-num*

Context **[Tree]** (config>app-assure>group>port-list port)

Full Context configure application-assurance group port-list port

Description This command specifies the server TCP or UDP port number to use in the port list definition.

The **no** form of this command restores the default by removing port number from the port list.

Default no port

Parameters *port-number* — Specifies the port number.

Values 0 to 65535

start-port-number — Specifies the start port number.

Values 0 to 65535

end-port-number — Specifies the end port number.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

port

Syntax **port** {*port-id* | **lag** *lag-id*} [**egress**] [**ingress**]
no port {*port-id* | **lag** *lag-id*} {[**egress**] [**ingress**]}

Context **[Tree]** (config>mirror>mirror-source port)

Full Context configure mirror mirror-source port

Description This command enables mirroring of traffic ingressing or egressing a port (Ethernet port, SONET/SDH channel, TDM channel, or Link Aggregation Group (LAG)).

The **port** command associates a port or LAG to a mirror source. The port is identified by the *port-id*. The defined port may be Ethernet, Access or network, SONET/SDH, or TDM channel access. A network port may be a single port or a Link Aggregation Group (LAG) ID. When a LAG ID is given as the *port-id*, mirroring is enabled on all ports making up the LAG. If the port is a SONET/SDH interface, the *channel-id* must be specified to identify which channel is being mirrored (applies to the 7450 ESS and 7750 SR). Either a LAG port member *or* the LAG port can be mirrored.

The port is only referenced in the mirror source for mirroring purposes. The mirror source association does not need to be removed before deleting the card to which the port belongs. If the port is removed from the system, the mirroring association will be removed from the mirror source.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The same port may not be associated with multiple mirror source definitions with the **ingress** parameter defined. The same port may not be associated with multiple mirror source definitions with the **egress** parameter defined.

If a SAP is mirrored on an access port, the SAP mirroring will have precedence over the access port mirroring when a packet matches the SAP mirroring criteria. Filter and label mirroring destinations will also precedence over a port-mirroring destination.

If the port is not associated with a **mirror-source**, packets on that port will not be mirrored. Mirroring may still be defined for a SAP, label or filter entry, which will mirror based on a more specific criteria.

The encapsulation type on an access port or channel cannot be changed to Frame Relay if it is being mirrored (applies to the 7750 SR and 7450 ESS).

The **no port** command disables port mirroring for the specified port. Mirroring of packets on the port may continue due to more specific mirror criteria. If the **egress** or **ingress** parameter keywords are specified in the **no** command, only the ingress or egress mirroring condition will be removed.

Parameters *port-id* — Specifies the port ID of the 7750 SR or 7950 XRS.

The following syntax applies to the 7750 SR:

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b
	aps-id	aps-*group-id*[.*channel*]	
		aps	keyword
		group-id	1 to 64
	bundle ID	bundle-*type-slot/mda.bundle-num*	
		bundle	keyword
		type	ima, ppp
		bundle-num	1 to 336
	bgrp-id	bpgrp-*type-bpgrp-num*	
		bgrp	keyword
		type	ima, ppp
		bgrp-num	1 to 2000
	ccag-id	ccag-*id*.*path-id cc-type*:*cc-id*	
		ccag	keyword
		id	1 to 8

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	path-id	a, b
	cc-type	sap-net, .net-sap
	cc-id	0 to 4094

The following syntax applies to the 7950 XRS:

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

lag-id — The LAG identifier, expressed as a decimal integer.

Note: On the 7950 XRS, the XMA ID takes the place of the MDA.

Values 1 to 800

egress — Specifies that packets egressing the port should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the port should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

Platforms All

port

Syntax **port** {*port-id* | **lag** *lag-id*} {[**egress**] [**ingress**]}
no port {**port-id** | **lag** *lag-id*} [**egress**] [**ingress**]

Context **[Tree]** (config>li>li-source port)

Full Context configure li li-source port

Description This command specifies the port to perform lawful intercept. It is recommended when configuring **li-source>port** criteria, the li-source should only contain ports. All other criteria such as SAPs and subscribers should use a different li-source.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id* — Specifies the port ID to perform lawful intercept.

port-id	*slot*/*mda*/*port* [.*channel*]	
bundle-id	bundle-<type>-slot/mda.<bundle-num>	
	bundle	keyword
	type	ima | fr | ppp
	bundle-num	1 to 336
aps-id	aps-<group-id>[.channel]	
	aps	keyword
	group-id	1 to 128
eth-sat-id	esat-<id>/<slot>/[u]<port>	
	esat	keyword
	id	1 to 20
	u	keyword for up-link port
tdm-sat-id	tsat-<id>/<slot>/[<u>]<port>.<channel>	
	tsat	keyword
	id	1 to 20
	u	keyword for up-link port
pxc-id	pxc-<id>.<sub-port>	
	pxc	keyword
	id	1 to 64
	sub-port	a, b

lag-id — The LAG identifier, expressed as a decimal integer.

Note: On the 7950 XRS, the XMA ID takes the place of the MDA.

Values 1 to 800

egress — Performs lawful intercept on egress traffic.

ingress — Performs lawful intercept on ingress traffic

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

port

Syntax **port** *tcp-port*
no port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>li>x-interfaces>lics>lic port)

Full Context configure li x-interfaces lics lic port

Description This command configures the TCP port associated with this LIC.

The **no** form of this command reverts to the default.

Parameters *tcp-port* — Specifies the TCP source port of the LIC.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

port

Syntax **port** *tcp-port*
no port

Context [Tree] (config>li>x-interfaces>x1 port)

Full Context configure li x-interfaces x1 port

Description This command configures the TCP port for the X1 interface. The system listens to this port and uses it as the source TCP port.

The **no** form of this command reverts to the default.

Parameters *tcp-port* — Specifies the TCP port.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

port

Syntax **port** {*port-id* | **lag** *lag-id*} {[**egress**] [**ingress**]}
no port {*port-id* | **lag** *lag-id*} [**egress**] [**ingress**]

Context [Tree] (debug>mirror-source port)

Full Context debug mirror-source port

Description This command enables mirroring of traffic ingressing or egressing a port (Ethernet port, SONET/SDH channel, TDM channel, or Link Aggregation Group (LAG)).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **port** command associates a port or LAG to a mirror source. The port is identified by the *port-id*. The defined port may be Ethernet, Access or network, SONET/SDH, or TDM channel access. A network port may be a single port or a Link Aggregation Group (LAG) ID. When a LAG ID is given as the *port-id*, mirroring is enabled on all ports making up the LAG. If the port is a SONET/SDH interface, the *channel-id* must be specified to identify which channel is being mirrored (applies to the 7450 ESS and 7750 SR). Either a LAG port member *or* the LAG port can be mirrored.

The port is only referenced in the mirror source for mirroring purposes. The mirror source association does not need to be removed before deleting the card to which the port belongs. If the port is removed from the system, the mirroring association will be removed from the mirror source.

The same port may not be associated with multiple mirror source definitions with the **ingress** parameter defined. The same port may not be associated with multiple mirror source definitions with the **egress** parameter defined.

If a SAP is mirrored on an access port, the SAP mirroring will have precedence over the access port mirroring when a packet matches the SAP mirroring criteria. Filter and label mirroring destinations will also precedence over a port-mirroring destination.

If the port is not associated with a **mirror-source**, packets on that port will not be mirrored. Mirroring may still be defined for a SAP, label or filter entry, which will mirror based on a more specific criteria.

The encapsulation type on an access port or channel cannot be changed to Frame Relay if it is being mirrored (applies to the 7750 SR and 7450 ESS).

The **no port** command disables port mirroring for the specified port. Mirroring of packets on the port may continue due to more specific mirror criteria. If the **egress** or **ingress** parameter keywords are specified in the **no** command, only the ingress or egress mirroring condition will be removed.

Parameters *port-id* — Specifies the port ID of the 7750 SR or 7950 XRS.

The following syntax applies to the 7750 SR:

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b
	aps-id	aps-*group-id*[.*channel*]	
		aps	keyword
		group-id	1 to 64
	bundle ID	bundle-*type-slot/mda.bundle-num*	

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	bundle	keyword
	type	ima, ppp
	bundle-num	1 to 336
bgrp-id	bpgrp-*type-bpgrp-num*	
	bgrp	keyword
	type	ima, ppp
	bgrp-num	1 to 2000
ccag-id	ccag-*id*.*path-id cc-type*:*cc-id*	
	ccag	keyword
	id	1 to 8
	path-id	a,b
	cc-type	sap-net, net-sap
	cc-id	0 to 4094

The following syntax applies to the 7950 XRS:

port-id	*slot*/*mda*/*port* [.*channel*]	
	eth-sat-id	esat-*id*/*slot*/*port*
		esat keyword
		id 1 to 20
	pxc-id	pxc-*id*.*sub-port*
		pxc keyword
		id 1 to 64
		sub-port a, b

lag-id — Specifies the LAG identifier, expressed as a decimal integer.

Note: On the 7950 XRS, the XMA ID takes the place of the MDA.

Values 1 to 800

egress — Specifies that packets egressing the port should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the port should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** {**lt** | **gt** | **eq**} *port-number*
port port-list *port-list-name*
port range *port-number port-number*
no port

Context **[Tree]** (config>filter>ip-filter>entry>match port)
[Tree] (config>filter>ipv6-filter>entry>match port)
[Tree] (config>filter>ipv6-exception>entry>match port)

Full Context configure filter ip-filter entry match port
configure filter ipv6-exception entry match port
configure filter ipv6-filter entry match port

Description This command configures a TCP/UDP/SCTP source or destination port match criterion in IPv4 and IPv6 CPM (SCTP not supported) and/or ACL filter policies. A packet matches this criterion if the packet TCP/UDP/SCTP (as configured by protocol/next-header match) source OR destination port matches either the specified port value or a port in the specified port range or port-list.

Operational Note: This command is mutually exclusive with src-port and dst-port commands. Configuring "port eq 0", may match non-initial fragments where the source/destination port values are not present in a packet fragment if other match criteria are also met.

The **no** form of this command deletes the specified port match criterion.

Default no port

Parameters **lt | gt | eq** — Specifies the operator to use relative to *port-number* for specifying the port number match criteria.

lt — Specifies that all port numbers less than *port-number* match.

gt — Specifies that all port numbers greater than *port-number* match.

eq — Specifies that the *port-number* must be an exact match.

port-number — Specifies a source or destination port to be used as a match criterion. The port number can be expressed as a decimal integer, as well as in hexadecimal or binary format. The following value shows a decimal integer only.

Values 0 to 65535

port-list *port-list-name* — Specifies an inclusive range of source or destination port values to be used as match criteria.

range *port-number port-number* — Specifies an inclusive range of source or destination port values to be used as match criteria.

Platforms All

- configure filter ipv6-filter entry match port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure filter ip-filter entry match port

VSR

- configure filter ipv6-exception entry match port

port

Syntax [**no**] **port** *port-number*
[**no**] **port range** *start end*

Context **[Tree]** (config>filter>match-list>port-list port)

Full Context configure filter match-list port-list port

Description This command adds a port or a range of ports to an existing port match list. The **no** form of this command deletes the specified port or range of ports form the list.

Parameters *port-number* — Specifies the port number to add to the list. The port number can be expressed as a decimal integer, as well as in hexadecimal or binary format. Below shows decimal integer only.

Values 0 to 65535

start end — Specifies an inclusive port range between two port numbers values. The *start* of the range and *end* of the range can be expressed as decimal integers, as well as in hexadecimal or binary format. The following value shows decimal integer only.

Values 0 to 65535

Platforms All

port

Syntax **port** *port-id*
no port

Context **[Tree]** (config>router>origin-validation>rpki-session port)

Full Context configure router origin-validation rpki-session port

Description This command configures the destination port number to use when contacting the cache server. The default port number is 323. The port cannot be changed without first shutting down the session.

Default no port

Parameters *port-id* — Specifies a port ID.

Values 0 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

port

Syntax **port** *port-name*
no port

Context **[Tree]** (config>router>if port)

Full Context configure router interface port

Description This command creates an association with a logical IP interface and a physical port.

An interface can also be associated with the system (loopback address).

The command returns an error if the interface is already associated with another port or the system. In this case, the association must be deleted before the command is re-attempted. The *port-id or port-id for* Ethernet ports can be in one of the following forms:

Ethernet interfaces

If the card in the slot has MDAs/XMAs, *port-id* is in the *slot_number*/MDA or XMA_*number*/*port_number* format; for example, **1/1/3** specifies port 3 of the MDA/XMA installed in MDA/XMA slot 1 on the card installed in chassis slot 1.

SONET/SDH interfaces

When the *port-id* represents a POS interface, the *port-id* must include the *channel-id.* The POS interface must be configured as a **network** port.

The **no** form of this command deletes the association with the port. The **no** form of this command can only be performed when the interface is administratively down.

Default no port

Parameters *port-name* — The physical port identifier to associate with the IP interface.

Values The following values apply to the 7750 SR and 7450 ESS:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 109 **Port Names**

port-name	port-id[:encap-val]	
	encap-val	0 for null
		[0 to 4094] for dot1q
		[0 to 4094].* [1 to 4094].[0to 4094] for qinq
port-id	slot/mda/port[.channel]	
	bundle-id	bundle-<type>-slot/mda.<bundle-num>
	bundle	keyword
	type	ima, fr, ppp
	bundle-num	1 to 336
	bpgrp-id	bpgrp-<type>-<bpgrp-num>
	bpgrp	keyword
	type	ima, ppp
	bpgrp-num	1 to 2000
	aps-id	aps-<group-id>[.channel]
	aps	keyword
	group-id	1 to 128
	ccag-id	ccag-<id>.<path-id>[cc-type]
	ccag	keyword
	id	1 to 8
	path-id	a, b
	cc-type	[.sap-net| .net-sap]
	eth-tunnel-id	eth-tunnel-<id>
	eth-tunnel	keyword
	id	1 to 1024
	lag-id	lag-<id>
	lag	keyword
	id	1 to 800

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 109 **Port Names**

	gtg-id	gmpls-tun-grp-<id>
	gmpls-tun-grp	keyword
	id	1 to 1024
	eth-sat-id	esat-<id>/<slot>/[u]<port>
	esat	keyword
	id	1 to 20
	u	keyword for up-link port

Values The following values apply to the 7950 XRS:

Table 110 **Port Names**

port-name	<port-id>[:encap-val]	
	encap-val	0 for null
		0 to 4094 for dot1q
		0 to 4094.* [1..4094].[0..4094] for qinq
port-id	slot/mda/port[.channel]	
	eth-tunnel-id	eth-tunnel-<id>
	eth-tunnel	keyword
	id	1 to 1024
	lag-id	lag-<id>
	lag	keyword
	id	1 to 800
	gtg-id	gmpls-tun-grp-<id>
	gmpls-tun-grp	keyword
	id	1 to 1024
	eth-sat-id	esat-<id>/<slot>/[u]<port>
	esat	keyword
	id	1 to 20

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 110 **Port Names**

	u	keyword for up-link port
	pxc-id	pxc-<id>.<sub-port>
	pxc	keyword
	id	1 to 64
	sub-port	a to b

Platforms All

port

Syntax **port** *port-id* **to** *port-id* [**create**]
no port *port-id*

Context **[Tree]** (config>system>port-topology port)

Full Context configure system port-topology port

Description This command is used for satellites. It identifies to the SR OS that there is an internal connection between two ports.

Permitted pairings of the two ports are:

First port	Second port
Router port	Satellite uplink port
Satellite uplink port	Router port

For satellites, this command configures the binding between a host port ID and the satellite uplink from the satellite chassis. The port topology can be configured with the host connected to a satellite uplink or the satellite uplink port connected to the specified host port. Both configurations are supported, as shown in the following examples:

```
*A:Dut-A# configure system port-topology port esat-1/1/u4 to 1/2/2 create
*A:Dut-A# configure system port-topology no port esat-1/1/u4
*A:Dut-A# configure system port-topology port 1/2/2 to esat-1/1/u4 create
*A:Dut-A# configure system port-topology no port 1/2/2
```

The **no** form of the command removes the internal connection.

Default no port port-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id* — Specifies one port of an internal port connection. These ports can be router ports or Ethernet satellite uplink ports. Acceptable pairings are defined in the command description.

Values

port-id (Router port)
slot/*mda*/*port*

slot	The slot number of the card in the chassis. The maximum slot number is platform dependent. Refer to the hardware installation guides for more information.
mda	[1 to 2]
port	[1 to 160] (depending on the MDA type)

(Ethernet satellite uplink port)
esat-id/slot/uport

esat	keyword
id	[1 to 20]
slot	[1]
u	keyword for up-link port
port	[1 to 4]

create — Specifies the keyword required to create the binding between the two ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

port

Syntax **port** *port-id*

Context **[Tree]** (config>system>satellite>port-template port)

Full Context configure system satellite port-template port

Description This command specifies the satellite port to be reconfigured.

The **no** form of this command deletes the specified port configuration.

Parameters *port-id* — Specifies the satellite physical port ID. This must use the format *slot*/*mda*/*port*. Currently, all satellites have a single slot and a single MDA, so these values will always be 1. For example, port 10 would be specified as 1/1/10.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** *port-id* [**create**]
no port *port-id*

Context **[Tree]** (config>system>ptp port)

Full Context configure system ptp port

Description This command configures PTP over Ethernet on the physical port. The PTP process shall transmit and receive PTP messages through the port using Ethernet encapsulation (as opposed to UDP/IPv4 encapsulation).

The frames are transmitted with no VLAN tags even if the port is configured for dot1q or qinq modes for encap-type. In addition, the received frames from the external PTP clock must also be untagged.

There are two reserved multicast addresses allocated for PTP messages (see *Annex F IEEE Std 1588™-2008*). Either address can be configured for the PTP messages sent through this port.

A PTP port may not be created if the PTP profile is set g8265dot1-2010.

If the port specified in the port-id supports 1588 port based timestamping, then a side effect of enabling PTP over Ethernet on the port shall be the enabling of Synchronous Ethernet on that port.

De-provisioning of the card or MDA containing the specified port is not permitted while the port is configured within PTP.

Changing the encapsulation or the port type of the Ethernet port is not permitted when PTP Ethernet Multicast operation is configured on the port.

To allocate an ethernet satellite client port as a PTP port, the ethernet satellite must first be enabled for the transparent clock function. For more information, see the **config>system>satellite>eth-sat ptp-tc** command.

The SyncE/1588 ports of the CPM and CCMs can be specified as a PTP port. These use the ‘A/3’ and ‘B/3’ designation and they both must be specified as two PTP ports if both are to be used. The active CPM sends and receives messages on both ports if they are specified and enabled.

Parameters *port-id* — Specifies a specific physical port.

Values *slot/mda/port*

create — Creates the PTP port. This keyword is required when first creating the PTP port, if the system is configured to require it (enabled in the environment create command). Once the PTP port is created, it is possible to navigate into the context without the create keyword.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** *value*
no port

Context **[Tree]** (config>log>syslog port)

Full Context configure log syslog port

Description This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

The **no** form of this command removes the value from the configuration.

Parameters *value* — Specifies the value that is the configured UDP port number used when sending syslog messages.

Values 1 **to** 65535

Platforms All

port

Syntax **port** *port*
no port

Context **[Tree]** (config>system>netconf port)

Full Context configure system netconf port

Description This command specifies the port on which the SR OS NETCONF server listens for new connections. Only one port can be configured for NETCONF management.

The configured port applies to both non-VPRN and VPRN management. New NETCONF connections are able to use the configured port. The SR OS NETCONF server errors if a port, different from the configured port, is used to SSH to the SR OS NETCONF server. For NETCONF connections not using VPRN management, active NETCONF connections are not disconnected if the port used to establish the connections is changed. For NETCONF connections using VPRN management, active NETCONF connections are disconnected if the port used to establish the connections is changed.

The **no** form of this command resets the port on which the SR OS NETCONF server listens to the default port of 830.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port* — Specifies the port on which NETCONF listens for new connections.

Values 22, 830

Default 830

Platforms All

port

Syntax **port** *tcp/udp port-number* [*mask*]
port port-list *port-list-name*
port range *tcp/udp port-number tcp/udp port-number*
no port

Context **[Tree]** (config>system>security>cpm-filter>ip-filter>entry>match port)
[Tree] (config>system>security>cpm-filter>ipv6-filter>entry>match port)

Full Context configure system security cpm-filter ip-filter entry match port
configure system security cpm-filter ipv6-filter entry match port

Description This command configures a TCP/UDP source or destination port match criterion in IPv4 and IPv6 CPM filter policies. A packet matches this criterion if packet's TCP/UDP (as configured by protocol/next-header match) source OR destination port matches either the specified port value or a port in the specified port range or port list.

This command is mutually exclusive with **src-port** and **dst-port** commands.

The **no** form of this command deletes the specified port match criterion.

Default no port

Parameters *tcp/udp port-number* — Specifies the source or destination port to be used as a match criterion specified as a decimal integer.

Values 0 to 65535

mask — Specifies the 16 bit mask to be applied when matching the port.

Values [0x0000 to 0xFFFF] | [0 to 65535] | [0b0000000000000000. to 0b1111111111111111]

range *tcp/udp port-number* — Specifies an inclusive range of source or destination port values to be used as match criteria. *start* of the range and *end* of the range are expressed as decimal integers.

Values start, end, port-number: 1 to 65535

port-list *port-list-name* — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** *port*
no port

Context **[Tree]** (config>system>security>radius port)

Full Context configure system security radius port

Description This command configures the TCP port number to contact the RADIUS server.

The **no** form of this command reverts to the default value.

Default port 1812 (as specified in RFC 2865, *Remote Authentication Dial In User Service* (*RADIUS*))

Parameters *port* — Specifies the TCP port number to contact the RADIUS server.

Values 1 to 65535

Platforms All

port

Syntax [**no**] **port** *port-number*
[**no**] **port range** *start end*

Context **[Tree]** (config>qos>match-list>port-list port)

Full Context configure qos match-list port-list port

Description This command adds a port or a range of ports to an existing port match list.

The **no** form of this command deletes the specified port or range of ports form the list.

Parameters *port-number* — Specifies the port number to add to the list. The port number can be expressed as a decimal integer, as well as in hexadecimal or binary format. Below shows decimal integer only.

Values 0 to 65535

range — Keyword specifying a range of port values.

start — Specifies the start of the port range, expressed as decimal integers, as well as in hexadecimal or binary format. The following value shows decimal integer only.

Values 0 to 65534

end — Specifies the end of the port range, expressed as decimal integers, as well as in hexadecimal or binary format. The following value shows decimal integer only.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port

Syntax **port** *port*
no port

Context **[Tree]** (config>system>grpc-tunnel>tunnel>handler port)

Full Context configure system grpc-tunnel tunnel handler port

Description This command assigns the TCP port number that the handler listens to internally.

The **no** form of this command disables the handler from listening to a TCP port.

Default no port

Parameters *port* — Specifies the TCP port number.

Values 1 to 65535

Platforms All

20.203 port-block-extensions

port-block-extensions

Syntax **port-block-extensions ports** *num-ports* **subscriber-limit** *number*
port-block-extension no ports

Context **[Tree]** (config>service>vprn>nat>outside>pool port-block-extensions)
[Tree] (config>router>nat>outside>pool port-block-extensions)

Full Context configure router nat outside pool port-block-extensions
configure service vprn nat outside pool port-block-extensions

Description This command configures a port block reserved for a dynamic NAT traffic flow for each subscriber with a port forwarding entry.

The **no** form of this command removes the values from the configuration.

Parameters *num-ports* — Specifies the size of extended port-block for L2-aware subscribers

Values 10 to 5000

number — Specifies the limit of L2-aware NAT subscribers per an outside IP address

Values 2 to 2000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.204 port-bw-oversub-factor

port-bw-oversub-factor

Syntax **port-bw-oversub-factor** *oversubscription-factor*
no port-bw-oversub-factor

Context **[Tree]** (config>qos>hs-pool-policy>mid-tier>mid-pool port-bw-oversub-factor)

Full Context configure qos hs-pool-policy mid-tier mid-pool port-bw-oversub-factor

Description This command modifies the size of the mid-pool when calculating the port-class pool sizes based on port bandwidth ratios. The command does not actually change the size of the mid-pool, only the size reported to the port-class pool sizing function.

Port-class pools can be sized in one of two ways: dynamically (proportionate to the bandwidth of each port) or explicitly (based on a percentage of the parent mid-pool). Explicit percentages require careful determination of the amount to give each pool. The dynamic sizing function attempts to automatically size each pool based on the relative amount of bandwidth each port-class pool is supporting compared to other port's port-class pools. This is accomplished by determining a dynamic weight for each port with port-class pools mapped to a given mid-pool. As true with any weighted behavior, the mid-pool buffer allocation resource is distributed in a non-oversubscribed manner to its child port-class pools. The **port-bw-oversub-factor** *oversubscription-factor* allows this distribution mechanism to become proportionally oversubscribed based on the defined factor. An oversubscription-factor of 1.5 causes the port-class pool dynamic sizes to be 1.5 times bigger, allowing for a potentially more efficient utilization of the buffers represented by mid-pool.

The **port-bw-oversub-factor** *oversubscription-factor* for a mid-pool can be modified at any time, causing the corresponding port-class pool dynamic sizes to be recalculated.

A similar behavior can be obtained by increasing the mid-pool's allocation-percent of its parent root-pool. However, the major difference in using **port-bw-oversub-factor** is that it provides larger port-class pools without allowing the mid-pool to use a higher number of buffers in the root pool.

The **no** form of the command reverts to the default.

Default port-bw-oversub-factor 1

Parameters *oversubscription-factor* — Specifies the factor by which the dynamically-sized port-class pools associated with the mid-pool may oversubscribe the mid-pool. This parameter is required when the **port-bw-oversub-factor** command is executed.

Values 1 to 10

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.205 port-control

port-control

Syntax **port-control** [**auto** | **force-auth** | **force-unauth**]

Context **[Tree]** (config>port>ethernet>dot1x port-control)

Full Context configure port ethernet dot1x port-control

Description This command configures the 802.1x authentication mode.

The **no** form of this command returns the value to the default.

Default port-control force-auth

Parameters **force-auth** — Disables 802.1x authentication and causes the port to transition to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without requiring 802.1x-based host authentication.

force-unauth — Causes the port to remain in the unauthorized state, ignoring all attempts by the hosts to authenticate. The switch cannot provide authentication services to the host through the interface.

auto — Enables 802.1x authentication. The port starts in the unauthorized state, allowing only EAPoL frames to be sent and received through the port. Both the router and the host can initiate an authentication procedure. The port will remain in unauthorized state (no traffic except EAPoL frames is allowed) until the first client is authenticated successfully. After this, traffic is allowed on the port for all connected hosts.

Platforms All

20.206 port-down

port-down

Syntax [**no**] **port-down**

Context **[Tree]** (config>subscr-mgmt>ancp>ancp-policy port-down)

Full Context configure subscriber-mgmt ancp ancp-policy port-down

Description Commands in this context configure the actions taken on port-down.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port-down

Syntax [**no**] **port-down** *port-id*

Context **[Tree]** (config>vrrp>policy>priority-event port-down)

Full Context configure vrrp policy priority-event port-down

Description This command configures a port down priority control event that monitors the operational state of a port or SONET/SDH channel. When the port or channel enters the operational down state, the event is considered set. When the port or channel enters the operational up state, the event is considered cleared.

Multiple unique **port-down** event nodes can be configured within the **priority-event** context up to the overall limit of 32 events. Up to 32 events can be defined in any combination of types.

The **port-down** command can reference an arbitrary port or channel. The port or channel does not need to be preprovisioned or populated within the system. The operational state of the **port-down** event is set as follows:

- Set – non-provisioned
- Set – not populated
- Set – down
- Cleared – up

When the port or channel is provisioned, populated, or enters the operationally up or down state, the event operational state is updated appropriately.

When the event enters the operationally down, non-provisioned, or non-populated state, the event is considered to be set. When an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instances in-use priority value. As the event transitions from cleared to set, a hold-set timer is loaded with the value configured by the events **hold-set** command. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the **hold-set** value, extending the time before another clear can take effect.

When the event enters the operationally up state, the event is considered to be cleared. Once the events **hold-set** expires, the effects of the events **priority** value are immediately removed from the in-use priority of all associated virtual router instances.

The actual effect on the virtual router instance in-use priority value depends on the defined event priority and its delta or explicit nature.

The **no** form of the command deletes the specific port or channel monitoring event. The event may be removed at anytime. When the event is removed, the in-use priority of all associated virtual router instances will be re-evaluated. The events **hold-set** timer has no effect on the removal procedure.

Default no port-down — No port down priority control events are defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id* — The port ID of the port monitored by the VRRP priority control event.

The *port-id* can only be monitored by a single event in this policy. The port can be monitored by multiple VRRP priority control policies. A port and a specific channel on the port are considered to be separate entities. A port and a channel on the port can be monitored by separate events in the same policy.

Values The following values apply to the 7750 SR:

port-id	*slot*/*mda*/*port*[.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b
	aps-id	aps-*group-id*[.*channel*]	
		aps	keyword
		group-id	1 to 64
	bundle-type-slot/mda.<bundle-num>		
		bundle	keyword
		type	ima, ppp
		bundle-num	1 to 256
	ccag-id	ccag-*id*. *path-id*[*cc-type*]	
		ccag	keyword
		id	1 to 8
		path-id	a, b
		cc-type	.sap-net, .net-sap

Values The following values apply to the 7450 ESS:

port-id	*slot*/*mda*/*port*[.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ccag-id	ccag-*id*.*path-id*[*cc-type*]		
	ccag	keyword	
	id	1 to 8	
	path-id	a, b	
	cc-type	.sap-net, .net-sap	

The POS channel on the port monitored by the VRRP priority control event. The *port-id*.*channel-id* can only be monitored by a single event in this policy. The channel can be monitored by multiple VRRP priority control policies. A port and a specific channel on the port are considered to be separate entities. A port and a channel on the port can be monitored by separate events in the same policy.

If the port is provisioned, but the *channel* does not exist or the port has not been populated, the appropriate event operational state is Set – non-populated.

If the port is not provisioned, the event operational state is Set – non-provisioned.

If the POS interface is configured as a clear-channel, the *channel-id* is 1 and the channel bandwidth is the full bandwidth of the port.

Platforms All

20.207 port-format

port-format

Syntax **port-format** *formatting*
no port-format

Context **[Tree]** (config>router>wpp>portals>portal port-format)
[Tree] (config>service>vprn>wpp>portals>portal port-format)

Full Context configure router wpp portals portal port-format
configure service vprn wpp portals portal port-format

Description This command specifies the encoding format of WPP port attribute.

The standard format is as follows:

<0 to 20 character system-name><1 character separator><2-digit slot><1-digit mda><2-digit port><4-digit top><5-digit bottom>

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

As a general rule, if a value is not present or is too large to fit in the field, is the field set to all zeros. The following rules apply to standard formats.

- With a standard port, when the separator is a "-" character, the slot is the *slot-id*, mda is the *mda-id*, and the port is the *port-id*.
- With an ESAT port, when the separator is a ":" character, the slot is the *satellite-id*, MDA is satellite *slot-id*, and the port is satellite *port-id*.
- With a PXC port, when separator is a "#" character, the MDA is the PXC *subport-id*, and the port is the PXC *port-id*.
- With a LAG port, the port is the *lag-id*.
- With a connector port, the slot is the *slot-id*, the MDA is the *mda-id*, and the port is the *connector-id*.

The vendor-specific format is as follows:

With dot1q, append "%u" with the top *vlan-id*.

With qinq, append "%u.%u" with the top *vlan-id* and the bottom *vlan-id*.

As a general rule, there can be no trailing zeros. The string truncates if it becomes too long. 0 to 16 characters are allowed for the system name. The following rules apply to vendor-specific formats.

- With a standard port, append "%s-%u/%u/%" with the *system-name*, *slot-id*, *mda-id*, and *port-id*.
- With an ESAT port, append "%s-S%u/%u/%u" with the *system-name*, *satellite-id*, *satellite-slot-id*, and *satellite-port-id*.
- With a PXC port, append "%s-P%u%c" with the *system-name*, PXC *port-id*, and PXC *subport-id* ? 'a' : 'b'.
- With a LAG port, append "%s-L%u" with the *system-name* and *lag-id*.
- With a connector port append "%s-%u%uc%u/%u" with the *system-name*, *slot-id*, *mda-id*, *connector-id*, and *connector-port-id*.

The **no** form of this command reverts to the default.

Default port-format standard

Parameters *formatting* — Specifies the encoding format of the WPP port attribute.

Values standard, vendor-specific

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.208 port-forwarding

port-forwarding

Syntax **port-forwarding**

Context **[Tree]** (config>service>nat port-forwarding)

Full Context configure service nat port-forwarding

Description Commands in this context configure NAT port forwarding parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.209 port-forwarding-dyn-block-reservation

port-forwarding-dyn-block-reservation

Syntax [**no**] **port-forwarding-dyn-block-reservation**

Context **[Tree]** (config>service>vprn>nat>outside>pool port-forwarding-dyn-block-reservation)
[Tree] (config>router>nat>outside>pool port-forwarding-dyn-block-reservation)

Full Context configure router nat outside pool port-forwarding-dyn-block-reservation
configure service vprn nat outside pool port-forwarding-dyn-block-reservation

Description This command will enable the reservation of the dynamic port blocks when the first port forward for the subscriber is created. The dynamic port bloc allocation is logged only if the block is being utilized (mapping are created). In other words, dynamic port block reservation due to the port forward creation but without any dynamic mapping, will not be logged.

The reserved port block will be released only when the last mapping in the block expires and there is not port forward associated with the subscriber. The de-allocation log (syslog or Radius) will be generated when the dynamic port block is completely released.

Dynamic port block reservation can be enabled only if the configured maximum number of subscriber per outside IP address is less or equal then the maximum number of configured port blocks per outside IP address.

Default no port-forwarding-dyn-block-reservation

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.210 port-forwarding-range

port-forwarding-range

Syntax **port-forwarding-range** *range-end*
no port-forwarding-range

Context **[Tree]** (config>service>vprn>nat>outside>pool port-forwarding-range)

Full Context configure service vprn nat outside pool port-forwarding-range

Description This command configures the end of the port range available for port forwarding. The start of the range is always equal to one.

The actual maximum value of the range end may be restricted to less than 65535 depending on the value of the objects port reservation type and port reservation value and on system specifications.

Default port-forwarding-range 1023

Parameters *range-end* — Specifies the mode of operation of this NAT pool.

Values 1023 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

port-forwarding-range

Syntax **port-forwarding-range** *range-end*
no port-forwarding-range

Context **[Tree]** (config>router>nat>outside>pool port-forwarding-range)
[Tree] (config>service>nat>nat-policy port-forwarding-range)
[Tree] (config>service>nat>firewall-policy port-forwarding-range)

Full Context configure router nat outside pool port-forwarding-range
configure service nat firewall-policy port-forwarding-range
configure service nat nat-policy port-forwarding-range

Description This command configures the end of the port range available for port forwarding. The start of the range is always equal to one.

The number of ports that can be configured is half of the available block => 64512 : 2 = 32256

In combination with port-forwarding-range the formulas are:

"max port-reservation blocks" = 65535 - "port-forwarding-range"

"max port-reservation ports" = (65535 - "port-forwarding-range") / 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

with:

the default min value for "port-forwarding-range" = 1023

Also, the same applies for max port-forwarding-range if the port-reservation is already configured:

"max port-forwarding-range" = 65535 - "port-reservation blocks"

"max port-forwarding-range" = 65535 - ("port-reservation ports" * 2)

The **no** form of the command reverts to the default.

Default port-forwarding-range 1023

Parameters *range-end* — Specifies the end of the port range available for port forwarding.

Values 1023 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.211 port-id

port-id

Syntax [**no**] **port-id**

Context **[Tree]** (config>router>if>dhcp>option>vendor-specific-option port-id)

Full Context configure router interface dhcp option vendor-specific-option port-id

Description This command enables sending of the port-id in the Nokia vendor specific suboption of the DHCP relay packet

The **no** form of this command disables the sending.

Default no port-id

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.212 port-id-subtype

port-id-subtype

Syntax **port-id-subtype** {**tx-if-alias** | **tx-if-name** | **tx-local**}

Context **[Tree]** (config>port>ethernet>lldp>dstmac port-id-subtype)

Full Context configure port ethernet lldp dest-mac port-id-subtype

Description This command specifies how to encode the PortID TLV transmit to the peer. The default setting **tx-local** (ifindex value) is required by some versions of the NSP NSM-P to properly build the Layer 2 topology map using LLDP. Changing this value to transmit the ifname (**tx-if-name**) or ifAlias (**tx-if-alias**) in place of the ifindex (**tx-local**) may affect the ability of the NSP NFM-P to build the Layer 2 topology map using LLDP.

Default port-id-subtype tx-local

Parameters **tx-if-alias** — Transmits the ifAlias String (subtype 1) that describes the port as stored in the IF-MIB, either user configured or the default entry (i.e. 10/100/Gig Ethernet SFP).

tx-if-name — Transmits the ifName string (subtype 5) that describes the port as stored in the IF-MIB ifName info.

tx-local — The interface ifIndex value (subtype 7) as the PortID.

Platforms All

20.213 port-limits

port-limits

Syntax **port-limits**

Context **[Tree]** (config>service>nat>nat-policy port-limits)
[Tree] (config>service>nat>firewall-policy port-limits)
[Tree] (config>service>nat>up-nat-policy port-limits)

Full Context configure service nat firewall-policy port-limits
configure service nat nat-policy port-limits
configure service nat up-nat-policy port-limits

Description This command configures the port limits of this policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service nat up-nat-policy port-limits
- configure service nat nat-policy port-limits

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy port-limits

20.214 port-list

port-list

Syntax **port-list** *port-list-name* [**create**]
no port-list *port-list-name*

Context **[Tree]** (config>app-assure>group port-list)

Full Context configure application-assurance group port-list

Description This command defines an AA group or partition named port-list, which contains a list of port numbers or port ranges. The port list is then referenced in AA policy app-filters, allowing increased flexibility in the use of server ports or HTTP proxy ports for application definition.

The **no** form of this command removes the list.

Parameters *port-list-name* — Specifies the name of the port list.

Default default

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

port-list

Syntax **port-list** *port-list-name* [**create**]
no port-list *port-list-name*

Context **[Tree]** (config>filter>match-list port-list)

Full Context configure filter match-list port-list

Description This command creates a list of TCP/UDP/SCTP port values or ranges for match criteria in IPv4 and IPv6 ACL and CPM filter policies.

The **no** form of this command deletes the specified list.

Operational notes:

SCTP port match is supported in ACL filter policies only.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A port-list must contain only TCP/UDP/SCTP port values or ranges.

A TCP/UDP/SCTP port match list cannot be deleted if it is referenced by a filter policy.

See general description related to match-list usage in filter policies.

Parameters *port-list-name* — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

port-list

Syntax **port-list** *port-list-name* [**create**]
no port-list *port-list-name*

Context **[Tree]** (config>qos>match-list port-list)

Full Context configure qos match-list port-list

Description This command creates a list of port values or ranges for match criteria in QoS policies.

The **no** form of this command deletes the specified list.

Parameters *port-list-name* — Specifies a port list name, up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.215 port-map

port-map

Syntax **port-map** *client-port-id* **primary** *primary-uplink-port-id* [**secondary** *secondary-uplink-port-id*]
port-map *client-port-id* **system-default**

Context **[Tree]** (config>system>satellite>eth-sat port-map)

Full Context configure system satellite eth-sat port-map

Description This command configures the mapping between a satellite client port and its associated uplink. This command allows both a primary and an optional secondary uplink to be configured.

If a secondary uplink is configured, it is used to forward traffic if the primary uplink is down for any reason.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Before an uplink can be used as either a primary or secondary uplink, it must be configured using the **port-topology** configuration command.

To return the uplink association to its default the **port-map** *client-port-id* **system-default** command should be used.

Parameters *client-port-id* — Specifies the satellite client port associated with the port mapping, in the format **esat**-*id*/*slot*/*port*.

primary-uplink-port-id — Specifies the primary satellite uplink to be associated with the associate client port, in the format **esat**-*id*/*slot*/*uport* where *id* is 1 to 20.

secondary-uplink-port-id — Specifies the secondary satellite uplink to be associated with the associate client port, in the format **esat**-*id*/*slot*/*uport* where *id* is 1 to 20.

system-default — Specifies to set the port map to the system default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.216 port-num

port-num

Syntax **port-num** *virtual-port-number*
no port-num [*virtual-port-number*]

Context **[Tree]** (config>service>vpls>sap>stp port-num)
[Tree] (config>service>vpls>spoke-sdp>stp port-num)

Full Context configure service vpls sap stp port-num
configure service vpls spoke-sdp stp port-num

Description This command configures the virtual port number which uniquely identifies a SAP within configuration bridge protocol data units (BPDUs). The internal representation of a SAP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it with its own virtual port number that is unique to every other SAP defined on the TLS. The virtual port number is assigned at the time that the SAP is added to the TLS. Since the order that the SAP was added to the TLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance.

The virtual port number cannot be administratively modified.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.217 port-overall-rate

port-overall-rate

Syntax **port-overall-rate** *packet-rate-limit* [**low-action-priority**]
no port-overall-rate

Context **[Tree]** (config>sys>security>cpu-protection port-overall-rate)

Full Context configure system security cpu-protection port-overall-rate

Description This command configures a per-port overall rate limit for CPU protection.

Default port-overall-rate max

Parameters *packet-rate-limit* — Specifies an overall per-port packet arrival rate limit in packets per second.

Values 1 to 65535, max (indicates no limit)

action-low-priority — Marks packets that exceed the rate as low-priority (for preferential discard later if there is congestion in the control plane) instead of discarding them immediately.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

20.218 port-parent

port-parent

Syntax **port-parent** [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no port-parent

Context **[Tree]** (config>qos>sap-egress>policer port-parent)

Full Context configure qos sap-egress policer port-parent

Description This command specifies whether this SAP egress policer feeds off a port-level scheduler. When configured, the policer is parented by a port-level scheduler. This requires that **policers-hqos-manageable** be configured in the SAP egress QoS policy. This command and the SAP egress policer **scheduler-parent** and the **parent** commands are mutually exclusive.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **port-parent** command defines a child/parent association between an egress policer and a port-based scheduler or between an intermediate service scheduler and a port-based scheduler. The **port-parent** command allows for a set of within-CIR and above-CIR parameters that define the port priority levels and weights for the policer. If the **port-parent** command is executed without any parameters, the default parameters are used.

In this context, the **port-parent** command and the **scheduler-parent** command (used to create a parent/child association between a queue and an intermediate scheduler) are mutually exclusive. Executing a **port-parent** command when a **scheduler-parent** definition exists causes the current intermediate scheduler association to be removed and replaced by the defined port-parent association. Executing a **scheduler-parent** command when a **port-parent** definition exists causes the port scheduler association to be removed and replaced by the defined intermediate scheduler association.

Changing the parent context on a SAP egress policy policer may cause a SAP or subscriber or a multiservice site context of the policer (policy associated with a SAP or subscriber profile or a multiservice site) to enter an orphaned state. If an instance of a policer is created on a port or channel that does not have a port scheduler enabled, and the SAP egress policy creating the policer has a port parent association, the policer will be allowed to run according to its own rate parameters and will not be controlled by a virtual scheduling context. If an instance of a policer is on a port or channel that has a port scheduler configured and the SAP egress policy defines the policer as having a non-existent intermediate scheduler parent, the policer will be treated as an orphan and will be handled according to the current orphan behavior on the port scheduler.

The **no** form of this command removes a port scheduler parent association for the policer. When removed, if a port scheduler is defined on the port on which the policer instance exists, the policer will be treated as orphaned to the port scheduler.

Default no port-parent

Parameters **weight** *weight* — Specifies the weight that the policer will use at the above-CIR port priority level (defined by the **level** parameter).

All weight values from all weighted active policers, queues, and schedulers with a common port parent are added together. Then, each individual active weight is divided by the total to determine the percentage of remaining bandwidth provided to the policer, queue, or scheduler after the higher priority level children have been serviced. A weight is considered to be active when the applicable policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit.

The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the **weight** parameter is set to a value of 0, the policer receives bandwidth only after other children with a non-zero weight at this level.

Values 0 to 100

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

level *level* — Specifies the port priority that the policer uses to receive bandwidth for its above-CIR offered load.

Values 1 to 8 (8 is the highest priority)

Default 1

cir-weight *cir-weight* — Specifies the weight that the policer uses at the within-CIR port priority level (defined by the **cir-level** parameter).

All **cir-weight** values from all weighted active policers, queues, and schedulers with a common port parent are added together. Then, each individual active weight is divided by the total to determine the percentage of remaining bandwidth provided to the policer, queue, or scheduler after the higher priority level children have been serviced. A weight is considered to be active when the applicable policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit.

The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the **cir-weight** parameter is set to a value of 0, the policer receives bandwidth only after the other children with a non-zero weight at this level.

Values 0 to 100

Default 0

cir-level *cir-level* — Specifies the port priority that the policer will use to receive bandwidth for its within-CIR offered load. If the **cir-level** parameter is set to a value of 0 (the default value), the policer does not receive bandwidth during the port schedulers within-CIR pass and the **cir-weight** parameter is ignored. If the **cir-level** parameter is 1 or greater, the **cir-weight** parameter is used.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-e, VSR

port-parent

Syntax **port-parent** [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no port-parent

Context **[Tree]** (config>qos>sap-egress>queue port-parent)

Full Context configure qos sap-egress queue port-parent

Description This command specifies whether this queue feeds off a port-level scheduler. When configured, this SAP egress queue is parented by a port-level scheduler. This object is mutually exclusive with SAP egress queue parent. Only one kind of parent is allowed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **port-parent** command defines a child/parent association between an egress queue and a port-based scheduler or between an intermediate service scheduler and a port-based scheduler. The **port-parent** command allows for a set of within-CIR and above-CIR parameters that define the port priority levels and weights for the queue or scheduler. If the **port-parent** command is executed without any parameters, the default parameters are assumed.

In this context, the **port-parent** command is mutually exclusive to the **parent** command (used to create a parent/child association between a queue and an intermediate scheduler). Executing a **port-parent** command when a parent definition is in place causes the current intermediate scheduler association to be removed and replaced by the defined port-parent association. Executing a **parent** command when a port-parent definition exists causes the port scheduler association to be removed and replaced by the defined intermediate scheduler name.

Changing the parent context on a SAP egress policy queue may cause a SAP or subscriber or multiservice site context of the queue (policy associated with a SAP or subscriber profile or multiservice site) to enter an orphaned state. If an instance of a queue is created on a port or channel that does not have a port scheduler enabled and the sap-egress policy creating the queue has a port-parent association, the queue will be allowed to run according to its own rate parameters and will not be controlled by a virtual scheduling context. If an instance of a queue is on a port or channel that has a port scheduler configured and the sap-egress policy defines the queue as having a non-existent intermediate scheduler parent, the queue will be treated as an orphan and will be handled according to the current orphan behavior on the port scheduler.

The **no** form of this command removes a port scheduler parent association for the queue or scheduler. If a port scheduler is defined on the port on which the queue or scheduler instance exists, the queue or scheduler will become orphaned if an port scheduler is configured on the egress port of the queue or scheduler.

Default no port-parent

Parameters **weight** *weight* — Specifies the weight the queue or scheduler will use at the above-CIR port priority level (defined by the level parameter).

Values 0 to 100

Default 1

level *level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its above-CIR offered-load.

Values 1 to 8 (8 is the highest priority)

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-weight *cir-weight* — Specifies the weight the queue or scheduler will use at the within-CIR port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 100

Default 0

cir-level *cir-level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its within-CIR offered-load. If the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms All

port-parent

Syntax **port-parent** [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no port-parent

Context **[Tree]** (config>qos>network-queue>queue port-parent)

Full Context configure qos network-queue queue port-parent

Description This command specifies whether this queue feeds off a port-level scheduler. For the network-queue policy context, only the port-parent command is supported. When a port scheduler exists on the port, network queues without a port-parent association will be treated as an orphan queue on the port scheduler and treated according to the current orphan behavior on the port scheduler. If the port-parent command is defined for a network queue on a port without a port scheduler defined, the network queue will operate as if a parent association does not exist. When a port scheduler policy is associated with the egress port, the port-parent command will come into effect.

When a network-queue policy is associated with an FP for ingress queue definition, the port-parent association of the queues is ignored.

The **no** form of this command removes a port scheduler parent association for the queue or scheduler. If a port scheduler is defined on the port then the queue or scheduler instance exists, the queue or scheduler will become orphaned.

Default no port-parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **weight** *weight* — Specifies the weight the queue or scheduler will use at the above-CIR port priority level (defined by the level parameter).

Values 0 to 100

Default 1

level *level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its above-CIR offered-load.

Values 1 to 8 (8 is the highest priority)

Default 1

cir-weight *cir-weight* — Specifies the weight the queue or scheduler will use at the within-CIR port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0, the queue or scheduler does not receive bandwidth during the port scheduler's within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter is used.

Values 0 to 100

Default 0

cir-level *cir-level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its within-CIR offered-load. If the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port scheduler's within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms All

port-parent

Syntax **port-parent** [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no port-parent

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue port-parent)

Full Context configure qos queue-group-templates egress queue-group queue port-parent

Description This command defines the port scheduling parameters used to control the queue's behavior when a virtual egress port scheduling is enabled where the egress queue group template is applied. The **port-parent** command follows the same behavior and provisioning characteristics as the **parent** command in the SAP egress QoS policy. The **port-parent** command and the **parent** command are mutually exclusive.

The **no** form of this command removes the values from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default none

Parameters **weight** *weight* — Specifies the weight the queue or scheduler will use at the above-CIR port priority level (defined by the level parameter).

Values 0 to 100

Default 1

level *level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its above-CIR offered-load.

Values 1 to 8 (8 is the highest priority)

Default 1

cir-weight *cir-weight* — Specifies the weight the queue or scheduler will use at the within-CIR port priority level (defined by the **cir-level** parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the **cir-weight** parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the **cir-level** parameter is ignored. If the **cir-weight** parameter is 1 or greater, the **cir-level** parameter is used.

Values 0 to 100

Default 0

cir-level *cir-level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its within-CIR offered-load. If the **cir-weight** parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-CIR pass and the **cir-level** parameter is ignored. If the **cir-weight** parameter is 1 or greater, the **cir-level** parameter is used.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms All

port-parent

Syntax **port-parent** [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no port-parent

Context **[Tree]** (config>qos>scheduler-policy>tier>scheduler port-parent)

Full Context configure qos scheduler-policy tier scheduler port-parent

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **port-parent** command defines a child/parent association between an egress scheduler and a port-based scheduler, or between an intermediate service scheduler and a port-based scheduler. The **port-parent** command allows for a set of within-CIR and above-CIR parameters that define the port priority levels and weights for the scheduler. If the **port-parent** command is executed without any parameters, the default parameters are assumed.

In this context, the **port-parent** command and the **parent** command (used to create a parent/child association to an intermediate scheduler) are mutually exclusive. Executing a **port-parent** command when a parent definition is in place causes the current intermediate scheduler association to be removed and replaced by the defined port-parent association. Executing a **parent** command when a port-parent definition exists causes the port scheduler association to be removed and replaced by the defined intermediate scheduler name.

Changing the parent context on a SAP egress policy policer or queue may cause a SAP or subscriber context of the policer or queue (policy associated with a SAP or subscriber profile) to enter an orphaned state. If an instance of a policer or queue is created on a port or channel that does not have a port scheduler enabled and the sap-egress policy creating the policer queue has a port-parent association, the policer or queue will be allowed to run according to its own rate parameters and will not be controlled by a virtual scheduling context. If an instance of a policer or queue is on a port or channel that has a port scheduler configured and the sap-egress policy defines the policer or queue as having a non-existent intermediate scheduler parent, the policer or queue will be treated as an orphan and will be handled according to the current orphan behavior on the port scheduler.

The **no** form of this command removes a port scheduler parent association for the scheduler. If a port scheduler is defined on the port that the scheduler instance exists, the scheduler will become orphaned if an port scheduler is configured on the egress port of the queue or scheduler.

Default no port-parent

Parameters **weight** *weight* — Specifies the weight the queue or scheduler will use at the above-CIR port priority level (defined by the **level** parameter).

Values 0 to 100

Default 1

level *level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its above-CIR offered-load.

Values 1 to 8 (8 is the highest priority)

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-weight *cir-weight* — Specifies the weight the queue or scheduler will use at the within-CIR port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the **cir-weight** parameter is set to a value of 0, the queue or scheduler does not receive bandwidth during the port scheduler's within-CIR pass and the **cir-level** parameter is ignored. If the **cir-weight** parameter is 1 or greater, the **cir-level** parameter comes into play.

Values 0 to 100

Default 0

cir-level *cir-level* — Specifies the port priority the queue or scheduler will use to receive bandwidth for its within-CIR offered-load. If the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port scheduler's within-CIR pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms All

20.219 port-policy

port-policy

Syntax **port-policy** [*port-policy*]
no port-policy

Context **[Tree]** (config>isa>wlan-gw-group port-policy)

Full Context configure isa wlan-gw-group port-policy

Description This command configures the port policy of this WLAN Gateway ISA group. If a port policy is associated with a WLAN Gateway ISA group, ports created for this group can take applicable configuration from that port policy. This port policy is applicable to those ports that take part in the per-tunnel QoS processing.

The **no** form of the command removes the **port-policy** name from the configuration.

Default no port-policy

Parameters *port-policy* — Specifies the port policy of this WLAN Gateway ISA group, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port-policy

Syntax **port-policy** *port-policy-name* [**create**]
no port-policy *port-policy-name*

Context **[Tree]** (config port-policy)

Full Context configure port-policy

Description This command either creates a new port-policy with create parameter or enters the configuration context of an existing port-policy.

The **no** form of this command removes the port policy name from the configuration.

Parameters *port-policy-name* — Specifies the name of *port-policy* up to 32 characters.

create — Creates the port-policy instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

port-policy

Syntax **port-policy** *policy-name*
no port-policy

Context **[Tree]** (config>isa>lns-group port-policy)

Full Context configure isa lns-group port-policy

Description This command enables policies referenced in the **config>port-policy** context to be created under **ports**. These are the ports that link the carrier IOM to the ISA, and are hidden within the system (they cannot be created through the CLI). They are created automatically. Use the **show port** command to view information.

Currently only the port scheduler policy is supported. Each lns-esm port in the lns-group receives an independent port scheduler instance. The port schedulers are instantiated in the carrier IOM on the lns-esm ports that carry PPPoE traffic in the downstream direction towards the ISA before the PPPoE traffic is L2TP encapsulated.

The **no** form of the command removes the policy name from the configuration.

Default no port-policy

Parameters *policy-name* — Specifies the port policy of this LNS group, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.220 port-range-block

port-range-block

Syntax [**no**] **port-range-block**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes port-range-block)

Full Context configure aaa isa-radius-policy acct-include-attributes port-range-block

Description This command enables the inclusion of the NAT port range block attributes.

The **no** form of the command excludes NAT port range block attributes.

Default no port-range-block

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.221 port-recorder

port-recorder

Syntax [**no**] **port-recorder**

Context **[Tree]** (debug>app-assure>group port-recorder)

Full Context debug application-assurance group port-recorder

Description This commands allows to stop or start the http-host-recorder. To reset the recorded values execute shutdown followed by **no** shutdown.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.222 port-redirect-group

port-redirect-group

Syntax **port-redirect-group** {**queue** *queue-id* | **policer** *policer-id* [**queue** *queue-id*]}
no port-redirect-group

Context **[Tree]** (config>qos>network>egress>fc port-redirect-group)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos network egress fc port-redirect-group

Description This command is used to redirect the FC of a packet of a pseudowire (PW) or network IP interface to an egress port queue group.

It defines the mapping of an FC to a queue ID or a policer ID and a queue ID and redirects the lookup of the queue or policer of the same ID in some egress port queue-group instance. However, the queue-group name and instance are explicitly provided only at the time the network QoS policy is applied to egress context of a spoke-sdp or a network IP interface.

The **no** version of this command removes the redirection of the FC.

Parameters *queue-id* — This parameter must be specified when executing the **port-redirect-group** command. The specified *queue-id* must exist within the egress port queue group on each IP interface where the network QoS policy is applied.

Values 1 to 8

policer id — The specified policer-id must exist within the queue-group template applied to the ingress context of the forwarding plane.

Values 1 to 8

Platforms All

20.223 port-reservation

port-reservation

Syntax **port-reservation blocks** *num-blocks*
port-reservation ports *num-ports*
no port-reservation

Context **[Tree]** (config>service>vprn>nat>outside>pool port-reservation)
[Tree] (config>router>nat>outside>pool port-reservation)

Full Context configure router nat outside pool port-reservation
configure service vprn nat outside pool port-reservation

Description This command configures the size of the port-block that will be assigned to a host that is served by this pool. The number of ports configured are available to UDP, TCP and ICMP (as identifiers).

Parameters *num-blocks* — Specifies the number of port-blocks per IP address. Setting this parameter to one (1) for large scale NAT enables 1:1 NAT for IP addresses in this pool.

Values 1 to 64512

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

num-ports — Specifies the number of ports per block.

Values 1 to 32256

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

port-reservation

Syntax **port-reservation** *num-ports*
no port-reservation

Context **[Tree]** (config>router>nat>outside>pool>deterministic port-reservation)
[Tree] (config>service>vprn>nat>outside>pool>deterministic port-reservation)

Full Context configure router nat outside pool deterministic port-reservation
configure service vprn nat outside pool deterministic port-reservation

Description This command is applicable only to deterministic NAT. It configures the number of deterministic ports per subscriber (for example a subscriber is an inside IP address in LSN44 or IPv6 address or prefix in DS-Lite). Once this command is enabled, the pool will transition into deterministic mode of operation. This means that the subscribers can use dynamic port-blocks in the pool only as a mean to expand the range of originally assigned deterministic ports. A pool with such property is referred to as deterministic pool. However, deterministic NAT and non-deterministic NAT cannot use the same pool simultaneously.

All subscribers in deterministic pool are pre-mapped during the configuration phase to outside IP addresses and deterministic port-blocks. Because of this, the deterministic pool cannot be oversubscribed with subscribers (first-come, first-served).

Once the deterministic pool becomes operational (no shutdown) a log is created. The same applies if the pool is disabled (shutdown). As a result of this one-time logging, there will be no additional logging when a subscriber starts using ports from the pre-assigned deterministic port block. This drastically reduces the logging overhead. However, when a deterministic port block is expanded by a dynamic port block, a log will be created on any allocation/ de-allocation of the dynamic port block. The logs are also created for static port forwards (including PCP).

The number of subscribers per outside IP address (subscriber-limit) multiplied by the number of deterministic ports per subscriber (port-reservation) will determine the port range of an outside IP address that will be dedicated to deterministic mappings. The number of subscribers per outside IP address in deterministic NAT must be power of 2 (2^n). Once the deterministic ports are allocated, the dynamic ports are carved out of the remaining port space of the same outside IP address according to the existing **port-reservation** command under the same hierarchy,

Parameters *num-ports* — Specifies the number of ports in a deterministic port block that is allocated and dedicated to a single subscribers during the configuration phase.

Values 1 to 65536

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port-reservation

Syntax [**no**] **port-reservation**

Context **[Tree]** (config>service>nat>pcp-server-policy>option port-reservation)

Full Context configure service nat pcp-server-policy option port-reservation

Description This command enables/disables support for the **port-reservation** option.

Default no port-reservation

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.224 port-role

port-role

Syntax [**no**] **port-role**

Context **[Tree]** (debug>service>id>stp port-role)

Full Context debug service id stp port-role

Description This command enables STP debugging for changes in port roles.

Platforms All

20.225 port-scheduler-policy

port-scheduler-policy

Syntax **port-scheduler-policy** *port-scheduler-policy-name*
no port-scheduler-policy

Context **[Tree]** (config>port>ethernet>access>egress>vport port-scheduler-policy)

Full Context configure port ethernet access egress vport port-scheduler-policy

Description This command specifies the destination and organization strings to be used for matching subscriber hosts with this Vport.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The parent Vport of a subscriber host queue, which has the port-parent option enabled, is determined by matching the destination string dest string associated with the subscriber and the organization string org string associated with the subscriber host with the strings defined under a Vport on the port associated with the subscriber.

If a given subscriber host policers or queue does not have the port-parent option enabled, it is foster-parented to the Vport used by this subscriber and which is based on matching the dest string and org string. If the subscriber could not be matched with a Vport on the egress port, the host policer or queue will not be bandwidth controlled and competes for bandwidth directly based on its own PIR and CIR parameters.

By default, a subscriber host policer or queue with the port-parent option enabled is scheduled within the context of the port's port scheduler policy.

The **agg-rate rate**, **port-scheduler-policy** and **scheduler-policy** commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an **agg-rate** or **port-scheduler-policy** involves removing the existing command and applying the new command. Applying a scheduler policy to a Vport is only applicable to Ethernet interfaces.

The **no** form of this command removes the *port-scheduler-policy-name* from the configuration.

The **agg-rate** *rate*, **port-scheduler-policy** and **scheduler-policy** commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an **agg-rate**/ **port-scheduler-policy** involves removing the existing command and applying the new command.

The **no** form of this command reverts to the default.

Parameters *port-scheduler-policy-name* — Specifies an existing **port-scheduler-policy** configured in the **config>qos** context.

Platforms All

port-scheduler-policy

Syntax **port-scheduler-policy** *port-scheduler-policy-name*
no port-scheduler-policy

Context **[Tree]** (config>port>sonet-sdh>path>access>egress>vport port-scheduler-policy)

Full Context configure port sonet-sdh path access egress vport port-scheduler-policy

Description This command specifies the destination and organization strings to be used for matching subscriber hosts with this Vport.

The parent Vport of a subscriber host queue, which has the port-parent option enabled, is determined by matching the destination string dest string associated with the subscriber and the organization string *org* string associated with the subscriber host with the strings defined under a Vport on the port associated with the subscriber.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a given subscriber host queue does not have the port-parent option enabled, it will be foster-parented to the Vport used by this subscriber and which is based on matching the *dest* string and *org* string. If the subscriber could not be matched with a Vport on the egress port, the host queue will not be bandwidth controlled and will compete for bandwidth directly based on its own PIR and CIR parameters.

By default, a subscriber host queue with the port-parent option enabled is scheduled within the context of the port's port scheduler policy.

The no form of this command removes the port-scheduler-policy-name from the configuration. The **agg-rate** *rate*, **port-scheduler-policy** and **scheduler-policy** commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an agg-rate/port-scheduler-policy involves removing the existing command and applying the new command.

Parameters *port-scheduler-policy-name* — Specifies an existing port-scheduler-policy configured in the config>qos context. The name can be up to 32 characters long.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

port-scheduler-policy

Syntax **port-scheduler-policy** *port-scheduler-policy-name*
no port-scheduler-policy

Context **[Tree]** (config>isa>aa-grp>qos>egress>from-subscriber port-scheduler-policy)
[Tree] (config>isa>aa-grp>qos>egress>to-subscriber port-scheduler-policy)

Full Context configure isa application-assurance-group qos egress from-subscriber port-scheduler-policy
configure isa application-assurance-group qos egress to-subscriber port-scheduler-policy

Description This command assigns an existing port scheduler policy as applicable to the specific application assurance group traffic.

Default no port-scheduler-policy

Parameters *port-scheduler-policy-name* — Specifies the name of an existing port scheduler policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

port-scheduler-policy

Syntax **port-scheduler-policy** *port-scheduler-name* [**create**]
no port-scheduler-policy *port-scheduler-name*

Context **[Tree]** (config>qos port-scheduler-policy)

Full Context configure qos port-scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When a port scheduler has been associated with an egress port, it is possible to override the following parameters:

- The max-rate allowed for the scheduler
- The maximum rate for each priority level (1 to 8)
- The cir associated with each priority level (1 to 8)

The orphan priority level (level 0) has no configuration parameters and cannot be overridden.

The **no** form of this command removes a port scheduler policy from the system. If the port scheduler policy is associated with an egress port or channel, the command will fail.

Parameters *port-scheduler-name* — Specifies an existing port scheduler name. Each port scheduler must be uniquely named within the system and can be up to 32 ASCII characters.

Platforms All

port-scheduler-policy

Syntax **port-scheduler-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy port-scheduler-policy)

Full Context configure qos copy port-scheduler-policy

Description This command copies existing QoS policy entries for a QoS policy to another QoS policy.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

If **overwrite** is not specified, an error will occur if the destination policy exists.

Parameters *src-name dst-name* — Indicates that the source policy and the destination policy are port scheduler policy IDs. Specify the source policy that the copy command will attempt to copy from and specify the destination policy name to which the command will copy a duplicate of the policy.

overwrite — Forces the destination policy name to be copied as specified. When forced, everything in the existing destination policy will be completely overwritten with the contents of the source policy.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.226 port-set

port-set

Syntax [**no**] **port-set**

Context **[Tree]** (config>service>nat>pcp-server-policy>option port-set)

Full Context configure service nat pcp-server-policy option port-set

Description This command enables PORT_SET option support. When this command is disabled, the PCP uses a plain MAP option to allocate a single port at a time. This is default behavior. Instead of asking for each individual port in multiple requests through the MAP option, this **port-set** option allows individual ports to ask the SR OS for a set of ports at once in a single request.

The **no** form of this command disables PORT_SET option support.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.227 port-state

port-state

Syntax [**no**] **port-state**

Context **[Tree]** (debug>service>id>stp port-state)

Full Context debug service id stp port-state

Description This command enables STP debugging for port states.

The **no** form of the command disables debugging.

Platforms All

20.228 port-template

port-template

Syntax **port-template** *template-name* **sat-type** *sat-type* [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no port-template *template-name*

Context [Tree] (config>system>satellite port-template)

Full Context configure system satellite port-template

Description This command creates a new port template context to define the port usage for a specific satellite type. A port template is specific to the specified satellite type. Port templates must be configured separately using different template names for each different satellite chassis type.

The **no** form of this command deletes the specified port template.

Parameters *template-name* — Specifies the name for the associated port template. This value must be unique in the network.

sat-type — Specifies the type of satellite chassis associated with the port-template.

Values es24-1gb-sfp, es24-1gb-tx, es24-sass-1gb-sfp, es48-1gb-sfp, es48-1gb-tx, es48-sass-1gb-sfp, es64-10gb-sfpp+4-100gb-cfp4, es24-sasmxp-1gb-sfp

create — Creates a new port template.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.229 port-threshold

port-threshold

Syntax **port-threshold** *value* [**action** {**dynamic-cost** | **static-cost** | **down**}] [**cost** *static-cost*]
no port-threshold

Context [Tree] (config>lag port-threshold)

Full Context configure lag port-threshold

Description This command configures the behavior for the Link Aggregation Group (LAG) if the number of operational links is equal to or below a threshold level.

Nokia recommends that operators use the **weight-threshold** or **hash-weight-threshold** command instead of the **port-threshold** command to control LAG operational status. For example, when 10GE and 100GE ports are mixed in a LAG, each 10GE port will have a weight of 1, while each 100GE port will have a weight of 10.

The **weight-threshold** or **hash-weight-threshold** command can also be used for LAGs with all ports of equal speed to allow a common operational model. For example, each port has a weight of 1 to mimic **port-threshold** and its related configuration.

The **no** form of this command reverts to the default values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default port-threshold 0 action down

Parameters *value* — Specifies the decimal integer threshold number of operational links for the LAG at or below which the configured action is invoked. If the number of operational links exceeds the **port-threshold** value, any action taken for being below the threshold value will cease.

Values 0 to 63

action — Specifies the action to take if the number of active links in the LAG is at or below the threshold value.

dynamic-cost — Specifies that dynamic costing is activated. As a result, the LAG remains operationally up with a cost relative to the number of operational links. The link is only regarded as operationally down when all links in the LAG are down.

static-cost — Specifies that static costing is activated. As a result, the LAG remains operationally up with the configured cost, regardless of the number of operational links. The link is only regarded as operationally down when all links in the LAG are down.

down — Specifies that LAG is brought operationally down if the number of operational links is equal to or less than the configured threshold value. The LAG is only regarded as up once the number of operational links exceeds the configured threshold value.

static-cost — Specifies decimal integer static cost of the LAG.

Values 1 to 16777215

Platforms All

20.230 port-topology

port-topology

Syntax **port-topology**

Context **[Tree]** (config>system port-topology)

Full Context configure system port-topology

Description This parameter creates or edits the context to configure intra-node port connections.

Default disabled

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.231 port-type

port-type

Syntax **port-type** *lag-port-type*
no port-type

Context **[Tree]** (config>lag port-type)

Full Context configure lag port-type

Description This command configures the port type for the link aggregation group.

The **no** form of this command reverts to the default.

Default port-type standard

Parameters *lag-port-type* — Specifies the type of ports allowed in this LAG.

Values standard — Allows all non-HS type ports to be added to this LAG
hs — Limits the LAG members to be HSQ IOMs (iom4-e-hs) ports

Platforms 7750 SR-7/12/12e

20.232 port-weight-speed

port-weight-speed

Syntax **port-weight-speed** *gbps*
no port-weight-speed

Context **[Tree]** (config>lag port-weight-speed)

Full Context configure lag port-weight-speed

Description This command enables mixed port-speed LAG operation.

Parameter specified with the command defines what type of ports are allowed in a LAG, and what is the weight of each port for total LAG weight calculation.

The **no** form specifies that all LAG links must be of the same speed. Each link weight is 1. The **no** form disables mixed port-speed LAG operation if there are no mixed-speed links. Issuing this command automatically checks that all links are the same speed and re-calibrates the link weights. If all links are not the same speed, **no-port-weight-speed** is rejected.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no port-weight-speed

Parameters *gbps* — The port weight speed in Gigabits per second.

Values 1, 10

port-weight-speed 1 — LAG supports any mix of 1GE, 10GE ports up to a total weight of 64 (for 64 link LAGs) or 32 (for 32 link LAGs). Each 1 GE port has a weight of 1; each 10GE port has a weight of 10.

port-weight-speed 10 — LAG supports any mix of 10GE, 40GE, 100GE ports up to a total weight of 64 (for 64 link LAGs) or 32 (for 32 link LAGs). Each 10 GE port has a weight of 1; each 40GE port has a weight of 4; each 100GE port has a weight of 10.

For existing LAGs:

no port-weight-speed can be changed to **port-weight-speed 1** when the LAG consists of only 1GE links. **no port-weight-speed** can be changed to **port-weight-speed 10** when the LAG consists of only 10GE links.

port-weight-speed 1 or **port-weight-speed 10** can be changed to **no port-weight-speed** in service, when all links of the LAG are 1GE, 10GE, 40GE, or 100GE.

All other configuration changes require shutdown of the LAG and removal of all ports first.

Platforms All

20.233 port-xc

port-xc

Syntax **port-xc**

Context **[Tree]** (config port-xc)

Full Context configure port-xc

Description Commands in this context configure port-cross connect functionality.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.234 port1

port1

Syntax **port1** {**eq** | **neq**} *port-num*
no port1

Context **[Tree]** (debug>app-assure>group>traffic-capture>match port1)

Full Context debug application-assurance group traffic-capture match port1

Description This command configures debugging on port 1.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.235 port2

port2

Syntax **port2** {**eq** | **neq**} *port-num*
no port2

Context **[Tree]** (debug>app-assure>group>traffic-capture>match port2)

Full Context debug application-assurance group traffic-capture match port2

Description This command configures debugging on port 2.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.236 portal

portal

Syntax **portal router** *router-instance* **name** *wpp-portal-name*
no portal

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>wpp portal)
[Tree] (config>service>ies>sub-if>grp-if>wpp portal)
[Tree] (config>service>vprn>sub-if>grp-if>wpp portal)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface group-interface wpp portal
configure service vprn subscriber-interface group-interface wpp portal
configure subscriber-mgmt local-user-db ipoe host wpp portal

Description This command specifies the web portal server that system talks to for the hosts on the group-interface. This command is mutually exclusive with the **portal-group** command.

The **no** form of this command removes the router instance or portal name from the configuration.

Parameters *router-instance* — Specifies the virtual router instance.

Values

router-name:	Base, management
service-id:	1 to 2147483647
service-name:	Specifies the service name up to 64 characters

Default Base

wpp-portal-name — Specifies the name of the web portal server up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

portal

Syntax [**no**] **portal router** *router-instance* **name** *wpp-portal-name*

Context **[Tree]** (config>aaa>wpp>portal-groups>portal-group portal)

Full Context configure aaa wpp portal-groups portal-group portal

Description This command configures the portal for this portal group.

Parameters *router-instance* — Specifies the virtual router instance.

Values

router-name:	Base, management
service-id:	1 to 2147483647
service-name:	Specifies the service name up to 64 characters

Default Base

wpp-portal-name — Specifies the name of the web portal server up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

portal

Syntax [**no**] **portal** *wpp-portal-name*

Context **[Tree]** (debug>router>wpp portal)

Full Context debug router wpp portal

Description This command enables WPP debugging for the specified WPP portal.

Parameters *wpp-portal-name* — Specifies the WPP portal name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

portal

Syntax [**no**] **portal**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query>state portal)

Full Context configure subscriber-mgmt wlan-gw ue-query state portal

Description This command enables matching on UEs in a portal state.

The **no** form of this command disables matching on UEs in a portal state, unless all state matching is disabled.

Default no portal

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.237 portal-group

portal-group

Syntax **portal-group** *portal-group-name*
no portal-group

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>wpp portal-group)

Full Context configure subscriber-mgmt local-user-db ipoe host wpp portal-group

Description This command configures the WPP portal group name. This command is mutually exclusive with the **portal** command.

Parameters *portal-group-name* — Specifies the WPP portal group name, up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

portal-group

Syntax **portal-group** *portal-group-name* [**create**]
no portal-group *portal-group-name*

Context **[Tree]** (config>aaa>wpp>portal-groups portal-group)

Full Context configure aaa wpp portal-groups portal-group

Description This command creates a new portal group or enters the configuration context of an existing port group.

Parameters *portal-group-name* — Specifies the portal group name up to 32 characters.

create — Keyword required to create the configuration context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

portal-group

Syntax **portal-group** *portal-group-name*
no portal-group

Context **[Tree]** (config>service>ies>sub-if>grp-if>wpp portal-group)
[Tree] (config>service>vprn>sub-if>grp-if>wpp portal-group)

Full Context configure service ies subscriber-interface group-interface wpp portal-group
configure service vprn subscriber-interface group-interface wpp portal-group

Description This command specifies the WPP portal group for the subscriber interface. This command is mutually exclusive with the **portal** command.

The **no** form of this command removes the name from the service configuration.

Parameters *portal-group-name* — Specifies the portal group name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.238 portal-groups

portal-groups

Syntax **portal-groups**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>aaa>wpp portal-groups)

Full Context configure aaa wpp portal-groups

Description Commands in this context configure portal group parameters for WPP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.239 portal-hold-time

portal-hold-time

Syntax **portal-hold-time** *seconds*
no portal-hold-time

Context [Tree] (config>subscr-mgmt>http-rdr-plcy portal-hold-time)

Full Context configure subscriber-mgmt http-redirect-policy portal-hold-time

Description This command configures the time for which the forwarding state applicable during redirect phase is held in the system, after the user has been authenticated on the portal. This allows the HTTP response from the portal to be forwarded back on the existing connection.

Parameters *seconds* — Specifies how long the system holds on to re-direct forwarding resources of a subscriber, after it has left the re-direct portal.

Values 1 to 60

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.240 portals

portals

Syntax **portals**

Context [Tree] (config>router>wpp portals)
[Tree] (config>service>vprn>wpp portals)

Full Context configure router wpp portals
configure service vprn wpp portals

Description Commands in this context configure WPP portal server parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.241 ports

ports

Syntax **ports**

Context **[Tree]** (config>qos>fp-resource-policy ports)

Full Context configure qos fp-resource-policy ports

Description This command enters the ports context.

Platforms 7750 SR-1, 7750 SR-s

20.242 post-policer-mapping

post-policer-mapping

Syntax **post-policer-mapping** *mapping-policy-name* [**create**]
no post-policer-mapping *mapping-policy-name*

Context **[Tree]** (config>qos post-policer-mapping)

Full Context configure qos post-policer-mapping

Description This command configures a post-policer mapping policy which is used to remap a packet's forwarding class and profile state to another forwarding class and profile state for post-policer traffic.

A post-policer mapping policy is created without any forwarding class or profile remapping statements. If an empty policy is applied to a SAP-egress QoS policy, no remapping occurs.

The **no** form of this command deletes the post-policer mapping policy. A post-policer mapping policy can only be deleted if there are no references to it.

Parameters *mapping-policy-name* — Specifies the name of the post-policer mapping policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

post-policer-mapping

Syntax **post-policer-mapping** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy post-policer-mapping)

Full Context configure qos copy post-policer-mapping

Description This command copies an existing post-policer mapping policy to another policy name.

The copy command is used to create new policies using existing policies and also allows bulk modifications to an existing policy with the use of the overwrite keyword.

Parameters *src-name* — Specifies the source policy name that the copy command attempts to copy from.

dst-name — Specifies the destination policy name to which the command copies a duplicate of the policy.

overwrite — Specifies that the existing destination policy is to be replaced. Everything in the existing destination policy is overwritten with the contents of the source policy. If overwrite is not specified, an error occurs if the destination policy name exists.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

post-policer-mapping

Syntax **post-policer-mapping** *mapping-policy-name*
no post-policer-mapping

Context **[Tree]** (config>qos>sap-egress post-policer-mapping)

Full Context configure qos sap-egress post-policer-mapping

Description This command applies a post-policer mapping policy in a SAP egress QoS policy. The policy contains forwarding class and profile remapping statements, which remap the forwarding class and profile state of an egress policed packet (the profile being the resulting profile after the packet has been processed by the egress policer) to another forwarding class and profile.

The remapping applies to all policers within the SAP egress QoS policy, including regular child policers and policers configured in an IP/IPv6 criteria action statement, except for dynamic policers.

Post-policer mapping is supported on FP3- and higher-based hardware, with the exception of the 7750 SR-a4/a8, which does not support egress policers resulting in the policy being ignored.

The **no** form of this command deletes the post-policer mapping policy from the SAP egress QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mapping-policy-name* — Specifies the name of the post-policer mapping policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.243 power

power

Syntax **power** *power-state*

Context **[Tree]** (config>system>bluetooth power)

Full Context configure system bluetooth power

Description This command sets the operating mode of the Bluetooth module. This can be powered off or powered on but requires the pairing button to initiate the pairing operation, or powered on and continuously pairing.

The **pairing-button** setting also impacts how pairing operations work.

Default power off

Parameters *power-state* — Specifies the power state.

Values off — Bluetooth radio disabled

enabled-manual — Bluetooth enabled (pairing requires the use of the pairing button)

enabled-automatic — Bluetooth is enabled and continuously attempts to pair whenever it is not actively paired to a device

Platforms 7750 SR-1, 7750 SR-s

20.244 power-priority-level

power-priority-level

Syntax **power-priority-level** *priority*
no power-priority-level

Context **[Tree]** (config>card>mda power-priority-level)
[Tree] (config>card>xiom>mda power-priority-level)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure card mda power-priority-level
configure card xiom mda power-priority-level

Description This command sets the power priority value for an XMA or MDA-s on platforms that support intelligent power management.

Default power-priority-level 150

Parameters *priority* — Specifies the power priority level. An operator must assign a priority value to each XMA or MDA-s using a range of number from 1 to 200. The lowest number has the highest priority. The priority number range from 1 to 100 should be used for modules considered essential for system operation. Lower priority values of 101 to 200 should be used for non-essential modules.

Values 1 to 200

Platforms 7750 SR-s

- configure card xiom mda power-priority-level

7750 SR-s, 7950 XRS

- configure card mda power-priority-level

20.245 power-safety-alert

power-safety-alert

Syntax **power-safety-alert** *wattage*

Context **[Tree]** (config>system>pwr-mgmt power-safety-alert)

Full Context configure system power-management power-safety-alert

Description This command sets a value in watts for the Power Safety Alert. The Power Safety Alert minor alarm is generated when the system power capacity drops below the Power Safety Level (in watts) plus the Power Safety Alert. This is a critical level, which when breached the system starts shutting down IO cards based on card priority. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Parameters *wattage* — Specifies the number of watts for the power safety alert level.

Values 0 to 102600

Default 0

Platforms 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.246 power-safety-level

power-safety-level

Syntax **power-safety-level** *percent*

Context **[Tree]** (config>system>pwr-mgmt power-safety-level)

Full Context configure system power-management power-safety-level

Description This command sets the Power Safety Level, which is a percentage of the calculated worst case power draw value. Once a Power Safety Level is configured by the operator, both the Basic and Advanced modes use the Power Safety Level as a reference for calculating the power redundancy using N+1 algorithm during startup and recovery from power depression. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Default power-safety-level 100

Parameters *percent* — Specifies the Power Safety Level as a percentage of the calculated worst case power draw value.

Values 0 to 100

Platforms 7750 SR-s, 7950 XRS

20.247 power-save

power-save

Syntax [**no**] **power-save**

Context **[Tree]** (config>card power-save)

Full Context configure card power-save

Description This command enables power-save mode on a specific card when it is not in use. Power-save mode allows a card to be installed and configured in a platform for future use, while having minimal impact on the overall power consumption. The card placed in power-save mode is forced into an idle state to consume minimal power. This command resets the card and then disallows the download of a software image when the card comes back up. To enable power-save mode, the desired card must first be shut down, then placed into power-save mode. In this mode, the card is not counted in the intelligent power management budget. Cards set to power-save mode do not pass traffic.

The **no** form of this command removes the card from power-save mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no power-save

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-2e, 7750 SR-2s, 7750 SR-3e, 7750 SR-7/12/12e, 7750 SR-7s, 7750 SR-a8, 7950 XRS

20.248 power-supply

power-supply

Syntax **power-supply** *power-supply-id type*

Context **[Tree]** (config>system power-supply)

Full Context configure system power-supply

Description This command configures information about the type of power supply used for each power feed connection on the router chassis. The information is used to populate queries made using the **show>chassis detail** and **show>chassis power-supply** commands.

Parameters *power-supply-id* — Specifies the power feed connection.

Values 1, 2

type — Specifies the type of power source that is connected to the power feed connection.

Values
- dc — Specifies that a single DC power source is connected to the power feed connector.
- ac single — Specifies that a single AC power source is connected to the power feed connector.
- ac multiple — Specifies that multiple AC power sources are connected to the power feed connector.
- default — Reverts the configured information to the default power source type for the chassis.
- none — Specifies that no power source is connected to the power feed connector.

Platforms 7450 ESS, 7750 SR-7/12

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.249 ppid

ppid

Syntax **ppid**

Context **[Tree]** (config>app-assure>group>statistics>tca>sctp-filter ppid)

Full Context configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid

Description This command configures a TCA for the counter capturing PPID hits for the specified SCTP filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ppid

Syntax **ppid**

Context **[Tree]** (config>app-assure>group>sctp-filter ppid)

Full Context configure application-assurance group sctp-filter ppid

Description Commands in this context configure actions for specific or default Payload Protocol Identifiers (PPIDs).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.250 ppid-range

ppid-range

Syntax **ppid-range direction** *direction* [**create**]
no ppid-range direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>sctp-filter ppid-range)

Full Context configure application-assurance group statistics threshold-crossing-alert sctp-filter ppid-range

Description This command configures a TCA for the counter capturing hits for the specified SCTP filter PPID range command. An PPIPD range TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a TCA.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ppid-range

Syntax **ppid-range min** *min-ppid* **max** *max-ppid*
no ppid-range

Context **[Tree]** (config>app-assure>group>sctp-filter ppid-range)

Full Context configure application-assurance group sctp-filter ppid-range

Description This command specifies the range of PPID values that are allowed by AA SCTP filter firewall.

The **no** form of this command removes this PPID range.

Default no ppid-range

Parameters *min-ppid* — Specifies the minimum SCTP Payload Protocol Identifier (PPID) to be permitted by the SCTP filter. The value must be less than or equal to the **max** *max-ppid* value.

Values 0 to 4294967295

max-ppid — Specifies the minimum SCTP Payload Protocol Identifier (PPID) to be permitted by the SCTP filter. The value must be greater or equal to the **min** *min-ppid* value.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.251 ppp

ppp

Syntax **ppp**

Context **[Tree]** (config>subscr-mgmt>loc-user-db ppp)

Full Context configure subscriber-mgmt local-user-db ppp

Description Commands in this context configure PPP host parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax **ppp**

Context **[Tree]** (config>router>l2tp>group ppp)
[Tree] (config>router>l2tp>group>tunnel ppp)
[Tree] (config>service>vprn>l2tp>group ppp)
[Tree] (config>service>vprn>l2tp>group>tunnel ppp)

Full Context configure router l2tp group ppp
configure router l2tp group tunnel ppp
configure service vprn l2tp group ppp
configure service vprn l2tp group tunnel ppp

Description This command configures PPP for the L2TP tunnel group.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax [**no**] **ppp** [**lcp**] [**pap**] [**chap**] [**ipcp**] [**ipv6cp**] [**other**]

Context **[Tree]** (debug>router>l2tp>assignment-id>packet ppp)
[Tree] (debug>router>l2tp>group>packet ppp)
[Tree] (debug>router>l2tp>packet ppp)
[Tree] (debug>router>l2tp>peer>packet ppp)

Full Context debug router l2tp assignment-id packet ppp
debug router l2tp group packet ppp
debug router l2tp packet ppp
debug router l2tp peer packet ppp

Description This command selects protocol for PPP packet debugging.

The **no** form of this command disables the protocols selection for PPP packet debugging.

Parameters **lcp** — Specifies the LCP protocol.

pap — Specifies the PAP protocol.

chap — Specifies the CHAP protocol.

ipcp — Specifies the IPCP protocol.

ipv6cp — Specifies the IPv6CP protocol.

other — Specifies any other protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ppp

Syntax [**no**] **ppp**

Context **[Tree]** (debug>service>id ppp)

Full Context debug service id ppp

Description This command enables and configures PPP debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax **ppp** [**terminate-only**]
no ppp

Context **[Tree]** (debug>service>id>ppp>event ppp)

Full Context debug service id ppp event ppp

Description This command enables debugging for PPP events.

Parameters **terminate-only** — Enables debugging for terminate-only PPP events.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax **ppp** [**lcp**] [**pap**] [**chap**] [**ipcp**]
no ppp

Context **[Tree]** (debug>service>id>ppp>packet ppp)

Full Context debug service id ppp packet ppp

Description This command enables debugging for specific PPP packets

Parameters **lcp** — Enables debugging for LCP packets.

pap — Enables debugging for PAP packets.

chap — Enables debugging for CHAP packets.

ipcp — Enables debugging for IPCP packets.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ppp

Syntax [**no**] **ppp**

Context **[Tree]** (config>service>ies>sub-if>grp-if ppp)
[Tree] (config>service>vprn>sub-if>grp-if ppp)

Full Context configure service ies subscriber-interface group-interface ppp
configure service vprn subscriber-interface group-interface ppp

Description This command configures PPP parameters.

The **no** form of this command reverts all PPP parameters from the PPP context to their defaults.

Default ppp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax **ppp**

Context **[Tree]** (debug>call-trace ppp)

Full Context debug call-trace ppp

Description Commands in this context set up call trace debugging for Point-to-Point Protocol sessions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax **ppp** [**lcp**] [**pap**] [**chap**] [**ipcp**] [**ipv6cp**] [**ipv6**]

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg>pppoe-client>brg-id ppp)

Full Context debug subscriber-mgmt vrgw brg pppoe-client brg-id ppp

Description This command specifies which messages in PPP setup are tracked by debugging. If no messages are specified, they are all tracked. LCP Echo Request and Echo Response are never shown during debugging.

Parameters **lcp** — Tracks lcp messages during debugging.

pap — Tracks pap messages during debugging.

chap — Tracks chap messages during debugging.

ipcp — Tracks ipcp messages during debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6cp — Tracks ipv6cp messages during debugging.

ipv6 — Tracks ipv6 messages during debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp

Syntax **ppp**

Context **[Tree]** (config>port>tdm>ds1>channel-group ppp)
[Tree] (config>port>tdm>ds3 ppp)
[Tree] (config>port>tdm>e1>channel-group ppp)
[Tree] (config>port>tdm>e3 ppp)

Full Context configure port tdm ds1 channel-group ppp
configure port tdm ds3 ppp
configure port tdm e1 channel-group ppp
configure port tdm e3 ppp

Description This command enables access to the context to configure the LCP operational parameters for a SONET/SDH PoS link, a DS--3/E-3 port or channel, a DS-1/E-1 channel or a DS-0 channel.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

ppp

Syntax **ppp**

Context **[Tree]** (config>port>sonet-sdh>path ppp)

Full Context configure port sonet-sdh path ppp

Description This command enables access to the context to configure the LCP operational parameters for a SONET/SDH Point-to-Point Protocol (PPP) link.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ppp

Syntax **ppp** *port-id*
no ppp [*port-id*]

Context **[Tree]** (debug ppp)

Full Context debug ppp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables/disables and configures debugging for PPP.

Parameters *port-id* — Specifies the physical port ID.

Values

port-id	*slot*/*mda*/*port* [.*channel*]		
	bundle ID	bundle-*type*-slot/mda.*bundle-num*	
		bundle	keyword
		type	ppp
		bundle-num	1 to 336
	bpgrp-id	bpgrp-*type*-*bpgrp-num*	
		bpgrp	keyword
		type	ppp
		bpgrp-num	1 to 2000
	aps-id	aps-*group-id*[.*channel*]	
		aps	keyword
		group-id	1 to 128

Platforms All

20.252 ppp-authentication

ppp-authentication

Syntax **ppp-authentication** {**pap** | **chap** | **pref-chap** | **pref-pap**}
no ppp-authentication

Context **[Tree]** (config>subscr-mgmt>ppp-policy ppp-authentication)

Full Context configure subscriber-mgmt ppp-policy ppp-authentication

Description This command configures the PPP protocol used to authenticate the PPP session.

Default ppp-authentication pref-chap

Parameters **pap** — Specifies to always use PAP to authenticate the sessions.

chap — Specifies to always use CHAP to authenticate the sessions.

pref-chap — Specifies to attempt to use CHAP and if it fails, use PAP.

pref-pap — Specifies to attempt to use PAP and if it fails, use CHAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.253 ppp-chap-challenge-length

ppp-chap-challenge-length

Syntax **ppp-chap-challenge-length min** *minimum-length* **max** *maximum-length*
no ppp-chap-challenge-length

Context **[Tree]** (config>subscr-mgmt>ppp-policy ppp-chap-challenge-length)

Full Context configure subscriber-mgmt ppp-policy ppp-chap-challenge-length

Description This command configures the minimum and maximum length of a PPP Chap Challenge.

When the Chap Challenge is exactly 16 bytes, it is send in the [60] CHAP-Challenge RADIUS attribute and copied in the RADIUS Authenticator field from the RADIUS Access Request.

Default ppp-chap-challenge-length min 32 max 64

Parameters **min** *minimum-length* — Specifies the minimum PPP CHAP challenge length.

Values 8 to 64

max *maximum-length* — Specifies the maximum PPP CHAP challenge length.

Values 8 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.254 ppp-initial-delay

ppp-initial-delay

Syntax [**no**] **ppp-initial-delay**

Context **[Tree]** (config>subscr-mgmt>ppp-policy ppp-initial-delay)

Full Context configure subscriber-mgmt ppp-policy ppp-initial-delay

Description This command delays the sending of an LCP-configure request after the discovery phase by 40 – 60 milliseconds.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.255 ppp-mtu

ppp-mtu

Syntax **ppp-mtu** *mtu-bytes*
no ppp-mtu

Context **[Tree]** (config>subscr-mgmt>ppp-policy ppp-mtu)

Full Context configure subscriber-mgmt ppp-policy ppp-mtu

Description This command configures the maximum PPP MTU size.

Parameters *mtu-bytes* — Specifies the maximum PPP MTU size.

Values 512 to 9212

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.256 ppp-options

ppp-options

Syntax **ppp-options**

Context **[Tree]** (config>subscr-mgmt>ppp-policy ppp-options)

Full Context configure subscriber-mgmt ppp-policy ppp-options

Description Commands in this context configure PPP options.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.257 ppp-policy

ppp-policy

Syntax **ppp-policy** *ppp-policy-name* [**create**]
no ppp-policy *ppp-policy-name*

Context **[Tree]** (config>subscr-mgmt ppp-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt ppp-policy

Description This command configures a PPP policy. These policies are referenced from interfaces configured for PPP. Multiple PPP policies may be configured.

The default policy cannot be modified or deleted.

Default ppp-policy default

Parameters *ppp-policy-name* — Specifies the PPP policy name, up to 32 characters.

create — Keyword used to create the entity. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ppp-policy

Syntax **ppp-policy** *ppp-pol-name*
no ppp-policy

Context **[Tree]** (config>service>vpls>sap ppp-policy)

Full Context configure service vpls sap ppp-policy

Description This command references a ppp-policy that defines session parameters (ppp-mtu, authentication options, and so on) during the session initiation phase. Normally, the PPP policy is referenced under the group-interface hierarchy. But with capture SAP is it not known at the session initiation phase to which group-interface the session belongs. This is why, with the capture SAP, the ppp-policy must be referenced directly under the capture SAP. The ppp-policy referenced under the **group-interface** must be the same as the ppp-policy referenced under the capture SAP. Otherwise the session will not come up.

The **no** form of this command reverts to the default.

Parameters *ppp-pol-name* — Specifies the PPP policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.258 ppp-sub-id-key

ppp-sub-id-key

Syntax **ppp-sub-id-key** *sub-id-key* [*sub-id-key*]
no ppp-sub-id-key

Context **[Tree]** (config>subscr-mgmt>auto-sub-id-key ppp-sub-id-key)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt auto-sub-id-key ppp-sub-id-key

Description This command enables certain fields to become the base for auto-generation of default sub-id name. The sub-id name is auto-generated if there is not a more specific method available. Examples of these specific methods would be a default sub-id name as a sap-id, a preconfigured static string or explicit mappings based on RADIUS/LUDB returned strings.

In case that a more specific sub-id name generation method is not available and the **auto-id** keyword is defined under the def-sub-id hierarchy, the sub-id name is generated by concatenating fields defined in this command separated by a "|" character.

The maximum sub-id name length is 32 characters while the concatenation of subscriber identification fields can easily exceed 32 characters. The subscriber host instantiation will fail if the sub-id name is based on subscriber identification fields whose concatenated length exceeds 32 characters. Failing the host creation rather than truncating sub-id name on a 32 character boundary will prevent collision of sub-ids (subscriber name duplication).

In case that a more specific sub-id name generation method is not available and the **auto-id** keyword is not defined under the def-sub-id hierarchy, the sub-id name is a random 10 character encoded string based on the fields defined under this command.

There is only one set of identification fields allowed per host type (IPoE or PPP) per chassis.

The **no** form of this command reverts to the default.

Default ppp-sub-id-key mac sap-id session-id

Parameters *sub-id-key* — Specifies the auto-generated sub-id keys for PPP hosts.

Values **mac** — Specifies that the MAC address can be combined with other subscriber host identification fields (circuit-id, remote-id, session-id or sap-id) to form a sub-id name in a user readable format or as a random 10 character encoded value.

In case that the mac address is used as a concatenation field in the sub-id name, then its format becomes a string xx:xx:xx:xx:xx:xx with the length 17B.

The MAC address as the subscriber host identification field is not applicable to static hosts.

circuit-id — Specifies that the circuit-id can be combined with other subscriber host identification fields (mac, remote-id, session-id or sap-id) to form a sub-id name in a user readable format or as a random 10 character encoded value.

If the circuit-id is used as a concatenation field in the sub-id name, then its format becomes access-node-id eth slot/port:[vlan-id] or access-node-id atm slot/port:vpi.vci with a variable length.

Note: If circuit-id contains any non-printable ASCII characters, the entire circuit-id string is formatted in hex in the sub-id name output. Otherwise all characters in circuit-id is converted to ASCII. ASCII printable characters contain bytes in range 0x20 to 0x7E.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the circuit-id is used as the subscriber identification field is not applicable to ARP hosts or static hosts.

remote-id — Specifies that the remote-id can be combined with other subscriber host identification fields (mac, circuit-id, session-id or sap-id) to form a sub-id name in a user readable format or as a random 10 character encoded value.

If the remote-id is used as a concatenation field in the sub-id name, then its format becomes a remote-id string with a variable length.

Note: If the remote ID contains any non-printable ASCII characters, the entire remote-id string is formatted in hex in the sub-id name output. Otherwise all characters in remote-id is converted to ASCII. ASCII printable characters contain bytes in range 0x20 to 0x7E.

The remote ID as the subscriber identification field is not applicable to ARP hosts or static hosts.

sap-id — The SAP ID can be combined with other subscriber host identification fields (mac, circuit-id, remote-id, or session-id) to form a sub-id name in a user readable format or as a random 10 character encoded value.

In case that the circuit-id is used as a concatenation field in the sub-id name, then its format becomes: slot/mda:[outer-vlan].[inner-vlan] with a variable length.

The SAP ID as the subscriber identification field is applicable to all hosts types with exception of static hosts.

session-id — The session ID can be combined with other subscriber host identification fields (mac, circuit-id, remote-id, or sap-id) to form a sub-id name in a user readable format or as a random 10 character encoded value.

In case that the circuit ID is used as a concatenation field in the sub-id name, then its format becomes a decimal number with variable length.

The session ID as the subscriber identification field is applicable only to PPPoE/PPPoEoA type hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.259 ppp-user-db

ppp-user-db

Syntax **ppp-user-db** *local-user-db-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ppp-user-db

Context [Tree] (config>service>vpls ppp-user-db)

Full Context configure service vpls ppp-user-db

Description This command enabled access to LUDB for PPPoE and PPPoEoA v4and v6 hosts under the capture SAP. The name of this local user database must match the name of local user database configured under the **config>service>vprn/ies>sub-if>grp-if>pppoe** hierarchy.

The **no** form of this command reverts to the default.

Parameters *local-user-db* — Specifies the name of the local-user-database, up to 256 characters.

20.260 ppp-user-name

ppp-user-name

Syntax **ppp-user-name append** *domain-name*
ppp-user-name default-domain *domain-name*
ppp-user-name replace *domain-name*
ppp-user-name strip
no ppp-user-name

Context [Tree] (config>subscr-mgmt>auth-plcy ppp-user-name)

Full Context configure subscriber-mgmt authentication-policy ppp-user-name

Description This command specifies the domain name manipulation action to perform on the PAP/CHAP user name prior to authentication.

The **no** form of this command reverts to the default.

Default The PAP/CHAP user name is not changed.

Parameters **append** *domain-name* — Appends an “@” delimiter followed by the specified *domain-name* to the PAP/CHAP user name, independent if a domain name is already present.

default-domain *domain-name* — Appends an “@” delimiter followed by the specified *domain-name* to the PAP/CHAP user name only if a domain name is not already present.

replace *domain-name* — Replaces the string after the “@” delimiter in the PAP/CHAP user name with the specified *domain-name*.

strip — Removes the “@” delimiter and all subsequent characters from the PAP/CHAP user name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.261 pppoe

pppoe

Syntax [**no**] **pppoe**

Context **[Tree]** (config>service>ies>sub-if>grp-if pppoe)
[Tree] (config>service>vprn>sub-if>grp-if pppoe)

Full Context configure service ies subscriber-interface group-interface pppoe
configure service vprn subscriber-interface group-interface pppoe

Description Commands in this context configure PPPoE parameters.

The **no** form of this command reverts all PPPoE parameters from the PPPoE context to their defaults.

Default pppoe

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pppoe

Syntax **pppoe** *type* **direction** {**ingress** | **egress**} **script** *name*
no pppoe *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy pppoe)

Full Context configure python python-policy pppoe

Description This command specifies the python-script for the specified PPPoE message type in the specified direction. Multiple **pppoe** command configuration are allowed in the same Python policy.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type.

Values session-lcp, session-pap, session-chap, session-ipcp, session-ip6cp, pado, padi, padr, pads, padt

direction {**ingress** | **egress**} — Specifies whether the event is incoming or outgoing. The system only invokes the configured script for the specified packet type in the specified direction.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

script — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

pppoe

Syntax **pppoe** *service-id*
no pppoe

Context **[Tree]** (config>service>vprn>if>sap>fwd-wholesale pppoe)
[Tree] (config>service>vprn>sub-if>grp-if>sap>fwd-wholesale pppoe)

Full Context configure service vprn interface sap fwd-wholesale pppoe
configure service vprn subscriber-interface group-interface sap fwd-wholesale pppoe

Description This command specifies that PPPoE packets on ingress on Ethertypes 0x8863 and 0x8864 are redirected to the specified service. The service referred to by *svc-id* must be an Epipe service. Redirection to VC-switching Epipe services is not supported.

The **no** form of this command removes the redirect.

Parameters *service-id* — Specifies the service ID of the Epipe to which packets are redirected.

Values 1 to 2147483647 | *svc-name* up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

pppoe

Syntax **pppoe** *service-id*
no pppoe

Context **[Tree]** (config>service>ies>if>sap>fwd-wholesale pppoe)
[Tree] (config>service>ies>sub-if>grp-if>sap>fwd-wholesale pppoe)

Full Context configure service ies interface sap fwd-wholesale pppoe
configure service ies subscriber-interface group-interface sap fwd-wholesale pppoe

Description This command specifies that PPPoE packets on ingress on Ethertypes 0x8863 and 0x8864 will be redirected to the specified service. The service referred to by *svc-id* must be an Epipe service. Redirection to VC-switching Epipe services is not supported.

The **no** form of this command removes the redirect.

Parameters *service-id* — Specifies the service ID of the Epipe to which packets are redirected.

Values 1 to 2147483647 | *svc-name* up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pppoe

Syntax **pppoe** *origin*

Context **[Tree]** (config>li>x-interfaces>correlation-id pppoe)

Full Context configure li x-interfaces correlation-id pppoe

Description This command specifies the type of RADIUS accounting session ID to use for PPPoE subscriber correlation.

Default host

Parameters *origin* — Specifies the correlation identifiers origin for PPPoE.

Values host, queue, session

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.262 pppoe-access-method

pppoe-access-method

Syntax **pppoe-access-method** {**none** | **padi** | **pap-chap**}
no pppoe-access-method

Context **[Tree]** (config>subscr-mgmt>auth-plcy pppoe-access-method)

Full Context configure subscriber-mgmt authentication-policy pppoe-access-method

Description This command indicates the authentication method used towards the RADIUS server in case the policy is used for PPPoE.

The **no** form of this command reverts to the default.

Parameters **none** — Indicates that the client is authenticated by the local user database defined under the group interface and not through RADIUS.

padi — Indicates that the client is authenticated by RADIUS as soon as the PADI packet comes in (there is no PPP authentication done in the session in this case).

pap-chap — Indicates that the RADIUS authentication of the client is delayed until the authentication protocol phase in the PPP session (PAP or CHAP) and authentication is performed with the user name and PAP password / CHAP response supplied by the client.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.263 pppoe-client

pppoe-client

Syntax **pppoe-client**

Context **[Tree]** (debug>subscr-mgmt>vrgw>brg pppoe-client)

Full Context debug subscriber-mgmt vrgw brg pppoe-client

Description Commands in this context debug pppoe-client information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.264 pppoe-client-policy

pppoe-client-policy

Syntax **pppoe-client-policy** *pppoe-client-policy-name* [**create**]
no pppoe-client-policy *pppoe-client-policy-name*

Context **[Tree]** (config>subscr-mgmt pppoe-client-policy)

Full Context configure subscriber-mgmt pppoe-client-policy

Description This command provisions a policy containing a set of parameters to be used to configure a PPPoE client.

The **no** form of this command removes the policy from the system. The policy can only be removed when it is not in use.

Parameters *pppoe-client-policy-name* — Specifies a unique name for the policy.

create — Mandatory keyword when creating a new policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.265 pppoe-lac

pppoe-lac

Syntax **pppoe-lac** *max-nr-of-sessions*
no pppoe-lac

Context **[Tree]** (config>subscr-mgmt>sla-profile>session-limits pppoe-lac)
[Tree] (config>subscr-mgmt>sub-profile>session-limits pppoe-lac)

Full Context configure subscriber-mgmt sla-profile session-limits pppoe-lac
configure subscriber-mgmt sub-profile session-limits pppoe-lac

Description This command configures the maximum number of PPPoE L2TP LAC sessions per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of PPPoE L2TP LAC sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of PPPoE L2TP LAC sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.266 pppoe-local

pppoe-local

Syntax **pppoe-local** *max-nr-of-sessions*
no pppoe-local

Context **[Tree]** (config>subscr-mgmt>sla-profile>session-limits pppoe-local)
[Tree] (config>subscr-mgmt>sub-profile>session-limits pppoe-local)

Full Context configure subscriber-mgmt sla-profile session-limits pppoe-local
configure subscriber-mgmt sub-profile session-limits pppoe-local

Description This command configures the maximum number of PPPoE local-terminated sessions (PTA) per SLA profile instance or per subscriber.

The **no** form of this command removes maximum number of PPPoE local-terminated sessions (PTA) limit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *max-nr-of-sessions* — Specifies the maximum number of PPPoE local-terminated sessions (PTA).

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.267 pppoe-overall

pppoe-overall

Syntax **pppoe-overall** *max-nr-of-sessions*
no pppoe-overall

Context **[Tree]** (config>subscr-mgmt>sla-profile>session-limits pppoe-overall)
[Tree] (config>subscr-mgmt>sub-profile>session-limits pppoe-overall)

Full Context configure subscriber-mgmt sla-profile session-limits pppoe-overall
configure subscriber-mgmt sub-profile session-limits pppoe-overall

Description This command configures the maximum number of PPPoE sessions per SLA profile instance or per subscriber.

The **no** form of this command removes the maximum number of PPPoE sessions limit.

Parameters *max-nr-of-sessions* — Specifies the maximum number of PPPoE sessions.

Values 0 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.268 pppoe-policy

pppoe-policy

Syntax **pppoe-policy** *pppoe-policy-name*
no pppoe-policy

Context **[Tree]** (config>service>vpls>sap pppoe-policy)

Full Context configure service vpls sap pppoe-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command references a pppoe-policy that defines session parameters (ppp-mtu, authentication options, and so on) during the session initiation phase. Normally, the PPPoE policy is referenced under the **group-interface** hierarchy. But with capture SAP is it not known at the session initiation phase to which group-interface the session belongs. This is why, with the capture SAP, the ppp-policy must be referenced directly under the capture SAP. The pppoe-policy referenced under the group-interface must be the same as the pppoe-policy referenced under the capture SAP. Otherwise the session will not come up.

The **no** form of this command reverts to the default.

Parameters *pppoe-policy-name* — Specifies the pppoe-policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.269 pppoe-python-policy

pppoe-python-policy

Syntax **pppoe-python-policy** *policy-name*
no pppoe-python-policy

Context **[Tree]** (config>service>vpls>sap pppoe-python-policy)

Full Context configure service vpls sap pppoe-python-policy

Description This command specified the Python policy for PPPoE packets sent/received on the capture SAP.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies an existing Python policy name, up to 32 characters.

Platforms All

20.270 pppoe-service-name

pppoe-service-name

Syntax [**no**] **pppoe-service-name**

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute pppoe-service-name)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute pppoe-service-name

Description This command enables the generation of the pppoe-service-name RADIUS attribute.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.271 pppoe-trace

pppoe-trace

Syntax **pppoe-trace** [**sap** *sap-id*] [**mac** *ieee-address*] **circuit-id** *circuit-id* [**remote-id** *remote-id*] [**username** *user-name*] [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]

pppoe-trace [**sap** *sap-id*] **mac** *ieee-address* [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**username** *user-name*] [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]

pppoe-trace sap *sap-id* [**mac** *ieee-address*] [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**username** *user-name*] [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]

pppoe-trace [**sap** *sap-id*] [**mac** *ieee-address*] [**circuit-id** *circuit-id*] **remote-id** *remote-id* [**username** *user-name*] [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]

pppoe-trace [**sap** *sap-id*] [**mac** *ieee-address*] [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] **username** *user-name* [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]

no pppoe-trace name *trace-name*

no pppoe-trace [**sap** *sap-id*] [**mac** *ieee-address*] [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**username** *user-name*]

Context **[Tree]** (debug>call-trace>ppp pppoe-trace)

Full Context debug call-trace ppp pppoe-trace

Description This command enables tracing locally terminated or LAC PPPoE sessions specified by the configured parameters. At least one filter rule must be provisioned. This command can trace a single session or multiple sessions, and can use wildcard characters.

This command can be executed multiple times to start multiple traces. When rules overlap, such as for a wildcard SAP and a specific SAP, the rule that a specific trace is associated with cannot be guaranteed.

The **no** form of this command prevents new traces from being configured and terminates all trace jobs that were previously started using the **trace** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *circuit-id* — Specifies a circuit ID, up to 255 characters, that is used to filter sessions to trace.

ieee-address — Specifies a MAC address that is used to identify a session to trace, in the format “ab:cd:ef:01:23:45”. A wildcard character can be used to match all remaining octets; for example, the format “ab:cd:ef:*” can be used to filter by OUI.

user-name — Specifies a username, up to 32 characters, that is used to filter sessions to trace. A wildcard character (*) can be used at the beginning and at the end of the filter.

num — Specifies the maximum number of jobs that may be started with this rule.

Values 1 to 50

Default 1

remote-id — Specifies a remote ID, up to 255 characters, that is used to filter sessions to trace.

sap-id — Specifies a SAP to trace. The following formats are accepted:

- *port*/*lag*/*pw-port*:*svlan*.*cvlan*
- *port*/*lag*/*pw-port*:*vlan*
- *port*/*lag*/*pw-port*
- *port*/*lag*/*pw-port*:*vlan*.*
- *port*/*lag*/*pw-port*:* (also matches *.*)

trace-existing-sessions — Specifies that existing PPPoE sessions are traced. If this parameter is not included, only new PPPoE sessions are traced.

trace-name — Specifies the name, up to 32 characters, by which the trace is referenced.

trace-profile-name — Specifies the name of the trace profile to be applied, up to 32 characters. The default parameters are used if a trace profile is not specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.272 pppoe-user-db

pppoe-user-db

Syntax **pppoe-user-db** *local-user-db-name*
no pppoe-user-db

Context **[Tree]** (config>service>vpls pppoe-user-db)

Full Context configure service vpls pppoe-user-db

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enabled access to LUDB for PPPoE and PPPoEoA v4and v6 hosts under the capture SAP. The name of this LUDB must match the name of the LUDB configured under the **config>service>vprn/ies>sub-if>grp-if>pppoe** hierarchy.

The **no** form of this command reverts to the default.

Parameters *local-user-db* — Specifies the name of the local user database, up to 256 characters.

pppoe-user-db

Syntax **pppoe-user-db** *ludb-name*
no pppoe-user-db

Context **[Tree]** (config>service>vpls>sap pppoe-user-db)

Full Context configure service vpls sap pppoe-user-db

Description This command enables LUDB authentication on capture SAPs for PPPoE(oA) clients. If this command is configured along with the **authentication-policy** command (RADIUS authentication), then the authentication-policy command takes precedence.

The **no** form of this command reverts to the default.

Parameters *ludb-name* — Specifies the name of the local user database up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.273 pptp

pptp

Syntax [**no**] **pptp**

Context **[Tree]** (config>service>nat>nat-policy>alg pptp)
[Tree] (config>service>nat>up-nat-policy>alg pptp)

Full Context configure service nat nat-policy alg pptp
configure service nat up-nat-policy alg pptp

Description This command enables PPTP ALG.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The call-id is captured in the outgoing call management messages and along with the source IP address and the source TCP, is translated by NAT. Once the PPTP call is established, the call-id in the associated GRE packet in the incoming direction (from outside to inside) is correspondingly translated so that it matches the call-id mapping established during the call establishment phase. The call IDs used in the mappings are selected randomly and they try to honor parity (odds/even).

A PPTP session can be initiated only from the inside of NAT.

GRE traffic is allowed through NAT only if the corresponding mapping exists. This mapping is created during the call negotiation phase.

There can be seven calls (GRE tunnels) per control session.

Default no pptp

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.274 pre-auth-policy

pre-auth-policy

Syntax **pre-auth-policy** *policy-name*
no pre-auth-policy

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host pre-auth-policy)

Full Context configure subscriber-mgmt local-user-db ppp host pre-auth-policy

Description This command configures the RADIUS pre-authentication policy to use to authenticate the PPP host.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the pre-authentication policy of the host, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.275 pre-login-message

pre-login-message

Syntax **pre-login-message** *login-text-string* [**name**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no pre-login-message

Context [Tree] (config>system>login-control pre-login-message)

Full Context configure system login-control pre-login-message

Description This command creates a message displayed prior to console login attempts on the console via Telnet.

Only one message can be configured. If multiple **pre-login-messages** are configured, the last message entered overwrites the previous entry.

It is possible to add the name parameter to an existing message without affecting the current **pre-login-message**.

The **no** form of this command removes the message.

Default no pre-login-message

Parameters *login-text-string* — Specifies the login text string up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Some special characters can be used to format the message text. The \n character can be used to create multi-line messages. A \n in the message moves to the beginning of the next line by sending ASCII/UTF-8 chars 0xA (LF) and 0xD (CR) to the client terminal. A \r in the message sends the ASCII/UTF-8 char 0xD (CR) to the client terminal.

name — When this keyword is specifies, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name.

Platforms All

20.276 pre-shared-key

pre-shared-key

Syntax **pre-shared-key** *pre-shared-key-index* [**encryption-type** *encryption-type*] [**create**]
no pre-shared-key *pre-shared-key-index*

Context [Tree] (config>macsec>conn-assoc>static-cak pre-shared-key)

Full Context configure macsec connectivity-association static-cak pre-shared-key

Description This command specifies the pre-shared key used to enable MACsec using static connectivity association key (CAK) security mode. This command also specifies the encryption algorithm used for encrypting the SAK.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A pre-shared key includes a connectivity association key name (CKN) and a connectivity association key (CAK). The pre-shared key-the CKN and CAK-must match on both ends of a link.

A pre-shared key is configured on both devices at each end of point-to-point link to enable MACsec using static CAK security mode. The MACsec Key Agreement (MKA) protocol is enabled after the successful MKA liveliness negotiation.

The encryption-type is used for encrypting the SAK and authenticating the MKA packet. The symmetric encryption key SAK (Security Association Key) needs to be encrypted (wrapped) via the MKA protocols. The AES key is derived via pre-shared-key.

The **no** form of this command removes the index.

Parameters *pre-shared-key-index* — Specifies the index of this pre-shared-key.

Values 1, 2

encryption-type — Specifies the type of encryption.

Values **aes-128-cmac**, **aes-256-cmac**

create — Mandatory to create an entry.

Platforms All

pre-shared-key

Syntax **pre-shared-key** *key* [**hash** | **hash2** | **custom**]
no pre-shared-key

Context **[Tree]** (config>ipsec>client-db>client>credential pre-shared-key)

Full Context configure ipsec client-db client credential pre-shared-key

Description This command specifies a pre-shared key used to authenticate peers.

The **no** form of this command reverts to the default.

Default no pre-shared-key

Parameters *key* — An ASCII string to use as the pre-shared key for dynamic keying. When the **hash** or **hash2** parameters are not used, the key is a clear text key; otherwise, the key text is encrypted.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

pre-shared-key

Syntax **pre-shared-key** *key* [**hash** | **hash2** | **custom**]
no pre-shared-key

Context [Tree] (config>service>ies>if>ipsec>ipsec-tunnel>dyn pre-shared-key)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn pre-shared-key)
[Tree] (config>service>ies>if>sap>ipsec-gw pre-shared-key)
[Tree] (config>service>vprn>if>sap>ipsec-gw pre-shared-key)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel>dynamic-keying pre-shared-key)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn pre-shared-key)
[Tree] (config>ipsec>trans-mode-prof>dyn pre-shared-key)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying pre-shared-key
configure router interface ipsec ipsec-tunnel dynamic-keying pre-shared-key
configure service ies interface ipsec ipsec-tunnel dynamic-keying pre-shared-key
configure service ies interface sap ipsec-gw pre-shared-key
configure service vprn interface ipsec ipsec-tunnel dynamic-keying pre-shared-key
configure service vprn interface sap ipsec-gw pre-shared-key
configure service vprn interface sap ipsec-tunnel dynamic-keying pre-shared-key

Description This command configures the pre-shared key for authentication.

The **no** form of this command reverts to the default.

Default no pre-shared-key

Parameters *key* — Specifies an ASCII string to use as the pre-shared key for dynamic keying. When the **hash** or **hash2** parameters are not used, the key is a clear text key; otherwise, the key text is encrypted.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec ipsec-transport-mode-profile dynamic-keying pre-shared-key
- configure service vprn interface sap ipsec-tunnel dynamic-keying pre-shared-key
- configure service vprn interface sap ipsec-gw pre-shared-key
- configure service ies interface sap ipsec-gw pre-shared-key

VSR

- configure router interface ipsec ipsec-tunnel dynamic-keying pre-shared-key
- configure service ies interface ipsec ipsec-tunnel dynamic-keying pre-shared-key
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying pre-shared-key

20.277 pre-update-time

pre-update-time

Syntax **pre-update-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update pre-update-time)

Full Context configure system security pki ca-profile auto-crl-update pre-update-time

Description This command specifies the pre-download time for next-update-based update.

Default pre-update-time hrs 1

Parameters *days* — Specifies the time period, in days, prior to the next update time of the current CRL.

Values 0 to 366

hours — Specifies the time period, in hours, prior to the next update time of the current CRL.

Values 0 to 23

minutes — Specifies the time period, in minutes, prior to the next update time of the current CRL.

Values 0 to 59

seconds — Specifies the time period, in seconds, prior to the next update time of the current CRL.

Values 0 to 59

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.278 prec

prec

Syntax **prec** *ip-prec-value* [**fc** *fc-name*] [**priority** {**high** | **low**}]
no prec *ip-prec-value*

Context **[Tree]** (config>qos>sap-ingress prec)

Full Context configure qos sap-ingress prec

Description This command explicitly sets the forwarding class or enqueuing priority when a packet is marked with an IP precedence value (*ip-prec-value)*. Adding an IP precedence rule on the policy forces packets that match the specified *ip-prec-value* to override the forwarding class and enqueuing priority based on the parameters included in the IP precedence rule.

When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy.

When the enqueuing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueuing priority derived from earlier matches in the classification hierarchy.

The *ip-prec-value* is derived from the most significant three bits in the IP header ToS byte field (precedence bits). The three precedence bits define eight Class-of-Service (CoS) values commonly used to map packets to per-hop Quality of Service (QoS) behavior. The precedence bits are also part of the DiffServ Code Point (DSCP) method of mapping packets to QoS behavior. The DSCP uses the most significant six bits in the IP header ToS byte and so overlaps with the precedence bits. Both IP precedence and DSCP classification rules are supported. DSCP rules have a higher match priority than IP precedence rules and where a *dscp-name* DSCP value overlaps an *ip-prec-value*, the DSCP rule takes precedence.

The **no** form of this command removes the explicit IP precedence classification rule from the SAP ingress policy. Removing the rule on the policy immediately removes the rule on all ingress SAPs using the policy.

Parameters *ip-prec-value* — The *ip-prec-value* is a required parameter that specifies the unique IP header ToS byte precedence bits value that will match the IP precedence rule. If the command is executed more than once with the same *ip-prec-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight IP precedence rules are allowed on a single policy.

The precedence is evaluated from the lowest to highest value.

Values 0 to 7

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc *fc-name* — The value given for the *fc-name* parameter must be one of the predefined forwarding classes in the system. Specifying the *fc-name* is optional. When a packet matches the rule, the forwarding class is only overridden when the **fc** *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

The *subclass-name* parameter is optional and used with the *fc-name* parameter to define a pre-existing subclass. The *fc-name* and *subclass-name* parameters must be separated by a period (.). If *subclass-name* does not exist in the context of *fc-name*, an error will occur. If *subclass-name* is removed using the **no fc** *fc-name.subclass-name* **force** command, the **default-fc** command will automatically drop the *subclass-name* and only use *fc-name* (the parent forwarding class for the subclass) as the forwarding class.

Values

fc: *class*[.*subclass*]

class: be, l2, af, l1, h2, ef, h1, nc

subclass: 29 characters max

Default Inherit (When **fc** is not defined, the rule preserves the previous forwarding class of the packet.)

priority — The priority parameter overrides the default enqueuing priority for all packets received on an ingress SAP using this policy that match this rule. Specifying the priority is optional. When a packet matches the rule, the enqueuing priority is only overridden when the priority parameter is defined on the rule. If the packet matches and priority is not explicitly defined in the rule, the enqueuing priority is inherited based on previous rule matches.

Values high, low

Default Inherits the priority defined by the default-priority statement.

high — This parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **high** for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

low — This parameter is used in conjunction with the **priority** parameter. Setting the enqueuing parameter to **low** for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. When the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prec

Syntax **prec** {*ip-prec-value* | **in-profile** *ip-prec-value* **out-profile** *ip-prec-value* [**exceed-profile** *ip-prec-value*]}
no prec

Context **[Tree]** (config>qos>sap-egress>fc prec)

Full Context configure qos sap-egress fc prec

Description This command defines a value to be used for remarking packets for the specified FC. If the optional in/out/exceed-profile is specified, the command will remark different IP precedence values depending on whether the packet was classified to be in, exceed, or out-of-profile. All inplus-profile traffic is marked with the same value as in-profile traffic.

Parameters *ip-prec-value* — This parameter specifies the IP precedence to be used to remark all traffic.

Values 0 to 7

exceed-profile *ip-prec-value* — This optional parameter specifies the IP precedence to be used to remark traffic that is exceed-profile. If not specified, this defaults to the same value configured for the **out-profile** parameter.

Values 0 to 7

in-profile *ip-prec-value* — This parameter specifies the IP precedence to be used to remark traffic that is in-profile.

Values 0 to 7

out-profile *ip-prec-value* — This parameter specifies the IP precedence to be used to remark traffic that is out-of-profile.

Values 0 to 7

Platforms All

prec

Syntax **prec** *ip-prec-value* [**fc** *fc-name*] [**profile** {**in** | **out** | **exceed** | **inplus**}]
no prec *ip-prec-value*

Context **[Tree]** (config>qos>sap-egress prec)

Full Context configure qos sap-egress prec

Description This command defines a specific IP precedence value that must be matched to perform the associated reclassification actions. If an egress packet on the SAP matches the specified IP precedence value, the forwarding class, or profile behavior may be overridden. By default, the forwarding class and profile of the packet is derived from ingress classification and profiling functions.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IP precedence bits used to match against precedence reclassification rules come from the Type of Service (ToS) field within the IPv4 header. If the packet does not have an IPv4 header, precedence-based matching is not performed.

The reclassification actions from a precedence reclassification rule may be overridden by a DSCP or IP flow matching event.

The **fc** keyword is optional. When specified, the egress classification rule will overwrite the forwarding class derived from ingress. The new forwarding class is used for egress remarking and queue mapping decisions. If a DSCP, ipv6-criteria, or ip-criteria match occurs after the IP precedence match, the new forwarding class may be overridden by the higher priority match actions. If the higher priority match actions do not specify a new fc, the fc from the IP precedence match will be used.

The **profile** keyword is optional. When specified, the egress classification rule will overwrite the profile of the packet derived from ingress. The new profile value is used for egress remarking and queue congestion behavior. If a DSCP, IPv6 criteria, or IP criteria match occurs after the IP precedence match, the new profile may be overridden by the higher priority match actions. If the higher priority match actions do not specify a new profile, the profile from the IP precedence match will be used.

The **no** form of this command removes the reclassification rule from the SAP egress QoS policy.

Parameters **fc** *fc-name* — This keyword is optional. When specified, packets matching the IP precedence value will be explicitly reclassified to the forwarding class specified as *fc-name* regardless of the ingress classification decision. The explicit forwarding class reclassification may be overwritten by a higher priority DSCP, IPv6 criteria, or IP criteria reclassification match. The FC name defined must be one of the eight forwarding classes supported by the system. To remove the forwarding class reclassification action for the specified precedence value, the **prec** command must be re-executed without the **fc** parameter defined.

Values be, l1, af, l2, h1, ef, h2 or nc

profile {in | out | exceed | inplus} — This keyword is optional. When specified, packets matching the IP precedence value will be explicitly reclassified to the specified profile regardless of the ingress profiling decision. The explicit profile reclassification may be overwritten by a higher priority DSCP, IPv6 criteria, or IP criteria reclassification match. To remove the profile reclassification action for the specified precedence value, the **prec** command must be re-executed without the **profile** parameter defined.

in — Specifies that any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out — Specifies that any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

exceed — Specifies that any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

inplus — Specifies that any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

Platforms All

prec

Syntax **prec** *ip-prec-value* **fc** *fc-name* **profile** {**in** | **out** | **exceed** | **inplus**}
no prec *ip-prec-value*

Context **[Tree]** (config>qos>network>egress prec)

Full Context configure qos network egress prec

Description This command defines a specific IP precedence value that must be matched in order to perform the associated reclassification actions. If an egress packet on an IES/VPRN interface spoke SDP, on a CSC network interface in a VPRN, or network interface that the network QoS policy is applied to, matches the specified IP precedence value, the forwarding class and profile may be overridden.

By default, the forwarding class and profile of the packet is derived from ingress classification and profiling functions.

The IP precedence bits used to match against the reclassification rules come from the Type of Service (ToS) field within the IPv4 header or the Traffic Class field from the IPv6 header. If the packet does not have an IP header, IP precedence-based matching is not performed.

The configuration of egress prec classification and the configuration of an egress IP criteria or IPv6 criteria entry statement within a network QoS policy are mutually exclusive.

The IP precedence-based and DSCP-based reclassification are supported on a network interface, on a CSC network interface in a VPRN, and on a PW used in an IES or VPRN spoke interface.

This command will block the application of a network QoS policy with the egress reclassification commands to a spoke SDP part of a Layer 2 service. Conversely, this command will not allow the user to add the egress reclassification commands to a network QoS policy if it is being used by a Layer 2 spoke SDP.

The egress reclassification commands will only take effect if the redirection of the spoke SDP or CSC interface to use an egress port queue-group succeeds. For example, the following commands will succeed:

- **config>service>vprn>if>spoke-sdp>egress>qos** *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*
- **config>service>ies>if>spoke-sdp>egress>qos** *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*
- **config>service>vprn>nw-if> qos** *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the redirection command fails in CLI, the PW will use the network QoS policy assigned to the network IP interface; however, any reclassification in the network QoS policy applied to the network interface will be ignored.

The **no** form of this command removes the egress reclassification rule.

Parameters *ip-prec-value* — 0 to 7

fc *fc-name* — be, l2, af, l1, h2, ef, h1, nc

*profile {***in** | **out | exceed | inplus***}* — The profile reclassification action is mandatory. When specified, packets matching the IP precedence value will be explicitly reclassified to the profile specified regardless of the ingress profiling decision. To remove the profile reclassification action for the specified IP precedence value, the **no prec** command must be executed.

This value may be overwritten by an explicit profile action in an DSCP reclassification match.

in - Specifies that any packets matching the reclassification rule will be treated as in-profile by the egress forwarding plane.

out - Specifies that any packets matching the reclassification rule will be treated as out-of-profile by the egress forwarding plane.

exceed - Specifies that any packets matching the reclassification rule will be treated as exceed-profile by the egress forwarding plane.

inplus - Specifies that any packets matching the reclassification rule will be treated as inplus-profile by the egress forwarding plane.

Platforms All

20.279 precedence

precedence

Syntax **precedence** {**primary** | **secondary**}
no precedence

Context **[Tree]** (config>eth-tunnel>path precedence)

Full Context configure eth-tunnel path precedence

Description This command specifies the precedence to be used for the path. Only two precedence options are supported: **primary** and **secondary**.

The **no** form of this command sets the precedence to the default value.

Default precedence secondary

Parameters **primary | secondary** — Specifies the path precedence as either primary or secondary.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

precedence

Syntax **precedence** [*precedence-value* | **primary**]
no precedence

Context **[Tree]** (config>service>apipe>spoke-sdp precedence)
[Tree] (config>service>cpipe>spoke-sdp precedence)
[Tree] (config>service>epipe>spoke-sdp precedence)
[Tree] (config>service>fpipe>spoke-sdp precedence)
[Tree] (config>service>ipipe>spoke-sdp precedence)

Full Context configure service apipe spoke-sdp precedence
configure service cpipe spoke-sdp precedence
configure service epipe spoke-sdp precedence
configure service fpipe spoke-sdp precedence
configure service ipipe spoke-sdp precedence

Description This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can only be assigned to one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding will begin to forward traffic.

The **no** form of this command returns the precedence value to the default.

Default precedence 4

Parameters *precedence-value* — Specifies the spoke SDP precedence.

Values 1 to 4

primary — Assigns primary precedence to the spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp precedence
- configure service fpipe spoke-sdp precedence

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp precedence

All

- configure service ipipe spoke-sdp precedence
- configure service epipe spoke-sdp precedence

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

precedence

Syntax **precedence** *prec-value*
precedence primary
no precedence

Context **[Tree]** (config>service>epipe>spoke-sdp-fec precedence)

Full Context configure service epipe spoke-sdp-fec precedence

Description This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can only be assigned to one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding will begin to forward traffic.

The **no** form of this command returns the precedence value to the default.

Default precedence 42

Parameters *prec-value* — Specifies the spoke SDP precedence.

Values 1 to 4

primary — Assigns primary precedence to this spoke SDP.

Platforms All

precedence

Syntax **precedence** [*precedence-value* | **primary**]
no precedence

Context **[Tree]** (config>service>vpls>spoke-sdp precedence)

Full Context configure service vpls spoke-sdp precedence

Description This command configures the precedence of this SDP bind when there are multiple SDP binds attached to one service endpoint. When an SDP bind goes down, the next highest precedence SDP bind begins forwarding traffic.

Parameters *precedence-value* — Specifies the precedence of this SDP bind

Values 1 to 4

primary — Assigns this as the primary spoke-SDP

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

precedence

Syntax **precedence** {*precedence-value* | **primary**}
no precedence

Context **[Tree]** (config>mirror>mirror-dest>spoke-sdp precedence)

Full Context configure mirror mirror-dest spoke-sdp precedence

Description This command indicates that the SDP is of type secondary with a specific precedence value or of type primary.

The mirror or LI service always uses the primary type as the active pseudowire and only switches to a secondary pseudowire when the primary is down. The mirror service switches the path back to the primary pseudowire when it is back up. The user can configure a timer to delay reverting back to primary or to never revert back.

If the active pseudowire goes down, the mirror service switches the path to a secondary sdp with the lowest precedence value. That is, secondary SDPs which are operationally up are considered in the order of their precedence value, 1 being the lowest value and 4 being the highest value. If the precedence value is the same, then the SDP with the lowest SDP ID is selected.

An explicitly named endpoint can have a maximum of one SAP and one ICB. Once a SAP is added to the endpoint, only one more object of type ICB SDP is allowed. An explicitly named endpoint, which does not have a SAP object, can have a maximum of four SDPs, which can include any of the following: a single primary SDP, one or many secondary SDPs with precedence, and a single ICB SDP.

An SDP is created with type secondary and with the lowest precedence value of 4.

Parameters *precedence-value* — Specifies the precedence of the SDP.

Values 1 to 4

primary — Specified that a special value of the precedence which assigns the SDP the lowest precedence and enables the revertive behavior.

Platforms All

20.280 preempt

preempt

Syntax [**no**] **preempt**

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp preempt)
[Tree] (config>service>vprn>sub-if>grp-if>srrp preempt)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface group-interface srrp preempt
configure service vprn subscriber-interface group-interface srrp preempt

Description When preempt is enabled, a newly initiated SRRP instance can overrides an existing Master SRRP instance if its priority value is higher than the priority of the current Master.

If preempt is disabled, an SRRP instance only becomes Master if the master down timer expires before an SRRP advertisement message is received from the adjacent SRRP enabled node.

The **no** form of this command reverts to the default.

Default preempt

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preempt

Syntax [**no**] **preempt**

Context **[Tree]** (config>service>ies>if>ipv6>vrrp preempt)

Full Context configure service ies interface ipv6 vrrp preempt

Description The preempt mode value controls whether a specific backup virtual router preempts a lower priority master.

When preempt is enabled, the virtual router instance overrides any non-owner master with an “in use” message priority value less than the virtual router instance in-use priority value. If preempt is disabled, the virtual router only becomes master if the master down timer expires before a VRRP advertisement message is received from another virtual router.

The IP address owner will always become master when available. Preempt mode cannot be disabled on the owner virtual router.

The **no** form of this command disables preempt mode.

Default preempt

Platforms All

preempt

Syntax [**no**] **preempt**

Context **[Tree]** (config>service>ies>if>vrrp preempt)

Full Context configure service ies interface vrrp preempt

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The preempt command provides the ability of overriding an existing non-owner master to the virtual router instance. Enabling preempt mode is almost required for proper operation of the base-priority and vrrp-policy-id definitions on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the effect of the dynamic changing of the in-use priority is greatly diminished.

The preempt command is only available in the non-owner vrrp virtual-router-id nodal context. The owner may not be preempted due to the fact that the priority of non-owners can never be higher than the owner. The owner will always preempt all other virtual routers when it is available.

Non-owner virtual router instances will only preempt when preempt is set and the current master has an in-use message priority value less than the virtual router instances in-use priority.

A master non-owner virtual router will only allow itself to be preempted when the incoming VRRP Advertisement message Priority field value is one of the following:

- Greater than the virtual router in-use priority value
- Equal to the in-use priority value and the source IP address (primary IP address) is greater than the virtual router instance primary IP address

The **no** form of this command prevents a non-owner virtual router instance from preempting another, less desirable virtual router. Use the preempt command to restore the default mode.

Default preempt

Platforms All

preempt

Syntax [**no**] **preempt**

Context **[Tree]** (config>service>vprn>if preempt)
[Tree] (config>service>vprn>if>ipv6>vrrp preempt)

Full Context configure service vprn interface ipv6 vrrp preempt
configure service vprn interface preempt

Description The preempt mode value controls whether a specific backup virtual router preempts a lower priority master.

When preempt is enabled, the virtual router instance overrides any non-owner master with an “in use” message priority value less than the virtual router instance in-use priority value. If preempt is disabled, the virtual router only becomes master if the master down timer expires before a VRRP advertisement message is received from another virtual router.

The IP address owner will always become master when available. Preempt mode cannot be disabled on the owner virtual router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default value for preempt mode is enabled.

Default preempt

Platforms All

preempt

Syntax [**no**] **preempt**

Context **[Tree]** (config>router>if>vrrp preempt)
[Tree] (config>router>if>ipv6>vrrp preempt)

Full Context configure router interface ipv6 vrrp preempt
configure router interface vrrp preempt

Description The preempt mode value controls whether a specific backup virtual router preempts a lower priority master.

When preempt is enabled, the virtual router instance overrides any non-owner master with an “in use” message priority value less than the virtual router instance in-use priority value. If preempt is disabled, the virtual router only becomes master if the master down timer expires before a VRRP advertisement message is received from another virtual router.

The IP address owner will always become master when available. Preempt mode cannot be disabled on the owner virtual router.

The default value for preempt mode is enabled.

Default preempt

Platforms All

20.281 preemption-timer

preemption-timer

Syntax **preemption-timer** *seconds*
no preemption-timer

Context **[Tree]** (config>router>rsvp preemption-timer)

Full Context configure router rsvp preemption-timer

Description This parameter configures the time in seconds a node holds to a reservation for which it triggered the soft preemption procedure.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The preempting node starts a separate preemption timer for each preempted LSP path. While this timer is on, the node should continue to refresh the Path and Resv for the preempted LSP paths. When the preemption timer expires, the node tears down the reservation if the head-end node has not already done so.

A value of zero means the LSP should be preempted immediately; hard preempted.

The **no** form of this command reverts to the default value.

Default preemption-timer 300

Parameters *seconds* — Specifies the time (in s), of the preemption timer.

Values 0 to 1800 seconds

Platforms All

20.282 prefer-failure

prefer-failure

Syntax [**no**] **prefer-failure**

Context **[Tree]** (config>service>nat>pcp-server-policy>option prefer-failure)

Full Context configure service nat pcp-server-policy option prefer-failure

Description This command enables/disables support for the **prefer-failure** option.

Default no prefer-failure

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.283 prefer-local-time

prefer-local-time

Syntax [**no**] **prefer-local-time**

Context **[Tree]** (config>system>time prefer-local-time)

Full Context configure system time prefer-local-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the preference to use local or UTC time in the system. This preference is applied to objects such as log file names, created and completed times reported in log files, NETCONF and gRPC date-and-time leafs, and rollback times displayed in **show** routines.

Note: The operator may force the timezone used for **show** outputs during a CLI session using an environment variable in the **environment**>**time-display {utc | local}** command.

Note: The preference for CLI output is set with the **environment time-display** command.

Note: The format used for the date-time strings may change when the **prefer-local-time** option is enabled. For example, when enabled, all date-time strings include a suffix of three to five characters that indicates the timezone used for the presentation. This suffix may not be present if the option in not enabled.

Note: The time format for timestamps on log events is controlled on a per-log basis using the **config**>**log**>**log-id**>**time-format {utc | local}** CLI command and not via **prefer-local-time**.

The **no** form of this command indicates preference for UTC time.

Default no prefer-local-time

Platforms All

20.284 prefer-mcast-tunnel-in-tunnel

prefer-mcast-tunnel-in-tunnel

Syntax [**no**] **prefer-mcast-tunnel-in-tunnel**

Context **[Tree]** (config>router>ldp prefer-mcast-tunnel-in-tunnel)

Full Context configure router ldp prefer-mcast-tunnel-in-tunnel

Description At a downstream router, this command specifies that for upstream FEC resolution a T-LDP session to the upstream peer is preferred over an I-LDP session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

At an upstream router, this command specifies that for downstream FEC resolution a T-LDP session to the downstream peer is preferred over an I-LDP session.

The **no** form of this command reverts to the default value.

Default no prefer-mcast-tunnel-in-tunnel

Platforms All

20.285 prefer-protocol-stitching

prefer-protocol-stitching

Syntax [**no**] **prefer-protocol-stitching**

Context **[Tree]** (config>router>ldp prefer-protocol-stitching)

Full Context configure router ldp prefer-protocol-stitching

Description This command stitches an LDP ILM to an SR NHLFE rather than to an LDP NHLFE when both LDP and SR NHLFEs exist.

The **no** form of this command stitches an LDP ILM to an LDP NHLFE by preference over an SR NHLFE.

Default no prefer-protocol-stitching

Platforms All

20.286 prefer-tunnel-in-tunnel

prefer-tunnel-in-tunnel

Syntax [**no**] **prefer-tunnel-in-tunnel**

Context **[Tree]** (config>router>ldp prefer-tunnel-in-tunnel)

Full Context configure router ldp prefer-tunnel-in-tunnel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies to use tunnel-in-tunnel over a simple LDP tunnel. Specifically, the user packets for LDP FECs learned over this targeted LDP session can be sent inside an RSVP LSP which terminates on the same egress router as the destination of the targeted LDP session. The user can specify an explicit list of RSVP LSP tunnels under the Targeted LDP session or LDP will perform a lookup in the Tunnel Table Manager (TTM) for the best RSVP LSP. In the former case, only the specified LSPs will be considered to tunnel LDP user packets. In the latter case, all LSPs available to the TTM and which terminate on the same egress router as this target ed LDP session will be considered. In both cases, the metric specified under the LSP configuration is used to control this selection.

The lookup in the TTM will prefer a LDP tunnel over an LDP-over-RSVP tunnel if both are available. Also, the tunneling operates on the dataplane only. Control packets of this targeted LDP session are sent over the IGP path.

Platforms All

20.287 preference

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>router>l2tp>group>tunnel preference)
[Tree] (config>service>vprn>l2tp>group>tunnel preference)

Full Context configure router l2tp group tunnel preference
configure service vprn l2tp group tunnel preference

Description This command configures a preference number that indicates the relative preference assigned to a tunnel when using a weighted session assignment.

The **no** form of this command removes the preference value from the tunnel configuration.

Default no preference

Parameters *preference* — Specifies the tunnel preference number with its group. The value 0 corresponds to the highest preference.

Values 0 to 16777215

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preference

Syntax **preference** *preference-level*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no preference

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>bundle preference)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel preference)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override preference)

Full Context configure mcast-management multicast-info-policy bundle channel preference
configure mcast-management multicast-info-policy bundle channel source-override preference
configure mcast-management multicast-info-policy bundle preference

Description This command sets the relative preference level for multicast channels. The preference of a channel specifies its relative importance over other multicast channels. Eight levels of preference are supported; 0 through 7. Preference value 7 indicates the highest preference level.

When the multicast ingress path manager is congested on one or more of the switch fabric multicast paths, it uses the preference values associated with each multicast record to determine which records are allowed on the path and which records be placed in a black-hole state.

The preference value is also compared to the bundles **cong-priority-threshold** setting to determine the congestion priority of the channel. The result also dictates the channels multicast CAC class level (high or low). When the channels preference value is less than the congestion priority threshold, it is considered to have a congestion priority and CAC class value equal to low. When the channels preference value is equal to or greater than the threshold, it is considered to have a congestion priority and a CAC class value equal to high.

The preference value is also compared to the bundles ecmp-opt-threshold setting to determine whether the channel is eligible for ECMP path dynamic optimization. If the preference value is equal to or less than the threshold, the channel may be optimized. If the preference value is greater than the threshold, the channel will not be dynamically optimized.

The preference command may be executed in three contexts; bundle, channel and source-override. The bundle default preference value is 0. The channel and **source-override** preference settings are considered overrides to the bundle setting and have a default value of null (undefined).

The **no** form of this command restores the default preference value (0 or null depending on the context).

Parameters *preference-level* — The preference-level parameter is required and defines the preference value of the channel.

Values 1 to 7

Bundle default:	0
Channel default:	Null (undefined)
Source-override default:	Null (undefined)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Override sequence — The channel setting overrides the bundle setting. The **source-override** setting overrides the channel and bundle settings.

Platforms All

preference

Syntax [**no**] **preference** *preference*

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy preference)

Full Context configure subscriber-mgmt bgp-peering-policy preference

Description This command configures the route preference for routes learned from the configured peer.

The lower the preference the higher the chance of the route being the active route. The OS assigns BGP routes highest default preference compared to routes that are direct, static or learned via MPLS or OSPF.

The **no** form of this command used at the global level reverts to default value.

Default preference 170

Parameters *preference* — The route preference, expressed as a decimal integer.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>aaa>diam-peer-plcy>peer preference)

Full Context configure aaa diameter-peer-policy peer preference

Description This command configures preference for a peer. Only the two peers with the lowest preference are used to carry traffic. Other peers can be in the Open state waiting to be utilized in case that one of the two active peers fail. Once the primary peer fails, the secondary peer carries traffic as long as the last transaction on it has succeeded (stickiness). Another peer in the Open state becomes secondary. Load balancing between peers is not supported.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default value.

Parameters *preference* — Specifies the preference of this diameter policy peer.

Values 1 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>aaa>diam>node>peer preference)

Full Context configure aaa diameter node peer preference

Description This command configures the Diameter routing preference for a peer. All open peers are installed in the Diameter realm routing table but only the one with the lowest numerical value for preference is used as next-hop for a given destination realm. If multiple peers with the same preference are configured for the same realm, the peer index with the lowest value is used to break the tie.

The **no** form of this command reverts to the default.

Default preference 50

Parameters *preference* — Specifies the peer preference.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>aaa>diam>node>peer>route preference)

Full Context configure aaa diameter node peer route preference

Description This command configures the preference of the static route. The lower value is preferred during route selection.

The **no** form of this command reverts to the default.

Default preference 50

Parameters *preference* — Specifies the static route preference.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

preference

Syntax **preference** *preference*
no preference

Context [Tree] (config>subscr-mgmt>sub-prof preference)

Full Context configure subscriber-mgmt sub-profile preference

Description This command sets the relative preference value for a subscriber profile. When multiple subscriber hosts/sessions of the same subscriber point to a different subscriber profile, the profile with the highest preference value is used. With equal preference, the subscriber profile of the last instantiated subscriber host/session is used.

Note: Nokia recommends not to configure a subscriber profile preference value unless explicitly required for the targeted design.

The **no** form of this command reverts to the default value.

Default preference 5

Parameters *preference* — Specifies the preference value. A lower number means a lower preference.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preference

Syntax **preference** [**create**] [**non-revertive**]
no preference

Context [Tree] (config>service>system>bgp-evpn>eth-seg>service-carving>manual preference)

Full Context configure service system bgp-evpn ethernet-segment service-carving manual preference

Description This command creates the preference context for the Ethernet Segment (ES) and determines whether the DF election for the ES is revertive or not. Creation of the **preference** context ensures that the PE will run the preference-based DF election algorithm.

Parameters **create** — Mandatory keyword required to create the preference context in an ES.

non-revertive — Configures a non-revertive ES, which ensures that when the Ethernet Segment comes back after a failure, it does not take over an existing active DF PE.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

preference

Syntax [**no**] **preference** *preference*

Context **[Tree]** (config>service>vprn>bgp preference)
[Tree] (config>service>vprn>bgp>group preference)

Full Context configure service vprn bgp group preference
configure service vprn bgp preference

Description This command configures the route preference for routes learned from the configured peer(s).

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The lower the preference the higher the chance of the route being the active route. The OS assigns BGP routes highest default preference compared to routes that are direct, static or learned via MPLS or OSPF.

The **no** form of this command, if used at the global level, reverts to default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default preference 170

Parameters *preference* — Specifies the route preference, expressed as a decimal integer.

Values 1 to 255

Platforms All

preference

Syntax **preference** *preference-value*
no preference

Context **[Tree]** (config>service>vprn>static-route-entry>grt preference)
[Tree] (config>service>vprn>static-route-entry>indirect preference)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel preference)
[Tree] (config>service>vprn>static-route-entry>black-hole preference)
[Tree] (config>service>vprn>static-route-entry>next-hop preference)

Full Context configure service vprn static-route-entry black-hole preference
configure service vprn static-route-entry grt preference
configure service vprn static-route-entry indirect preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn static-route-entry ipsec-tunnel preference
configure service vprn static-route-entry next-hop preference

Description This command specifies the route preference to be assigned to the associated static route. The lower the preference value the more preferred the route is considered.

Table 111 lists the default route preference based on the route source.

Table 111 **Default Route Preference**

Label	Preference	Configurable
Direct attached	0	No
Static route	5	Yes
OSPF Internal routes	10	Yes
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
Aggregate	130	No
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

The **no** form of this command returns the returns the associated static route preference to its default value.

Default preference 5

Parameters *preference-value* — Specifies the route preference value.

Values 1 to 255

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>service>vprn>isis>level preference)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn isis level preference

Description This command configures the preference level of either IS-IS Level 1 or IS-IS Level 2 internal routes. By default, the preferences are listed in the table below.

A route can be learned by the router by different protocols, in which case, the costs are not comparable. When this occurs, the preference is used to decide to which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the table below. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision what route to use is determined by the configuration of the **ecmp** in the config>router context.

Default Default preferences are listed in Table 112.

Table 112 **Default Preferences**

Route Type	Preference	Configurable
Direct attached	0	No
Static route	5	Yes
MPLS	7	—
OSPF internal routes	10	No
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes [1]
IS-IS level 2 external	165	Yes [1]
BGP	170	Yes

Note:

1. External preferences are changed using the **external-preference** command in the **config>router>isis>level** *level-number* context.

Parameters *preference* — The preference for external routes at this level expressed as a decimal integer.

Values 1 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>service>vprn>ospf preference)
[Tree] (config>service>vprn>ospf3 preference)

Full Context configure service vprn ospf preference
configure service vprn ospf3 preference

Description This command configures the preference for OSPF internal routes.

A route can be learned by the router from different protocols in which case the costs are not comparable, when this occurs the preference is used to decide to which route will be used.

Different protocols should not be configured with the same preference. If the same preference is configured, the tiebreaker is per the default preference table as defined in Table 113. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the **ecmp** in the **config**>**router** context.

The **no** form of this command reverts to the default value.

Table 113 **Default Route Preferences**

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes (see Note 1)
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes

Note:

1. Preference for OSPF internal routes is configured with the **preference** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default preference 10 — OSPF internal routes have a preference of 10.

Parameters *preference* — The preference for internal routes expressed as a decimal integer. Defaults for different route types are listed in the following table.

Values 1 to 255

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>service>vprn>rip preference)
[Tree] (config>service>vprn>rip>group preference)
[Tree] (config>service>vprn>rip>group>neighbor preference)
[Tree] (config>service>vprn>ripng preference)
[Tree] (config>service>vprn>ripng>group preference)
[Tree] (config>service>vprn>ripng>group>neighbor preference)

Full Context configure service vprn rip group neighbor preference
configure service vprn rip group preference
configure service vprn rip preference
configure service vprn ripng group neighbor preference
configure service vprn ripng group preference
configure service vprn ripng preference

Description This command sets the route preference assigned to RIP routes. This value can be overridden by route policies.

The **no** form of this command resets the *preference* to the default.

Default no preference

Parameters *preference* — Specifies the preference value.

Values 1 to 255

Default 100

Platforms All

preference

Syntax **preference** *preference-value*
no preference

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy preference)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls forwarding-policies forwarding-policy preference

Description This command configures the preference of an MPLS forwarding policy.

The **no** form of this command removes the preference parameter from the MPLS forwarding policy.

Default preference 255

Parameters *preference-value* — Specifies the preference value.

The *preference-value* parameter allows the user to configure multiple label-binding forwarding policies with the same binding label or multiple endpoint policies with the same endpoint address. This provides the capability to achieve a 1:N backup strategy for the forwarding policy. Only the most preferred, lowest numerically preference value, policy is activated in data path.

Values 1 to 255

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy>p2mp-candidate-path preference)

Full Context configure router p2mp-sr-tree p2mp-policy p2mp-candidate-path preference

Description This command sets the candidate path preference for the P2MP SR tree. The candidate path with the highest preference is the active candidate path.

The **no** form of this command removes the candidate path preference.

Default no preference

Parameters *preference* — Specifies the preference of the candidate path.

Values 0 to 1024

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>router>static-route-entry>black-hole preference)
[Tree] (config>router>static-route-entry>indirect preference)
[Tree] (config>router>static-route-entry>next-hop preference)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router static-route-entry black-hole preference
configure router static-route-entry indirect preference
configure router static-route-entry next-hop preference

Description This command specifies the route preference to be assigned to the associated static route. The lower the preference value the more preferred the route is considered.

Table 114 shows the default route preference based on the route source.

Table 114 **Default Route Preference**

Label	Preference	Configurable
Direct attached	0	No
Static route	5	Yes
OSPF Internal routes	10	Yes
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
Aggregate	130	No
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

The **no** form of this command returns the returns the associated static route preference to its default value.

Default preference 5

Parameters *preference* — Specifies the route preference value.

Values 1 to 255

Platforms All

preference

Syntax [**no**] **preference** *preference*

Context **[Tree]** (config>router>bgp preference)
[Tree] (config>router>bgp>group preference)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>bgp>group>neighbor preference)

Full Context configure router bgp group neighbor preference
configure router bgp group preference
configure router bgp preference

Description This command configures the route preference for routes learned from the configured peers.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The lower the preference the higher the chance of the route being the active route. The router assigns BGP routes highest default preference compared to routes that are direct, static or learned via MPLS or OSPF.

The **no** form of this command used at the global level reverts to default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default preference 170

Parameters *preference* — Specifies the route preference expressed as a decimal integer.

Values 1 to 255

Platforms All

preference

Syntax **preference** *preference*
no preference

Context [Tree] (config>router>isis>level preference)

Full Context configure router isis level preference

Description This command configures the preference level of either IS-IS Level 1 or IS-IS Level 2 internal routes. By default, the preferences are listed in the table below.

A route can be learned by the router by different protocols, in which case, the costs are not comparable. When this occurs, the preference is used to decide to which route will be used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the following table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision what route to use is determined by the configuration of the **ecmp** in the **config>router** context.

Default preference (Level 1) — 15

preference (Level 2) — 18

Parameters *preference* — Specifies the preference for external routes at this level expressed as a decimal integer. The default preferences are listed in Table 115.

Table 115 **Default Internal Route Preferences**

Route Type	Preference	Configurable
Direct attached	0	—
Static-route	5	Yes
OSPF internal routes	10	—
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes [1]
IS-IS level 2 external	165	Yes [1]
BGP	170	Yes

Note:

1. External preferences are changed using the external-preference command in the **config>router>isis>level** *level-number* context.

Values 1 to 255

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>router>ospf preference)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ospf3 preference)

Full Context configure router ospf preference
configure router ospf3 preference

Description This command configures the preference for OSPF internal routes.

A route can be learned by the router from different protocols, in which case, the costs are not comparable. When this occurs, the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in Table 116. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the **ecmp** in the **config>router** context.

The **no** form of this command reverts to the default value.

Default preference 10

Parameters *preference* — Specifies the preference for internal routes expressed as a decimal integer. Defaults for different route types are listed in Table 116.

Table 116 **Route Preference Defaults by Route Type**

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes [1]
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

Note:

1. Preference for OSPF internal routes is configured with the **preference** command.

Values 1 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

preference

Syntax **preference** {**none** | **all**}
no preference

Context **[Tree]** (config>router>ospf>lfa>mhp preference)

Full Context configure router ospf loopfree-alternates multi-homed-prefix preference

Description This command configures the preference for the programming of the multi-homed prefix LFA backup path. This knob can be enabled at a LFA computing node to force the programming of the multi-homed prefix LFA backup path which, in some topologies, can avoid transiting using the best ABR or ASBR.

The **no** form of this command reverts to the default value.

Default preference none

Parameters **none** — Specifies to prefer a LFA, TI-LFA, or RLFA backup path over the multi-homed prefix LFA backup path. Only in cases when the prefix is not protected by LFA, RLFA, or TI-LFA is the multi-homed prefix LFA programmed.

all — Specifies to force the programming of the multi-homed prefix LFA backup path regardless of the outcome of the LFA, TI-LFA, or RLFA backup path computation.

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>router>rip preference)
[Tree] (config>router>rip>group preference)
[Tree] (config>router>rip>group>neighbor preference)
[Tree] (config>router>ripng preference)
[Tree] (config>router>ripng>group preference)
[Tree] (config>router>ripng>group>neighbor preference)

Full Context configure router rip group neighbor preference
configure router rip group preference
configure router rip preference
configure router ripng group neighbor preference
configure router ripng group preference
configure router ripng preference

Description This command configures the preference for RIP routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A route can be learned by the router from different protocols in which case the costs are not comparable. When this occurs, the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in Table 117. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the **ecmp** in the **config>router** context.

The **no** form of the command reverts to the default value.

Default preference 100

Parameters *preference* — Specifies the preference for RIP routes expressed as a decimal integer. Defaults for different route types are listed in Table 117.

Table 117 **Route Preference Defaults by Route Type**

Route Type	Preference	Configurable
Direct attached	0	—
Static routes	5	Yes
OSPF internal	10	Yes
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

Values 0 to 255

Platforms All

preference

Syntax **preference** *preference*

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy preference)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router segment-routing sr-policies static-policy preference

Description This command associates a preference value with a statically defined-segment routing policy. This is an optional parameter.

When there are multiple policies for the same (color, endpoint) combination that are targeted for local installation, only one is selected as the active path for the (color, endpoint). In this selection process (which considers both static local policies and BGP signaled policies), the policy with the highest preference value is preferred over all policies with a lower preference value.

The **no** form of this command reverts to the default value.

Default preference 100

Parameters *preference* — Specifies the preference ID.

Values 0 to 4294967295

Platforms All

preference

Syntax **preference** *preference*
no preference

Context **[Tree]** (config>router>policy-options>policy-statement>name>default-action preference)
[Tree] (config>router>policy-options>policy-statement>entry>action preference)

Full Context configure router policy-options policy-statement entry action preference
configure router policy-options policy-statement name default-action preference

Description This command assigns a route preference to routes matching the route policy statement entry.

If no preference is specified, the default Route Table Manager (RTM) preference for the protocol is used.

The **no** form of this command disables setting an RTM preference in the route policy entry.

Note: This command is supported with the following protocols: RIP import, BGP import, VPRN VRF import (**vrf-import**), and VPRN GRT lookup export (**export-grt**).

Default no preference

Parameters *preference* — Specifies the route preference expressed as a decimal integer.

Values 1 to 255 (0 represents unset - MIB only)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name — The preference parameter variable name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

20.288 preference-option

preference-option

Syntax [**no**] **preference-option**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>asel preference-option)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>asel>clnt-mac preference-option)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>asel>srvr preference-option)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>asel preference-option)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>asel>clnt-mac preference-option)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>asel>srvr preference-option)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>asel preference-option)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>asel>clnt-mac preference-option)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>asel>srvr preference-option)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac preference-option
configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection preference-option
configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server preference-option
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac preference-option
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection preference-option
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server preference-option
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection client-mac preference-option
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection preference-option
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection server preference-option

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the DHCPv6 preference option that is inserted in the DHCPv6 advertise message.

The **no** form of this command removes the preference option.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.289 preferred

preferred

Syntax [**no**] **preferred**

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy preferred)

Full Context configure isa nat-group inter-chassis-redundancy preferred

Description This command sets the preference for activity of a **nat-group** in stateful inter-chassis redundancy configuration if both nodes have equal health. An example of where this can be useful is in a load balancing environment where the activity of NAT groups can be distributed between the two redundant nodes.

A **nat-group** with **preferred** command configured on a node that freshly became part of multi-chassis redundancy, takes over activity from an existing and traffic-serving node with equal health that does not have the **preferred** command configured. This causes a switchover and a brief interruption in traffic flow.

By default the preferred status is not set for the node.

The **no** form of this command reverts to the default.

Default no preferred

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.290 preferred-lifetime

preferred-lifetime

Syntax **preferred-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
preferred-lifetime infinite
no preferred-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>ipv6-lease-times preferred-lifetime)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ipv6-lease-times preferred-lifetime)

Full Context configure subscriber-mgmt local-user-db ipoe host ipv6-lease-times preferred-lifetime
configure subscriber-mgmt local-user-db ppp host ipv6-lease-times preferred-lifetime

Description This command specifies the preferred lifetime for the lease times. When the preferred lifetime expires, then any derived addresses are deprecated.

The **no** form of this command reverts to the default.

Parameters **infinite** — Specifies that the valid lifetime is infinite.

preferred-lifetime — Specifies the preferred lifetime.

Values

days *days*	0 to 3650
hrs *hours*	0 to 23
min *minutes*	0 to 59
sec *seconds*	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preferred-lifetime

Syntax **preferred-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no preferred-lifetime

Context [Tree] (config>router>dhcp6>server>defaults preferred-lifetime)
[Tree] (config>router>dhcp6>server>pool>prefix preferred-lifetime)
[Tree] (config>service>vprn>dhcp6>server>defaults preferred-lifetime)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix preferred-lifetime)

Full Context configure router dhcp6 local-dhcp-server defaults preferred-lifetime
configure router dhcp6 local-dhcp-server pool prefix preferred-lifetime
configure service vprn dhcp6 local-dhcp-server defaults preferred-lifetime
configure service vprn dhcp6 local-dhcp-server pool prefix preferred-lifetime

Description This command configures the preferred lifetime.

The **no** form of this command reverts to the default value.

Default preferred-lifetime hrs 1

Parameters *preferred-lifetime* — Specifies the preferred time for a prefix.

Values

days:	0 to 3650
hours:	0 to 23

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

minutes:	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router dhcp6 local-dhcp-server pool prefix preferred-lifetime
- configure service vprn dhcp6 local-dhcp-server pool prefix preferred-lifetime

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn dhcp6 local-dhcp-server defaults preferred-lifetime
- configure router dhcp6 local-dhcp-server defaults preferred-lifetime

preferred-lifetime

Syntax **preferred-lifetime** *seconds*
preferred-lifetime infinite
no preferred-lifetime

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6>pfx-delegate>prefix preferred-lifetime)
[Tree] (config>service>vprn>if>ipv6>dhcp6>pfx-delegate>prefix preferred-lifetime)

Full Context configure service ies interface ipv6 dhcp6-server prefix-delegation prefix preferred-lifetime
configure service vprn interface ipv6 dhcp6-server prefix-delegation prefix preferred-lifetime

Description This command configures the IPv6 prefix/mask preferred lifetime. The preferred-lifetime value cannot be bigger than the valid-lifetime value.

The **no** form of this command reverts to the default value.

Default **preferred-lifetime** 604800 (7 days)

Parameters *seconds* — Specifies the time, in seconds, that this prefix remains preferred.

Values 1 to 4294967294

infinite — Specifies that this prefix remains preferred infinitely.

Platforms All

preferred-lifetime

Syntax **preferred-lifetime** *seconds*
preferred-lifetime infinite
no preferred-lifetime

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>rtr-adv>pfx-opt preferred-lifetime)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>ipv6>rtr-adv>pfx-opt preferred-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv>pfx-opt preferred-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv>pfx-opt preferred-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements prefix-options preferred-lifetime
configure service ies subscriber-interface ipv6 router-advertisements prefix-options preferred-lifetime
configure service vprn subscriber-interface group-interface ipv6 router-advertisements prefix-options preferred-lifetime
configure service vprn subscriber-interface ipv6 router-advertisements prefix-options preferred-lifetime

Description This command specifies the remaining time for this prefix to be preferred, thus time until deprecation.

The **no** form of this command reverts to the default.

Default preferred-lifetime 3600

Parameters *seconds* — Specifies the time for the prefix to remain preferred on this group-interface in seconds.

Values 0 to 4294967295

infinite — Specifies that the remaining time will never expire. The value 4294967295 is interpreted as infinite.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preferred-lifetime

Syntax **preferred-lifetime** *seconds*
preferred-lifetime infinite
no preferred-lifetime

Context [Tree] (config>subscr-mgmt>rtr-adv>pfx-opt>stateful preferred-lifetime)
[Tree] (config>subscr-mgmt>rtr-adv>pfx-opt>stateless preferred-lifetime)

Full Context configure subscriber-mgmt router-advertisement-policy prefix-options stateful preferred-lifetime
configure subscriber-mgmt router-advertisement-policy prefix-options stateless preferred-lifetime

Description This command specifies the remaining time for this prefix to be preferred.

The **no** form of this command reverts to the default.

Default preferred-lifetime 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the time, in seconds, for the prefix to remain preferred.

Values 0, 900 to 86400

infinite — Specifies that the remaining time never expires.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

preferred-lifetime

Syntax **preferred-lifetime infinite**
preferred-lifetime [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no preferred-lifetime

Context **[Tree]** (config>service>ies>sub-if>ipv6>dhcp6>proxy-server preferred-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy-server preferred-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>proxy-server preferred-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server preferred-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server preferred-lifetime
configure service ies subscriber-interface ipv6 dhcp6 proxy-server preferred-lifetime
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server preferred-lifetime
configure service vprn subscriber-interface ipv6 dhcp6 proxy-server preferred-lifetime

Description This command configures the preferred lifetime. When the preferred lifetime expires, any derived addresses are deprecated.

Default preferred-lifetime hrs 1

Parameters **infinite** — Specifies that the preferred lifetime is infinite.

days *days* — Specifies the number of days of a preferred lifetime.

Values 0 to 49710

hrs *hours* — Specifies the number of hours of a preferred lifetime.

Values 0 to 23

min *minutes* — Specifies the number of minutes of a preferred lifetime.

Values 0 to 59

sec *seconds* — Specifies the number of seconds of a preferred lifetime.

Values 0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

preferred-lifetime

Syntax [**no**] **preferred-lifetime** {*seconds* | **infinite**}

Context **[Tree]** (config>router>router-advert>if>prefix preferred-lifetime)
[Tree] (config>service>vprn>router-advert>if>prefix preferred-lifetime)

Full Context configure router router-advertisement interface prefix preferred-lifetime
configure service vprn router-advertisement interface prefix preferred-lifetime

Description This command configures the remaining length of time in seconds that this prefix will continue to be preferred, such as, time until deprecation. The address generated from a deprecated prefix should not be used as a source address in new communications, but packets received on such an interface are processed as expected.

Default preferred-lifetime 604800

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be preferred.

Values 0 to 4294967294

infinite — Specifies that the prefix will always be preferred. A value of 4,294,967,295 represents infinity.

Platforms All

20.291 prefix

prefix

Syntax **prefix** *ipv6-addr/prefix-length* [**failover** {**local** | **remote** | **access-driven**}] [**pd**] [**wan-host**] [**create**]
no prefix *ipv6-addr/prefix-length*

Context **[Tree]** (config>router>dhcp6>server>pool prefix)
[Tree] (config>service>vprn>dhcp6>server>pool prefix)

Full Context configure router dhcp6 local-dhcp-server pool prefix
configure service vprn dhcp6 local-dhcp-server pool prefix

Description This command allocates a prefix to a pool from which Prefix Delegation prefixes and or WAN addresses can be assigned for DHCP6.

The **no** form of this command removes the prefix parameters from the configuration.

Default prefix failover local

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *prefix ipv6-addr/prefix-length* — Specifies the prefix.

Values

ipv6-address	x:x:x:x:x:x:x	(eight 16-bit pieces)
		x:x:x:x:x:d.d.d.d
		x [0 to FFFF]H
		d [0 to 255]D
prefix-length		1 to 128

failover {**local** | **remote | access-driven**} — This command designates a prefix as local, remote, or access-driven. This is used when multi-chassis synchronization is enabled.

Values **local** — An IPv6 prefix designated as local is used for new lease grants or to renew the existing lease grants. Local prefix designation should be always paired with the remote designation of the same prefix on the peering node.

The IPv6 prefix configured as local on one node can only be configured as remote on the other node. No other combination is allowed between the two nodes for an IPv6 prefix that is configured as local.

The DHCPv6 relay could point to both IPv6 DHCP server addresses— the one hosting the local IPv6 prefix and the one hosting the corresponding remote IPv6 prefix. Under normal circumstances the new lease will always be allocated from the local IPv6 prefix while the leases can be renewed from either IPv6 prefix (local or remote). Under network failure, the remote IPv6 prefix can be taken over according to the intercommunication link state transitions and associated timers.

remote — A prefix designated as remote is used only to renew the existing DHCP leases. The new leases are assigned from it only after the **maximum-client-lead-time** and **partner-down-delay** *time* elapses.

To ensure faster takeover, the partner-down-delay can be set to 0 and the MCLT time can be ignored. Extra caution should be exercised when enabling this mode of operation, as described in the configuration guides.

The IPv6 prefix configured as remote on one node can only be configured as local on the other node. No other combination is allowed between the two nodes for an IP address ranges that is configured as remote.

access-driven — A prefix designated as access-driven is like local (a new prefix assignment as well as a renewal). However, as the prefix is shared between the redundant server pair, the following additional conditions should be met to avoid duplicate address allocations:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- A dual home access protection mechanism such as SRRP or MC-LAG must ensure a single active path from the DHCP client to the server.
- The DHCP relay should point to the local server only.

pd — Specifies that this aggregate is used by IPv6 ESM hosts for DHCPv6 prefix-delegation.

wan-host — Specifies that this aggregate is used by IPv6 ESM hosts for local addressing or by a routing gateway's WAN interface.

create — Keyword used to create the prefix configuration. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax [**no**] **prefix** *ipv6-address/prefix-length*

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6-server>pfx-delegate prefix)

Full Context configure service ies interface ipv6 dhcp6-server prefix-delegation prefix

Description This command specifies the IPv6 prefix that is delegated by this system.

The **no** form of this command reverts to the default.

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address on the interface

Values

ipv6-address/prefix:	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x [0 to FFFF]H
		d [0 to 255]D
prefix-length		1 to 128

Platforms All

prefix

Syntax **prefix** *ipv6-address/prefix-length* [**pd**] [**wan-host**]
no prefix *ipv6-address/prefix-length*

Context **[Tree]** (config>service>ies>sub-if>ipv6>sub-pfx prefix)
[Tree] (config>service>vprn>sub-if>ipv6>sub-pfx prefix)

Full Context configure service ies subscriber-interface ipv6 subscriber-prefixes prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface ipv6 subscriber-prefixes prefix

Description This command allows a list of prefixes (using the prefix command multiple times) to be routed to hosts associated with this subscriber interface. Each prefix is represented in the associated FDB with a reference to the subscriber interface. Prefixes are defined as being for prefix delegation (pd) or use on a WAN interface or host (wan-host).

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the 128-bit IPv6 address.

Values 128-bit hexadecimal IPv6 address in compressed form

prefix-length — Specifies the length of any associated aggregate prefix.

Values 32 to 63

pd — Specifies that this aggregate is used by IPv6 ESM hosts for DHCPv6 prefix-delegation.

wan-host — Specifies that this aggregate is used by IPv6 ESM hosts for local addressing or by a routing gateway's WAN interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax **prefix** *low-order-vsi-id*
no prefix

Context **[Tree]** (config>service>vpls>bgp-ad>vsi-id prefix)

Full Context configure service vpls bgp-ad vsi-id prefix

Description This command specifies the low-order 4 bytes used to compose the Virtual Switch Instance Identifier (VSI-ID) to use for NLRI in BGP auto-discovery in this VPLS service.

If no value is set, the system IP address will be used.

Default no prefix

Parameters *low-order-vsi-id* — Specifies a unique VSI ID

Values 0— 4294967295

Platforms All

prefix

Syntax [**no**] **prefix** *ip-prefix*|*prefix-length*

Context **[Tree]** (config>service>vprn>bgp>group>dynamic-neighbor>match prefix)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn bgp group dynamic-neighbor match prefix

Description This command configures a prefix to accept dynamic BGP sessions (sessions from source IP addresses not matching any configured neighbor addresses). A dynamic session is associated with the group having the longest match prefix entry for the source IP address of the peer. The group association determines local parameters that apply to the session, including the local AS, the local IP address, the MP-BGP families, the import and export policies, and so on.

The **no** form of this command removes a prefix entry.

Parameters *ip-prefix/prefix-length* — Specifies a prefix from which to accept dynamic BGP sessions.

Values
ipv4-prefix — a.b.c.d (host bits must be 0)
ipv4-prefix-length — 0 to 32
ipv6-prefix — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — [0 to FFFF]H
d — [0 to 255]D
ipv6-prefix-length — 0 to 128

Platforms All

prefix

Syntax [**no**] **prefix** *ipv6-prefixIprefix-length*

Context **[Tree]** (config>service>vprn>router-advert>if prefix)

Full Context configure service vprn router-advertisement interface prefix

Description This command configures an IPv6 prefix in the router advertisement messages. To support multiple IPv6 prefixes, use multiple prefix statements. No prefix is advertised until explicitly configured using prefix statements.

Parameters *ipv6-prefix* — Specifies the IP prefix for prefix list entry in dotted decimal notation.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-length	0 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix-length — Specifies a route must match the most significant bits and have a prefix length.

Values 1 to 128

Platforms All

prefix

Syntax **prefix** *prefix-string*
no prefix

Context **[Tree]** (config>app-assure>group>cflowd>export-override prefix)

Full Context configure application-assurance group cflowd export-override prefix

Description This command specifies the *prefix-string* associated with the **export-override**.

Parameters *prefix-string* — Up to an 8 character string. If the 8 character prefix is "ABCDEFG_" for a particular node, the cflowd export override would generate IPv4 interface names such as ABCDEFG_255.255.255.255 or IPv6 as ABCDEFG_2001:DB8:EF01:2345::/64. By default the prefix will be left blank.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax **prefix** *ip-prefix/ip-prefix-length* [**name** *prefix-name*]
no prefix *ip-prefix/ip-prefix-length*

Context **[Tree]** (config>app-assure>group>ip-prefix-list prefix)

Full Context configure application-assurance group ip-prefix-list prefix

Description This command configures an IP prefix within the list.

The **no** form of this command removes the IP prefix from the configuration.

Parameters *ip-prefix/ip-prefix-length* — The IP address in dotted decimal notation.

Values

ipv4-prefix	*a.b.c.d* (host bits must be 0)	
ipv4-prefix-length	0 to 32	
ipv6-prefix	*x:x:x:x:x:x:x:x* (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	prefix-name	32 characters max

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax **prefix** *ip-prefix/length* **subscriber-type** *nat-sub-type* **nat-policy** *nat-policy-name* [**create**]
prefix *p-prefix/length* **subscriber-type** *nat-sub-type*
no prefix *ip-prefix/length* **subscriber-type** *nat-sub-type*

Context **[Tree]** (config>service>vprn>nat>inside>deterministic prefix)
[Tree] (config>router>nat>inside>deterministic prefix)

Full Context configure router nat inside deterministic prefix
configure service vprn nat inside deterministic prefix

Description This command is applicable only to deterministic NAT (LSN44 or DS-Lite). It configures prefixes on the inside and their association with outside deterministic pools via the nat-policy. Subscribers within the prefix will be deterministically mapped to outside IP addresses and corresponding port-ranges in the associated pool.

Multiple prefixes within an inside routing instance can be defined and they can reference different nat-policies (and therefore outside pools and routing instances). Moreover, prefixes from multiple routing instances can share the same deterministic pool.

Non-deterministic NAT can be used simultaneously with deterministic NAT within the same inside routing instance. However, they cannot share the same pool.

Prefixes can be added/removed under the condition that the associated deterministic pool is in a **no shutdown** mode.

Removing a prefix or modifying the map statement under it requires that the prefix be in a ‘shutdown’ mode.

The subscribers under the prefix are mapped deterministically into the outside IPv4 addresses and port ranges. The subscribers in LSN44 are the IPv4 addresses under the configured prefix, while in DS-Lite the subscribers are IPv6 source addresses that fall under the configured prefix OR IPv6 sub-prefixes whose length is determined by the DS-Lite subscriber-prefix-length command.

Parameters *ip-prefix/length* — A prefix on the inside encompassing subscribers that will be deterministically mapped to an outside IP address and port block in the corresponding pool.

Values

<ip-prefix/ip-pref*>	<ipv4-prefix>/<ipv4-prefix-length>
	<ipv6-prefix>/<ipv6-prefix-length>

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

<ipv4-prefix>	a.b.c.d (host bits must be 0)
<ipv4-prefix-length>	[0 to 32]
<ipv6-prefix>	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0 to FFFF]H d - [0 to 255]D
<ipv6-prefix-length>	[0 to 128]
<nat-sub-type>	classic-lsn-sub, dslite-lsn-sub
<nat-policy-name>	Reference to a nat-policy that points to an outside pool and outside routing instance up to 32 characters in length.

create — Keyword used to create the particular prefix instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax **prefix** *ipv6-prefix/prefix-length*
no prefix

Context **[Tree]** (config>service>vprn>nat>inside>nat64 prefix)
[Tree] (config>router>nat>inside>nat64 prefix)

Full Context configure router nat inside nat64 prefix
configure service vprn nat inside nat64 prefix

Description This command configures the IPv6 prefix used to derive the IPv6 address from the IPv4 address, and is same as the prefix used by DNS64 to generate AAAA record returned for IPv4 endpoint resolution. NAT64 node announces this prefix in routing to attract traffic from IPv6 hosts. If the prefix is not configured, then a well-known prefix, 64:FF9B::/96, is used.

The **no** form of the command removes the prefix from the NAT64 configuration.

Parameters *ipv6-prefix/prefix-length* — Specifies the NAT64 destination prefix.

Values

ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0..FFFF]H d - [0..255]D
prefix-length	32, 40, 48, 56, 64, 96

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix

Syntax **prefix** *ip-prefix/length* [**nat-policy** *nat-policy-name*]
no prefix *ip-prefix/length*

Context **[Tree]** (config>service>nat>nat-prefix-list prefix)

Full Context configure service nat nat-prefix-list prefix

Description This command creates a prefix entry in the nat-prefix-list.

This prefix can be used to identify traffic with specific destination IP that needs to be associated with corresponding nat-policy (and implicitly the NAT pool) for L2-aware subscribers. In this fashion, a single L2-aware subscriber can direct traffic to multiple NAT pools, depending on the traffic destination.

Another use for a prefix is in DNAT-only application (DNAT without SNAPT). In this case the prefix identifies the inside source IP range that will be explicitly configured to ensure proper downstream routing in dNAT-only case.

The nat-prefix-list cannot reference the default nat-policy (the one that is referenced in the subscriber-profile).

The **no** form of the command reverts to the default.

Default none

Parameters *ip-prefix/length* — Specifies the IP prefix for nat prefix list entry in dotted decimal notation.

Values *ip-prefix:* a.b.c.d (host bits must be 0) *ipv4-prefix-length:* 0 to 32

nat-policy *nat-policy-name* — Specifies the NAT policy name. Allowed values are any string up to 32 characters composed of printable,7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes..

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax **prefix** *prefixIprefix-length* [**create**]
no prefix *prefixIprefix-length*

Context **[Tree]** (config>router>firewall>domain prefix)
[Tree] (config>service>vprn>firewall>domain prefix)

Full Context configure router firewall domain prefix
configure service vprn firewall domain prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a prefix for which firewall functionality will apply within the domain. Prefixes cannot be shared or duplicated across multiple domains in the same routing context. A domain can contain multiple prefixes.

The **no** form of the command removes the prefix from the domain.

Parameters **create** — Mandatory keyword used when creating a prefix entry.

prefix/prefix-length — Specifies the prefix.

Values *prefix* — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — 0 to FFFF (in hexadecimal)
d — 0 to 255 (in decimal)
prefix-length — 1 to 64

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

prefix

Syntax **prefix** *ip-address*
no prefix

Context **[Tree]** (config>router>bier>template>sub-domain prefix)

Full Context configure router bier template sub-domain prefix

Description This command specifies the prefix used for BFR. The prefix should be an IPv4 /32 address. The prefix can be a loopback interface or system IP address.

The **no** form of this command removes the prefix.

Parameters *ip-address* — Specifies the IP address to be used as the BFR prefix in dotted decimal format.

Platforms All

prefix

Syntax **prefix** *ip-prefix/prefix-length* [**create**]
no prefix *ip-prefix/prefix-length*

Context **[Tree]** (config>test-oam>twamp>server prefix)

Full Context configure test-oam twamp server prefix

Description This command configures an IP address prefix containing one or more TWAMP clients. For a TWAMP client to connect to the TWAMP server (and subsequently conduct tests) it must establish the control connection using an IP address that is part of a configured prefix.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix/prefix-length* — Specifies an IPv4 or IPv6 address prefix.

Values

ipv4-prefix:	a.b.c.d (host bits must be 0)
ipv4-prefix-le:	0 to 32
ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-le:	0 to 128

prefix length — Specifies the prefix length.

Values 0 to128

create — Creates a prefix instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

prefix

Syntax **prefix** *ip-prefix/prefix-length* [**create**]
no prefix *ip-prefix/prefix-length*

Context **[Tree]** (config>router>twamp-light>reflector prefix)
[Tree] (config>service>vprn>twamp-light>reflector prefix)

Full Context configure router twamp-light reflector prefix
configure service vprn twamp-light reflector prefix

Description This command defines which TWAMP Light packet prefixes the reflector processes.

The **no** form of this command with the specific prefix removes the accepted source.

Parameters *ip-prefix/prefix-length* — Specifies the IPv4 or IPv6 address and length.

Values

ipv4-prefix:	a.b.c.d (host bits must be 0)
ipv4-prefix-le:	0 to 32
ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-le:	0 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Creates a prefix instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

prefix

Syntax [**no**] **prefix** *ip-prefix/prefix-length*

Context **[Tree]** (config>qos>match-list>ip-prefix-list prefix)

Full Context configure qos match-list ip-prefix-list prefix

Description This command adds an IPv4 address prefix to an existing IPv4 address prefix match list.

To add a set of unique prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv4 address space.

An IPv4 prefix addition will be blocked, if resource exhaustion is detected anywhere in the system because of QoS Policies that use this IPv4 address prefix list.

The **no** form of this command deletes the specified prefix from the list.

Parameters *ip-prefix* — A valid IPv4 address prefix in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (host bit must be 0)

prefix-length — Length of the entered IP prefix

Values 1 to 32

Platforms All

prefix

Syntax [**no**] **prefix** *ipv6-prefix/prefix-length*

Context **[Tree]** (config>qos>match-list>ipv6-prefix-list prefix)

Full Context configure qos match-list ipv6-prefix-list prefix

Description This command adds an IPv6 address prefix to an existing IPv6 address prefix match list.

To add set of unique prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv6 address space.

An IPv6 prefix addition will be blocked if resource exhaustion is detected anywhere in the system because of QoS Policies that use this IPv6 address prefix list.

The **no** form of this command deletes the specified prefix from the list.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-prefix* — Specifies the IPv6 prefix for the IP match criterion in hex digits.

Values ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

prefix-length — Specifies the IPv6 prefix length for the IPv6 address expressed as a decimal integer.

Values 1 to 128

Platforms All

prefix

Syntax [**no**] **prefix** *ip-prefix/prefix-length*

Context **[Tree]** (config>filter>match-list>ip-prefix-list prefix)

Full Context configure filter match-list ip-prefix-list prefix

Description This command adds an IPv4 address prefix to an existing IPv4 address prefix match list.

The **no** form of this command deletes the specified prefix from the list.

Operational Notes:

To add set of unique prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv4 address space.

An IPv4 prefix addition will be blocked, if resource exhaustion is detected anywhere in the system because of filter policies that use this IPv4 address prefix list.

Parameters *ip-prefix* — Specifies a valid IPv4 address prefix in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (host bit must be 0)

prefix-length — Specifies the length of the entered IPv4 prefix.

Values 0 to 32

Platforms All

prefix

Syntax [**no**] **prefix** *ipv6-prefix/prefix-length*

Context **[Tree]** (config>filter>match-list>ipv6-prefix-list prefix)

Full Context configure filter match-list ipv6-prefix-list prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command adds an IPv6 address prefix to an existing IPv6 address prefix match list.

The **no** form of this command deletes the specified prefix from the list.

Operational Notes:

To add set of different prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv6 address space.

An IPv6 prefix addition will be blocked, if resource exhaustion is detected anywhere in the system because of filter policies that use this IPv6 address prefix list.

Parameters *ipv6-prefix/prefix-length* — Specifies an IPv6 address prefix written as hexadecimal numbers separated by colons with host bits set to 0. One string of zeros can be omitted, so 2001:db8::700:0:217A is equivalent to 2001:db8:0:0:0:700:0:217A.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

prefix-length — Specifies the length of the entered IPv6 prefix.

Values 1 to 128

Platforms All

prefix

Syntax [**no**] **prefix** *ipv6-prefixIprefix-length*

Context **[Tree]** (config>router>router-advert>if prefix)

Full Context configure router router-advertisement interface prefix

Description This command configures an IPv6 prefix in the router advertisement messages. To support multiple IPv6 prefixes, use multiple prefix statements. No prefix is advertised until explicitly configured using prefix statements.

Parameters *ipv6-prefix* — The IP prefix for prefix list entry in dotted decimal notation.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D
ipv6-prefix-length	0 to 128	

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix-length — Specifies a route must match the most significant bits and have a prefix length.

Values 1 to 128

Platforms All

prefix

Syntax [**no**] **prefix** *ip-prefix/ip-prefix-length*

Context **[Tree]** (config>router>bgp>group>dynamic-neighbor>match prefix)

Full Context configure router bgp group dynamic-neighbor match prefix

Description This command configures a prefix to accept dynamic BGP sessions (sessions from source IP addresses not matching any configured neighbor addresses). A dynamic session is associated with the group having the longest match prefix entry for the source IP address of the peer. The group association determines local parameters that apply to the session, including the local AS, the local IP address, the MP-BGP families, the import and export policies, and so on.

The **no** form of this command removes a prefix entry.

Parameters *ip-prefix/ip-prefix-length* — Specifies a prefix from which to accept dynamic BGP sessions.

Values *ipv4-prefix* — a.b.c.d (host bits must be 0)
ipv4-prefix-length — 0 to 32
ipv6-prefix — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — [0 to FFFF]H
d — [0 to 255]D
ipv6-prefix-length — 0 to 128

Platforms All

prefix

Syntax [**no**] **prefix** *ip-prefix/prefix-length* [**exact** | **longer** | **through** *length* | **prefix-length-range** *length1-length2* | **to** *ip-prefix/prefix-length* | **address-mask** *mask-pattern*]

Context **[Tree]** (config>router>policy-options>prefix-list prefix)

Full Context configure router policy-options prefix-list prefix

Description This command creates a prefix entry in the route policy prefix list.

The **no** form of this command deletes the prefix entry from the prefix list.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix/prefix-length* — Specifies the IP prefix and length for the prefix list entry in dotted decimal notation.

Values ipv4-prefix:
- a.b.c.d (host bits must be 0)

ipv4-prefix-length: [0 to 32]

ipv6-prefix:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

ipv6-prefix-length: [0 to 128]

exact — Specifies the prefix list entry only matches the route with the specified *ip-prefix* and prefix *mask* (length) values.

longer — Specifies the prefix list entry matches any route that matches the specified *ip-prefix* and prefix *mask* length values equal to or greater than the specified mask.

through *length* — Specifies the prefix list entry matches any route that matches the specified ip-prefix and has a prefix length between the specified *length* values inclusive.

Values 0 to 32

prefix-length-range *length1* **-** *length2* — Specifies a route must match the most significant bits and have a prefix length with the given range. The range is inclusive of start and end values.

Values 0 to 32, *length2* > *length1*

to *ip-prefix/prefix-length* — Specifies a second IP prefix and length used in route policy prefix lists. A route matches prefix1 to prefix2 if it matches prefix1 and prefix2 according to their respective prefix lengths and if the route's own prefix length is between the prefix lengths of prefix1 and prefix2. It could take many individual 'exact' match prefix entries to reproduce the same logic.

mask-pattern — Specifies the address mask to use for matching entries to this prefix entry. A route matches a prefix and address mask combination if the bitwise logical AND of this prefix and the mask equals the bitwise logical AND of the route's address and the same mask and, additionally, the prefix length of the route matches the prefix length of the prefix entry.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

prefix

Syntax **prefix**

Context **[Tree]** (config>router>segment-routing>srv6>locator prefix)

Full Context configure router segment-routing segment-routing-v6 locator prefix

Description Commands in this context configure IPv6 prefix parameters for an SRv6 locator.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

20.292 prefix-attributes-tlv

prefix-attributes-tlv

Syntax [**no**] **prefix-attributes-tlv**

Context **[Tree]** (config>service>vprn>isis prefix-attributes-tlv)

Full Context configure service vprn isis prefix-attributes-tlv

Description This command enables IS-IS Prefix Attributes TLV support to exchange extended IPv4 and IPv6 reachability information. Extended reachability information is required for traffic engineering features using path computation element (PCE) or optimal route reflection.

The **no** form of this command removes the **prefix-attributes-tlv** configuration.

Default no prefix-attributes-tlv

Platforms All

prefix-attributes-tlv

Syntax [**no**] **prefix-attributes-tlv**

Context **[Tree]** (config>router>isis prefix-attributes-tlv)

Full Context configure router isis prefix-attributes-tlv

Description This command enables IS-IS Prefix Attributes TLV support to exchange extended IPv4 and IPv6 reachability information. Extended reachability information is required for traffic engineering features using path computation element (PCE) or optimal route reflection.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the **prefix-attributes-tlv** configuration.

Default no prefix-attributes-tlv

Platforms All

20.293 prefix-delegation

prefix-delegation

Syntax [**no**] **prefix-delegation**

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6-server prefix-delegation)

Full Context configure service ies interface ipv6 dhcp6-server prefix-delegation

Description This command enables the prefix delegation options for delegating a long-lived prefix from a delegating router to a requesting router, where the delegating router does not require knowledge about the topology of the links in the network to which the prefixes are assigned.

The **no** form of this command disables prefix-delegation.

Platforms All

20.294 prefix-exclude

prefix-exclude

Syntax **prefix-exclude** *policy-name* [*policy-name*]
no prefix-exclude

Context **[Tree]** (config>router>ldp>aggregate-prefix-match prefix-exclude)

Full Context configure router ldp aggregate-prefix-match prefix-exclude

Description This command specifies the policy name containing the prefixes to be excluded from the aggregate prefix match procedures. In this case, LDP will perform an exact match of a specific FEC element prefix as opposed to a longest match of one or more LDP FEC element prefixes, against this prefix when it receives a FEC-label binding or when a change to this prefix occurs in the routing table.

The **no** form of this command removes all policies from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no prefix-exclude

Parameters *policy-name* — Specifies the route policy name, up to five. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

Platforms All

prefix-exclude

Syntax [**no**] **prefix-exclude** *ip-prefix/prefix-length*

Context **[Tree]** (config>filter>match-list>ip-pfx-list prefix-exclude)

Full Context configure filter match-list ip-prefix-list prefix-exclude

Description This command excludes IPv4 prefix(es) from an **ip-prefix-list.** The **prefix-exclude** command is mutually exclusive with **apply-path**.

The **no** form of this command deletes the specified excluded prefixes from the **ip-prefix-list**.

Parameters *ip-prefix* — Specifies a valid IPv4 address prefix in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (host bit must be 0)

prefix-length — Specifies the length of the entered IPv4 prefix.

Values 0 to 32

Platforms All

prefix-exclude

Syntax [**no**] **prefix** *ipv6-prefix/prefix-length*

Context **[Tree]** (config>filter>match-list>ipv6-pfx-list prefix-exclude)

Full Context configure filter match-list ipv6-prefix-list prefix-exclude

Description This command excludes IPv6 prefix(es) from an **ipv6-prefix-list**.The **prefix-exclude** command is mutually exclusive with **apply-path**.

The **no** form of this command deletes the specified excluded prefixes from the **ipv6-prefix-list**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-prefix/prefix-length* — Specifies an IPv6 address prefix written as hexadecimal numbers separated by colons with host bits set to 0. One string of zeros can be omitted, so 2001:db8::700:0:217A is equivalent to 2001:db8:0:0:0:700:0:217A.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

prefix-length — Specifies the length of the entered IPv6 prefix.

Values 1 to 128

Platforms All

20.295 prefix-ipv4

prefix-ipv4

Syntax **prefix-ipv4** {**enable** | **disable**}

Context **[Tree]** (config>router>ldp>if-params>if>ipv4>fec-type-capability prefix-ipv4)
[Tree] (config>router>ldp>if-params>if>ipv6>fec-type-capability prefix-ipv4)
[Tree] (config>router>ldp>session-params>peer>fec-type-capability prefix-ipv4)

Full Context configure router ldp interface-parameters interface ipv4 fec-type-capability prefix-ipv4
configure router ldp interface-parameters interface ipv6 fec-type-capability prefix-ipv4
configure router ldp session-parameters peer fec-type-capability prefix-ipv4

Description This command enables or disables IPv4 prefix FEC capability on the session or interface.

The **config>router>ldp>if-params>if>ipv6>fec-type-capability>prefix-ipv4** command is not supported on the 7450 ESS.

Platforms All

20.296 prefix-ipv6

prefix-ipv6

Syntax **prefix-ipv6** {**enable** | **disable**}

Context **[Tree]** (config>router>ldp>if-params>if>ipv4>fec-type-capability prefix-ipv6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ldp>if-params>if>ipv6>fec-type-capability prefix-ipv6)
[Tree] (config>router>ldp>session-params>peer>fec-type-capability prefix-ipv6)

Full Context configure router ldp interface-parameters interface ipv4 fec-type-capability prefix-ipv6
configure router ldp interface-parameters interface ipv6 fec-type-capability prefix-ipv6
configure router ldp session-parameters peer fec-type-capability prefix-ipv6

Description This command enables or disables IPv6 prefix FEC capability on the session or interface.

This command is not supported on the 7450 ESS.

Platforms All

20.297 prefix-limit

prefix-limit

Syntax **prefix-limit** *limit*
no prefix-limit

Context [Tree] (config>subscr-mgmt>bgp-prng-plcy prefix-limit)

Full Context configure subscriber-mgmt bgp-peering-policy prefix-limit

Description This command configures the maximum number of routes BGP can learn from a peer.

When the number of routes reaches 90% of this limit, an SNMP trap is sent. When the limit is exceeded, the BGP peering is dropped and disabled.

The **no** form of this command removes the **prefix-limit**.

Parameters *limit* — The number of routes that can be learned from a peer, expressed as a decimal integer.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

prefix-limit

Syntax **prefix-limit** *family limit* [**log-only**] [**threshold** *percent***age**] [**idle-timeout** {*minutes* | **forever**}] [**log-only**] [**post-import**]
no prefix-limit *family*

Context [Tree] (config>service>vprn>bgp>group prefix-limit)
[Tree] (config>service>vprn>bgp>group>neighbor prefix-limit)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn bgp group neighbor prefix-limit
configure service vprn bgp group prefix-limit

Description This command configures the maximum number of BGP routes that can be received from a peer before administrative action is taken. The administrative action can be the generation of a log event or taking down the session. If a session is taken down, then it can be brought back up automatically after an idle-timeout period, or else it can be configured to stay down ('forever') until the operator performs a reset.

The **prefix-limit** command allows each address family to have its own limit; a set of address family limits can be applied to one neighbor or to all neighbors in a group.

The **no** form of this command removes the **prefix-limit**.

Default No prefix limits for any address family.

Parameters *percent* — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 1 to 100

family — The address family to which the limit applies.

Values ipv4, label-ipv4, ipv6, mcast-ipv4, flow-ipv4, flow-ipv6, mcast-ipv6

limit — The number of routes that can be learned from a peer expressed as a decimal integer.

Values 1 to 4294967295

minutes — Specifies duration in minutes before automatically re-establishing a session.

Values 1 to 1024

forever — Specifies that the session is reestablished only after **clear router bgp** command is executed.

log-only — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is reached. However, the BGP session is not taken down.

post-import — Specifies that the limit should be applied only to the number of routes that are accepted by import policies.

Platforms All

prefix-limit

Syntax **prefix-limit** *limit* [**log-only**] [**threshold** *percent*] [**overload-timeout** {*seconds* | **forever**}]
no prefix-limit

Context **[Tree]** (config>service>vprn>isis prefix-limit)

Full Context configure service vprn isis prefix-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of prefixes that IS-IS can learn, and use to protect the system from a router that has accidentally advertised a large number of prefixes. If the number of prefixes reaches the configured percentage of this limit, an SNMP trap is sent. If the limit is exceeded, IS-IS will go into overload.

The **overload-timeout** option controls the length of time that IS-IS is in the overload state when the prefix limit is reached. The system automatically attempts to restart IS-IS at the end of this duration. If the **overload-timeout forever** option is used, IS-IS is not restarted automatically and stays in overload until the condition is manually cleared by the administrator. This is also the default behavior when the **overload-timeout** option is not configured.

The **no** form of this command removes the **prefix-limit**.

Default prefix-limit overload-timeout forever

Parameters *limit* — Specifies the number of prefixes that can be learned, expressed as a decimal integer.

Values 1 to 4294967296

log-only — Enables a warning message to be sent at the specified threshold percentage and also when the limit is exceeded. However, overload is not set when this parameter is configured.

percent — Specifies the threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

overload-timeout — Keyword used to control the length of time that IS-IS is in the overload state when the prefix limit is reached.

seconds — Specifies the time in minutes before IS-IS is restarted.

Values 1 to 1800

forever — Specifies that IS-IS should be restarted only after the execution of the **clear router isis overload prefix-limit** command.

Platforms All

prefix-limit

Syntax **prefix-limit** *family limit* [**threshold** *percentage*] [**idle-timeout** {*minutes* | **forever**} | **log-only**] [**post-import**]
no prefix-limit *family*

Context **[Tree]** (config>router>bgp>group prefix-limit)
[Tree] (config>router>bgp>group>neighbor prefix-limit)

Full Context configure router bgp group neighbor prefix-limit
configure router bgp group prefix-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of BGP routes that can be received from a peer before some administrative action is taken. The administrative action can be the generation of a log event or taking down the session. If a session is taken down, then it can be brought back up automatically after an idle-timeout period, or else it can be configured to stay down ('forever') until the operator performs a reset.

No prefix limits for any address family are configured by default.

The **prefix-limit** command allows each address family to have its own limit; a set of address family limits can be applied to one neighbor or to all neighbors in a group.

The **no** form of this command removes the **prefix-limit**.

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is reached. However, the BGP session is not taken down.

percentage — Specifies the threshold value (as a percentage) that triggers a warning message to be sent.

Values 1 to 100

family — Specifies the address family to which the limit applies.

Values ipv4, label-ipv4, vpn-ipv4, ipv6, label-ipv6, vpn-ipv6, mcast-ipv4, l2-vpn, mvpn-ipv4, mdt-safi, ms-pw, flow-ipv4, route-target, mcast-vpn-ipv4, mvpn-ipv6, flow-ipv6, evpn, mcast-ipv6, bgp-ls, sr-policy-ipv4, sr-policy-ipv6

limit — Specifies the number of routes that can be learned from a peer expressed as a decimal integer.

Values 1 to 4294967295

minutes — Specifies duration in minutes before automatically re-establishing a session.

Values 1 to 1024

forever — Specifies that the session is reestablished only after **clear router bgp** command is executed.

post-import — Specifies that the limit should be applied only to the number of routes that are accepted by import policies.

Platforms All

prefix-limit

Syntax **prefix-limit** *limit* [**log-only**] [**threshold** *percent*] [**overload-timeout** {*seconds* | **forever**}]
no prefix-limit

Context **[Tree]** (config>router>isis prefix-limit)

Full Context configure router isis prefix-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of prefixes that IS-IS can learn, and use to protect the system from a router that has accidentally advertised a large number of prefixes. If the number of prefixes reaches the configured percentage of this limit, an SNMP trap is sent. If the limit is exceeded, IS-IS will go into overload.

The **overload-timeout** option controls the length of time that IS-IS is in the overload state when the **prefix-limit** is reached. The system automatically attempts to restart IS-IS at the end of this duration. If the **overload-timeout forever** option is used, IS-IS is not restarted automatically and stays in overload until the condition is manually cleared by the administrator. This is also the default behavior when the **overload-timeout** option is not configured.

The **no** form of this command removes the **prefix-limit**.

Default no prefix-limit

Parameters **log-only** — Enables a warning message to be sent at the specified threshold percentage and also when the limit is exceeded. However, overload is not set when this parameter is configured.

limit — Specifies the number of prefixes that can be learned expressed as a decimal integer.

Values 1 to 4294967296

percent — Specifies the threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

seconds — Specifies the time in minutes before IS-IS is restarted.

Values 1 to 1800

forever — Specifies that IS-IS should be restarted only after the execution of the **clear router isis overload prefix-limit** command.

Platforms All

20.298 prefix-list

prefix-list

Syntax **prefix-list** *name* [{**all** | **none** | **any**}]
no prefix-list [*name*] [{**all** | **none** | **any**}]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect prefix-list)
[Tree] (config>service>vprn>static-route-entry>next-hop prefix-list)
[Tree] (config>service>vprn>static-route-entry>black-hole prefix-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn static-route-entry black-hole prefix-list
configure service vprn static-route-entry indirect prefix-list
configure service vprn static-route-entry next-hop prefix-list

Description This command associates a new constraint to the associated static route such that the static route is only active if **any**, **none**, or **all** of the routes in the prefix list are present and active in the route-table.

Default no prefix-list

Parameters *name* — Specifies the name of a currently configured prefix-list.

all — Specifies that the static route condition is met if all prefixes in the prefix-list must be present in the active static route.

none — Specifies that the static route condition is met if none of the prefixes in the named prefix-list can be present in the active static route.

any — Specifies that the static route condition is met if any prefixes in the prefix-list are present in the active static route.

Platforms All

prefix-list

Syntax **prefix-list** *prefix-list-name* [{**all** | **none**}]
no prefix-list [*prefix-list-name*] [{**all** | **none**}]

Context **[Tree]** (config>router>static-route-entry>black-hole prefix-list)
[Tree] (config>router>static-route-entry>indirect prefix-list)
[Tree] (config>router>static-route-entry>next-hop prefix-list)

Full Context configure router static-route-entry black-hole prefix-list
configure router static-route-entry indirect prefix-list
configure router static-route-entry next-hop prefix-list

Description This command associates a new constraint to the associated static route such that the static route is only active if **none** or **all** of the routes in the prefix list are present and active in the route-table.

Default no prefix-list

Parameters *prefix-list-name* — Specifies the name of a currently configured prefix-list.

all — Specifies that the static route condition is met if all prefixes in the prefix-list must be present in the active route-table.

none — Specifies that the static route condition is met if none of the prefixes in the named prefix-list can be present in the active route-table.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix-list

Syntax [**no**] **prefix-list** *name*

Context **[Tree]** (config>router>policy-options prefix-list)

Full Context configure router policy-options prefix-list

Description This command creates a context to configure a prefix list to use in route policy entries.

The **no** form of this command deletes the named prefix list.

Parameters *name* — Specifies the prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end"," @variable@end", or "start@variable@".

An empty prefix list can be configured for pre-provisioning. This empty prefix list will not find a match when referred to by a policy. When removing member prefixes from a prefix list, the prefix list will not be automatically removed when the last member is removed. If required, an empty prefix list must be explicitly removed using the **no** form of this command.

Platforms All

prefix-list

Syntax **prefix-list** *name* [*name*]
no prefix-list

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from prefix-list)
[Tree] (config>router>policy-options>policy-statement>entry>to prefix-list)

Full Context configure router policy-options policy-statement entry from prefix-list
configure router policy-options policy-statement entry to prefix-list

Description This command configures a prefix list as a match criterion for a route policy statement entry.

If no prefix list is specified, any network prefix is considered a match.

An empty prefix list will evaluate as if 'no match' was found.

The prefix lists specify the network prefix (this includes the prefix and length) a specific policy entry applies.

A maximum of 28 prefix names can be specified.

The **no** form of this command removes the prefix list match criterion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no prefix-list

Parameters *name* — Specifies the prefix list name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must be enclosed by at-signs (@) and may be midstring; for example, "@variable@," "start@variable@end"," @variable@end", or "start@variable@".

Platforms All

20.299 prefix-options

prefix-options

Syntax [**no**] **prefix-options**

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv prefix-options)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 prefix-options)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv prefix-options)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv prefix-options)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 prefix-options)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv prefix-options)
[Tree] (config>subscr-mgmt>rtr-adv-plcy prefix-options)

Full Context configure service ies subscriber-interface group-interface ipv6 prefix-options
configure service ies subscriber-interface group-interface ipv6 router-advertisements prefix-options
configure service ies subscriber-interface ipv6 router-advertisements prefix-options
configure service vprn subscriber-interface group-interface ipv6 prefix-options
configure service vprn subscriber-interface group-interface ipv6 router-advertisements prefix-options
configure service vprn subscriber-interface ipv6 router-advertisements prefix-options
configure subscriber-mgmt router-advertisement-policy prefix-options

Description This command configures Router Advertisement parameters for IPv6 prefixes returned via RADIUS Framed-IPv6-Prefix. All prefixes will inherit these configuration parameters.

The **no** form of this command unconfigures the Router Advertisement parameters for IPv6 prefixes returned via RADIUS Framed-IPv6-Prefix.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.300 prefix-policy

prefix-policy

Syntax **prefix-policy** *prefix-policy* [*prefix-policy*]
no prefix-policy

Context **[Tree]** (config>service>vprn>isis>loopfree-alternates>exclude prefix-policy)

Full Context configure service vprn isis loopfree-alternates exclude prefix-policy

Description This command specifies the name of the policy for the prefixes to exclude from the LFA SPF calculation in this ISIS instance.

The **no** form of this command deletes the exclude prefix policy.

Default no prefix-policy

Parameters **prefix-policy** *prefix-policy* — Specifies the name of the prefix policy, up to 32 characters. Up to five prefix policies can be specified. The specified name must have been already defined.

Platforms All

prefix-policy

Syntax [**no**] **prefix-policy** *prefix-policy* [*prefix-policy*]

Context **[Tree]** (config>service>vprn>ospf>loopfree-alternates>exclude prefix-policy)
[Tree] (config>service>vprn>ospf3>loopfree-alternates>exclude prefix-policy)

Full Context configure service vprn ospf loopfree-alternates exclude prefix-policy
configure service vprn ospf3 loopfree-alternates exclude prefix-policy

Description This command specifies the name of the policy for the prefixes to exclude from the LFA SPF calculation in this OSPF or OSPF3 instance.

The **no** form of this command deletes the exclude prefix policy.

Default no prefix-policy

Parameters **prefix-policy** *prefix-policy* — Specifies the name of the prefix policy, up to 32 characters. Up to five prefix policies can be specified. The specified name must have been already defined.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix-policy

Syntax **prefix-policy** *prefix-policy* [*prefix-policy*]
no prefix-policy

Context **[Tree]** (config>router>isis>loopfree-alternates>exclude prefix-policy)

Full Context configure router isis loopfree-alternates exclude prefix-policy

Description This command excludes from LFA SPF calculation prefixes that match a prefix entry or a tag entry in a prefix policy.

The implementation already allows the user to exclude an interface in IS-IS or OSPF, an OSPF area, or an IS-IS level from the LFA SPF.

If a prefix is excluded from LFA, then it will not be included in LFA calculation regardless of its priority. The prefix tag will, however, be used in the main SPF.

This command specifies the name of the policy for the prefixes to exclude from the LFA SPF calculation in this IS-IS instance.

Note: Prefix tags are defined for the IS-IS protocol but not for the OSPF protocol.

The default action, when not explicitly specified by the user in the prefix policy, is a "reject". Thus, regardless if the user did or did not explicitly add the statement "default-action reject" to the prefix policy, a prefix that did not match any entry in the policy will be accepted into LFA SPF.

The **no** form of this command deletes the exclude prefix policy.

Default no prefix-policy

Parameters **prefix-policy** *prefix-policy* — Specifies the name of the prefix policy, up to 32 characters. Up to five prefix policies can be specified. The specified name must have been already defined.

Platforms All

prefix-policy

Syntax **prefix-policy** *prefix-policy* [*prefix-policy*]
no prefix-policy

Context **[Tree]** (config>router>ospf>loopfree-alternates>exclude prefix-policy)
[Tree] (config>router>ospf3>loopfree-alternates>exclude prefix-policy)

Full Context configure router ospf loopfree-alternates exclude prefix-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf3 loopfree-alternates exclude prefix-policy

Description This command excludes from LFA SPF calculation prefixes that match a prefix entry or a tag entry in a prefix policy.

The implementation already allows the user to exclude an interface in IS-IS or OSPF, an OSPF area, or an IS-IS level from the LFA SPF.

If a prefix is excluded from LFA, then it will not be included in LFA calculation regardless of its priority. The prefix tag will, however, be used in the main SPF.

This command specifies the name of the policy for the prefixes to exclude from the LFA SPF calculation in this OSPF or OSPF3 instance.

Note: Prefix tags are defined for the IS-IS protocol but not for the OSPF protocol.

The default action, when not explicitly specified by the user in the prefix policy, is a “reject”. Thus, regardless if the user did or did not explicitly add the statement “default-action reject” to the prefix policy, a prefix that did not match any entry in the policy will be accepted into LFA SPF.

The **no** form of this command deletes the exclude prefix policy.

Default no prefix-policy

Parameters *prefix-policy* — Specifies the name of the prefix policy, up to 32 characters. Up to five prefix policies can be specified. The specified name must have been already defined.

Platforms All

20.301 prefix-sid-range

prefix-sid-range

Syntax **prefix-sid-range global**
prefix-sid-range start-label *start-label* **max-index** *max-index*
no prefix-sid-range

Context **[Tree]** (config>router>bgp>segment-routing prefix-sid-range)

Full Context configure router bgp segment-routing prefix-sid-range

Description This command configures the label block that BGP segment routing is allowed to use.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The s**tart-label** and **max-index** parameters specify that BGP should be restricted to a subrange of the SRGB, with the subrange starting at **start-label** and ending at **max-index**.

It is not possible to enable segment routing (perform a **no shutdown**) unless the **prefix-sid-range** is configured using the **global** keyword or using the **start-label** and **max-index** parameters.

The **no** form of the command allocates no labels for BGP segment-routing.

Default no prefix-sid-range

Parameters **global** — Specifies that BGP is allowed to allocate labels from the entire space of the SRGB, as defined under **config**>**router**>**mpls-labels**>**sr-labels**.

start-label — Specifies the first label value that is available to BGP in a contiguous range of labels.

Values 0 to 524287

max-index — Specifies the last label value that is available to BGP in a contiguous range of labels.

Values 1 to 524287

Platforms All

prefix-sid-range

Syntax **prefix-sid-range** {**global** | **start-label** *label-value* **max-index** *index-value*}
no prefix-sid-range

Context **[Tree]** (config>router>isis>segment-routing prefix-sid-range)

Full Context configure router isis segment-routing prefix-sid-range

Description This command configures the prefix SID index range and offset label value for a given IGP instance.

The key parameter is the configuration of the prefix SID index range and the offset label value which this IGP instance will use. Since each prefix SID represents a network global IP address, the SID index for a prefix must be network-wide unique. Thus, all routers in the network are expected to configure and advertise the same prefix SID index range for a given IGP instance. However, the label value used by each router to represent this prefix; that is, the label programmed in the ILM can be local to that router by the use of an offset label, referred to as a start label:

Local Label (Prefix SID) = start-label + {SID index}

The label operation in the network becomes thus very similar to LDP when operating in the independent label distribution mode (RFC 5036, *LDP Specification*) with the difference that the label value used to forward a packet to each downstream router is computed by the upstream router based on advertised prefix SID index using the above formula.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

There are two mutually exclusive modes of operation for the prefix SID range on the router. In the **global** mode of operation, the user configures the global value and this IGP instance will assume the start label value is the lowest label value in the SRGB and the prefix SID index range size equal to the range size of the SRGB. Once one IGP instance selected the global option for the prefix SID range, all IGP instances on the system will be restricted to do the same. The user must shutdown the segment routing context and delete the **prefix-sid-range** command in all IGP instances in order to change the SRGB. Once the SRGB is changed, the user must re-enter the **prefix-sid-range** command again. The SRGB range change will be failed if an already allocated SID index/label goes out of range.

In the per-instance mode of operation, the user partitions the SRGB into non-overlapping sub-ranges among the IGP instances. The user thus configures a subset of the SRGB by specifying the start label value and the prefix SID index range size. All resulting net label values (start-label + index} must be within the SRGB or the configuration will be failed. Furthermore, the code checks for overlaps of the resulting net label value range across IGP instances and will strictly enforce that these ranges do not overlap. The user must shutdown the segment routing context of an IGP instance in order to change the SID index/label range of that IGP instance using the **prefix-sid-range** command. In addition, any range change will be failed if an already allocated SID index/label goes out of range. The user can however change the SRGB on the fly as long as it does not reduce the current per IGP instance SID index/label range defined with the **prefix-sid-range**. Otherwise, the user must shutdown the segment routing context of the IGP instance and delete and re-configure the **prefix-sid-range** command.

Default no prefix-sid-range

Parameters *label-value* — Specifies the label offset for the SR label range of this IGP instance.

Values 0 to 524287

index-value — Specifies the maximum value of the prefix SID index range for this IGP instance.

Values 1 to 524287

Platforms All

prefix-sid-range

Syntax **prefix-sid-range global**
prefix-sid-range start-label *label-value* **max-index** *index-value*
no prefix-sid-range

Context **[Tree]** (config>router>ospf>segm-rtng prefix-sid-range)
[Tree] (config>router>ospf3>segm-rtng prefix-sid-range)

Full Context configure router ospf segment-routing prefix-sid-range
configure router ospf3 segment-routing prefix-sid-range

Description This command configures the prefix SID index range and offset label value for an IGP instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The key parameter is the configuration of the prefix SID index range and the offset label value that this IGP instance will use. Because each prefix SID represents a network global IP address, the SID index for a prefix must be unique network-wide. Therefore, all routers in the network are expected to configure and advertise the same prefix SID index range for an IGP instance. However, the label value used by each router to represent this prefix, that is, the label programmed in the ILM, can be local to that router by the use of an offset label, referred to as a start label:

Local Label (Prefix SID) = start-label + {SID index}

The label operation in the network is very similar to LDP when operating in independent label distribution mode (RFC 5036, *LDP Specification*), with the difference being that the label value used to forward a packet to each downstream router is computed by the upstream router based on the advertised prefix SID index using the above formula.

There are two mutually exclusive modes of operation for the prefix SID range on the router. In the **global** mode of operation, the user configures the global value and this IGP instance will assume the start label value is the lowest label value in the SRGB and the prefix SID index range size equal to the range size of the SRGB. After one IGP instance selected the global option for the prefix SID range, all IGP instances on the system will be restricted to do the same. The user must shutdown the segment routing context and delete the **prefix-sid-range** command in all IGP instances in order to change the SRGB. After the SRGB is changed, the user must re-enter the **prefix-sid-range** command again. The SRGB range change will be failed if an already allocated SID index/label goes out of range.

In per-instance mode, the user partitions the SRGB into non-overlapping sub-ranges among the IGP instances. The user configures a subset of the SRGB by specifying the start label value and the prefix SID index range size. All resulting net label values (start-label + index) must be within the SRGB or the configuration will fail. The 7750 SR checks for overlaps of the resulting net label value range across IGP instances and will strictly enforce no overlapping of these ranges. The user must shut down the segment routing context of an IGP instance in order to change the SID index/label range of that IGP instance using the **prefix-sid-range** command. A range change will fail if an already allocated SID index/label goes out of range. The user can change the SRGB without shutting down the segment routing context as long as it does not reduce the current per-IGP instance SID index/label range defined with the **prefix-sid-range** command. Otherwise, shut down the segment routing context of the IGP instance, and disable and re-enable the **prefix-sid-range** command.

Default no prefix-sid-range

Parameters *label-value* — Specifies the label offset for the SR label range of this IGP instance.

Values 0 to 524287

index-value — Specifies the maximum value of the prefix SID index range for this IGP.

Values 1 to 524287

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.302 prefix-sids

prefix-sids

Syntax **prefix-sids** *ip-int-name*
no prefix-sids *ip-int-name*

Context **[Tree]** (config>router>segment-routing>sr-mpls prefix-sids)

Full Context configure router segment-routing sr-mpls prefix-sids

Description This command configures the prefix SIDs for an interface.

The **no** form of this command removes the prefix SIDs list instance.

Default no prefix-sids

Parameters *ip-int-name* — Specifies the loopback or system interface name that owns the prefix to be advertised, up to 32 characters.

Platforms All

20.303 preserve-key

preserve-key

Syntax [**no**] **preserve-key**

Context **[Tree]** (config>system>security>ssh preserve-key)

Full Context configure system security ssh preserve-key

Description After enabling this command, private keys, public keys, and host key file are saved by the server. It is restored following a system reboot or the ssh server restart.

The **no** form of this command specifies that the keys are held in memory by an SSH server and is not restored following a system reboot.

Default no preserve-key

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.304 primary

primary

Syntax **primary**

Context **[Tree]** (config>aaa>radius-scr-plcy primary)

Full Context configure aaa radius-script-policy primary

Description Commands in this context configure a primary script.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

primary

Syntax **primary**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol primary)

Full Context configure subscriber-mgmt sub-ident-policy primary

Description Commands in this context configure primary identification script parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

primary

Syntax **primary** *path-name*
no primary

Context **[Tree]** (config>router>mpls>lsp primary)

Full Context configure router mpls lsp primary

Description This command specifies a preferred path for the LSP. This command is optional only if the **secondary** *path-name* is included in the LSP definition. Only one primary path can be defined for an LSP.

Some of the attributes of the LSP such as the bandwidth, and hop-limit can be optionally specified as the attributes of the primary path. The attributes specified in the **primary path** *path-name* command, override the LSP attributes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the association of this *path-name* from the LSP *lsp-name*. All configurations specific to this primary path, such as record, bandwidth, and hop limit, are deleted. The primary path must be shutdown first in order to delete it. The **no primary** command will not result in any action except a warning message on the console indicating that the primary path is administratively up.

Parameters *path-name* — Specifies the case-sensitive alphanumeric name label for the LSP path up to 64 characters in length.

Platforms All

primary

Syntax [**no**] **primary** [*mda-id* | *esa-vm-id*]

Context **[Tree]** (config>isa>aa-grp primary)

Full Context configure isa application-assurance-group primary

Description This command assigns an AA ISA or ESA-VM configured in the specified location to this application assurance group. Primary and backup ISAs have equal operational status and when both ISAs are coming up, the one that becomes operational first becomes the active ISA.

On an activity switch from the primary ISA, all configurations are already on the backup ISA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When AA service goes down (all ISAs in the group are down) or comes back up (an ISA in the group becomes active)
- When AA redundancy fails (one of the ISAs in the group is down) or recovers (the failed MDA comes back up)
- When an AA activity switch occurred.

The **no** form of this command removes the specified ISA from the application assurance group.

Parameters *mda-id* — Specifies the slot/mda or esa/vm, identifying a provisioned AA ISA.

Values

slot/*mda*	
slot	1 to 10, depending on chassis model
mda	1 to 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

esa-vm-id — Specifies the ESA and VM, identifying a provisioned ESA-VM. The value of the esa-vm-id for application assurance is used as the esa-id plus 128. For example, an ESA 1 with VM2 would be referred to as esa-129/2.

Values

esa-id+128/vm-id	
esa-id	1 to 16
vm-id	1 to 4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

primary

Syntax **primary** *mda-id*
no primary

Context **[Tree]** (config>isa>tunnel-grp primary)

Full Context configure isa tunnel-group primary

Description This command assigns an ISA IPsec module configured in the specified slot to this IPsec group. The backup ISA IPsec provides the IPsec group with warm redundancy when the primary ISA IPsec in the group is configured. Primary and backup ISA IPsec have equal operational status and when both MDAs are coming up, the one that becomes operational first becomes the active ISA IPsec.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPsec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPsec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPsec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPsec activity switch took place.

The **no** form of this command removes the specified primary ID from the group's configuration.

Default no primary

Parameters *mda-id* — Specifies the card/slot identifying a provisioned IPsec ISA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

primary

Syntax **primary** *primary* **secondary** *secondary*

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>dyn>cert>status-verify primary)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn>cert>status-verify primary)
[Tree] (config>service>ies>if>sap>ipsec-gw>cert>status-verify primary)
[Tree] (config>service>vprn>if>sap>ipsec-gw>cert>status-verify primary)
[Tree] (config>service>vprn>if>sap>ipsec-tun>dyn>cert>status-verify primary)
[Tree] (config>router>if>ipsec>ipsec-tun>dyn>cert>status-verify primary)
[Tree] (config>ipsec>trans-mode-prof>dyn>cert>status-verify primary)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying cert primary
configure router interface ipsec ipsec-tunnel dynamic-keying cert status-verify primary
configure service ies interface ipsec ipsec-tunnel dynamic-keying cert status-verify primary
configure service ies interface sap ipsec-gw cert status-verify primary
configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert status-verify primary
configure service vprn interface sap ipsec-gw cert status-verify primary
configure service vprn interface sap ipsec-tunnel dynamic-keying cert status-verify primary

Description This command specifies the primary and secondary CVS methods used to verify the revocation status of the peer's certificate.

OCSP or CRL uses the corresponding configuration in the CA profile of the issuer of the certificate in question.

Default primary crl

Parameters *primary* — Specifies the primary CSV method used to verify the revocation status of the peer's certificate.

Values **ocsp** — Specifies that the OCSP protocol should be used. The OCSP server is configured in the corresponding CA profile.

crl — Specifies that the local CRL file should be used. The CRL file is configured in the corresponding CA profile.

Default crl

secondary — Specifies the secondary CSV method used to verify the revocation status of the peer's certificate.

Values **ocsp** — Specifies that the OCSP protocol should be used. The OCSP server is configured in the corresponding CA profile.

crl — Specifies that the local CRL file should be used. The CRL file is configured in the corresponding CA profile.

none — Specifies that no secondary method of CSV is used.

Default none

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-gw cert status-verify primary

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface sap ipsec-tunnel dynamic-keying cert status-verify primary
- configure service ies interface sap ipsec-gw cert status-verify primary

VSR

- configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert status-verify primary
- configure router interface ipsec ipsec-tunnel dynamic-keying cert status-verify primary
- configure service ies interface ipsec ipsec-tunnel dynamic-keying cert status-verify primary

primary

Syntax [**no**] **primary** *mda-id*

Context **[Tree]** (config>isa>video-group primary)

Full Context configure isa video-group primary

Description This command configures the primary video group ISA. Only one primary can be configured per video group when ad insertion is enabled. The maximum number of primaries per video-group for FCC and RD is 4.

Parameters *mda-id* — Specifies the slot and MDA number for the primary video group ISA.

Values

slot/mda

slot	1 to 10 (depending on the chassis model)
mda	1 to 2

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

20.305 primary-cf

primary-cf

Syntax **primary-cf** *cflash-id*

Context **[Tree]** (config>call-trace primary-cf)

Full Context configure call-trace primary-cf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies which compact-flash is used as the primary CF for call-trace operation.

Default primary-cf cf1

Parameters *cflash-id* — Specifies the compact flash card to be used as the primary local storage location to save the generated call trace log files.

Values cf1, cf2

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.306 primary-config

primary-config

Syntax **primary-config** *file-url*
no primary-config

Context **[Tree]** (bof primary-config)

Full Context bof primary-config

Description This command specifies the name and location of the primary configuration file.

The system attempts to use the configuration specified in **primary-config**. If the specified file cannot be located, the system automatically attempts to obtain the configuration from the location specified in **secondary-config** and then the **tertiary-config**.

If an error in the configuration file is encountered, the boot process aborts.

The **no** form of this command removes the **primary-config** configuration.

Parameters *file-url* — Specifies the primary configuration file location, expressed as a file URL.

Values

file-url	{*local-url* | *remote-url*} (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.307 primary-dns

primary-dns

Syntax **primary-dns** *ip-address*
no primary-dns

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp primary-dns)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp primary-dns)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp primary-dns
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp primary-dns

Description This command configures the primary DNS address to be returned via DHCP on WLAN-GW ISA.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the primary DNS address.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

primary-dns

Syntax **primary-dns** *ip-address*
no primary-dns

Context **[Tree]** (config>service>vprn>dns primary-dns)

Full Context configure service vprn dns primary-dns

Description This command configures the primary DNS server used for DNS name resolution. DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of this command removes the primary DNS server from the configuration.

Default no primary-dns — No primary DNS server is configured.

Parameters *ip-address* — The IP or IPv6 address of the primary DNS server.

Values
ipv4-address -a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0..FFFF]H
d: [0..255]D
interface - 32 characters max, for link local addresses.

Platforms All

primary-dns

Syntax **primary-dns** *ip-address*
no primary-dns [*ip-address*]

Context **[Tree]** (bof primary-dns)

Full Context bof primary-dns

Description This command configures the primary DNS server used for DNS name resolution. DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of this command removes the primary DNS server from the configuration.

Default no primary-dns

Parameters *ip-address* — Specifies the IP or IPv6 address of the primary DNS server.

Values

ipv4-address	*a.b.c.d*
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
interface	32 chars max, for link local addresses

Note: IPv6 is applicable to the 7750 SR and 7950 XRS only.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.308 primary-image

primary-image

Syntax **primary-image** *file-url*
no primary image

Context **[Tree]** (bof primary-image)

Full Context bof primary-image

Description This command specifies the primary directory location for runtime image file loading.

The system attempts to load all runtime image files configured in the **primary-image** first. If this fails, the system attempts to load the runtime images from the location configured in the **secondary-image**. If the secondary image load fails, the tertiary image specified in **tertiary-image** is used.

All runtime image files (*.tim files) must be located in the same directory.

The **no** form of this command removes the **primary-image** configuration.

Parameters *file-url* — Specifies the *file-url* can be either local (this CPM) or a remote FTP server.

Values

file-url	{*local-url* | *remote-url*} (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

20.309 primary-ip-address

primary-ip-address

Syntax **primary-ip-address** *ipv4-address*
no primary-ip-address

Context **[Tree]** (config>router>bgp>orr>location primary-ip-address)

Full Context configure router bgp optimal-route-reflection location primary-ip-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the primary IP address of a reference location used for BGP optimal route reflection. Up to three IPv4 addresses and three IPv6 addresses can be specified per location.

If the TE DB is unable find a node in its topology database that matches a primary address of the location, then it tries to find a node matching a secondary address. If this attempt also fails, the TE DB tries to find a node matching a tertiary address.

The IP addresses specified for a location should be topologically “close” to a set of clients that should all receive the same optimal path for that location.

The **no** form of this command removes the primary IP address information.

Default no primary-ip-address

Parameters *ipv4-address* — Specifies the primary IPv4 address of a location expressed in dotted decimal notation.

Values a.b.c.d

Platforms All

20.310 primary-ipv6-address

primary-ipv6-address

Syntax **primary-ipv6-address** *ipv6-address*
no primary-ipv6-address

Context **[Tree]** (config>router>bgp>orr>location primary-ipv6-address)

Full Context configure router bgp optimal-route-reflection location primary-ipv6-address

Description This command specifies the primary IPv6 address of a reference location used for BGP optimal route reflection. Up to three IPv4 addresses and three IPv6 addresses can be specified per location.

If the TE DB is unable find a node in its topology database that matches a primary address of the location, then it tries to find a node matching a secondary address. If this attempt also fails, the TE DB tries to find a node matching a tertiary address.

The IP addresses specified for a location should be topologically “close” to a set of clients that should all receive the same optimal path for that location.

The **no** form of this command removes the primary IPv6 address information.

Default no primary-ipv6-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-address* — Specifies the primary IPv6 address of a location expressed in dotted decimal notation.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

20.311 primary-location

primary-location

Syntax **primary-location** *file-url*
no primary-location

Context **[Tree]** (config>system>software-repository primary-location)

Full Context configure system software-repository primary-location

Description This command configures the primary location for the files in the software repository. See the **software-repository** command description for more information.

The **no** form of the command removes the primary location.

Parameters *file-url* — Specifies the primary location to be used to access the files in the software repository.

Values

file url	*local-url* | *remote-url*	
local-url	[*cflash-id/*][*file-path*]	200 chars maximum, including cflash-id directory length 99 characters maximum each
remote-url	[{ftp://} *login:pswd@remote-locn/*][*file-path*]	
	243 characters maximum	
	directory length 99 characters maximum each	
	remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
	ipv4-address	*a.b.c.d*
	ipv6-address	*x:x:x:x:x:x:x:x*[*-interface*]
		x:x:x:x:x:x:d.d.d.d[*-interface*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x - [0 to FFFF]H
d - [0 to 255]D
interface - 32 characters max, for link local addresses

cflash-id cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.312 primary-nbns

primary-nbns

Syntax **primary-nbns** *ip-address*
no primary-nbns

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp primary-nbns)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp primary-nbns)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp primary-nbns
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp primary-nbns

Description This command configures the primary NBNS address to be returned via DHCP on WLAN-GW ISA.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the primary NBNS address.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.313 primary-next-hop

primary-next-hop

Syntax [**no**] **primary-next-hop**

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy>nh-grp primary-next-hop)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group primary-next-hop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the primary next hop of an NHG entry in a forwarding policy.

The **no** form of this command removes the primary next-hop context from an NHG entry in a forwarding policy.

Platforms All

20.314 primary-p2mp-instance

primary-p2mp-instance

Syntax [**no**] **primary-p2mp-instance** *instance-name*

Context **[Tree]** (config>router>mpls>lsp primary-p2mp-instance)

Full Context configure router mpls lsp primary-p2mp-instance

Description This command creates the primary instance of a P2MP LSP. The primary instance of a P2MP LSP is modeled as a set of root-to-leaf (S2L) sub-LSPs. The root, for example a head-end node triggers signaling using one path message per S2L path. The leaf sub-LSP paths are merged at branching points.

This command is not supported on the 7450 ESS.

Parameters *instance-name* — Specifies a name that identifies the P2MP LSP instance. The instance name can be up to 32 characters long and must be unique.

Platforms All

20.315 primary-path

primary-path

Syntax **primary-path**

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2-paths primary-path)

Full Context configure mcast-management bandwidth-policy t2-paths primary-path

Description Commands in this context configure primary path parameters.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.316 primary-ports

primary-ports

Syntax **primary-ports**

Context **[Tree]** (config>service>vpls>mac-move primary-ports)
[Tree] (config>service>template>vpls-template>mac-move primary-ports)

Full Context configure service template vpls-template mac-move primary-ports
configure service vpls mac-move primary-ports

Description Commands in this context define primary VPLS ports. VPLS ports that were declared as secondary prior to the execution of this command will be moved from secondary port-level to primary port-level. Changing a port to the tertiary level can only be done by first removing it from the secondary port-level.

Platforms All

20.317 primary-tunnel-interface

primary-tunnel-interface

Syntax **primary-tunnel-interface ldp-p2mp** *p2mp-identifier* **sender** *ip-address*
primary-tunnel-interface rsvp-p2mp *lsp-name* **sender** *ip-address*
no primary-tunnel-interface

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle primary-tunnel-interface)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel primary-tunnel-interface)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override primary-tunnel-interface)

Full Context configure mcast-management multicast-info-policy bundle channel primary-tunnel-interface
configure mcast-management multicast-info-policy bundle channel source-override primary-tunnel-interface
configure mcast-management multicast-info-policy bundle primary-tunnel-interface

Description This command allows the user to define a bundle in the multicast-info-policy and specify channels in the bundle that must be received from the primary tunnel interface associated with an RSVP P2MP LSP. The multicast info policy is applied to the base router instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The egress LER can accept multicast packets via two different methods. The regular RPF check on unlabeled IP multicast packets, which is based on routing table lookup. The static assignment which specifies the receiving of a multicast group <*,G> or a specific <S,G> from a primary tunnel-interface associated with an RSVP P2MP LSP.

One or more primary tunnel interfaces in the base router instance can be configured. That is, the user can specify to receive different multicast groups, <*,G> or specific <S,G>, from different P2MP LSPs. This assumes that there are static joins configured for the same multicast groups at the ingress LER to forward over a tunnel interface associated with the same P2MP LSP.

At any given time, packets of the same multicast group can be accepted from either the primary tunnel interface associated with a P2MP LSP or from a PIM interface. These are mutually exclusive options. As soon as a multicast group is configured against a primary tunnel interface in the multicast info policy, it is blocked from other PIM interfaces.

A multicast packet received on a tunnel interface associated with a P2MP LSP can be forwarded over a PIM or IGMP interface which can be an IES interface, a spoke SDP terminated IES interface, or a network interface.

The **no** form of this command removes the static RPF check.

Parameters *lsp-name* — Species a string of up to 32 characters identifying the LSP name as configured at the ingress LER.

ip-address — Specifies a string of 15 characters representing the IP address of the ingress LER for the LSP.

p2mp-id — Identifier used for signaling mLDP P2MP LSP (applies only to the 7750 SR).

Values 1 to 4294967296

Platforms All

20.318 primary-url

primary-url

Syntax **primary-url** *url*
no primary-url

Context **[Tree]** (config>python>py-script primary-url)

Full Context configure python python-script primary-url

Description This command specifies the location of the primary Python script. The system supports three locations for each Python script. Users can store the script file on either a local CF card or an FTP server.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the URL.

Parameters **url** — Specifies the primary URL of the Python script up to 180 characters, either a local CF card url or a FTP server URL.

Platforms All

20.319 prio-code-point

prio-code-point

Syntax **prio-code-point** *priority-code-point*
no prio-code-point

Context **[Tree]** (config>test-oam>build-packet>header>dot1q prio-code-point)

Full Context configure test-oam build-packet header dot1q prio-code-point

Description This command defines the priority code point to be used in the test Dot1Q header.

The **no** form of this command removes the priority code point value.

Default prio-code-point 0 (BE)

Parameters *priority-code-point* — Specifies the priority code point to be used in the test Dot1Q header.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

prio-code-point

Syntax **prio-code-point** *priority-code-point*
no prio-code-point

Context **[Tree]** (debug>oam>build-packet>packet>field-override>header>dot1q prio-code-point)

Full Context debug oam build-packet packet field-override header dot1q prio-code-point

Description This command configures a Priority Code Point (PCP) for an IEEE 802.1Q packet header to be launched by the OAM **find-egress** tool.

The **no** form of this command removes the priority code point value.

Default no override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *priority-code-point* — Specifies the priority code point to be used in the test Dot1Q header.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.320 priority

priority

Syntax **priority** *level*

Context **[Tree]**
(config>subscr-mgmt>sub-prof>ingress>policer-control-policy>priority-mbs-thresholds priority)
[Tree]
(config>subscr-mgmt>sub-prof>egress>policer-control-policy>priority-mbs-thresholds priority)

Full Context configure subscriber-mgmt sub-profile egress policer-control-policy priority-mbs-thresholds priority
configure subscriber-mgmt sub-profile ingress policer-control-policy priority-mbs-thresholds priority

Description The **priority** level command contains the **mbs-contribution** configuration command for a given strict priority level. Eight levels are supported numbered 1 through 8 with 8 being the highest strict priority.

Each of the eight priority CLI nodes always exists and do not need to be created. While parameters exist for each priority level, the parameters are only applied when the priority level within a parent policer instance is currently supporting child policers.

Parameters *level* — Specifies the priority level override.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

priority

Syntax **priority** *priority* **source {python | diameter-gx | ludb | radius | diameter-nasreq | gtp | dhcp | local-address-assignment}**
no priority *priority*

Context **[Tree]** (config>subscr-mgmt>auth-orig priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt authentication-origin priority

Description This command allows the relative order of authentication priorities to be swapped between RADIUS and LUDB by configuring the RADIUS source priority to value 3. By moving RADIUS to the third position, LUDB, and all the origins below LUDB, are pushed down.The active order of priorities can be displayed in the output of the **show subscriber-mgmt authentication-origin** command.

The **no** form of this command deletes the priority value. To restore defaults, the priority configuration must be deleted.

Parameters *priority* — Specifies the authentication origin priority override.

Values 1 to 7

source — Specifies the source of authentication priority. Only **radius** can be configured. RADIUS as the authentication origin can be assigned priority 3 which places it above LUDB.

Values python, diameter-gx, ludb, radius, diameter-nasreq, gtp, dhcp, local-address-assignment

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>service>ies>sub-if>grp-if>srrp priority)
[Tree] (config>service>vprn>sub-if>grp-if>srrp priority)

Full Context configure service ies subscriber-interface group-interface srrp priority
configure service vprn subscriber-interface group-interface srrp priority

Description This command overrides the default base priority for the SRRP instance. The SRRP instance priority is advertised by the SRRP instance to its neighbor router and is compared to the priority received from the neighbor router. The router with the best (highest) priority enters the master state while the other router enters the backup state. If the priority of each router is the same, the router with the lowest source IP address in the SRRP advertisement message assumes the master state.

The base priority of an SRRP instance can be managed by VRRP policies. A VRRP policy defines a set of connectivity or verification tests which, when they fail, may lower an SRRP instances base priority (creating an in-use priority for the instance). Every time an SRRP instances in-use priority changes when in master state, it sends an SRRP advertisement message with the new priority. If the dynamic priority drops to zero or receives an SRRP Advertisement message with a better priority, the SRRP instance transitions to the *becoming backup* state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the priority command is not specified, or the no priority command is executed, the system uses a default base priority of 100. The priority command may be executed at any time.

The **no** form of this command restores the default base priority to the SRRP instance. If a VRRP policy is associated with the SRRP instance, it will use the default base priority as the basis for any modifications to the SRRP instances in-use priority.

Default priority 100

Parameters *priority* — Specifies a base priority for the SRRP instance to override the default.

Values 1 to 254

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

priority

Syntax [**no**] **priority** *level*

Context **[Tree]**
(config>card>fp>ingress>access>queue-group>policer-control-override>priority-mbs-thresholds priority)
[Tree]
(config>card>fp>ingress>network>queue-group>policer-control-override>priority-mbs-thresholds priority)

Full Context configure card fp ingress access queue-group policer-control-override priority-mbs-thresholds priority
configure card fp ingress network queue-group policer-control-override priority-mbs-thresholds priority

Description The **priority** level command contains the **mbs-contribution** configuration command for a given strict priority level. Eight levels are supported numbered 1 through 8 with 8 being the highest strict priority.

Each of the eight priority CLI nodes always exists and do not need to be created. While parameters exist for each priority level, the parameters are only applied when the priority level within a parent policer instance is currently supporting child policers.

Parameters *level* — Specifies the priority level.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority

Syntax **priority** *priority-value*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no priority

Context [Tree] (config>port>ethernet>eth-cfm>mep>ais-enable priority)
[Tree] (config>lag>eth-cfm>mep>ais-enable priority)

Full Context configure lag eth-cfm mep ais-enable priority
configure port ethernet eth-cfm mep ais-enable priority

Description This command specifies the priority of the AIS messages generated by the node.

The **no** form of the command reverts to the default values.

Parameters *priority-value* — Specifies the priority value of the AIS messages originated by the node.

Values 0 to 7

Default 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax **priority** *priority*
no priority

Context [Tree] (config>eth-ring>path>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>lag>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>port>ethernet>eth-cfm>mep>grace>eth-ed priority)

Full Context configure eth-ring path eth-cfm mep grace eth-ed priority
configure eth-tunnel path eth-cfm mep grace eth-ed priority
configure lag eth-cfm mep grace eth-ed priority
configure port ethernet eth-cfm mep grace eth-ed priority

Description This command sets the priority bits and determines the forwarding class based on the mapping of priority to FC.

The **no** form of this command disables the local priority configuration and sets the priority to the **ccm-ltm-priority** associated with this MEP.

Default no priority

Parameters *priority* — Specifies the priority bit.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax [**no**] **priority** *level*

Context **[Tree]** (config>service>apipe>sap>egress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>apipe>sap>ingress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>cpipe>sap>egress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>cpipe>sap>ingress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>epipe>sap>egress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>epipe>sap>ingress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>fpipe>sap>egress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>fpipe>sap>ingress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>ipipe>sap>egress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>ipipe>sap>ingress>policy-ctrl-over>mbs-thrshlds priority)

Full Context configure service apipe sap egress policer-control-override priority-mbs-thresholds priority
configure service apipe sap ingress policer-control-override priority-mbs-thresholds priority
configure service cpipe sap egress policer-control-override priority-mbs-thresholds priority
configure service cpipe sap ingress policer-control-override priority-mbs-thresholds priority
configure service epipe sap egress policer-control-override priority-mbs-thresholds priority
configure service epipe sap ingress policer-control-override priority-mbs-thresholds priority
configure service fpipe sap egress policer-control-override priority-mbs-thresholds priority
configure service fpipe sap ingress policer-control-override priority-mbs-thresholds priority
configure service ipipe sap egress policer-control-override priority-mbs-thresholds priority
configure service ipipe sap ingress policer-control-override priority-mbs-thresholds priority

Description The priority-level level override CLI node contains the specified priority level's mbs-contribution override value.

This node does not need to be created and will not be output in show or save configurations unless an mbs-contribution override exist for level.

Parameters *level* — The level parameter is required when specifying priority-level and identifies which of the parent policer instances priority level's the mbs-contribution is overriding.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress policer-control-override priority-mbs-thresholds priority
- configure service fpipe sap ingress policer-control-override priority-mbs-thresholds priority
- configure service cpipe sap ingress policer-control-override priority-mbs-thresholds priority
- configure service cpipe sap egress policer-control-override priority-mbs-thresholds priority

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap ingress policer-control-override priority-mbs-thresholds priority
- configure service ipipe sap egress policer-control-override priority-mbs-thresholds priority
- configure service epipe sap egress policer-control-override priority-mbs-thresholds priority
- configure service ipipe sap ingress policer-control-override priority-mbs-thresholds priority

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap egress policer-control-override priority-mbs-thresholds priority
- configure service apipe sap ingress policer-control-override priority-mbs-thresholds priority

priority

Syntax **priority** *priority-value*
no priority

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep priority)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>aid-enable priority)

Full Context configure service epipe sap eth-cfm mep priority
configure service epipe spoke-sdp eth-cfm aid-enable priority

Description This command specifies the priority of AIS messages originated by the node.

Parameters *priority-value* — Specifies the priority value of the AIS messages originated by the node.

Values 0 to 7

Default 1

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace>eth-ed priority)

Full Context configure service epipe sap eth-cfm mep grace eth-ed priority
configure service epipe spoke-sdp eth-cfm mep grace eth-ed priority
configure service ipipe sap eth-cfm mep grace eth-ed priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the priority bits and determines the forwarding class based on the mapping of priority to FC.

The **no** form of this command disables the local priority configuration and sets the priority to the **ccm-ltm-priority** associated with this MEP.

Default no priority

Parameters *priority* — Specifies the priority bit.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax **priority** *stp-priority*
no priority [*stp-priority*]

Context **[Tree]** (config>service>vpls>stp priority)
[Tree] (config>service>template>vpls-sap-template>stp priority)
[Tree] (config>service>template>vpls-template>stp priority)

Full Context configure service template vpls-sap-template stp priority
configure service template vpls-template stp priority
configure service vpls stp priority

Description The bridge-priority command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent. All values are truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

The **no** form of this command returns the bridge priority to the default value.

Default priority 4096

Parameters *bridge-priority* — Specifies the bridge priority for the STP instance

Values Allowed values are integers in the range of 4096 to 65535 with 4096 being the highest priority. The actual bridge priority value stored/ used is the number entered with the lowest 12 bits masked off which means the actual range of values is 4096 to 61440 in increments of 4096.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *stp-priority*
no priority

Context **[Tree]** (config>service>vpls>sap>stp priority)
[Tree] (config>service>vpls>spoke-sdp priority)
[Tree] (config>service>vpls>spoke-sdp>stp priority)

Full Context configure service vpls sap stp priority
configure service vpls spoke-sdp priority
configure service vpls spoke-sdp stp priority

Description This command configures the Nokia Spanning Tree Protocol (STP) priority for the SAP or spoke SDP.

STP priority is a configurable parameter associated with a SAP or spoke SDP. When configuration BPDUs are received, the priority is used in some circumstances as a tie breaking mechanism to determine whether the SAP or spoke SDP be designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the SAP or spoke SDP priority. The remaining 4 bits are used to extend the port ID field into a 12 bit virtual port number field. The virtual port number uniquely references a SAP or spoke SDP within the STP instance.

STP computes the actual priority by taking the input value and masking out the lower four bits. The result is the value that is stored in the SDP priority parameter. For instance, if a value of 0 is entered, masking out the lower 4 bits results in a parameter value of 0. If a value of 255 is entered, the result is 240.

The **no** form of this command returns the STP priority to the default value.

Default priority 128

Parameters *stp-priority* — Specifies the STP priority value for the SAP or spoke SDP. 0 is the highest priority. The actual value used for STP priority (and stored in the configuration) is the result of masking out the lower 4 bits, therefore the actual value range is 0 to 240 in increments of 16.

Values 0 to 255

Platforms All

priority

Syntax **priority** *priority-value*
no priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable priority)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable priority)

Full Context configure service vpls mesh-sdp eth-cfm mep ais-enable priority
configure service vpls spoke-sdp eth-cfm mep ais-enable priority

Description This command specifies the priority of AIS messages originated by the node.

Parameters *priority-value* — Specifies the priority value of the AIS messages originated by the node

Values 0 to 7

Default 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax **priority** *priority*
no priority

Context [Tree] (config>service>vpls>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace>eth-ed priority)

Full Context configure service vpls eth-cfm mep grace eth-ed priority
configure service vpls mesh-sdp eth-cfm mep grace eth-ed priority
configure service vpls sap eth-cfm mep grace eth-ed priority
configure service vpls spoke-sdp eth-cfm mep grace eth-ed priority

Description This command sets the priority bits and determines the forwarding class based on the mapping of priority to FC.

The **no** form of this command disables the local priority configuration and sets the priority to the **ccm-ltm-priority** associated with this MEP.

Default no priority

Parameters *priority* — Specifies the priority bit.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax [**no**] **priority** *level*

Context [Tree] (config>service>vpls>sap>egress>policy-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>vpls>sap>ingress>policy-ctrl-over>mbs-thrshlds priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls sap egress policer-control-override priority-mbs-thresholds priority
configure service vpls sap ingress policer-control-override priority-mbs-thresholds priority

Description The priority-level level override CLI node contains the specified priority level's mbs-contribution override value.

This node does not need to be created and will not be output in show or save configurations unless an mbs-contribution override exist for level.

The **no** form of this command sets the MBS contribution for the associated priority to its default value.

Parameters *level* — Specifies that the level parameter is required when specifying priority-level and identifies which of the parent policer instances priority level's the mbs-contribution is overriding

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority

Syntax **priority** *base-priority*
no priority

Context **[Tree]** (config>service>ies>if>ipv6>vrrp priority)

Full Context configure service ies interface ipv6 vrrp priority

Description This command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

This command is only available in the non-owner vrrp virtual-router-id nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.

The **no** form of this command restores the default value of 100 to base-priority.

Default **priority** 100

Parameters *base-priority* — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP Priority Control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

Values 1 to 254

Default 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *priority*
no priority

Context [Tree] (config>service>ies>if>sap>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed priority)

Full Context configure service ies interface sap eth-cfm mep grace eth-ed priority
configure service ies interface spoke-sdp eth-cfm mep grace eth-ed priority
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed priority

Description This command sets the priority bits and determines the forwarding class based on the mapping of priority to FC.

The **no** form of this command disables the local priority configuration and sets the priority to the **ccm-ltm-priority** associated with this MEP.

Default no priority

Parameters *priority* — Specifies the priority bit.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed priority

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep grace eth-ed priority
- configure service ies interface spoke-sdp eth-cfm mep grace eth-ed priority

priority

Syntax [**no**] **priority** *level*

Context [Tree] (config>service>ies>if>sap>egress>policer-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>ies>if>sap>ingress>policer-ctrl-over>mbs-thrshlds priority)

Full Context configure service ies interface sap egress policer-control-override priority-mbs-thresholds priority
configure service ies interface sap ingress policer-control-override priority-mbs-thresholds priority

Description The priority-level level override CLI node contains the specified priority level's mbs-contribution override value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This node does not need to be created and will not be output in show or save configurations unless an mbs-contribution override exist for level.

The **no** form of this command sets the MBS contribution for the associated priority to its default value.

Parameters *level* — Specifies that the level parameter is required when specifying priority-level and identifies which of the parent policer instances priority level's the mbs-contribution is overriding.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority

Syntax **priority** *base-priority*
no priority

Context **[Tree]** (config>service>ies>if>vrrp priority)

Full Context configure service ies interface vrrp priority

Description The priority command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

The priority command is only available in the non-owner vrrp virtual-router-id nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.

The **no** form of this command restores the default value of 100 to base-priority.

Parameters *base-priority* — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP Priority Control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

Values 1 to 254

Default 100

Platforms All

priority

Syntax **priority** {**low** | **high**}
no priority [{**low** | **high**}]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect>forwarding-class priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel>forwarding-class priority)
[Tree] (config>service>vprn>static-route-entry>next-hop>forwarding-class priority)

Full Context configure service vprn static-route-entry indirect forwarding-class priority
configure service vprn static-route-entry ipsec-tunnel forwarding-class priority
configure service vprn static-route-entry next-hop forwarding-class priority

Description This optional command associates an enqueuing priority with the static route. The options are either high or low, with low being the default. This parameter has the ability to affect the likelihood that a packet will be enqueued at SAP ingress in the face of ingress congestion.

Once a packet is enqueued into an ingress buffer, the significance of this parameter is lost.

Default priority low

Parameters **low** — Setting the enqueuing parameter for a packet to **low** decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. Once the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

high — Setting the enqueuing parameter for a packet to **high** increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. Once the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax **priority** *priority*
no priority

Context [Tree] (config>service>vprn>if>sap>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace>eth-ed priority)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed priority)

Full Context configure service vprn interface sap eth-cfm mep grace eth-ed priority
configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed priority
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed priority

Description This command sets the priority bits and determines the forwarding class based on the mapping of priority to FC.

The **no** form of this command disables the local priority configuration and sets the priority to the **ccm-ltm-priority** associated with this MEP.

Default no priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *priority* — Specifies the priority bit.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed priority

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed priority
- configure service vprn interface sap eth-cfm mep grace eth-ed priority

priority

Syntax [**no**] **priority** *level*

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-ctrl-over>mbs-thrshlds priority)
[Tree] (config>service>vprn>if>sap>ingress>policer-ctrl-over>mbs-thrshlds priority)

Full Context configure service vprn interface sap egress policer-control-override priority-mbs-thresholds priority
configure service vprn interface sap ingress policer-control-override priority-mbs-thresholds priority

Description The priority-level level override CLI node contains the specified priority level's mbs-contribution override value.

This node does not need to be created and will not be output in show or save configurations unless an mbs-contribution override exist for level.

The **no** form of this command sets the MBS contribution for the associated priority to its default value.

Parameters *level* — Specifies that the level parameter is required when specifying priority-level and identifies which of the parent policer instances priority level's the mbs-contribution is overriding.

Values 1 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>service>vprn>if>vrrp priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>ipv6>vrrp priority)

Full Context configure service vprn interface ipv6 vrrp priority
configure service vprn interface vrrp priority

Description The priority command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

The priority command is only available in the non-owner **vrrp** *virtual-router-id* nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.

The **no** form of this command restores the default value of 100 to base-priority.

Parameters *base-priority* — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP priority control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

Values 1 to 254

Default 100

Platforms All

priority

Syntax **priority** *number*
no priority

Context **[Tree]** (config>service>vprn>isis>if>level priority)

Full Context configure service vprn isis interface level priority

Description This command configures the priority of the IS-IS router interface for designated router election on a multi-access network.

This priority is included in hello PDUs transmitted by the interface on a multi-access network. The router with the highest priority is the preferred designated router. The designated router is responsible for sending LSPs with regard to this network and the routers that are attached to it.

The **no** form of this command reverts to the default value.

Default priority 64

Parameters *number* — Specifies the priority for this interface at this level.

Values 0 to 127

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *number*
no priority

Context **[Tree]** (config>service>vprn>ospf>area>if priority)
[Tree] (config>service>vprn>ospf3>area>if priority)

Full Context configure service vprn ospf area interface priority
configure service vprn ospf3 area interface priority

Description This command configures the priority of the OSPF interface that is used to elect the designated router (DR) on the subnet.

This parameter is only used if the interface is of type **broadcast**. The router with the highest priority interface becomes the DR. A router with priority 0 is not eligible to be the designated router or backup designated router.

The **no** form of this command resets the interface priority to the default value.

Default priority 1

Parameters *number* — The interface priority expressed as a decimal integer. A value of 0 indicates the router is not eligible to be the Designated Router of Backup Designated Router on the interface subnet.

Values 0 to 255

Platforms All

priority

Syntax **priority** *dr-priority*
no priority

Context **[Tree]** (config>service>vprn>pim>if priority)

Full Context configure service vprn pim interface priority

Description This command sets the priority value to become the rendezvous point (RP) that is included in bootstrap messages sent by the router. The RP is sometimes called the bootstrap router. The **priority** command indicates whether the router is eligible to be a bootstrap router.

The **no** form of this command disqualifies the router to participate in the bootstrap election.

Default priority 1 (The router is the least likely to become the designated router.)

Parameters *dr-priority* — Specifies the priority to become the designated router. The higher the value, the higher the priority.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

priority

Syntax **priority** *bootstrap-priority*

Context **[Tree]** (config>service>vprn>pim>rp>bsr-candidate priority)
[Tree] (config>service>vprn>pim>rp>ipv6>bsr-candidate priority)

Full Context configure service vprn pim rp bsr-candidate priority
configure service vprn pim rp ipv6 bsr-candidate priority

Description This command defines the priority used to become the rendezvous point (RP). The higher the priority value the more likely that this router becomes the RP. If there is a tie, the router with the highest IP address is elected.

Parameters *bootstrap-priority* — The priority to become the bootstrap router.

Values 0 to 255

Default 0 (the router is not eligible to be the bootstrap router)

Platforms All

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>service>vprn>pim>rp>rp-candidate priority)

Full Context configure service vprn pim rp rp-candidate priority

Description This command defines the priority used to become the rendezvous point (RP). The higher the priority value, the more likely that this router will become the RP.

Use the **no** form of this command to revert to the default value.

Default priority 192

Parameters *priority* — Specifies the priority to become the designated router. The higher the value the more likely the router will become the RP.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *priority-level*
no priority

Context **[Tree]** (config>router>ldp>lsp-bfd priority)

Full Context configure router ldp lsp-bfd priority

Description This command configures a priority value that is used to order prefix list processing if multiple prefix lists are configured.

The **no** form of this command restores the default priority value.

Default priority 1

Parameters *priority-level* — Specifies the priority value of the prefix list.

Values 1 to 16

Platforms All

priority

Syntax **priority** *setup-priority hold-priority*
no priority

Context **[Tree]** (config>router>mpls>lsp>primary priority)
[Tree] (config>router>mpls>lsp>secondary priority)
[Tree] (config>router>mpls>lsp-template priority)

Full Context configure router mpls lsp primary priority
configure router mpls lsp secondary priority
configure router mpls lsp-template priority

Description This command enables the soft preemption procedures for this LSP path. The operator enables the soft preemption mechanism on a specific LSP name by explicitly configuring the setup and holding priorities for the primary path at the head-end node. The operator can similarly configure priority values for a secondary path for this LSP name. Different values could be used for the primary and for any of the secondary paths. In the absence of explicit user configuration, the setup priority is internally set to the default value of 7 and the holding priority is set to the default value of 0.

Note: Valid user-entered values for these two parameters require that the holding priority be numerically lower than or equal to the setup priority, otherwise preemption loops can occur.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

preemption is effected when a router preempting node processes a new RSVP session reservation and there is not enough available bandwidth on the RSVP interface, or the Class Type (CT) when Diff-Serv is enabled, to satisfy the bandwidth in the FlowSpec object while there exist other session reservations for LSP paths with a strictly lower holding priority (numerically higher holding priority value) than the setup priority of the new LSP reservation. If enough available bandwidth is freed on the link or CT to accommodate the new reservation by preempting one or more lower priority LSP paths, the preempting node allows temporary overbooking of the RSVP interface and honors the new reservation.

The preempting node will immediately set the ‘Preemption pending’ flag (0x10) in the IPv4 Sub-Object in the RRO object in the Resv refresh for each of the preempted LSP paths. The IPv4 Sub-Object corresponds to the outgoing interface being used by the preempting and preempted LSP paths; however, the bandwidth value in the FlowSpec object is not changed. The Resv flag must also be set if the preempting node is a merge point for the primary LSP path and the backup bypass LSP or detour LSP and the backup LSP is activated.

When evaluating if enough available bandwidth will be freed, the preempting node considers the reservations in order from the lowest holding priority (numerically higher holding priority value) to the holding priority just below the setup priority of the new reservation. A new reservation cannot preempt a reservation which has a value of the holding priority equal to the new reservation setup priority.

When Diff-Serv is enabled on the preempting node and the MAM bandwidth allocation model is used, a new reservation can only preempt a reservation in the same Class Type (CT).

LSP paths which were not flagged at the head-end for soft preemption will be hard preempted. LSP paths with the default holding priority of 0 cannot be preempted. LSP paths with zero bandwidth do not preempt other LSP paths regardless of the values of the path setup priority and the path holding priority. They can also not be preempted.

When evaluating if enough available bandwidth will be freed, the preempting node considers the reservations in order from the lowest holding priority (numerically higher holding priority) to the holding priority just below the setup priority of the new reservation. There is no specific order in which the reservations in the same holding priority are considered.

The preempting node starts a preemption timer for each of the preempted LSP paths. While this timer is on, the node should continue to refresh the Path and Resv for the preempted LSP paths. When the preemption timer expires, the node tears down the reservation if the head-end node has not already done so.

A head-end node upon receipt of the Resv refresh message with the ‘Preemption pending’ flag must immediately perform a make-before-break on the affected adaptive CSPF LSP. Both IGP metric and TE metric based CSPF LSPs are included. If an alternative path that excludes the flagged interface is not found, then the LSP is put on a retry in a similar way to the Global Revertive procedure at a head-end node. However, the number of retries and the retry timer are governed by the values of the **retry-limit** and **retry-timer** parameters: **config>router>mpls>lsp>retry-limit**; **config>router>mpls>lsp>retry-timer**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

MPLS will keep the address list of flagged interfaces for a maximum of 60 s (not user-configurable) from the time the first Resv message with the 'Preemption pending' flag is received. This actually means that MPLS will request CSPF to find a path that excludes the flagged interfaces in the first few retries until success or until 60 s have elapsed. Subsequent retries after the 60 s will not exclude the flagged interfaces as it is assumed IGP has converged by then and the Unreserved Bandwidth sub-TLV for that priority, or TE Class, in the TE database will show the updated value taking into account the preempting LSP path reservation or a value of zero if overbooked.

If the LSP has a configured secondary standby which is operationally UP, the router will switch the path of the LSP to it and then start the MBB. If no standby path is available and a secondary non-standby is configured, the router will start the MBB and signal the path of the secondary. The LSP path will be switched to either the secondary or the new primary, whichever comes up first.

The **no** form of this command reverts the LSP path priority to the default values and results in setting the setup priority to 7, in setting the hold priority to 0, and in clearing the 'soft preemption desired' flag in the RRO in the Resv refresh message.

Default no priority

Parameters *setup-priority* — Specifies the priority of the reservation for this session at setup time.

Values 0 to 7 (0 is the highest priority and 7 is the lowest priority.)

Default 7 — This session does not preempt any other session.

holding-priority — Specifies the priority of the reservation for this session at preemption action.

Values 0 to 7 (0 is the highest priority and 7 is the lowest priority.)

Default 0 — This session does not get preempted by any other session.

Platforms All

priority

Syntax **priority** *value*
no priority

Context **[Tree]** (config>app-assure>aarp priority)

Full Context configure application-assurance aarp priority

Description This command defines the priority for the AARP instance. The priority value is used to determine the master/backup upon initialization or re-balance.

The **no** form of this command reverts to the default value.

Default priority 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies an integer that defines the priority of an AARP instance.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

priority

Syntax **priority** *priority-level*
no priority

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action>remark priority)

Full Context configure application-assurance group policy app-qos-policy entry action remark priority

Description This command configures remark discard priority action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured discard priority.

Default no priority

Parameters *priority-level* — Specifies the priority to apply to a packet.

Values high, low

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group priority)

Full Context configure redundancy multi-chassis peer mc-ipsec tunnel-group priority

Description This command specifies the local priority of the tunnel-group, this is used to elect master, higher number win. If priority are same, then the peer has more active ISA win; and priority and the number of active ISA are same, then the peer with higher IP address win.

The **no** form of this command removes the priority value from the configuration.

Default priority 100

Parameters *priority* — Specifies the priority of this tunnel-group.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *dr-priority*
no priority

Context **[Tree]** (config>router>pim>interface priority)

Full Context configure router pim interface priority

Description This command sets the priority value to elect the designated router (DR). The DR election priority is a 32-bit unsigned number and the numerically larger priority is always preferred.

The **no** form of this command reverts to the default value.

Default priority 1

Parameters *priority* — Specifies the priority to become the designated router. The higher the value, the higher the priority.

Values 1 to 4294967295

Platforms All

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>router>pim>rp>rp-candidate priority)
[Tree] (config>router>pim>rp>ipv6>rp-candidate priority)

Full Context configure router pim rp ipv6 rp-candidate priority
configure router pim rp rp-candidate priority

Description This command configures the Candidate-RP priority for becoming a rendezvous point (RP). This value is used to elect RP for a group range.

The **no** form of this command reverts to the default value.

Default priority 192

Parameters *priority* — Specifies the priority to become a rendezvous point (RP). A value of 0 is considered as the highest priority.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>oam-pm>session>ethernet priority)

Full Context configure oam-pm session ethernet priority

Description This command defines the CoS priority across all tests configured under this session. This CoS value is exposed to the various QoS policies the frame passes through and does not necessarily map directly to the CoS value on the wire.

The **no** form of this command removes changes the priority to the default value.

Default priority 0

Parameters *priority* — Specifies the CoS value.

Values 0 to 7

Default 0

Platforms All

priority

Syntax **priority** *level*

Context **[Tree]** (config>qos>plcr-ctrl-plcy>root>priority-mbs-thresholds priority)

Full Context configure qos policer-control-policy root priority-mbs-thresholds priority

Description The **priority** level command contains the **mbs-contribution** configuration command for a given strict priority level. Eight levels are supported numbered 1 through 8 with 8 being the highest strict priority.

Each of the eight priority CLI nodes always exists and do not need to be created. While parameters exist for each priority level, the parameters are only applied when the priority level within a parent policer instance is currently supporting child policers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority

Syntax **priority** [*priority*]
no priority

Context **[Tree]** (config>filter>redirect-policy>dest priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter redirect-policy destination priority

Description Redirect policies can contain multiple destinations. Each destination is assigned an initial or base **priority** which describes its relative importance within the policy.

Default priority 100

Parameters *priority* — Specifies the priority, expressed as a decimal integer, used to weigh the destination's relative importance within the policy.

Values 1 to 255

Platforms All

priority

Syntax **priority** {**low** | **high**}
no priority [{**low** | **high**}]

Context **[Tree]** (config>router>static-route-entry>indirect>forwarding-class priority)
[Tree] (config>router>static-route-entry>next-hop>forwarding-class priority)

Full Context configure router static-route-entry indirect forwarding-class priority
configure router static-route-entry next-hop forwarding-class priority

Description This optional command associates an enqueuing priority with the static route. The options are either high or low, with low being the default. This parameter has the ability to affect the likelihood that a packet will be enqueued at SAP ingress in the face of ingress congestion.

Once a packet is enqueued into an ingress buffer, the significance of this parameter is lost.

Default priority low

Parameters **low** — Setting the enqueuing parameter for a packet to **low** decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. Once the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

high — Setting the enqueuing parameter for a packet to **high** increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. Once the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax **priority** *priority*
no priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>if>eth-cfm>mep>grace>eth-ed priority)

Full Context configure router interface eth-cfm mep grace eth-ed priority

Description This command sets the priority bits and determines the forwarding class based on the mapping of priority to FC.

The **no** form of this command disables the local priority configuration and sets the priority to the **ccm-ltm-priority** associated with this MEP.

Default no priority

Parameters *priority* — Specifies the priority bit.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

priority

Syntax **priority** *priority*
no priority

Context [Tree] (config>router>fad>flex-algo priority)

Full Context configure router flexible-algorithm-definitions flex-algo priority

Description This command configures the priority of the FAD. This priority is used as a tie-breaker when the router has received multiple FADs for the same flexible algorithm.

Every router that is configured to participate in a particular flexible algorithm uses the same tie-breaker logic to select the winning FAD. This allows for consistent FAD definition selection in cases where routers advertise different definitions for a specific flexible algorithm. The following rules apply to the breaker mechanism.

- From the advertisements of the FAD in the area (including both locally generated advertisements and received advertisements), select the one with the highest priority value.
- If there are multiple advertisements of the FAD with the same highest priority, select the one that is originated from the router with either the highest system ID or router ID.

The **no** form of this command sets the priority to the default value.

Default priority 100

Parameters *priority* — Configures the priority of this FAD.

Values 0 to 255

Default 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority

Syntax **priority** *priority*
no priority

Context **[Tree]** (config>router>if>vrrp priority)
[Tree] (config>router>if>ipv6>vrrp priority)

Full Context configure router interface ipv6 vrrp priority
configure router interface vrrp priority

Description This command configures the base router priority for the virtual router instance used in the master election process.

The priority is the most important parameter set on a non-owner virtual router instance. The priority defines a virtual router's selection order in the master election process. Together, the priority value and the **preempt** mode allow the virtual router with the best priority to become the master virtual router.

The *base-priority* is used to derive the in-use priority of the virtual router instance as modified by any optional VRRP priority control policy. VRRP priority control policies can be used to either override or adjust the base priority value depending on events or conditions within the chassis.

The **priority** command is only available in the non-owner **vrrp** nodal context. The priority of **owner** virtual router instances is permanently set to 255 and cannot be changed.

For non-owner virtual router instances, the default base priority value is 100.

The **no** form of the command reverts to the default value.

Default priority 100

Parameters *priority* — The base priority used by the virtual router instance expressed as a decimal integer. If no VRRP priority control policy is defined, the *base-priority* is the in-use priority for the virtual router instance.

Values 1 to 254

Platforms All

priority

Syntax **priority** *priority-level* [{**delta** | **explicit**}]
no priority

Context **[Tree]** (config>vrrp>policy>priority-event>host-unreachable priority)
[Tree] (config>vrrp>policy>priority-event>lag-port-down>number-down priority)
[Tree] (config>vrrp>policy>priority-event>lag-port-down>weight-down priority)
[Tree] (config>vrrp>policy>priority-event>port-down priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>vrrp>policy>priority-event>route-unknown priority)

Full Context
configure vrrp policy priority-event host-unreachable priority
configure vrrp policy priority-event lag-port-down number-down priority
configure vrrp policy priority-event lag-port-down weight-down priority
configure vrrp policy priority-event port-down priority
configure vrrp policy priority-event route-unknown priority

Description
This command controls the effect the set event has on the virtual router instance in-use priority.

When the event is set, the *priority-level* is either subtracted from the base priority of each virtual router instance or it defines the explicit in-use priority value of the virtual router instance depending on whether the **delta** or **explicit** keywords are specified.

Multiple set events in the same policy have interaction constraints:

- If any set events have an explicit **priority** value, all the delta **priority** values are ignored.
- The set event with the lowest explicit **priority** value defines the in-use priority that are used by all virtual router instances associated with the policy.
- If no set events have an explicit **priority** value, all the set events delta **priority** values are added and subtracted from the base priority value defined on each virtual router instance associated with the policy.
- If the delta priorities sum exceeds the **delta-in-use-limit** parameter, then the **delta-in-use-limit** parameter is used as the value subtracted from the base priority value defined on each virtual router instance associated with the policy.

If the **priority** command is not configured on the priority event, the *priority-value* defaults to 0 and the qualifier keyword defaults to **delta**, therefore, there is no impact on the in-use priority.

The **no** form of the command configures the set event to subtract 0 from the base priority (no effect).

Default
no priority

Parameters
priority-level — The priority level adjustment value expressed as a decimal integer.

Values 0 to 254

delta — Configures what effect the *priority-level* will have on the base priority value. The default base priority value is **delta**.

When **delta** is specified, the *priority-level* value is subtracted from the associated virtual router instance's base priority when the event is set and no explicit events are set. The sum of the priority event *priority-level* values on all set delta priority events are subtracted from the virtual router base priority to derive the virtual router instance in-use priority value. If the **delta** priority event is cleared, the *priority-level* is no longer used in the in-use priority calculation.

explicit — Configures what effect the *priority-level* will have on the base priority value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When **explicit** is specified, the *priority-level* value is used to override the base priority of the virtual router instance if the priority event is set and no other **explicit** priority event is set with a lower *priority-level*. The set **explicit** priority value with the lowest *priority-level* determines the actual in-use protocol value for all virtual router instances associated with the policy.

Platforms All

priority

Syntax **priority** *priority-level* **explicit**
no priority

Context **[Tree]** (config>vrrp>policy>priority-event>mc-ipsec-non-forwarding priority)

Full Context configure vrrp policy priority-event mc-ipsec-non-forwarding priority

Description This command controls the effect the set event has on the virtual router instance in-use priority.

When the event is set, the *priority-level* is either subtracted from the base priority of each virtual router instance or it defines the explicit in-use priority value of the virtual router instance depending on whether the **delta** or **explicit** keywords are specified.

Multiple set events in the same policy have interaction constraints:

- If any set events have an explicit **priority** value, all the delta **priority** values are ignored.
- The set event with the lowest explicit **priority** value defines the in-use priority that are used by all virtual router instances associated with the policy.
- If no set events have an explicit **priority** value, all the set events delta **priority** values are added and subtracted from the base priority value defined on each virtual router instance associated with the policy.
- If the delta priorities sum exceeds the **delta-in-use-limit** parameter, then the **delta-in-use-limit** parameter is used as the value subtracted from the base priority value defined on each virtual router instance associated with the policy.

If the **priority** command is not configured on the priority event, the *priority-value* defaults to 0 and the qualifier keyword defaults to **delta**, therefore, there is no impact on the in-use priority.

The **no** form of the command configures the set event to subtract 0 from the base priority (no effect).

Default no priority

Parameters *priority-level* — The priority level adjustment value expressed as a decimal integer.

Values 0 to 254

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

explicit — When **explicit** is specified, the *priority-level* value is used to override the base priority of the virtual router instance if the priority event is set and no other **explicit** priority event is set with a lower *priority-level*. The set **explicit** priority value with the lowest *priority-level* determines the actual in-use protocol value for all virtual router instances associated with the policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

priority

Syntax **priority** *bridge-priority*
no priority

Context **[Tree]** (config>service>pw-template>stp priority)

Full Context configure service pw-template stp priority

Description The **bridge-priority** command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent. All values will be truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

The **no** form of this command returns the bridge priority to the default value.

Default priority 4096

Parameters *bridge-priority* — Specifies the bridge priority for the STP instance.

Values Allowed values are integers in the range of 4096 to 65535 with 4096 being the highest priority. The actual bridge priority value stored/ used is the number entered with the lowest 12 bits masked off which means the actual range of values is 4096 to 61440 in increments of 4096.

Platforms All

priority

Syntax **priority** *number*
no priority

Context **[Tree]** (config>router>isis>if>level priority)

Full Context configure router isis interface level priority

Description This command configures the priority of the IS-IS router interface for designated router election on a multi-access network.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This priority is included in hello PDUs transmitted by the interface on a multi-access network. The router with the highest priority is the preferred designated router. The designated router is responsible for sending LSPs with regard to this network and the routers that are attached to it.

The **no** form of this command reverts to the default value.

Default priority 64

Parameters *number* — Specifies the priority for this interface at this level.

Values 0 to 127

Platforms All

priority

Syntax **priority** *number*
no priority

Context **[Tree]** (config>router>ospf>area>interface priority)
[Tree] (config>router>ospf3>area>interface priority)

Full Context configure router ospf area interface priority
configure router ospf3 area interface priority

Description This command configures the priority of the OSPF interface that is used in an election of the designated router on the subnet.

This parameter is only used if the interface is of type broadcast. The router with the highest priority interface becomes the designated router. A router with priority 0 is not eligible to be Designated Router or Backup Designated Router.

The **no** form of this command reverts the interface priority to the default value.

Default priority 1

Parameters *number* — Specifies the interface priority expressed as a decimal integer. A value of 0 indicates the router is not eligible to be the Designated Router or Backup Designated Router on the interface subnet.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.321 priority-event

priority-event

Syntax [**no**] **priority-event**

Context **[Tree]** (config>vrrp>policy priority-event)

Full Context configure vrrp policy priority-event

Description This command creates the context to configure VRRP priority control events used to define criteria to modify the VRRP in-use priority.

A priority control event specifies an object to monitor and the effect on the in-use priority level for an associated virtual router instance.

Up to 32 priority control events can be configured within the **priority-event** node.

The **no** form of the command clears any configured priority events.

Platforms All

20.322 priority-marking

priority-marking

Syntax **priority-marking dscp** *dscp-name*
priority-marking prec *ip-prec-value*
no priority-marking

Context **[Tree]** (config>service>vpls>gsmp>group>neighbor priority-marking)
[Tree] (config>service>vprn>gsmp>group>neighbor priority-marking)

Full Context configure service vpls gsmp group neighbor priority-marking
configure service vprn gsmp group neighbor priority-marking

Description This command configures the type of priority marking to be used.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *dscp-name* — Specifies the DSCP code-point to be used.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

ip-prec-value — Specifies the precedence value to be used.

Values 0 to 7

Platforms All

20.323 priority-mbs-thresholds

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context **[Tree]** (config>subscr-mgmt>sub-prof>ingress>policer-control-policy priority-mbs-thresholds)
[Tree] (config>subscr-mgmt>sub-prof>egress>policer-control-policy priority-mbs-thresholds)

Full Context configure subscriber-mgmt sub-profile egress policer-control-policy priority-mbs-thresholds
configure subscriber-mgmt sub-profile ingress policer-control-policy priority-mbs-thresholds

Description The **priority-mbs-thresholds** command contains the root arbiter parent policer's **min-thresh-separation** command and each priority level's **mbs-contribution** command that is used to internally derive each priority level's shared-portion and fair-portion values. The system uses each priority level's shared-portion and fair-portion value to calculate each priority level's discard-unfair and discard-all MBS thresholds that enforce priority sensitive rate-based discards within the root arbiter's parent policer.

The **priority-mbs-thresholds** CLI node always exists and does not need to be created.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context **[Tree]** (config>card>fp>ingress>access>queue-group>policer-control-override priority-mbs-thresholds)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>card>fp>ingress>network>queue-group>policer-control-override priority-mbs-thresholds)

Full Context configure card fp ingress access queue-group policer-control-override priority-mbs-thresholds
configure card fp ingress network queue-group policer-control-override priority-mbs-thresholds

Description This command contains the root arbiter parent policer's **min-thresh-separation** command and each priority level's **mbs-contribution** command that is used to internally derive each priority level's shared-portion and fair-portion values. The system uses each priority level's shared-portion and fair-portion value to calculate each priority level's discard-unfair and discard-all MBS thresholds that enforce priority sensitive rate-based discards within the root arbiter's parent policer.

The **priority-mbs-thresholds** CLI node always exists and does not need to be created.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context [Tree] (config>service>apipe>sap>egress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>apipe>sap>ingress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>cpipe>sap>egress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>cpipe>sap>ingress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>epipe>sap>egress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>epipe>sap>ingress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>fpipe>sap>egress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>fpipe>sap>ingress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>ipipe>sap>egress>policer-control-override priority-mbs-thresholds)
[Tree] (config>service>ipipe>sap>ingress>policer-control-override priority-mbs-thresholds)

Full Context configure service apipe sap egress policer-control-override priority-mbs-thresholds
configure service apipe sap ingress policer-control-override priority-mbs-thresholds
configure service cpipe sap egress policer-control-override priority-mbs-thresholds
configure service cpipe sap ingress policer-control-override priority-mbs-thresholds
configure service epipe sap egress policer-control-override priority-mbs-thresholds
configure service epipe sap ingress policer-control-override priority-mbs-thresholds
configure service fpipe sap egress policer-control-override priority-mbs-thresholds
configure service fpipe sap ingress policer-control-override priority-mbs-thresholds
configure service ipipe sap egress policer-control-override priority-mbs-thresholds
configure service ipipe sap ingress policer-control-override priority-mbs-thresholds

Description This command overrides the CLI node contains the configured min-thresh-separation and the various priority level mbs-contribution override commands.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe sap ingress policer-control-override priority-mbs-thresholds
- configure service fpipe sap egress policer-control-override priority-mbs-thresholds
- configure service cpipe sap ingress policer-control-override priority-mbs-thresholds
- configure service cpipe sap egress policer-control-override priority-mbs-thresholds

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap ingress policer-control-override priority-mbs-thresholds
- configure service ipipe sap egress policer-control-override priority-mbs-thresholds
- configure service epipe sap egress policer-control-override priority-mbs-thresholds
- configure service epipe sap ingress policer-control-override priority-mbs-thresholds

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress policer-control-override priority-mbs-thresholds
- configure service apipe sap egress policer-control-override priority-mbs-thresholds

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context **[Tree]** (config>service>vpls>sap>egress>policer-ctrl-over priority-mbs-thresholds)
[Tree] (config>service>vpls>sap>ingress>policer-ctrl-over priority-mbs-thresholds)

Full Context configure service vpls sap egress policer-control-override priority-mbs-thresholds
configure service vpls sap ingress policer-control-override priority-mbs-thresholds

Description This command overrides the CLI node contains the configured min-thresh-separation and the various priority level mbs-contribution override commands.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context **[Tree]** (config>service>ies>if>sap>egress>policer-ctrl-over priority-mbs-thresholds)
[Tree] (config>service>ies>if>sap>ingress>policer-ctrl-over priority-mbs-thresholds)

Full Context configure service ies interface sap egress policer-control-override priority-mbs-thresholds
configure service ies interface sap ingress policer-control-override priority-mbs-thresholds

Description This command overrides the CLI node contains the configured min-thresh-separation and the various priority level mbs-contribution override commands.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-ctrl-over priority-mbs-thresholds)
[Tree] (config>service>vprn>if>sap>ingress>policer-ctrl-over priority-mbs-thresholds)

Full Context configure service vprn interface sap egress policer-control-override priority-mbs-thresholds
configure service vprn interface sap ingress policer-control-override priority-mbs-thresholds

Description This command overrides the CLI node contains the configured min-thresh-separation and the various priority level mbs-contribution override commands.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

priority-mbs-thresholds

Syntax **priority-mbs-thresholds**

Context **[Tree]** (config>qos>plcr-ctrl-plcy>root priority-mbs-thresholds)

Full Context configure qos policer-control-policy root priority-mbs-thresholds

Description The **priority-mbs-thresholds** command contains the root arbiter parent policer's **min-thresh-separation** command and each priority level's **mbs-contribution** command that is used to internally derive each priority level's shared-portion and fair-portion values. The system uses each priority level's shared-portion and fair-portion value to calculate each priority level's discard-unfair and discard-all MBS thresholds that enforce priority-sensitive rate-based discards within the root arbiter's parent policer.

The **priority-mbs-thresholds** CLI node always exists and does not need to be created.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.324 priority-sessions

priority-sessions

Syntax [**no**] **priority-sessions**

Context **[Tree]** (config>service>nat>nat-policy priority-sessions)
[Tree] (config>service>nat>firewall-policy priority-sessions)
[Tree] (config>service>nat>up-nat-policy priority-sessions)

Full Context configure service nat firewall-policy priority-sessions
configure service nat nat-policy priority-sessions

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service nat up-nat-policy priority-sessions

Description This command configures the prioritized sessions of this NAT or residential firewall policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy priority-sessions
- configure service nat nat-policy priority-sessions

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy priority-sessions

20.325 priority1

priority1

Syntax **priority1** *priority-value*
no priority1

Context **[Tree]** (config>system>ptp priority1)

Full Context configure system ptp priority1

Description This command configures the priority1 value of the local clock. This parameter is only used when the profile is set to ieee1588-2008. This value is used by the Best Master Clock Algorithm to determine which clock should provide timing for the network.

This value is used for the value to advertise in the Announce messages and for the local clock value in data set comparisons.

The **no** form of the command reverts to the default configuration.

Default priority1 128

Parameters *priority-value* — Specifies the value of the priority1 field.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.326 priority2

priority2

Syntax **priority2** *priority-value*
no priority2

Context **[Tree]** (config>system>ptp priority2)

Full Context configure system ptp priority2

Description This command configures the priority2 value of the local clock. This parameter is only used when the profile is set to ieee1588-2008 or g8275dot1-2014. The parameter is ignored when any other profile is selected.

This value is used by the Best Master Clock algorithm to determine which clock should provide timing for the network.

Note: This value is used for the value to advertise in the Announce messages and for local clock value in data set comparisons.

The **no** form of the command reverts to the default configuration.

Default priority2 128

Parameters *priority-value* — Specifies the value of the priority2 field.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.327 priv-lvl

priv-lvl

Syntax **priv-lvl** *priv-lvl user-profile-name*
no priv-lvl *priv-lvl*

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus>priv-lvl-map priv-lvl)

Full Context configure service vprn aaa remote-servers tacplus priv-lvl-map priv-lvl

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command maps a specific TACACS+ priv-lvl to a locally configured profile for authorization. This mapping is used when the **use-priv-lvl** option is specified for TACPLUS authorization.

Parameters *priv-lvl* — Specifies the privilege level used when sending a TACACS+ ENABLE request.

Values 0 to 15

user-profile-name — Specifies the user profile for this mapping.

Platforms All

priv-lvl

Syntax **priv-lvl** *priv-lvl user-profile-name*
no priv-lvl *priv-lvl*

Context **[Tree]** (config>system>security>tacplus>priv-lvl-map priv-lvl)

Full Context configure system security tacplus priv-lvl-map priv-lvl

Description This command maps a specific TACACS+ priv-lvl to a locally configured profile for authorization. This mapping is used when the **use-priv-lvl** option is specified for TACPLUS authorization.

Parameters *priv-lvl* — Specifies the privilege level used when sending a TACACS+ ENABLE request.

Values 0 to 15

user-profile-name — Specifies the user profile for this mapping.

Platforms All

20.328 priv-lvl-map

priv-lvl-map

Syntax [**no**] **priv-lvl-map**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus priv-lvl-map)

Full Context configure service vprn aaa remote-servers tacplus priv-lvl-map

Description Commands in this context specify a series of mappings between TACACS+ priv-lvl and locally configured profiles for authorization. These mappings are used when the use-priv-lvl option is specified for tacplus authorization.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default priv-lvl-map

Platforms All

priv-lvl-map

Syntax [**no**] **priv-lvl-map**

Context **[Tree]** (config>system>security>tacplus priv-lvl-map)

Full Context configure system security tacplus priv-lvl-map

Description Commands in this context specify a series of mappings between TACACS+ priv-lvl and locally configured profiles for authorization. These mappings are used when the use-priv-lvl option is specified for tacplus authorization.

The **no** form of this command reverts to the default.

Default priv-lvl-map

Platforms All

20.329 private-interface

private-interface

Syntax **private-interface** *ip-int-name*
no private-interface

Context **[Tree]** (config>ipsec>client-db>client private-interface)

Full Context configure ipsec client-db client private-interface

Description This command specifies the private interface name that is used for tunnel setup.

The **no** form of this command reverts to the default.

Default no private-interface

Parameters *ip-int-name* — Specifies the name of the private interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.330 private-ki

private-ki

Syntax **private-ki** *hex-string*
no private-ki

Context **[Tree]** (config>li>x-interfaces>lics>lic>authentication private-ki)

Full Context configure li x-interfaces lics lic authentication private-ki

Description This command configures the private key for the X1 and X2 interfaces.

The **no** form of this command reverts to the default.

Parameters *hex-string* — Specifies the password. Must contain exactly 32 hex nibbles.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.331 private-retail-subnets

private-retail-subnets

Syntax [**no**] **private-retail-subnets**

Context **[Tree]** (config>service>vprn>sub-if private-retail-subnets)

Full Context configure service vprn subscriber-interface private-retail-subnets

Description This command controls the export of retail subnets and prefixes to the wholesale forwarding service. When this attribute is configured, subnets and prefixes configured on the retail subscriber interface are no longer exported to the associated wholesale VPRN and remain private to the retail VPRN. This is useful in a IPoE or PPPoE business service context, as it allows retail services to use overlapping IP address spaces even if those services are associated with the same wholesale service. IPoE and PPPoE sessions are actually terminated in the retail service although their traffic transits on a SAP belonging to the wholesale service.

Configuring private retail subnets is not supported for IPv4 static hosts and ARP hosts. If PPPoE sessions need to coexist with IPv4 host types, then this attribute should not be configured on the retail subscriber interface.

This command fails if the subscriber interface is not associated with a wholesale service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the retail VPRN is of the type **hub**, this attribute is mandatory. In this case, private retail subnets are enabled by default and cannot be unconfigured.

The **no** form of this command disables overlapping IP addresses between different retailers referring to this interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.332 private-service

private-service

Syntax **private-service** *service-id*
private-service name *service-name*
no private-service

Context **[Tree]** (config>ipsec>client-db>client private-service)

Full Context configure ipsec client-db client private-service

Description This command specifies the private service ID that is used for tunnel setup.

The **no** form of this command reverts to the default.

Default no private-service

Parameters *service-id* — Specifies the service ID of the tunnel delivery service.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **private-service name** *service-name* variant can be used in all configuration modes.

Values {*id* | *svc-name*}

id:	1 to 2147483647
svc-name:	up to 64 characters (*svc-name* is an alias for input only. The *svc-name* gets replaced with an id automatically by SR OS in the configuration).

name *service-name* — Identifies the service, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.333 private-tcp-mss-adjust

private-tcp-mss-adjust

Syntax **private-tcp-mss-adjust** *octets*
private-tcp-mss-adjust default
no private-tcp-mss-adjust

Context **[Tree]** (config>router>l2tp>group>l2tpv3 private-tcp-mss-adjust)
[Tree] (config>router>l2tp>group>tunnel>l2tpv3 private-tcp-mss-adjust)
[Tree] (config>service>vprn>l2tp>l2tpv3 private-tcp-mss-adjust)
[Tree] (config>service>vprn>l2tp>group>l2tpv3 private-tcp-mss-adjust)
[Tree] (config>service>vprn>l2tp>group>tunnel>l2tpv3 private-tcp-mss-adjust)

Full Context configure router l2tp group l2tpv3 private-tcp-mss-adjust
configure router l2tp group tunnel l2tpv3 private-tcp-mss-adjust
configure service vprn l2tp group l2tpv3 private-tcp-mss-adjust
configure service vprn l2tp group tunnel l2tpv3 private-tcp-mss-adjust
configure service vprn l2tp l2tpv3 private-tcp-mss-adjust

Description This command enables TCP MSS adjust for L2TPv3 tunnels on the private side of the group or tunnel level. When this command is configured, the system updates the TCP MSS option value of the received TCP SYN packet on the private side.

Note that this command can be overridden by the corresponding configuration on the group or tunnel level.

With the **default** parameter, the system uses the upper-level configuration. With the non-default parameter, the system uses this configuration instead of the upper level configuration.

The **no** form of this command disables TCP MSS adjust on the private side.

Default no private-tcp-mss-adjust

Parameters *octets* — Specifies the new TCP MSS value in octets.

Values 512 to 9000

default — Specifies to use the upper-level configuration

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

private-tcp-mss-adjust

Syntax **private-tcp-mss-adjust** *bytes*
private-tcp-mss-adjust *octets*
no private-tcp-mss-adjust

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>ipsec>tnl-temp private-tcp-mss-adjust)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel private-tcp-mss-adjust)
[Tree] (config>service>ies>if>sap>ip-tunnel private-tcp-mss-adjust)
[Tree] (config>router>if>ipsec>ipsec-tunnel private-tcp-mss-adjust)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel private-tcp-mss-adjust)
[Tree] (config>service>vprn>if>sap>ip-tunnel private-tcp-mss-adjust)
[Tree] (config>service>vprn>if>sap>ipsec-tun private-tcp-mss-adjust)

Full Context
configure ipsec tunnel-template private-tcp-mss-adjust
configure router interface ipsec ipsec-tunnel private-tcp-mss-adjust
configure service ies interface ipsec ipsec-tunnel private-tcp-mss-adjust
configure service ies interface sap ip-tunnel private-tcp-mss-adjust
configure service vprn interface ipsec ipsec-tunnel private-tcp-mss-adjust
configure service vprn interface sap ip-tunnel private-tcp-mss-adjust
configure service vprn interface sap ipsec-tunnel private-tcp-mss-adjust

Description
This command enables TCP MSS to adjust for L2TPv3 tunnels, IPsec, or IP tunnels on the private side. When the command is configured, the system updates the TCP MSS option to the value of the received TCP SYN packet on the private side.

The **no** form of this command disables TCP MSS adjust on the private side.

Default
no private-tcp-mcc-adjust

Parameters
bytes — Specifies the new TCP MSS value in bytes.

Values 512 to 9000

octets — Specifies the new TCP MSS value in octets.

Values 512 to 9000

Platforms
7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec tunnel-template private-tcp-mss-adjust
- configure service vprn interface sap ip-tunnel private-tcp-mss-adjust
- configure service ies interface sap ip-tunnel private-tcp-mss-adjust
- configure service vprn interface sap ipsec-tunnel private-tcp-mss-adjust

VSR

- configure service ies interface ipsec ipsec-tunnel private-tcp-mss-adjust
- configure service vprn interface ipsec ipsec-tunnel private-tcp-mss-adjust
- configure router interface ipsec ipsec-tunnel private-tcp-mss-adjust

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.334 probe-count

probe-count

Syntax **probe-count** *probes-per-hop*
no probe-count

Context **[Tree]** (config>saa>test>type-multi-line>lsp-trace>sr-policy probe-count)

Full Context configure saa test type-multi-line lsp-trace sr-policy probe-count

Description This command configures the number of probes per hop.

The **no** form of this command reverts to the default value.

Default probe-count 1

Parameters *probes-per-hop* — Specifies the probes-per-hop count, expressed as number of packets.

Values 1 to 10

Default 1

Platforms All

20.335 probe-fail-enable

probe-fail-enable

Syntax [**no**] **probe-fail-enable**

Context **[Tree]** (config>saa>test>trap-gen probe-fail-enable)

Full Context configure saa test trap-gen probe-fail-enable

Description This command enables the generation of an SNMP trap when the consecutive probe failure threshold (configured using the **probe-fail-threshold** command) is reached during the execution of the SAA ping test. This command is not applicable to SAA trace route tests.

The **no** form of this command disables the generation of an SNMP trap.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.336 probe-fail-threshold

probe-fail-threshold

Syntax **probe-fail-threshold** *threshold*
no probe-fail-threshold

Context **[Tree]** (config>saa>test>trap-gen probe-fail-threshold)

Full Context configure saa test trap-gen probe-fail-threshold

Description This command configures the threshold for trap generation after ping probe failure.

This command has no effect when **probe-fail-enable** is disabled. This command is not applicable to SAA trace route tests.

The **no** form of this command returns the threshold value to the default.

Default probe-fail-threshold 1

Parameters *threshold* — Specifies the number of consecutive ping probe failures required to generate a trap.

Values 0 to 15

Platforms All

20.337 probe-history

probe-history

Syntax **probe-history** {**keep** | **drop** | **auto**}

Context **[Tree]** (config>saa>test probe-history)

Full Context configure saa test probe-history

Description Specifies history probe behavior. Defaults are associated with various configured parameters within the SAA test. Auto (keep) is used for test with probe counts of 100 or less, and intervals of 1 second and above. Auto (drop) only maintains summary information for tests marked as continuous with file functions, probe counts more than 100 and intervals of less than 1 second. SAA tests that are not continuous with a write to file defaults to Auto (keep). The operator is free to change the default behaviors for each type. Each test that maintains per probe history consumes more system memory. When per probe entries are required, the probe history is available at the completion of the test.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default probe-history auto

Parameters **auto** — An auto selector that determines the storage of the history information.

drop — Stores summarized min/max/avg data not per probe information for test runs. This may be configured for all tests to conserve memory.

keep — Stores per probe information for tests. This consumes significantly more memory than summary information and should only be used if necessary.

Platforms All

20.338 process-cpm-traffic-on-sap-down

process-cpm-traffic-on-sap-down

Syntax **process-cpm-traffic-on-sap-down**
[**no**] **process-cpm-traffic-on-sap-down**

Context **[Tree]** (config>service>vpls>sap process-cpm-traffic-on-sap-down)

Full Context configure service vpls sap process-cpm-traffic-on-sap-down

Description This command is applicable to simple SAPs configured on LAGs that are not part of any “endpoint” configurations or complicated resiliency schemes like MC-LAG with inter-chassis-backup (ICB) configurations. When configured, a simple LAG SAP will not be removed from the forwarding plane and flooded traffic (unknown unicast, broadcast and multicast) will be dropped on egress. This allows applicable control traffic that is extracted at the egress interface to be processed by the CPM. This command will not prevent a VPLS service from entering an Operational Down state if it is the last active connection to enter a non-operational state. By default, without this command, when a SAP on a LAG enters a non-operational state it is removed from the forwarding plane and no forwarding occurs to the egress.

The **no** form of this command means a SAP over a LAG that is not operational will be removed from the forwarding process.

Default no process-cpm-traffic-on-sap-down

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.339 profile

profile

Syntax **profile** *profile-name* [**create**]
no profile *profile-name*

Context **[Tree]** (config>app-assure>group>url-filter>web-service profile)

Full Context configure application-assurance group url-filter web-service profile

Description This command configures the category profiles of the web service.

The **no** form of this command removes the category profiles configuration.

Parameters *profile-name* — Specifies the name of the category profile, up to 256 characters.

create — Keyword that specifies to create a category profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

profile

Syntax [**no**] **profile** *user-profile-name*

Context **[Tree]** (config>system>security profile)

Full Context configure system security profile

Description This command creates a context to create user profiles for command authorization and other functions associated with a user.

Profiles can be used to deny or permit user access to entire command branches or to specific commands.

Once the profiles are created, the **user** command assigns users to one or more profiles. You can define up to 16 user profiles but a maximum of 8 profiles can be assigned to a user.

The **no** form of this command deletes a user profile.

Parameters *user-profile-name* — Specifies the user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

profile

Syntax **profile** {**in** | **out**}
no profile

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy profile)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy profile)

Full Context configure saa test type-multi-line lsp-ping sr-policy profile
configure saa test type-multi-line lsp-trace sr-policy profile

Description This command configures the profile state of the MPLS echo request packet.

The **no** form of this command reverts to the default value.

Default profile out

Parameters **in** — Specifies “in” as the profile state of the MPLS echo request packet.

out — Specifies “out” as the profile state of the MPLS echo request packet.

Platforms All

profile

Syntax **profile** {**in** | **out**}
no profile

Context **[Tree]** (config>oam-pm>session>ip profile)

Full Context configure oam-pm session ip profile

Description This command defines whether the TWAMP Light PDU packet should be treated as in-profile or out-of-profile. The default has been selected because the forwarding class defaults to best effort.

The **no** form of this command restores the default value.

Default profile out

Parameters **in** — Specifies that the TWAMP Light PDU packet is sent as in-profile.

out — Specifies that the TWAMP Light PDU packet is sent as out-of-profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

profile

Syntax **profile** {**in** | **out**}
no profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>oam-pm>session>mpls profile)

Full Context configure oam-pm session mpls profile

Description This command defines whether the DM PDU packet should be treated as in profile or out-of-profile.

The **no** form of this command reverts the default value.

Default profile out

Parameters **in** — Marks the PDU in profile.

out — Marks the PDU out of profile.

Default out

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

profile

Syntax **profile** {**in** | **out**}
no profile

Context [Tree] (config>qos>sap-ingress>fc profile)

Full Context configure qos sap-ingress fc profile

Description This command places a forwarding class or subclass into a color aware profile mode. Normally, packets associated with a class are considered in-profile or out-of-profile solely based on the dynamic rate of the ingress queue relative to its CIR. Explicitly defining a class as in-profile or out-of-profile overrides this function by handling each packet with the defined profile state.

The profile command may only be executed when the forwarding class or the parent forwarding class (for a subclass) is mapped to a queue that has been enabled to support color aware profile packets. The queue may only be configured for profile-mode at the time the queue is created in the SAP ingress QoS policy.

A queue operating in profile-mode may support in-profile, out-of-profile, and non-profiled packets simultaneously. However, the high- and low-priority classification actions are ignored when the queue is in profile-mode.

The **no** form of this command removes an explicit in-profile or out-of-profile configuration on a forwarding class or subclass.

Default no profile — The default profile state of a forwarding class or subclass is not to treat ingress packets as color aware. An explicit definition for in-profile or out-of-profile must be specified on the forwarding class or subclass.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **in** — The **in** keyword is mutually exclusive to the **out** keyword. When the profile in command is executed, all packets associated with the class will be handled as in-profile. Packets explicitly handled as in-profile or out-of-profile still flow through the ingress service queue associated with the class to preserve order within flows. In-profile packets will count against the CIR of the queue, diminishing the amount of CIR available to other classes using the queue that are not configured with an explicit profile.

out — The **out** keyword is mutually exclusive to the **in** keyword. When the profile out command is executed, all packets associated with the class will be handled as out-of-profile. Packets explicitly handled as in-profile or out-of-profile still flow through the ingress service queue associated with the class to preserve order within flows. Out-of-profile packets will not count against the CIR of the queue, allowing other classes using the queue that are not configured with an explicit profile to be measured against the full CIR.

Platforms All

profile

Syntax **profile** {**g8265dot1-2010** | **ieee1588-2008** | **g8275dot1-2014**}

Context **[Tree]** (config>system>ptp profile)

Full Context configure system ptp profile

Description This command configures the profile for the internal PTP clock, which defines the Best Master Clock Algorithm (BMCA) behavior.

The profile setting for the clock cannot be changed unless PTP is shutdown.

The **clock-type** is restricted based on the PTP profile setting.

- If the profile is **ieee1588-2008**, the **clock-type** is not restricted.
- If the profile is **g8265dot1-2010**, the **clock type** may only be ordinary slave or ordinary master; boundary clock is not allowed
- If the profile is **g8275dot1-2014**, the **clock-type** may only be boundary clock or ordinary slave; ordinary master is not allowed

When the profile is changed, the domain changes to the default value for the new profile. Any command parameters that are set to default for the original profile are changed to the default for the new profile. This applies to the following:

- **log-anno-interval** set for the clock
- **log-sync-interval** set for a peer or a port
- **log-delay-interval** set for a port

Non-default parameter values for the original profile remain unchanged.

Default profile g8265dot1-2010

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **g8265dot1-2010** — Conforms to the ITU-T G.8265.1 specification.

ieee1588-2008 — Conforms to the 2008 version of the IEEE1588 standard.

g8275dot1-2014 — Conforms to the ITU-T G.8275.1 specification.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

profile

Syntax **profile** *name* [**create**]
no profile *name*

Context **[Tree]** (config>system>network-element-discovery profile)

Full Context configure system network-element-discovery profile

Description This command configures a profile to be used by IGP to advertise the network element information to its neighbors.

The **no** form of this command deletes the specified profile.

Parameters *name* — Specifies the name of the profile, up to 32 characters.

Platforms All

profile

Syntax **profile** *user-profile-name*
no profile

Context **[Tree]** (config>system>security>user-template profile)

Full Context configure system security user-template profile

Description This command configures the command authorization profile to associate with a user template. See the **user-template** command for more details.

Parameters *user-profile-name* — The user profile name entered as a character string. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

Platforms All

profile

Syntax **profile** *quality-of-service-profile*

Context **[Tree]** (config>test-oam>link-meas>template>twl profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure test-oam link-measurement measurement-template twamp-light profile

Description This command configures the QoS profile. The profile indicator determines if the packet is treated as in or out of profile as it moves through the local node.

Default profile in

Parameters *quality-of-service-profile* — Specifies the QoS profile used when launching the link measurement test belonging to the specified template.

Values in, out

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.340 profile-capped

profile-capped

Syntax [**no**] **profile-capped**

Context **[Tree]** (config>qos>sap-ingress>policer profile-capped)
[Tree] (config>qos>sap-egress>policer profile-capped)
[Tree] (config>qos>qgrps>ingress>queue-group profile-capped)
[Tree] (config>qos>qgrps>egr>queue-group profile-capped)

Full Context configure qos queue-group-templates egress queue-group profile-capped
configure qos queue-group-templates ingress queue-group profile-capped
configure qos sap-egress policer profile-capped
configure qos sap-ingress policer profile-capped

Description Profile-capped mode enforces an overall in-profile burst limit to the CIR bucket for ingress undefined, ingress explicit in-profile, egress soft-in-profile, and egress explicit in-profile packets. The default behavior when profile-capped mode is not enabled is to ignore the CIR output state when an explicit in-profile packet is handled by an ingress or egress policer.

The profile-capped mode makes two changes:

- At egress, soft-in-profile packets (packets received from ingress as in-profile) are treated the same as explicit in-profile (unless explicitly reclassified as out-of-profile) and have an initial policer state of in-profile.
- At both ingress and egress, any packet output from the policer with a non-conforming CIR state are treated as out-of-profile (out-of-profile state is ignored for initial in-profile packets when profile-capped mode is not enabled).

Default no profile-capped

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

profile-capped

Syntax [**no**] **profile-capped**

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer profile-capped)
[Tree] (config>qos>qgrps>ing>qgrp>policer profile-capped)

Full Context configure qos queue-group-templates egress queue-group policer profile-capped
configure qos queue-group-templates ingress queue-group policer profile-capped

Description This command enables a limit on the profile.

Default no profile-capped

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.341 profile-out-preserve

profile-out-preserve

Syntax [**no**] **profile-out-preserve**

Context **[Tree]** (config>qos>sap-egress>policer profile-out-preserve)

Full Context configure qos sap-egress policer profile-out-preserve

Description This command specifies whether to preserve the color of offered out-of-profile traffic at sap-egress policer (profile of the packet can change based on egress CIR state).

When enabled, traffic determined as out-of-profile at ingress policer will be treated as out-of-profile at sap-egress policer.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.342 profile-preferred

profile-preferred

Syntax **profile-preferred**
no profile-preferred

Context **[Tree]** (config>qos>plcr-ctrl-plcy>root profile-preferred)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos policer-control-policy root profile-preferred

Description The **profile-preferred** command ensures that the root policer provides a preference to consume its PIR bucket tokens at a given priority level to packets that have their profile state set to in-profile by the output of the child policer CIR bucket.

Default no profile-preferred

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

20.343 profiled-traffic-only

profiled-traffic-only

Syntax [**no**] **profiled-traffic-only**

Context **[Tree]** (config>subscr-mgmt>msap-policy>sub-sla-mgmt>single-sub profiled-traffic-only)

Full Context configure subscriber-mgmt msap-policy sub-sla-mgmt single-sub-parameters profiled-traffic-only

Description This command specifies whether only profiled traffic is applicable for an MSAP. When enabled, all queues are deleted.

The **no** form of this command reverts to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

profiled-traffic-only

Syntax [**no**] **profiled-traffic-only**

Context **[Tree]** (config>service>ies>if>sap>sub-sla-mgmt>single-sub profiled-traffic-only)
[Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt>single-sub profiled-traffic-only)
[Tree] (config>service>vpls>sap>sub-sla-mgmt>single-sub-parameters profiled-traffic-only)
[Tree] (config>service>vprn>if>sap>sub-sla-mgmt>single-sub profiled-traffic-only)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt>single-sub profiled-traffic-only)

Full Context configure service ies interface sap sub-sla-mgmt single-sub profiled-traffic-only
configure service ies subscriber-interface group-interface sap sub-sla-mgmt single-sub-parameters profiled-traffic-only
configure service vpls sap sub-sla-mgmt single-sub-parameters profiled-traffic-only
configure service vprn interface sap sub-sla-mgmt single-sub profiled-traffic-only
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt single-sub-parameters profiled-traffic-only

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies whether only profiled traffic is applicable for this SAP. The profiled traffic refers to single subscriber traffic on a dedicated SAP (in the VLAN-per-subscriber model). When enabled, subscriber queues are instantiated through the QOS policy defined in the sla-profile and the associated SAP queues are deleted. This can increase subscriber scaling by reducing the number of queues instantiated per subscriber (in the VLAN-per-subscriber model). In order for this to be achieved, any configured multi-sub-sap limit must be removed (leaving the default of 1).

The **no** form of this command disables the command.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.344 progress-indicator

progress-indicator

Syntax **progress-indicator**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment progress-indicator)

Full Context configure system management-interface cli md-cli environment progress-indicator

Description Commands in this context configure progress indicator parameters.

Platforms All

20.345 prompt

prompt

Syntax **prompt**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment prompt)

Full Context configure system management-interface cli md-cli environment prompt

Description Commands in this context configure prompt parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.346 propagate-admin-group

propagate-admin-group

Syntax [**no**] **propagate-admin-group**

Context **[Tree]** (config>router>mpls>lsp>fast-reroute propagate-admin-group)
[Tree] (config>router>mpls>lsp-template>fast-reroute propagate-admin-group)

Full Context configure router mpls lsp fast-reroute propagate-admin-group
configure router mpls lsp-template fast-reroute propagate-admin-group

Description The command enables the signaling of the primary LSP path admin-group constraints in the FRR object at the ingress.

When this command is executed, the admin-group constraints configured in the context of the P2P LSP primary path, or the ones configured in the context of the LSP and inherited by the primary path, are copied into the FAST_REROUTE object. The admin-group constraints are copied into the 'include-any' or 'exclude-any' fields.

The ingress LER thus propagates these constraints to the downstream nodes during the signaling of the LSP to allow them to include the admin-group constraints in the selection of the FRR backup LSP for protecting the LSP primary path.

The ingress LER inserts the FAST_REROUTE object by default in a primary LSP path message. If the user disables the object using the following command, the admin-group constraints will not be propagated: **config>router>mpls>no frr-object**.

Note that the same admin-group constraints can be copied into the Session Attribute object. They are intended for the use of an LSR, typically an ABR, to expand the ERO of an inter-area LSP path. They are also used by any LSR node in the path of a CSPF or non-CSPF LSP to check the admin-group constraints against the ERO regardless if the hop is strict or loose. These are governed strictly by the command:

config>router>mpls>lsp>propagate-admin-group

In other words, the user may decide to copy the primary path admin-group constraints into the FAST_REROUTE object only, or into the Session Attribute object only, or into both. Note, however, that the PLR rules for processing the admin-group constraints can make use of either of the two object admin-group constraints.

This feature is supported with the following LSP types and in both intra-area and inter-area TE where applicable:

- Primary path of a RSVP P2P LSP.
- S2L path of an RSVP P2MP LSP instance
- LSP template for an S2L path of an RSVP P2MP LSP instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the signaling of administrative group constraints in the FRR object.

Default no propagate-admin-group

Platforms All

propagate-admin-group

Syntax [**no**] **propagate-admin-group**

Context **[Tree]** (config>router>mpls>lsp propagate-admin-group)
[Tree] (config>router>mpls>lsp-template propagate-admin-group)

Full Context configure router mpls lsp propagate-admin-group
configure router mpls lsp-template propagate-admin-group

Description This command enables propagation of session attribute object with resource affinity (C-type 1) in PATH message. If an LSR receives a session attribute with resource affinity, then it will check the compatibility of admin-groups received in PATH message against configured admin-groups on the egress interface of LSP.

To support admin-group for inter-area LSP, the ingress node must configure propagating admin-groups within the session attribute object. If a PATH message is received by an LSR node that has the **cspf-on-loose-hop** option enabled and the message includes admin-groups, then the ERO expansion by CSPF to calculate the path to the next loose hop includes the admin-group constraints received from ingress node.

If this option is disabled, then the session attribute object without resource affinity (C-Type 7) is propagated in PATH message and CSPF at the LSR node does not include admin-group constraints.

This admin group propagation is supported with a P2P LSP, a P2MP LSP instance, and an LSP template.

The user can change the value of the **propagate-admin-group** option on the fly. A RSVP P2P LSP performs a Make-Before-Break (MBB) on changing the configuration. A S2L path of an RSVP P2MP LSP performs a Break-Before-Make on changing the configuration.

The **no** form of this command reverts to the default value.

Default no propagate-admin-group

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.347 propagate-hold-time

propagate-hold-time

Syntax **propagate-hold-time** *second*
no propagate-hold-time

Context **[Tree]** (config>eth-cfm>redundancy>mc-lag propagate-hold-time)

Full Context configure eth-cfm redundancy mc-lag propagate-hold-time

Description This command configures the delay, in seconds, that fault propagation is delayed because of port or MC-LAG state changes. This provides the amount of time for system stabilization during a port state changes that may be protected by MC-LAG. This command requires the standby-mep-shutdown command in order to take effect.

The **no** form of the command reverts to the default.

Default propagate-hold-time 1

Parameters *seconds* — Specifies the amount of time in seconds. Zero means no delay.

Values 0 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.348 propagate-mac-flush

propagate-mac-flush

Syntax [**no**] **propagate-mac-flush**

Context **[Tree]** (config>service>vpls propagate-mac-flush)

Full Context configure service vpls propagate-mac-flush

Description This command enabled propagation of mac-flush messages received from the specified T-LDP on all spoke and mesh-SDPs within the context of the VPLS service. The propagation will follow split-horizon principles and any data-path blocking in order to avoid looping of these messages.

Default no propagate-mac-flush

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.349 propagate-mac-flush-from-bvpls

propagate-mac-flush-from-bvpls

Syntax [**no**] **propagate-mac-flush-from-bvpls**

Context **[Tree]** (config>service>vpls>pbb propagate-mac-flush-from-bvpls)

Full Context configure service vpls pbb propagate-mac-flush-from-bvpls

Description This command enables the propagation in the local PBB of any regular LDP MAC Flush received in the related B-VPLS. If an LDP MAC flush-all-but-mine is received in the B-VPLS context, the command controls also whether a flush is performed for all the customer MACs in the associated FDB. The command does not have any effect on a PBB MAC Flush (LDP MAC flush with PBB TLV) received in the related B-VPLS context.

The **no** form of this command disables the propagation of LDP MAC Flush i from the related B-VPLS.

Default no propagate-mac-flush-from-bvpls

Platforms All

20.350 propagate-metric

propagate-metric

Syntax [**no**] **propagate-metric**

Context **[Tree]** (config>service>vprn>rip propagate-metric)

Full Context configure service vprn rip propagate-metric

Description This command enables the BGP MED to be used to configure the RIP metric at the BGP to RIP transition on egress routers. BGP always configures the BGP MED to the RIP metric at the ingress router. When **propagate-metric** is configured, the RIP metric at egress routers is configured as the BGP MED attribute added to the optional value configured with the **metric-out** command.

The **no** version of this command sets the RIP metric to the optional value configured with the **metric-out** command plus 1.

Default no propagate-metric

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.351 propagate-pmtu-v4

propagate-pmtu-v4

Syntax [**no**] **propagate-pmtu-v4**

Context **[Tree]** (config>ipsec>tnl-temp propagate-pmtu-v4)
[Tree] (config>router>if>ipsec>ipsec-tunnel propagate-pmtu-v4)
[Tree] (config>service>ies>if>sap>ip-tunnel propagate-pmtu-v4)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel propagate-pmtu-v4)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel propagate-pmtu-v4)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel propagate-pmtu-v4)
[Tree] (config>service>vprn>if>sap>ip-tunnel propagate-pmtu-v4)

Full Context configure ipsec tunnel-template propagate-pmtu-v4
configure router interface ipsec ipsec-tunnel propagate-pmtu-v4
configure service ies inter ipsec ipsec-tunnel propagate-pmtu-v6
configure service ies interface sap ip-tunnel propagate-pmtu-v6
configure service vprn interface ipsec ipsec-tunnel propagate-pmtu-v4
configure service vprn interface sap ip-tunnel propagate-pmtu-v4
configure service vprn interface sap ipsec-tunnel propagate-pmtu-v4

Description This command enables the system to propagate the path MTU learned from public side to private side (IPv4 hosts).

The **no** form of this command prevents the learned path MTU propagation.

Default propagate-pmtu-v4

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ip-tunnel propagate-pmtu-v4
- configure ipsec tunnel-template propagate-pmtu-v4
- configure service ies interface sap ip-tunnel propagate-pmtu-v6
- configure service vprn interface sap ipsec-tunnel propagate-pmtu-v4

VSR

- configure service vprn interface ipsec ipsec-tunnel propagate-pmtu-v4
- configure router interface ipsec ipsec-tunnel propagate-pmtu-v4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.352 propagate-pmtu-v6

propagate-pmtu-v6

Syntax [**no**] **propagate-pmtu-v6**

Context **[Tree]** (config>ipsec>tnl-temp propagate-pmtu-v6)
[Tree] (config>router>if>ipsec>ipsec-tunnel propagate-pmtu-v6)
[Tree] (config>service>ies>if>sap>ip-tunnel propagate-pmtu-v6)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel propagate-pmtu-v6)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel propagate-pmtu-v6)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel propagate-pmtu-v6)
[Tree] (config>service>vprn>if>sap>ip-tunnel propagate-pmtu-v6)

Full Context configure ipsec tunnel-template propagate-pmtu-v6
configure router interface ipsec ipsec-tunnel propagate-pmtu-v6
configure service ies interface ipsec ipsec-tunnel propagate-pmtu-v6
configure service ies interface sap ip-tunnel propagate-pmtu-v6
configure service vprn interface ipsec ipsec-tunnel propagate-pmtu-v6
configure service vprn interface sap ip-tunnel propagate-pmtu-v6
configure service vprn interface sap ipsec-tunnel propagate-pmtu-v6

Description This command enables the system to propagate the path MTU learned from public side to private side (IPv6 hosts).

The **no** form of this command prevents the learned path MTU propagation.

Default propagate-pmtu-v6

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ip-tunnel propagate-pmtu-v6
- configure ipsec tunnel-template propagate-pmtu-v6
- configure service ies interface sap ip-tunnel propagate-pmtu-v6
- configure service vprn interface sap ipsec-tunnel propagate-pmtu-v6

VSR

- configure service vprn interface ipsec ipsec-tunnel propagate-pmtu-v6
- configure router interface ipsec ipsec-tunnel propagate-pmtu-v6
- configure service ies interface ipsec ipsec-tunnel propagate-pmtu-v6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.353 propagate-topology-change

propagate-topology-change

Syntax [**no**] **propagate-topology-change**

Context **[Tree]** (config>eth-ring>sub-ring>interconnect propagate-topology-change)

Full Context configure eth-ring sub-ring interconnect propagate-topology-change

Description This command configures the G.8032 sub-ring to propagate topology changes. From the sub-ring to the major ring as specified in the G.8032 interconnection flush logic. This command is only valid on the sub-ring and on the interconnection node. Since this command is only valid on a Sub-ring, a virtual link or non-virtual link must be specified to configure this command. The command is blocked on major rings (when both path a and b are specified on a ring).

The **no** form of this command reverts propagate to the default value.

Default no propagate-topology-change

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.354 protect-bundle

protect-bundle

Syntax [**no**] **protect-bundle** *bundle-id*

Context **[Tree]** (config>port>multilink-bundle protect-bundle)

Full Context configure port multilink-bundle protect-bundle

Description This command configures a protect bundle that is part of this BPGrp.

Parameters *bundle-id* — Specifies the protection multilink bundle in the bundle protection group. The command syntax must be configured as follows:

Values bundle-*type-slot/mda.bundle-num*

bundle-PPP or IMA-*slot/mda.bundle-num*	Creates an MLPPP or IMA bundle.
where:	**bundle**: keyword *slot*: IOM/MDA slot numbers *bundle-num*: 1 to 336

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For example:
router1>config>port>ml-bundle> protect-bundle bundle-ima-1/1.1

Platforms 7450 ESS, 7750 SR-7/12/12e

20.355 protect-circuit

protect-circuit

Syntax **protect-circuit** *port-id*
no protect-circuit

Context **[Tree]** (config>port>aps protect-circuit)

Full Context configure port aps protect-circuit

Description This command configures a physical port that will act as the protection circuit for this APS group. The protect circuit port must contain only the default configuration and cannot belong to another APS group. The protect circuit port must be of the same type as the working circuit for the APS group, for the port to be added to an APS group port. If that's not the case, the command will return an error.

A protection circuit can only be added if the working circuit already exists; the protection circuit must be removed from the configuration before the working circuit is removed.

When a port is a protect-circuit of an APS group, the configuration options available in the **config>port** *port-id***>sonet-sdh** context is not allowed for that port unless it is part of the noted exceptions. The exception list includes these SONET/SDH commands:

- clock-source
- [no] loopback
- [no] report-alarm
- section-trace
- [no] threshold

When is port configured as a protection circuit of an APS group, the configurations described above and all service configurations related to APS port are operationally inherited by the protect circuit. If the protect circuit cannot inherit the configurations (due to resource limitations), the configuration attempt fails and an error is returned to the user.

The protect circuit must be shutdown before it can be removed from the APS group port. The inherited configuration for the circuit and APS operational commands for that circuit are not preserved when the circuit is removed from the APS group.

The **no** form of this command removes the protect-circuit.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port-id* — Specifies the physical port that will act as the protection circuit for this APS group in the following format.

port-id	*slot*/*mda*/*port*		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

Refer to “Modifying Hold-Down Timer Values” in the **config**>**port**>**aps** **working-circuit** command description for information about modifying the timer defaults in the event of communication delays between the APS controllers.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

20.356 protect-path

protect-path

Syntax **protect-path** *path-name*
no protect-path

Context **[Tree]** (config>router>gmpls>lsp protect-path)

Full Context configure router gmpls lsp protect-path

Description This command specifies the protect path for a GMPLS LSP. At least one protect path must be specified if a GMPLS LSP uses 1-to-N end-to-end protection. The *path-name* parameter must correspond to a path defined under **config>router>gmpls>path**.

The **no** form of the command removes the **protect-path** definition.

Default no protect-path

Parameters *path-name* — The name of the path used by the protect path.

Values 32 characters maximum text string

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.357 protect-tp-path

protect-tp-path

Syntax [**no**] **protect-tp-path**

Context **[Tree]** (config>router>mpls>lsp protect-tp-path)

Full Context configure router mpls lsp protect-tp-path

Description This command creates or edits the protect path for an MPLS-TP LSP. At least one working path must exist before a protect path can be created for an MPLS-TP LSP. If MPLS-TP linear protection is also configured, then this is the path that is used as the default protect path for the LSP. The protect path must be deleted before the working path. Only one protect path can be created for each MPLS-TP LSP.

The following commands are applicable to the working-tp-path: **lsp-num, in-label, out-label, mep, shutdown**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.358 protecting-nexthop-id

protecting-nexthop-id

Syntax **protecting-nexthop-id** *next-hop-index*
no protecting-nexthop-id

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment>next-hop-id protecting-nexthop-id)

Full Context configure router p2mp-sr-tree replication-segment next-hop-id protecting-nexthop-id

Description This command provides the ID of the protection next-hop used for FRR.

The protection next-hop outgoing SID is pushed on top of the next-hop SID list.

The **no** form of this command removes the protection next-hop.

Parameters *next-hop-index* — Specifies the ID of the protection next-hop.

Values 1 to 4096

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.359 protection

protection

Syntax **protection none**
protection hmac-sha256 key *key* [**hash** | **hash2** | **custom**]
no protection

Context **[Tree]** (config>python>py-script protection)

Full Context configure python python-script protection

Description This command specifies the format of the Python script file(s) in this python-script. Unintentional changing of Python script file could be prevented by using protected format.

The **no** form of this command equals to **protection none**.

Parameters **none** — Indicates the Python script is stored in plain text, without any mechanism in place to ensure the integrity nor the confidentiality of the content of the Python script.

hmac-sha256 — Indicates the first line of the Python script must consist of the hash value obtained by hashing the rest of the Python script using the **hmac-sha256** hashing algorithm.

key — The specified key along with original Python script file content are used to compute the hash. The computed hash will be compared to the hash in the Python script file. If there is no match, then system will fail to load the script.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the key entered is a customized hashing scheme.

Platforms All

protection

Syntax **protection** *protection*
no protection

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc>func>end-x protection)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end-x protection

Description This command configures the protection type of the SID.

The **no** form of this command reverts to the default value of **protected**.

Default protection protected

Parameters *protection* — Specifies whether or not the adjacency SID is protected

Values protected, unprotected

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

20.360 protection-template

protection-template

Syntax **protection-template** *name*
no protection-template

Context **[Tree]** (config>router>mpls>mpls-tp protection-template)

Full Context configure router mpls mpls-tp protection-template

Description Protection templates are used to define generally applicable protection parameters for MPLS-TP tunnels. Only linear protection is supported, and so the application of a named template to an MPLS-TP LSP implies that linear protection is used. A protection template is applied under the MEP context of the protect-path of an MPLS-TP LSP.

The protection-template command creates or edits a named protection template.

Default no protection-template

Parameters *name* — Specifies the protection template name as a text string of up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

protection-template

Syntax **protection-template** *name*
no protection-template

Context **[Tree]** (config>router>mpls>lsp>protect-tp-path>mep protection-template)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls lsp protect-tp-path mep protection-template

Description This command applies a protection template name to an MPLS-TP LSP that the protect path is configured under. If the template is applied, then MPLS-TP 1:1 linear protection is enabled on the LSP, using the parameters specified in the named template.

A named protection template can only be applied to the protect path context of an MPLS-TP LSP.

The no form of this command removes the template and thus disables mpls-tp linear protection on the LSP.

Default no protection-template

Parameters *name* — Specifies at text string for the template up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.361 protection-type

protection-type

Syntax **protection-type** {**g8031-1to1** | **loadsharing**}

Context **[Tree]** (config>eth-tunnel protection-type)

Full Context configure eth-tunnel protection-type

Description This command configures the model used for determining which members are actively receiving and transmitting data.

When the value is set to “g8031-1to1 (1)”, as per the G.8031 specification, only two members are allowed, and only one of them can be active at one point in time.

When the value is set to “loadsharing (2)”, multiple members can be active at one point in time.

Default protection-type g8031-1to1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

protection-type

Syntax **protection-type** {**link** | **node**}
no protection-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>route-next-hop-policy>template protection-type)

Full Context configure router route-next-hop-policy template protection-type

Description This command configures the protection type constraint into the route next-hop policy template.

The user can select if link protection or node protection is preferred in the selection of an LFA next-hop for all IP prefixes and LDP FEC prefixes to which a route next-hop policy template is applied. The default in SR OS implementation is node protection. The implementation will fall back to the other type if no LFA next-hop of the preferred type is found.

When the route next-hop policy template is applied to an IP interface, all prefixes using this interface as a primary next-hop will follow the protection type preference specified in the template.

The **no** form deletes the protection type constraint from the route next-hop policy template.

Default protection-type node

Parameters **{link | node}** — Specifies the two possible values for the protection type.

Default node

Platforms All

20.362 protocol

protocol

Syntax **protocol** *protocol-id*
no protocol

Context [Tree] (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>match protocol)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry match protocol

Description This command configures the protocol ID to be matched in this entry of the VAS filter.

The **no** form of this command removes the protocol ID from the match criterium in the entry.

Parameters *protocol-id* — Specifies the protocol to match.

Values protocol-id: *protocol-number* | *protocol-name*
protocol-number: 1, 6, 17]D
[0x1,0x6,0x11]H [0b1,0b110,0b10001]B
protocol-name: none, icmp, tcp, udp
* udp/tcp wildcard

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax **protocol** *protocol-type*
no protocol

Context **[Tree]** (config>port>sonet-sdh>path>atm>ilmi protocol)

Full Context configure port sonet-sdh path atm ilmi protocol

Description This command configures the protocol.

Parameters *protocol-type* — The *protocol-type* is an enumerated integer whose value indicates the ILMI version of either 3.1 or 4.0 that is advertised by IME and also indicates the ILMI IME type of either user-side or network-side.

Values 4_0-user, 4_0-network. 3_1-user, 3_1-network

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

protocol

Syntax **protocol** *protocol-name*

Context **[Tree]** (config>app-assure protocol)

Full Context configure application-assurance protocol

Description This command configures the shutdown of protocols system-wide.

Parameters *protocol-name* — A string of up to 32 characters identifying a predefined protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax **protocol** {**eq** | **neq**} *protocol-name*
no protocol

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry protocol)

Full Context configure application-assurance group policy app-filter entry protocol

Description This command configures protocol signature in the application definition.

The **no** form of this command restores the default (removes protocol from match application defined by this app-filter entry).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no protocol

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-name — A string of up to 32 characters identifying a predefined protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax **protocol** *protocol-name* **export-using** *export-method*
no protocol *protocol-name*

Context **[Tree]** (config>app-assure>group>statistics>aa-sub protocol)

Full Context configure application-assurance group statistics aa-sub protocol

Description This command configures aa-sub accounting statistics for export of protocols of a given AA ISA group/partition.

The no form of this command removes the protocol name.

Parameters *protocol-name* — Specifies an existing protocol name up to 32 characters in length.

export-using *export-method* — Specifies that the method of stats export to be used. Accounting-policy is the only option for protocol statistics.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax **protocol**

Context **[Tree]** (config>app-assure>group>statistics protocol)

Full Context configure application-assurance group statistics protocol

Description Commands in this context configure accounting and statistics collection parameters per-system for protocols of application assurance for a given AA ISA group/partition.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax **protocol** *ipsec-protocol*
no protocol

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>ipsec>static-sa protocol)

Full Context configure ipsec static-sa protocol

Description This command configures the security protocol to use for an IPsec manual SA. The **no** statement resets to the default value.

Default protocol esp

Parameters *ipsec-protocol* — Identifies the IPsec protocol used with this static SA.

Values **ah** — Specifies the Authentication Header protocol.**esp** — Specifies the Encapsulation Security Payload protocol.

Platforms All

protocol

Syntax **protocol any**
protocol *protocol-id* **port opaque**
protocol *protocol-id* **port any**
protocol *protocol-id* **port from** *begin-port-id* **to** *end-port-id*
no protocol

Context [Tree] (config>ipsec>ts-list>local>entry protocol)
[Tree] (config>ipsec>ts-list>remote>entry protocol)

Full Context configure ipsec ts-list local entry protocol
configure ipsec ts-list remote entry protocol

Description This command specifies the protocol and port range in the IKEv2 traffic selector.

The SR OS supports OPAQUE ports and port ranges for the following protocols:

- TCP
- UDP
- SCTP
- ICMP
- ICMPv6
- MIPv6

For ICMP and ICMPv6, the *port* value takes the form *icmp-type*/*icmp-code*. For MIPv6, the *port* value is the mobility header type. For other protocols, only the **port any** configuration can be used.

Default no protocol

Parameters *protocol-id* — Specifies the protocol ID. The value can be a number, a protocol name, or **any**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

begin-port-id — Specifies the beginning of the port range.

Values For TCP, UDP, and SCTP, the value is the port number.
For ICMP and ICMPv6, the value takes the form *icmp-type*/*icmp-code*; for example, 0/0.
For MIPv6, the value is the mobility header type.

end-port-id — Specifies the end of the port range

Values For TCP, UDP, and SCTP, the value is the port number.
For ICMP and ICMPv6, the value takes the form *icmp-type*/*icmp-code*; for example, 0/0.
For MIPv6, the value is the mobility header type.

opaque — Specifies OPAQUE ports.

any — Specifies any port.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax [**no**] **protocol** {*number* | **any**}

Context **[Tree]** (config>service>nat>firewall-policy>unknown-protocols protocol)

Full Context configure service nat firewall-policy unknown-protocols protocol

Description This command configures the protocol numbers that are allowed to create unknown flows.

Protocol or IPv6 extension header values that are explicitly supported by SR OS can be configured but will not be treated as unknown protocols.

The **no** form of the command removes the allowance for the specified protocol to create unknown flows.

Parameters **any** — Specifies that unknown flows can be created by any protocol.

number — Specifies the IANA number of a protocol that needs to be allowed to create unknown flows.

Values 0 to 255

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

protocol

Syntax [**no**] **protocol** *protocol-id*

Context **[Tree]** (config>filter>match-list>protocol-list protocol)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter match-list protocol-list protocol

Description This command adds a protocol to the match protocol list.

The **no** form of this command removes the protocol from the **protocol-list**.

Parameters *protocol-id* — *protocol-number*, *protocol-name*

protocol-number — Specifies the protocol number value to be added or removed from the protocol list. The value can be expressed as a decimal integer, or in hexadecimal or binary format.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — Specifies the protocol name to be added or removed from the protocol list.

Values icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp.

Platforms All

protocol

Syntax **protocol** *protocol*
no protocol [*protocol*]

Context **[Tree]** (config>vrrp>policy>priority-event>route-unknown protocol)

Full Context configure vrrp policy priority-event route-unknown protocol

Description This command adds one or more route sources to match the route unknown IP route prefix for a route unknown priority control event.

If the route source does not match one of the defined protocols, the match is considered unsuccessful and the **route-unknown** event transitions to the set state.

The **protocol** command is optional. If the **protocol** command is not executed, the comparison between the RTM prefix return and the **route-unknown** IP route prefix will not include the source of the prefix. The **protocol** command cannot be executed without at least one associated route source parameter. All parameters are reset each time the **protocol** command is executed and only the explicitly defined protocols are allowed to match.

The **no** form of the command removes protocol route source as a match criteria for returned RTM route prefixes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To remove specific existing route source match criteria, execute the **protocol** command and include only the specific route source criteria. Any unspecified route source criteria is removed.

Default no protocol — No route source for the route unknown priority event is defined.

Parameters *protocol* — Explicitly defined protocols

Values **bgp** - This parameter defines BGP as an eligible route source for a returned route prefix from the RTM when looking up the **route-unknown** route prefix. The **bgp** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **bgp** parameter, a returned route prefix with a source of BGP will not be considered a match and will cause the event to enter the set state. This parameter only applies to the 7750 SR and 7950 XRS.

bgp-vpn - This parameter defines **bgp-vpn** as an eligible route source for a returned route prefix from the RTM when looking up the **route-unknown** route prefix. The **bgp-vpn** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **bgp-vpn** parameter, a returned route prefix with a source of **bgp-vpn** will not be considered a match and will cause the event to enter the set state. This parameter only applies to the 7750 SR and 7950 XRS.

ospf - This parameter defines OSPF as an eligible route source for a returned route prefix from the RTM when looking up the **route-unknown** route prefix. The **ospf** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **ospf** parameter, a returned route prefix with a source of OSPF will not be considered a match and will cause the event to enter the set state.

is-is - This parameter defines IS-IS as an eligible route source for a returned route prefix from the RTM when looking up the **route-unknown** route prefix. The **is-is** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **is-is** parameter, a returned route prefix with a source of IS-IS will not be considered a match and will cause the event to enter the set state.

rip - This parameter defines RIP as an eligible route source for a returned route prefix from the RTM when looking up the **route-unknown** route prefix. The **rip** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **rip** parameter, a returned route prefix with a source of RIP will not be considered a match and will cause the event to enter the set state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

static - This parameter defines a static route as an eligible route source for a returned route prefix from the RTM when looking up the **route-unknown** route prefix. The **static** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **static** parameter, a returned route prefix with a source of static route will not be considered a match and will cause the event to enter the set state.

Platforms All

protocol

Syntax **protocol** *protocol-id*
no protocol

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry protocol)

Full Context configure system security management-access-filter ip-filter entry protocol

Description This command configures an IP protocol type to be used as a management access filter match criterion.

The protocol type, such as TCP, UDP, and OSPF, is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17).

The **no** form the command removes the protocol from the match criteria.

Parameters *protocol* — Specifies the protocol number for the match criterion.

Values 1 to 255 (decimal)

Platforms All

protocol

Syntax [**no**] **protocol** *name* [**create**]

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy protocol)

Full Context configure system security dist-cpu-protection policy protocol

Description This command creates the protocol for control in the policy.

Explanatory notes for some of the protocols:

- bfd-cpm: includes all bfd handled on the CPM including cpm-np type, single hop and multi-hop, and MPLS-TP CC and CV bfd
- dhcp: includes dhcp for IPv4 and IPv6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- eth-cfm: 802.1ag and includes Y.1731. Eth-cfm packets on port and LAG based facility MEPs are not included (but packets on Tunnel MEPs are).
- icmp: includes IPv4 and IPv6 ICMP (including RS/RA/Redirect) except NS/NA Neighbor Discovery packets which are classified as a separate protocol “ndis”
- icmp-ping-check: includes those packets associated with ping-template functions
- isis: includes isis used for SPBM
- ldp: includes ldp and t-ldp
- mpls-ttl: MPLS packets that are extracted due to an expired mpls ttl field
- ndis: IPv6 NS/NA Neighbor Discovery (not including RS/RA/Redirect which are classified as part of the protocol “icmp”)
- ospf: includes all OSPFv2 and OSPFv3 packets.
- pppoe-pppoa: includes PADx, LCP, PAP/CHAP and NCPs
- all-unspecified: a special “protocol”. When configured, this treats all extracted control packets that are not explicitly created in the dist-cpu-protection policy as a single aggregate flow (or “virtual protocol”). It lumps together “all the rest of the control traffic” to allow it to be rate limited as one flow. It includes all control traffic of all protocols that are extracted and sent to the CPM (even protocols that cannot be explicitly configured with the distributed cpu protection feature). Control packets that are both forwarded and copied for extraction are not included. If an operator later explicitly configures a protocol, then that protocol is suddenly no longer part of the “all-unspecified” flow. The “all-unspecified” protocol must be explicitly configured in order to operate.

“no protocol x” means packets of protocol x are not monitored and not enforced (although they do count in the fp protocol queue) on the objects to which this dist-cpu-protection policy is assigned, although the packets will be treated as part of the all-unspecified protocol if the all-unspecified protocol is created in the policy.

Parameters *names* — Signifies the protocol name.

Values arp, dhcp, http-redirect, icmp, icmp-ping-check, igmp, mld, ndis, pppoe-pppoa, all-unspecified, mpls-ttl, bfd-cpm, bgp, eth-cfm, isis, ldp, ospf, pim, rsvp.

Platforms All

protocol

Syntax **protocol** *protocol* [**all** | {**instance** *instance*}]
protocol *protocol2* [*protocol2* (up to 5 max)]
no protocol

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from protocol)

Full Context configure router policy-options policy-statement entry from protocol

Description This command configures a routing protocol as a match criterion for a route policy statement entry. This command is used for both import and export policies depending how it is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The **instance** command cannot be used if multiple protocol names are specified for the *protocol2* parameter.

The **no** form of this command removes the protocol match criterion.

Default no protocol

Parameters *protocol* — Specifies the protocol name for the match criterion.

Values direct, static, bgp, isis, ospf, rip, aggregate, bgp-vpn, igmp, pim, ospf3, ldp, sub-mgmt, mld, managed, vpn-leak, nat, periodic, ipsec, dhcpv6-pd, dhcpv6-na, dhcpv6-ta, dhcpv6-pd-excl, ripng, bgp-label, direct-interface, arp-nd, rib-api, evpn-if

instance — Specifies the OSPF, OSPFv3, or IS-IS protocol instance.

Values isis-inst — 0 to 127
ospf-inst — 0 to 31
ospf3-inst — 0 to 31, 64 to 95

protocol2 — Specifies up to five protocol names to match on.

Values direct, static, isis, aggregate, bgp, bgp-label, direct-interface

all — Keyword that specifies to match on any OSPF, OSPFv3, or IS-IS protocol instance.

Platforms All

protocol

Syntax **protocol** *protocol* [**all** | **instance** *instance*]
protocol bgp bgp-label
no protocol

Context **[Tree]** (config>router>policy-options>policy-statement>entry>to protocol)

Full Context configure router policy-options policy-statement entry to protocol

Description This command configures a routing protocol as a match criterion for a route policy statement entry. This command is used for both import and export policies depending how it is used.

The **no** form of this command removes the protocol match criterion.

Default no protocol

Parameters *protocol* — Specifies the protocol name to match on.

Values bgp, isis, ospf, rip, bgp-vpn, ospf3, vpn-leak, ldp, ripng, bgp-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

instance — Specifies the OSPF, OSPFv3, or IS-IS instance.

Values isis-inst — 0 to 127
ospf-inst — 0 to 31
ospf3-inst — 0 to 31, 64 to 95

all — Keyword that specifies to match on any OSPF, OSPFv3, or IS-IS protocol instance.

Platforms All

20.363 protocol-configuration-options

protocol-configuration-options

Syntax **protocol-configuration-options** {**apco** | **pco**}
no protocol-configuration-options

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile protocol-configuration-options)

Full Context configure subscriber-mgmt gtp peer-profile protocol-configuration-options

Description This command configures the Information Element to use for the Protocol Configuration Options.

The **no** form of this command reverts to the default value.

Default protocol-configuration-options pco

Parameters **apco** — Specifies that the system uses the Protocol Configuration Options Information Element.

pco — Specifies that the system uses the Additional Protocol Configuration Options Information Element.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

20.364 protocol-list

protocol-list

Syntax **protocol-list** *protocol-list-name* [**create**]
no protocol-list *protocol-list-name*

Context **[Tree]** (config>filter>match-list protocol-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter match-list protocol-list

Description This command creates a list of IP protocols that can be used in line card IP and IPv6 filters.

The **no** form of this command removes the IP protocol list.

Default no protocol-list

Parameters *protocol-list-name* — Specifies the name of the protocol list.

create — This keyword is required to create the protocol list. After it is created, the protocol list can be enabled with or without the **create** keyword.

Platforms All

20.365 protocol-port

protocol-port

Syntax [**no**] **protocol-port**

Context **[Tree]** (config>cflowd>collector>aggregation protocol-port)

Full Context configure cflowd collector aggregation protocol-port

Description This command specifies that flows be aggregated based on the IP protocol, source port number, and destination port number.

The **no** form of this command removes this type of aggregation from the collector configuration.

Platforms All

20.366 protocol-protection

protocol-protection

Syntax **protocol-protection** [**allow-sham-links**] [**block-pim-tunneled**]
no protocol-protection

Context **[Tree]** (config>sys>security>cpu-protection protocol-protection)

Full Context configure system security cpu-protection protocol-protection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command causes the network processor on the CPM to discard all packets received for protocols that are not configured on the particular interface. This helps mitigate DoS attacks by filtering invalid control traffic before it hits the CPU. For example, if an interface does not have IS-IS configured, then protocol protection will discard any IS-IS packets received on that interface.

Default no protocol-protection

Parameters **allow-sham-links** — Allows sham links. As OSPF sham links form an adjacency over the MPLS-VPRN backbone network, when protocol-protection is enabled, the tunneled OSPF packets to be received over the backbone network must be explicitly allowed.

block-pim-tunneled — - Blocks extraction and processing of PIM packets arriving at the SR OS node inside a tunnel (for example, MPLS or GRE) on a network interface. With protocol-protection enabled and tunneled pim blocked, PIM in an mVPN on the egress DR will not switch traffic from the (*,G) to the (S,G) tree.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

20.367 provider-tunnel

provider-tunnel

Syntax [**no**] **provider-tunnel**

Context **[Tree]** (config>service>vpls provider-tunnel)

Full Context configure service vpls provider-tunnel

Description Commands in this context configure the use of a P2MP LSP to forward Broadcast, Unknown unicast, and Multicast (BUM) packets of a VPLS or B-VPLS instance. The P2MP LSP is referred to as the Provider Multicast Service Interface (PMSI).

Platforms All

provider-tunnel

Syntax **provider-tunnel**

Context **[Tree]** (config>service>vprn>mvpn provider-tunnel)

Full Context configure service vprn mvpn provider-tunnel

Description This command enables context to configure tunnel parameters for the MVPN.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

provider-tunnel

Syntax **provider-tunnel**

Context **[Tree]** (config>router>gtm provider-tunnel)

Full Context configure router gtm provider-tunnel

Description This command enables context to configure tunnel parameters for the GTM.

Platforms All

20.368 proxy

proxy

Syntax **proxy**

Context **[Tree]** (config>aaa>diam-peer-plcy proxy)

Full Context configure aaa diameter-peer-policy proxy

Description Commands in this context configure the diameter peer policy proxy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.369 proxy-arp

proxy-arp

Syntax [**no**] **proxy-arp**

Context **[Tree]** (config>service>vpls proxy-arp)

Full Context configure service vpls proxy-arp

Description Commands in this context configure the proxy-ARP parameters in a VPLS service.

Default no proxy-arp

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

proxy-arp

Syntax [**no**] **proxy-arp** [**mac** [*ieee-address*]] [**ip** [*ipaddr*] **all**]]

Context **[Tree]** (debug>service>id proxy-arp)

Full Context debug service id proxy-arp

Description This command enables the debug of the proxy-arp function for a specified service. Alternatively, the debug can be enabled only for certain entries given by their IP or MAC addresses.

Platforms All

proxy-arp

Syntax [**no**] **proxy-arp**

Context **[Tree]** (config>service>vprn>nw-if proxy-arp)

Full Context configure service vprn nw-if proxy-arp

Description This command enables proxy ARP on the interface.

Default no proxy-arp

20.370 proxy-arp-nd

proxy-arp-nd

Syntax **proxy-arp-nd**

Context **[Tree]** (config>service proxy-arp-nd)

Full Context configure service proxy-arp-nd

Description Commands in this context configure the service-level **proxy-arp-nd** commands.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.371 proxy-arp-policy

proxy-arp-policy

Syntax [**no**] **proxy-arp-policy** *policy-name* [*policy-name*]

Context **[Tree]** (config>service>ies>if proxy-arp-policy)
[Tree] (config>service>ies>sub-if>grp-if proxy-arp-policy)
[Tree] (config>service>vprn>if proxy-arp-policy)
[Tree] (config>service>vprn>sub-if>grp-if proxy-arp-policy)

Full Context configure service ies interface proxy-arp-policy
configure service ies subscriber-interface group-interface proxy-arp-policy
configure service vprn interface proxy-arp-policy
configure service vprn subscriber-interface group-interface proxy-arp-policy

Description This command specifies an existing policy-statement to analyze match and action criteria that controls the flow of routing information to and from a given protocol, set of protocols, or a neighbor.

The **no** form of this command disables the proxy ARP capability.

Parameters *policy-name* — Specifies the export route policy name. Allowed values are any string, up to 32 characters, composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified name must already be defined.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface proxy-arp-policy
- configure service ies subscriber-interface group-interface proxy-arp-policy

All

- configure service vprn interface proxy-arp-policy
- configure service ies interface proxy-arp-policy

proxy-arp-policy

Syntax **proxy-arp-policy** *policy-name* [*policy-name*]
no proxy-arp-policy

Context **[Tree]** (config>subscr-mgmt>git>ipv4 proxy-arp-policy)

Full Context configure subscriber-mgmt group-interface-template ipv4 proxy-arp-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a proxy ARP policy for the interface.

The **no** form of this command disables the proxy ARP capability.

Default no proxy-arp-policy

Parameters *policy-name* — Specifies the export route policy name. Allowed values are any string, up to 32 characters, composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. A maximum of five policy names can be specified.

Note: The specified policy name must already be defined.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

proxy-arp-policy

Syntax **proxy-arp-policy** *policy-name* [*policy-name*]
no proxy-arp-policy

Context **[Tree]** (config>router>if proxy-arp-policy)

Full Context configure router interface proxy-arp-policy

Description This command enables and configure proxy ARP on the interface and specifies an existing policy-statement to analyze match and action criteria that controls the flow of routing information to and from a given protocol, set of protocols, or a specific neighbor. The policy-name is configured in the **config>router>policy-options** context.

Use proxy ARP so the router responds to ARP requests on behalf of another device. Static ARP is used when a router needs to know about a device on an interface that cannot or does not respond to ARP requests. Therefore, the router configuration can state that if it has a packet that has a certain IP address to send it to the corresponding ARP address.

Default no proxy-arp-policy

Parameters *policy-name* — Specifies the export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. A maximum of five policy names can be specified in a single statement. The specified policy names must already be defined.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.372 proxy-authentication

proxy-authentication

Syntax [**no**] **proxy-authentication**

Context **[Tree]** (config>router>l2tp>group>ppp proxy-authentication)
[Tree] (config>router>l2tp>group>tunnel>ppp proxy-authentication)
[Tree] (config>service>vprn>l2tp>group>ppp proxy-authentication)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp proxy-authentication)

Full Context configure router l2tp group ppp proxy-authentication
configure router l2tp group tunnel ppp proxy-authentication
configure service vprn l2tp group ppp proxy-authentication
configure service vprn l2tp group tunnel ppp proxy-authentication

Description This command configures the use of the authentication AVPs received from the LAC.

Default no proxy-authentication

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.373 proxy-lcp

proxy-lcp

Syntax [**no**] **proxy-lcp**

Context **[Tree]** (config>router>l2tp>group>ppp proxy-lcp)
[Tree] (config>router>l2tp>group>tunnel>ppp proxy-lcp)
[Tree] (config>service>vprn>l2tp>group>ppp proxy-lcp)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp proxy-lcp)

Full Context configure router l2tp group ppp proxy-lcp
configure router l2tp group tunnel ppp proxy-lcp
configure service vprn l2tp group ppp proxy-lcp
configure service vprn l2tp group tunnel ppp proxy-lcp

Description This command configures the use of the proxy LCP AVPs received from the LAC.

Default no proxy-lcp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.374 proxy-nd

proxy-nd

Syntax [**no**] **proxy-nd**

Context **[Tree]** (config>service>vpls proxy-nd)

Full Context configure service vpls proxy-nd

Description Commands in this context configure the proxy-ND parameters in a VPLS service.

Default no proxy-nd

Platforms All

proxy-nd

Syntax [**no**] **proxy-nd** [**mac** [*ieee-address*]] [**ip** [*ipaddr*] **all**]]

Context **[Tree]** (debug>service>id proxy-nd)

Full Context debug service id proxy-nd

Description This command enables the debug of the proxy-nd function for a specified service. Alternatively, the debug can be enabled only for certain entries given by their IPv6 or MAC addresses.

Platforms All

20.375 proxy-nd-policy

proxy-nd-policy

Syntax **proxy-nd-policy** *policy-name* [*policy-name*]
no proxy-nd-policy

Context **[Tree]** (config>service>ies>if>ipv6 proxy-nd-policy)

Full Context configure service ies interface ipv6 proxy-nd-policy

Description This command configures a proxy neighbor discovery policy for the interface. This policy determines networks and sources for which proxy ND is attempted, when local proxy neighbor discovery is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Parameters *policy-name* — Specifies up to five the export route policy names. Allowed values are any string, up to 32 characters, composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

Up to 5 policy-names can be specified in a single statement.

Platforms All

proxy-nd-policy

Syntax **proxy-nd-policy** *policy-name* [*policy-name*]
no proxy-nd-policy

Context **[Tree]** (config>service>vprn>if>ipv6 proxy-nd-policy)

Full Context configure service vprn interface ipv6 proxy-nd-policy

Description This command configures a proxy neighbor discovery policy for the interface.

Parameters *policy-name* — Specifies up to five existing policy names.

Platforms All

proxy-nd-policy

Syntax **proxy-nd-policy** *policy-name* [*policy-name*]
no proxy-nd-policy

Context **[Tree]** (config>router>if>ipv6 proxy-nd-policy)

Full Context configure router interface ipv6 proxy-nd-policy

Description This command configure a proxy neighbor discovery policy for the interface.

Parameters *policy-name* — The neighbor discovery policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. A maximum of five policy names can be specified in a single statement. The specified policy names must already be defined.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.376 proxy-server

proxy-server

Syntax **proxy-server**

Context **[Tree]** (config>service>ies>if>dhcp proxy-server)
[Tree] (config>service>ies>sub-if>grp-if>dhcp proxy-server)
[Tree] (config>service>vpls>sap>dhcp proxy-server)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp proxy-server)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp proxy-server)

Full Context configure service ies interface dhcp proxy-server
configure service ies subscriber-interface group-interface dhcp proxy-server
configure service vpls sap dhcp proxy-server
configure service vprn subscriber-interface group-interface dhcp proxy-server
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp proxy-server

Description Commands in this context configure DHCP proxy server parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp proxy-server
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp proxy-server
- configure service ies subscriber-interface group-interface dhcp proxy-server

All

- configure service vpls sap dhcp proxy-server
- configure service ies interface dhcp proxy-server

proxy-server

Syntax [**no**] **proxy-server**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 proxy-server)

Full Context configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server

Description This command allows access to the DHCP6 proxy server context. Within this context, DHCP6 proxy server parameters of the group interface can be configured.

Default no proxy-server

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

proxy-server

Syntax [**no**] **proxy-server**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6 proxy-server)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server

Description This command allows access to the DHCP6 proxy server context. Within this context, DHCP6 proxy server parameters of the group interface can be configured

Default no proxy-server

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.377 ps-information

ps-information

Syntax [**no**] **ps-information**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>avp ps-information)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp ps-information

Description This command includes the following AVPs in Diameter DCCA CCR messages encapsulated in [3GPP-873] Service-Information or [3GPP-874] PS-Information grouped AVPs:

- [8] Framed-IP-Address
- [30] Called-Station-Id
- [97] Framed-IPv6-Prefix
- [123] Delegated-IPv6-Prefix
- [6527-99] Alc-IPv6-Address
- [10415-1] 3GPP-IMSI
- [10415-2] 3GPP-Charging-Id
- [10415-5] 3GPP-GPRS-Negotiated-QoS-Profile
- [10415-7] 3GPP-GGSN-Address
- [10415-10] GGSN-NSAPI
- [10415-11] 3GPP-Session-Stop-Indicator
- [10415-12] 3GPP-Selection-Mode
- [10415-13] 3GPP-Charging-Characteristics
- [10415-16] 3GPP-GGSN-IPv6-Address
- [10415-21] 3GPP-RAT-Type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- [10415-847] GGSN-Address
- [10415-1004] Charging-Rule-Base-Name
- [10415-1247] PDP-Context-Type

The AVPs are included when configured in the **include-avp** context.

By default, these AVPs are included at the command level.

The **no** form of this command resets to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.378 psi-payload

psi-payload

Syntax **psi-payload**

Context **[Tree]** (config>port>otu psi-payload)

Full Context configure port otu psi-payload

Description Commands in this context configure payload structure identifier payload parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.379 psid-offset

psid-offset

Syntax **psid-offset** *psid-offset-length*
no psid-offset

Context **[Tree]** (config>service>nat>map-domain>mapping-rule psid-offset)

Full Context configure service nat map-domain mapping-rule psid-offset

Description This command configures the length of the high order bits in the protocol port field whose aggregate value should always be greater than 0. This automatically excludes certain ports (such as well-known ports) from the translation.

It is a function of the CE to make sure that the psid-offset bits are always greater than 0. The VSR does not check whether those bits are 0.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default psid-offset 6

Parameters *psid-offset-length* — Specifies the length of the psid-offset bits in the protocol port field.

Values 0 to 16

Platforms VSR

20.380 psnp-authentication

psnp-authentication

Syntax [**no**] **psnp-authentication**

Context **[Tree]** (config>service>vprn>isis psnp-authentication)
[Tree] (config>service>vprn>isis>level psnp-authentication)

Full Context configure service vprn isis level psnp-authentication
configure service vprn isis psnp-authentication

Description This command enables authentication of individual ISIS packets of partial sequence number PDU (PSNP) type.

The **no** form of this command suppresses authentication of PSNP packets.

Platforms All

psnp-authentication

Syntax [**no**] **psnp-authentication**

Context **[Tree]** (config>router>isis psnp-authentication)
[Tree] (config>router>isis>level psnp-authentication)

Full Context configure router isis level psnp-authentication
configure router isis psnp-authentication

Description This command enables authentication of individual IS-IS packets of partial sequence number PDU (PSNP) type.

The **no** form of this command suppresses authentication of PSNP packets.

Default psnp-authentication

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.381 ptp

ptp

Syntax [**no**] **ptp**

Context **[Tree]** (config>service>vprn ptp)

Full Context configure service vprn ptp

Description Commands in this context configure PTP parameters for the VPRN service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ptp

Syntax **ptp**

Context **[Tree]** (config>system ptp)

Full Context configure system ptp

Description Commands in this context configure parameters for IEEE 1588-2008, *Precision Time Protocol.*

This command is only available on the control assemblies that support 1588.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ptp

Syntax **ptp**

Context **[Tree]** (config>system>sync-if-timing ptp)

Full Context configure system sync-if-timing ptp

Description Commands in this context configure parameters for system timing via IEEE 1588-2008, Precision Time Protocol.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.382 ptp-asymmetry

ptp-asymmetry

Syntax **ptp-asymmetry** *nanoseconds*
no ptp-asymmetry

Context **[Tree]** (config>port>ethernet ptp-asymmetry)

Full Context configure port ethernet ptp-asymmetry

Description This command configures the PTP asymmetry delay on an Ethernet port. The command is used to correct for known asymmetry as part of time of day or phase recovery using PTP packets on both local and downstream PTP clocks.

Default no ptp-asymmetry

Parameters *nanoseconds* — Specifies the value, in nanoseconds, that the forward path delay varies from the mean path delay; the value can be a negative number.

Values -2147483648 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.383 ptp-hw-assist

ptp-hw-assist

Syntax [**no**] **ptp-hw-assist**

Context **[Tree]** (config>service>ies>if ptp-hw-assist)

Full Context configure service ies interface ptp-hw-assist

Description This command configures the 1588 port based timestamping assist function for the interface. This capability is supported on a specific set of hardware. The command may be blocked if not all hardware has the required level of support.

Only one interface per physical port can have ptp-hw-assist enabled.

no ptp-hw-assist

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ptp-hw-assist

Syntax [**no**] **ptp-hw-assist**

Context **[Tree]** (config>service>vprn>if ptp-hw-assist)

Full Context configure service vprn interface ptp-hw-assist

Description This command configures the 1588 port based timestamping assist function for the interface. This capability is supported on a specific set of hardware. The command may be blocked if not all hardware has the required level of support.

If the SAP configuration of the interface is removed, the ptp-hw-assist configuration will be removed.

If the IPv4 address configuration of the interface is removed, the ptp-hw-assist configuration will be removed.

Only one interface per physical port can have ptp-hw-assist enabled.

Default no ptp-hw-assist

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ptp-hw-assist

Syntax [**no**] **ptp-hw-assist**

Context **[Tree]** (config>router>if ptp-hw-assist)

Full Context configure router interface ptp-hw-assist

Description This command configures the 1588 port based timestamping assist function for the interface. Various checks are performed to ensure that this feature can be enabled. If a check fails:

- The command is blocked/rejected with an appropriate error message.
- If the SAP configuration of the interface is removed, the ptp-hw-assist configuration will be removed.
- If the IPv4 address configuration of the interface is removed, the ptp-hw-assist configuration will be removed.

The port will validate the destination IP address on received 1588 messages. If the 1588 messages are sent to a loopback address within the node rather than the address of the interface, then the loopback address must be configured in the **config**>**system**>**security**>**source-address application ptp** context.

Default no ptp-hw-assist

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.384 ptp-tc

ptp-tc

Syntax [**no**] **ptp-tc**

Context **[Tree]** (config>system>satellite>eth-sat ptp-tc)

Full Context configure system satellite eth-sat ptp-tc

Description This command enables the ethernet satellite IEEE1588 transparent clock function. This provides increased accuracy on the PTP event messages transiting the satellite. When a IEEE1588 event message transits the ethernet satellite, the correction field of the message is updated with the residence time of that message. This is used in PTP time calculations. All ports of the satellite are enabled for this capability with the one setting. This feature must be enabled to allow the assignment of one of the satellite's client ports as a PTP port under **config>system>ptp>port**. This feature is only valid when using PTP over Ethernet encapsulation; it is not valid for PTP over IP encapsulation.

To enable this command, the satellite must have first been configured to support the feature using the **config>system>satellite>eth-sat>feature transparent-clock-eth** and must have been enabled for synchronous ethernet with **config>system>satellite>eth-sat>sync-e**.

All host ports connecting to this satellite must support 1588 port-based timestamping.

The **no** version of this command disables the specific satellite functionality.

Default no ptp-tc

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.385 ptsf

ptsf

Syntax **ptsf**

Context **[Tree]** (config>system>ptp ptsf)

Full Context configure system ptp ptsf

Description Commands in this context configure PTSF-unusable configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.386 public-key-authentication

public-key-authentication

Syntax [**no**] **public-key-authentication**

Context **[Tree]** (config>system>security>ldap public-key-authentication)

Full Context configure system security ldap public-key-authentication

Description This command enables public key retrieval from the LDAP server. If disabled (**no public-key-authentication**), password authentication is attempted via LDAP.

Default no public-key-authentication

Platforms All

20.387 public-key-min-bits

public-key-min-bits

Syntax **public-key-min-bits** *bits*
no public-key-min-bits

Context **[Tree]** (config>service>ies>if>ipv6>secure-nd public-key-min-bits)

Full Context configure service ies interface ipv6 secure-nd public-key-min-bits

Description This command configures the minimum acceptable key length for public keys used in the generation of a Cryptographically Generated Address (CGA).

Parameters *bits* — Specifies the number of bits.

Values 512 to 1024

Platforms All

public-key-min-bits

Syntax **public-key-min-bits** *bits*
[**no**] **public-key-min-bits**

Context **[Tree]** (config>service>vprn>if>secure-nd public-key-min-bits)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface secure-nd public-key-min-bits

Description This command configures the minimum acceptable key length for public keys used in the generation of a Cryptographically Generated Address (CGA).

Parameters *bits* — Specifies the number of bits.

Values 512 to 1024

public-key-min-bits

Syntax **public-key-min-bits** *bits*
no public-key-min-bits

Context **[Tree]** (config>router>if>ipv6>secure-nd public-key-min-bits)

Full Context configure router interface ipv6 secure-nd public-key-min-bits

Description This command configures the minimum acceptable key length for public keys used in the generation of a Cryptographically Generated Address (CGA).

Parameters *bits* — Specifies the number of bits.

Values 512 to 1024

Platforms All

20.388 public-keys

public-keys

Syntax **public-keys**

Context **[Tree]** (config>system>security>user public-keys)

Full Context configure system security user public-keys

Description This command allows the user to enter the context to configure public keys for SSH.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.389 public-tcp-mss-adjust

public-tcp-mss-adjust

Syntax **public-tcp-mss-adjust** *octets*
public-tcp-mss-adjust default
no public-tcp-mss-adjust

Context **[Tree]** (config>router>l2tp>group>l2tpv3 public-tcp-mss-adjust)
[Tree] (config>service>vprn>l2tp>l2tpv3 public-tcp-mss-adjust)
[Tree] (config>service>vprn>l2tp>group>l2tpv3 public-tcp-mss-adjust)
[Tree] (config>service>vprn>l2tp>group>tunnel>l2tpv3 public-tcp-mss-adjust)

Full Context configure router l2tp group l2tpv3 public-tcp-mss-adjust
configure service vprn l2tp group l2tpv3 public-tcp-mss-adjust
configure service vprn l2tp group tunnel l2tpv3 public-tcp-mss-adjust
configure service vprn l2tp l2tpv3 public-tcp-mss-adjust

Description This command enables TCP MSS adjust for L2TPv3 tunnels on the public side on the group or tunnel level. When the command is configured, the system updates the TCP MSS option value of the received TCP SYN packet on the public side that is encapsulated in the L2TPv3 tunnel.

Note that this command can be overridden by the corresponding configuration on the group or tunnel level.

With the **default** parameter, the system uses the upper level configuration. With the non-default parameter, the system uses this configuration instead of the upper level configuration.

The **no** form of this command disables TCP MSS adjust on the public side.

Default no public-tcp-mss-adjust

Parameters *octets* — Specifies the new TCP MSS value in octets

Values 512 to 9000

default — Specifies to use the upper-level configuration

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

public-tcp-mss-adjust

Syntax **public-tcp-mss-adjust** *bytes*
public-tcp-mss-adjust *octets*
public-tcp-mss-adjust auto

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no public-tcp-mss-adjust

Context [Tree] (config>ipsec>tnl-temp public-tcp-mss-adjust)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel public-tcp-mss-adjust)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel public-tcp-mss-adjust)
[Tree] (config>service>vprn>if>sap>ipsec-tun public-tcp-mss-adjust)
[Tree] (config>service>vprn>if>ip-tunnel public-tcp-mss-adjust)
[Tree] (config>service>ies>if>sap>ip-tunnel public-tcp-mss-adjust)
[Tree] (config>router>if>ipsec>ipsec-tunnel public-tcp-mss-adjust)

Full Context configure ipsec tunnel-template public-tcp-mss-adjust
configure router interface ipsec ipsec-tunnel public-tcp-mss-adjust
configure service ies interface ipsec ipsec-tunnel public-tcp-mss-adjust
configure service ies interface sap ip-tunnel public-tcp-mss-adjust
configure service vprn interface ip-tunnel public-tcp-mss-adjust
configure service vprn interface ipsec ipsec-tunnel public-tcp-mss-adjust
configure service vprn interface sap ipsec-tunnel public-tcp-mss-adjust

Description This command enables the Maximum Segment Size (MSS) for the TCP traffic in an IPsec tunnel which is sent from the public network to the private network. The system may use this value to adjust or insert the MSS option in TCP SYN packet.

If the **auto** parameter is specified, the system derives the new MSS value based on the public MTU and IPsec overhead.

The **no** form of this command disables TCP MSS adjust on the public side.

Default no public-tcp-mss-adjust

Parameters **auto** — Derive the new MSS value based on the public MTU and IPsec overhead.

bytes — Specifies the new TCP MSS value in bytes.

Values 512 to 9000

octets — Specifies the new TCP MSS value in octets

Values 512 to 9000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec tunnel-template public-tcp-mss-adjust
- configure service ies interface sap ip-tunnel public-tcp-mss-adjust
- configure service vprn interface sap ipsec-tunnel public-tcp-mss-adjust

VSR

- configure service vprn interface ipsec ipsec-tunnel public-tcp-mss-adjust
- configure service ies interface ipsec ipsec-tunnel public-tcp-mss-adjust
- configure router interface ipsec ipsec-tunnel public-tcp-mss-adjust

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.390 purge-timeout

purge-timeout

Syntax **purge-timeout** *seconds*
no purge-timeout

Context **[Tree]** (config>system>grpc>rib-api purge-timeout)

Full Context configure system grpc rib-api purge-timeout

Description This command configures the purge timeout associated with the RibApi gRPC service.

If a gRPC client used the RibApi gRPC service to program RIB entries into the router, and then the TCP connection drops for any reason, the associated RIB entries are immediately marked as stale and a timer with the **purge-timeout** value is started. Upon timer expiration, all of the stale entries are removed. While the timer is running, the stale entries remain valid and usable for forwarding but are less preferred than any non-stale entry. The **purge-timeout** gives an opportunity for the disconnected client, or some other client, to re-program the necessary RIB entries so that forwarding can continue uninterrupted.

The **no** form of this command resets to the default value of 0. Entries are immediately deleted when the TCP connection drops.

Default no purge-timeout

Parameters *seconds* — Specifies the number of seconds until the stale entries are purged.

Values 1 to 100 000

Default 0

Platforms All

20.391 purge-timer

purge-timer

Syntax **purge-timer** *minutes*
no purge-timer

Context **[Tree]** (config>router>bgp purge-timer)

Full Context configure router bgp purge-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description When the system sends a VPN-IP Route-Refresh to a peer it sets all the VPN-IP routes received from that peer (in the RIB-IN) to stale and starts the purge-timer. If the routes are not updated (refreshed) before the purge-timer has expired then the routes are removed.

The BGP purge timer configures the time before stale routes are purged.

The **no** form of this command reverts to the default.

Default purge-timer 10

Parameters *minutes* — Specifies the maximum time before stale routes are purged.

Values 1 to 60

Platforms All

20.392 push

push

Syntax **push** {*label* | **implicit-null-label**} **nexthop** *ip-address*
no push {*out-label* | **implicit-null-label**}

Context **[Tree]** (config>router>mpls>static-lsp push)

Full Context configure router mpls static-lsp push

Description This command specifies the label to be pushed on the label stack and the next hop IP address for the static LSP.

The **no** form of this command removes the association of the label to push for the static LSP.

Parameters *implicit-null-label* — Specifies the use of the implicit label value for the push operation.

label — The label to push on the label stack. Label values 16 through 1,048,575 are defined as follows:

- label values 16 through 31 are reserved
- label values 32 through 1,023 are available for static assignment
- label values 1,024 through 2,047 are reserved for future use
- label values 2,048 through 18,431 are statically assigned for services
- label values 28,672 through 131,071 are dynamically assigned for both MPLS and services
- label values 131,072 through 1,048,575 are reserved for future use

Values 16 to 1048575

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nexthop *ip-address* — Specifies the IP address of the next hop towards the LSP egress router. If an ARP entry for the next hop exists, then the static LSP is marked operational. If ARP entry does not exist, software sets the operational status of the static LSP to down and continues to ARP for the configured nexthop. Software continuously tries to ARP for the configured nexthop at a fixed interval.

Platforms All

20.393 pushed-labels

pushed-labels

Syntax **pushed-labels** *label* [*label*]
no pushed-labels

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy>nh-grp>bkup pushed-labels)
[Tree] (config>router>mpls>fwd-policies>fwd-policy>nh-grp>pri pushed-labels)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group backup-next-hop pushed-labels
configure router mpls forwarding-policies forwarding-policy next-hop-group primary-next-hop pushed-labels

Description This command configures the pushed label stack for the primary or backup next hop of a next-hop group of an MPLS forwarding policy.

The **no** form of this command removes the pushed label stack.

Parameters *label* — Specifies the label value; up to a maximum of 10 labels.

Values 0 to 1048575

Platforms All

20.394 pw-cap-list

pw-cap-list

Syntax **pw-cap-list** {**ethernet** | **ethernet-vlan**} [{**ethernet** | **ethernet-vlan**}]
no pw-cap-list

Context **[Tree]** (config>service>vprn>l2tp>group>l2tpv3 pw-cap-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn l2tp group l2tpv3 pw-cap-list

Description This command configures the allowable pseudowire capability list that is advertised to the far end. An empty list results in both pseudowire capabilities being advertised. Up to two capabilities are allowed to be advertised.

The **no** form of this command removes the list and advertises both pseudowire capabilities to the far end.

Default no pw-cap-list

Parameters **ethernet** — Specifies that the Ethernet pseudo-wire type is advertised.

ethernet-vlan — Specifies that the Ethernet-VLAN pseudo-wire type is advertised.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

20.395 pw-path-id

pw-path-id

Syntax [**no**] **pw-path-id**

Context **[Tree]** (config>service>apipe>spoke-sdp pw-path-id)
[Tree] (config>service>cpipe>spoke-sdp pw-path-id)
[Tree] (config>service>epipe>spoke-sdp pw-path-id)
[Tree] (config>service>ies>if>spoke-sdp pw-path-id)
[Tree] (config>service>vpls>spoke-sdp pw-path-id)
[Tree] (config>service>vprn>if>spoke-sdp pw-path-id)
[Tree] (config>service>vprn>red-if>spoke-sdp pw-path-id)

Full Context configure service apipe spoke-sdp pw-path-id
configure service cpipe spoke-sdp pw-path-id
configure service epipe spoke-sdp pw-path-id
configure service ies interface spoke-sdp pw-path-id
configure service vpls spoke-sdp pw-path-id
configure service vprn interface spoke-sdp pw-path-id
configure service vprn redundant-interface spoke-sdp pw-path-id

Description Commands in this context configure an MPLS-TP Pseudowire Path Identifier for a spoke-sdp. All elements of the PW path ID must be configured in order to enable a spoke-sdp with a PW path ID.

For an IES or VPRN spoke-sdp, the pw-path-id is only valid for ethernet spoke-sdps.

The **pw-path-id** is only configurable if all of the following is true:

- SDP signaling is off

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- control-word is enabled (control-word is disabled by default)
- the service type is Epipe, VPLS, Cpipe, Apipe, or IES/VPRN interface
- mate SDP signaling is off for vc-switched services

The **no** form of this command deletes the PW path ID.

Default no pw-path-id

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn redundant-interface spoke-sdp pw-path-id

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp pw-path-id
- configure service epipe spoke-sdp pw-path-id
- configure service vprn interface spoke-sdp pw-path-id
- configure service ies interface spoke-sdp pw-path-id
- configure service vpls spoke-sdp pw-path-id

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp pw-path-id

pw-path-id

Syntax [**no**] **pw-path-id**

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp pw-path-id)
[Tree] (config>mirror>mirror-dest>spoke-sdp pw-path-id)

Full Context configure mirror mirror-dest remote-source spoke-sdp pw-path-id
configure mirror mirror-dest spoke-sdp pw-path-id

Description Commands in this context configure an MPLS-TP Pseudowire Path Identifier for a spoke SDP. All elements of the PW path ID must be configured in order to enable a spoke SDP with a PW path ID.

For an IES or VPRN spoke SDP, the *pw-path-id* is only valid for Ethernet spoke SDPs.

The **pw-path-id** is only configurable if all of the following is true:

- SDP signaling is off
- control-word is enabled (control-word is disabled by default)
- the service type is Epipe, Cpipe, Apipe, IES, VPLS, or VPRN interface
- mate SDP signaling is off for VC-switched services

The **no** form of this command deletes the PW path ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

20.396 pw-port

pw-port

Syntax **pw-port** *pw-port-id* [**pw-headend**]
no pw-port

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg pw-port)

Full Context configure service system bgp-evpn ethernet-segment pw-port

Description This command configures a PW port associated to the Ethernet Segment. When the Ethernet Segment is configured as **all-active**, only a LAG or a PW port can be associated to the Ethernet Segment. When the Ethernet Segment is configured as **single-active**, then a LAG, port or SDP can be associated to the Ethernet Segment, but not a PW port unless the **pw-headend** parameter is configured. In either case, only one of the four objects can be configured in the Ethernet Segment. A specified PW port can be part of only one Ethernet Segment.

The **no** version of this command removes the PW port from the Ethernet Segment.

Default no pw-port

Parameters *pw-port-id* — Specifies the PW port identifier.

Values 1 to 32767

pw-headend — Keyword used to specify multihoming procedures are run in the PW port stitching Epipe and the routes advertised in the context of the stitching Epipe contain the ESI of the Ethernet Segment.

Platforms All

pw-port

Syntax **pw-port** *id* [**create**]
no pw-port *id*

Context **[Tree]** (config pw-port)

Full Context configure pw-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a PW port that can be bound to a physical port or associated with an FPE (anchored PW port). A PW port's purpose is to provide, through a PW SAP, access level (or SAP level) capability to customer traffic that is tunneled to the SR OS node through an IP/MPLS network.

The **no** form of this command removes the **pw-port** ID.

Default no pw-port

Parameters *id* — Specifies the ID of the PW port.

Values 1 to 32767

create — Keyword required to create the configuration context.

Platforms All

pw-port

Syntax **pw-port** *pw-port-id* [**vc-id** *vc-id*] [**create**]
no pw-port *pw-port-id*

Context **[Tree]** (config>service>sdp>binding pw-port)

Full Context configure service sdp binding pw-port

Description This command creates a pseudowire port.

The **no** form of the command removes the pseudowire port ID from the configuration.

Default none

Parameters *pw-port-id* — Specifies a unique identifier of the pseudowire port.

Values 1 to 10239

vc-id — Specifies a virtual circuit identifier signaled to the peer.

Values 1 to 4294967295

create — This keyword is required when a new pseudowire is being created.

Platforms All

pw-port

Syntax **pw-port** *pw-port-id* [**fpe** *fpe-id*] [**create**]
no pw-port

Context **[Tree]** (config>service>epipe pw-port)

Full Context configure service epipe pw-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to associate the PW-port with the PXC ports or PXC based LAGs referenced in the FPE. That is, the PW-port becomes anchored by the PXC. This enables an external PW that is mapped to the anchored PW-port to be seamlessly rerouted between the I/O ports without interruption of service on the PW-port. This mapping between the external PW (spoke SDP) and the PXC based PXC-port is performed via an Epipe operating in vc-switching mode (creation time parameter).

Default no pw-port

Parameters *pw-port-id* — Specifies the PW-port associated with this service.

Values 1 to 10239

fpe *fpe-id* — Specifies the FPE object which contains the PXC-based ports or PXC-based LAGs.

Values 1 to 64

Platforms All

pw-port

Syntax **pw-port** *pw-port-id* [**fpe** *fpe-id*] [**create**]
no pw-port

Context **[Tree]** (config>service>epipe pw-port)

Full Context configure service epipe pw-port

Description This command is only applicable for VSR configurations. This command associates a Flex PW port with any of the following constructs:

- an MPLS-based spoke SDP (PW)
- L2oGRE tunnel using IPv4 or IPv6 transport

With this configuration, a PW that is terminated on a Flex PW port can be seamlessly rerouted between I/O ports.

The payload from the PW is extracted from the Flex PW port and processed in accordance with the configured application (a capture SAP in ESM, a PW SAP for business services, and so on). The Epipe that associates the Flex PW port with the spoke SDP or with the tunnel is a regular Epipe service (not of type *vc-switching*).

This command must be configured before a spoke SDP is added to the Epipe.

The **no** form of this command removes the *pw-port-id* from the configuration.

Parameters *pw-port-id* — Specifies the PW port associated with the PW.

Values 1 to 32767

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fpe-id — Specifies the FPE object.

Values 1 to 64

create — Keyword required to create the configuration context.

Platforms All

20.397 pw-port-extension

pw-port-extension

Syntax [**no**] **pw-port-extension**

Context **[Tree]** (config>fwd-path-ext>fpe pw-port-extension)

Full Context configure fwd-path-ext fpe pw-port-extension

Description Commands in this context configure the type of the cross-connect required to terminate an external tunnel to an anchored PW port. The system automatically builds the internal infrastructure required to perform the tunnel termination on a PW port.

PW ports support the following types of tunnels:

- GRE/MPLS PW with SDP of type MPLS or GRE
- L2oGRE bridged Ethernet over GRE, where GRE protocol number is 0x6558

The **no** form of this command removes the cross-connect type from the configuration.

Default no pw-port-extension

Platforms All

20.398 pw-port-list

pw-port-list

Syntax **pw-port-list**

Context **[Tree]** (config>service>system pw-port-list)

Full Context configure service system pw-port-list

Description Commands in this context configure a port list to bind to Flex PW ports.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms VSR

20.399 pw-routing

pw-routing

Syntax **pw-routing**

Context **[Tree]** (config>service pw-routing)

Full Context configure service pw-routing

Description Commands in this context configure dynamic multi-segment pseudowire (MS-PW) routing. Pseudowire routing must be configured on each node that will be a T-PE or an S-PE.

Platforms All

20.400 pw-sap-secondary-shaper

pw-sap-secondary-shaper

Syntax **pw-sap-secondary-shaper** *pw-sap-sec-shaper-name*
no pw-sap-secondary-shaper

Context **[Tree]** (config>service>sdp>binding>pw-port>egress>shaper pw-sap-secondary-shaper)

Full Context configure service sdp binding pw-port egress shaper pw-sap-secondary-shaper

Description This command configures a default secondary shaper applicable to pw-saps under normal interfaces.

The **no** form of the command removes the shaper name from the configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.401 pw-status-signaling

pw-status-signaling

Syntax [**no**] **pw-status-signaling**

Context **[Tree]** (config>service>epipe>spoke-sdp pw-status-signaling)

Full Context configure service epipe spoke-sdp pw-status-signaling

Description This command enables pseudowire status signaling for this spoke SDP binding.

The **no** form of this command disables the status signaling.

Default pw-status-signaling

Platforms All

pw-status-signaling

Syntax [**no**] **pw-status-signaling**

Context **[Tree]** (config>service>vpls>spoke-sdp pw-status-signaling)

Full Context configure service vpls spoke-sdp pw-status-signaling

Description This command specifies the type of signaling used by this multi-segment pseudowire provider-edge for this service.

When no pw-status-signaling is enabled, a 7450 ESS, 7750 SR, and 7950 XRS will not include the pseudowire status TLV in the initial label mapping message of the pseudowire used for a spoke-SDP. This will force both 7450 ESS, 7750 SR, and 7950 XRS PEs to use the pseudowire label withdrawal method for signaling pseudowire status.

If pw-status-signaling is configured, the node will include the use of the pseudowire status TLV in the initial label mapping message for the pseudowire.

Platforms All

20.402 pw-template

pw-template

Syntax **pw-template** *policy-id* [**use-provisioned-sdp** | [**prefer-provisioned-sdp**] [**auto-gre-sdp**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

][**create**] [**name** *name*]
no **pw-template** *policy-id*

Context **[Tree]** (config>service pw-template)

Full Context configure service pw-template

Description This command configures an SDP template.

Parameters *policy-id* — Specifies a number that uniquely identifies a template for the creation of an SDP.

Values *policy-id*: 1 to 2147483647

use-provisioned-sdp — Specifies whether to use an already provisioned SDP. When specified, the tunnel manager is consulted for an existing active SDP (with a matching far-end address), and the SDP with the lowest metric is chosen. If there are multiple SDPs with the same metric, then the highest SDP identifier that is oper-up is chosen. The choice of SDP can be configured by applying **sdp-include/exclude** in the PW template together with an sdp-group in the provisioned SDPs. This option, and the **auto-gre-sdp** option, are mutually exclusive.

prefer-provisioned-sdp — Specifies that if an existing matching SDP that conforms to any restrictions defined in the **pw-template** is found (for example, **sdp-include**/**exclude** *group*), then it will be used, following the same logic as for the **use-provisioned-sdp** parameter. Otherwise, the command will automatically create an SDP in the same manner as if the user did not specify any option. This option and the **use-provisioned-sdp** option are mutually exclusive.

auto-gre-sdp — Specifies that an SDP should automatically be created using a GRE tunnel. This option and the **use-provisioned-sdp** option are mutually exclusive. The PW template parameters **hash-label**, **entropy-label** and **sdp-include/exclude** are ignored when an GRE SDP is auto-created.

auto-mpls-sdp — Specifies that an SDP should automatically be created using an MPLS tunnel. This is the default.

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the **create** keyword.

name *name* — A name of the operator's choice, up to 64 characters. The name is saved as part of the configuration.

If a name is not specified at creation time, then SR OS assigns a string version of the policy-id as the name.

Values *name*: 64 characters maximum

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.403 pw-template-bind

pw-template-bind

Syntax **pw-template-bind** *policy-id*
no pw-template-bind

Context **[Tree]** (config>service>epipe>spoke-sdp-fec pw-template-bind)

Full Context configure service epipe spoke-sdp-fec pw-template-bind

Description This command binds includes the parameters included in a specific PW template to a spoke SDP.

The **no** form of this command removes the values from the configuration.

Parameters *policy-id* — Specifies the existing policy ID.

Values 1 to 2147483647

Platforms All

20.404 pw-template-binding

pw-template-binding

Syntax **pw-template-binding** *policy-id* [**import-rt** {*ext-community* [*ext-community*]}] [**endpoint** *endpoint-name*]
no pw-template-binding *policy-id*

Context **[Tree]** (config>service>epipe>bgp pw-template-binding)

Full Context configure service epipe bgp pw-template-binding

Description This command binds the advertisements received with the route targets (RT) that match the configured list (either the generic or the specified import) to a specific pw-template. If the RT list is not present, or if multiple matches are found, the numerically lowest pw-template is used.

The pw-template-binding applies to BGP-VPWS when enabled in the Epipe.

For BGP VPWS, the following additional rules govern the use of pseudowire-template:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- On transmission, the settings for the L2-Info extended community in the BGP updates are derived from the pseudowire template attributes. If multiple pseudowire template bindings (with or without import-rt) are specified for the same VPWS instance the first pw-template entry will be used for the information in the BGP update sent.
- On reception, the values of the parameters in the L2-Info extended community of the BGP updates are compared with the settings from the corresponding pseudowire template bindings. The following steps are used to determine the local pw-template:
  - The RT values are matched to determine the pw-template. The route targets configured for each pw-template-binding are compared to the route targets within the BGP update. The PW template corresponding to **pw-template-binding** with the first matching route target is used to for the SDP. The matching is performed from the lowest PW template binding identifier to the highest.
  - If no pw-template-binding matches are found from the previous step, the first (numerically lowest) configured pw-template entry without any route-target configured will be used.

If the value used for Layer 2 MTU (unless the value zero is received), or control word does not match, the pseudowire is created but with the operationally down state.

If the value used for the S (sequenced delivery) flags is not zero the pseudowire is not created.

The **tools perform** commands can be used to control the application of changes in pw-template for BGP-VPWS.

The **no** form of this command removes the values from the configuration.

Parameters *policy-id* — Specifies an existing policy ID.

Values 1 to 2147483647

import-rt *ext-comm* — Specifies the communities, up to five, allowed to be accepted from remote PE neighbors. An extended BGP community in the type:x:y format. The value x can be an integer or IP address. The type can be the target or origin.

Values
target:{*ip-addr*:*comm-val* | *2byte-asnumber*:*ext-comm-val*| *4byte-snumber*:*comm-val*}

ip-addr	a.b.c.d
comm-val	0 to 65535
2byte-asnumber	0 to 65535
ext-comm-val	0 to 4294967295
4byte-asnumber	0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

endpoint-name — Specifies the name of the endpoint the BGP PW template is associated with, up to 32 characters. When the configured endpoint is associated to the **pw-template-binding** of a BGP VPWS service, EVPN MPLS can also be configured and associated to the same endpoint in the same Epipe service. Modifying this element causes the parent element to be recreated automatically in order for the new value to take effect.

Platforms All

pw-template-binding

Syntax **pw-template-binding** *policy-id* [**split-horizon-group** *group-name*] [**import-rt** {*ext-community*}]
no pw-template-bind *policy-id*

Context **[Tree]** (config>service>vpls>bgp-ad pw-template-binding)
[Tree] (config>service>vpls>bgp pw-template-binding)

Full Context configure service vpls bgp pw-template-binding
configure service vpls bgp-ad pw-template-binding

Description This command binds the advertisements received with the route target (RT) that matches the configured list (either the generic or the specified import) to a specific PW template. If the RT list is not present the pw-template is used for all of them.

The **pw-template-binding** applies to both BGP-AD and BGP-VPLS if these features are enabled in the VPLS.

For BGP VPLS the following additional rules govern the use of pseudowire-template.

- On transmission, the settings for the L2-Info extended community in the BGP update are derived from the pseudowire template attributes. If multiple pseudowire template bindings (with or without import-rt) are specified, the first pw-template entry will be used for the information in the BGP update sent.
- On reception, the values of the parameters in the L2-Info extended community of the BGP update are compared with the settings from the corresponding pw-template. The following steps are used to determine the local pw-template.
  - The RT values are matched to determine the pw-template. The route targets configured for each pw-template-binding are compared to the route targets within the BGP update. The PW template corresponding to pw-template-binding with the first matching route target is used to for the SDP. The matching is performed from the lowest PW template binding identifier to the highest
  - If no pw-templates matches are found from the previous step, the first (numerically lowest) configured pw-template entry without any route-target configured will be used.

If the values used for Layer 2 MTU (unless the value zero is received) or control word flag do not match, the pseudowire is created but with the operationally down state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the value used for the S (sequenced delivery) flags is not zero, the pseudowire is not created.

The tools perform commands can be used to control the application of changes in pw-template for both BGP-AD and BGP-VPLS.

The **no** form of this command removes the values from the configuration.

Parameters *policy-id* — Specifies an existing policy ID

Values 1 to 2147483647

group-name — The specified group-name overrides the split horizon group template settings

import-rt ext-comm — Specifies communities allowed to be accepted from remote PE neighbors. An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers. A maximum of five *import-rt ext-com* can be specified.

Values target:{*ip-addr:comm-val*| *2byte-asnumber:ext-comm-val*| *4byte-asnumber:comm-val*}

ip-addr: a.b.c.d

comm-val: [0 to 65535]

2byte-as-number: [0 to 65535]

ext-comm-val: [0 to 4294967295]

4byte-asnumber: [0 to 4294967295]

Platforms All

20.405 pw-template-id-range

pw-template-id-range

Syntax **pw-template-id-range start** *pw-template-id* **end** *pw-template-id*
no pw-template-id-range

Context **[Tree]** (config>service>md-auto-id pw-template-id-range)

Full Context configure service md-auto-id pw-template-id-range

Description This command specifies the range of IDs used by SR OS to automatically assign an ID to PW templates that are created in model-driven interfaces without an ID explicitly specified by the user or client.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A PW template created with an explicitly-specified ID cannot use an ID in this range. In the classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed, which causes any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **config**>**service md-auto-id** command for further details.

Default no pw-template-id-range

Parameters **start** *pw-template-id* — Specifies the lower value of the ID range. The value must be less than or equal to the **end** value.

Values 1 to 2147483647

end *pw-template-id* — Specifies the upper value of the ID range. The value must be greater than or equal to the **start** value.

Values 1 to 2147483647

Platforms All

20.406 pw-type

pw-type

Syntax **pw-type ethernet-vlan** *vlan-id*
pw-type ethernet
no pw-type

Context **[Tree]** (config>service>epipe>sap>l2tpv3-session pw-type)
[Tree] (config>service>vpls>sap>l2tpv3-session pw-type)

Full Context configure service epipe sap l2tpv3-session pw-type
configure service vpls sap l2tpv3-session pw-type

Description This command specifies the PW-type for the associated L2TPv3 session.

The support types are either Ethernet or Ethernet-VLAN. If Ethernet-VLAN is configured, a VLAN value must be specified as well.

The **no** form of this command deletes the PW-type configuration.

Parameters *vlan-id* — Specifies the VLAN-ID.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.407 pwc

pwc

Syntax **pwc** [**previous**]

Context **[Tree]** (global pwc)

Full Context global pwc

Description This command displays the present or previous working context of the CLI session. The **pwc** command provides a user who is in the process of dynamically configuring a chassis a way to display the current or previous working context of the CLI session. The **pwc** command displays a list of the CLI nodes that hierarchically define the current context of the CLI instance of the user.

The following example is from a 7750 SR:

```
A:ALA-1>config>router>bgp>group# pwc
------------------------------------------------
Present Working Context :
------------------------------------------------
<root>
  configure
  router Base
  bgp
  group test
  ospf
  area 1
------------------------------------------------
A:ALA-1>config>router>bgp>group#
```

When the **previous** keyword is specified, the previous context displays. This is the context entered by the CLI parser upon execution of the **exit** command. The current context of the CLI is not affected by the **pwc** command.

The following example is from a 7450 ESS:

```
*A:ALA-1>config>router>ospf>area>if# pwc previous
------------------------------------------------------------
Previous Working Context :
------------------------------------------------------------
 <root>
  configure
  router "Base"
  ospf
  area "0.0.0.0"
------------------------------------------------------------
*A:ALA-1config>router>ospf>area>if#
```

Parameters **previous** — Displays the previous present working context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.408 pxc

pxc

Syntax **pxc** *pxc-id* [**create**]
no pxc *pxc-id*

Context **[Tree]** (config>port-xc pxc)

Full Context configure port-xc pxc

Description This command creates a port cross-connect (PXC) object. Referencing an Ethernet port within the PXC object will automatically configure this Ethernet port as a loopback port. The node will automatically create two PXC sub-ports under this Ethernet port. The configuration of PXC sub-ports can be accessed through the CLI.

Parameters *pxc-id* — Specifies the port cross-connect identifier.

Values 1 to 64

Platforms All

20.409 pxc-pxc-id.sub-port-id

pxc-pxc-id.sub-port-id

Syntax **pxc-***pxc-id.sub-port-id*

Context **[Tree]** (config>port pxc-pxc-id.sub-port-id)

Full Context configure port pxc-pxc-id.sub-port-id

Description This command enables access to PXC sub-port level parameters. The PXC sub-ports are automatically created once the external Ethernet port is configured inside of an PXC object. The PXC sub-ports are by default administratively disabled (shutdown). In order for PXC sub-ports to became operational, both, the underlying external Ethernet port and the PXC object must be operationally up.

Parameters *pxc-id* — Specifies the unique identifier of this PXC.

Values 1 to 64

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-port-id — When this the *pxc-id* is configured, two logical sub-ports are automatically created. These logical sub-ports are used to create two paths within the loop; one upstream path, and one downstream path. These sub-ports are destroyed when either this PXC row is destroyed, this object is de-provisioned.

Values a, b

20.410 python

python

Syntax **python**

Context **[Tree]** (config python)

Full Context configure python

Description Commands in this context configure Python parameters.

Platforms All

python

Syntax [**no**] **python**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync python)

Full Context configure redundancy multi-chassis peer sync python

Description This command enables syncing of python-policy cached entries to the peer.

Use the **mcs-peer** command in the Python policy to enable syncing for a specific Python policy.

The **no** form of this command reverts to the default.

Default no python

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.411 python-policy

python-policy

Syntax **python-policy** *python-name*
no python-policy

Context **[Tree]** (config>service>ies>if>dhcp python-policy)
[Tree] (config>service>ies>if>ipv6>dhcp6-relay python-policy)
[Tree] (config>service>ies>sub-if>dhcp python-policy)
[Tree] (config>service>ies>sub-if>grp-if>dhcp python-policy)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6 python-policy)
[Tree] (config>service>vprn>if>dhcp python-policy)
[Tree] (config>service>vprn>if>ipv6>dhcp6-relay python-policy)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6 python-policy)
[Tree] (config>service>vprn>sub-if>dhcp python-policy)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp python-policy)
[Tree] (config>service>vprn>sub-if python-policy)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server python-policy)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>proxy python-policy)

Full Context configure service ies interface dhcp python-policy
configure service ies interface ipv6 dhcp6-relay python-policy
configure service ies subscriber-interface dhcp python-policy
configure service ies subscriber-interface group-interface dhcp python-policy
configure service ies subscriber-interface ipv6 dhcp6 python-policy
configure service vprn interface dhcp python-policy
configure service vprn interface ipv6 dhcp6-relay python-policy
configure service vprn subscriber-interface dhcp python-policy
configure service vprn subscriber-interface group-interface dhcp python-policy
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server python-policy
configure service vprn subscriber-interface ipv6 dhcp6 proxy python-policy
configure service vprn subscriber-interface ipv6 dhcp6 python-policy
configure service vprn subscriber-interface python-policy

Description This command specifies the Python policy to be used for DHCPv6 relay.

The **no** form of this command reverts to the default.

Parameters *python-name* — Specifies the name of an existing python script, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface ipv6 dhcp6 python-policy
- configure service vprn subscriber-interface ipv6 dhcp6 python-policy
- configure service vprn subscriber-interface group-interface dhcp python-policy
- configure service ies subscriber-interface group-interface dhcp python-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn subscriber-interface dhcp python-policy
- configure service ies subscriber-interface dhcp python-policy

All

- configure service vprn interface dhcp python-policy
- configure service ies interface dhcp python-policy
- configure service ies interface ipv6 dhcp6-relay python-policy
- configure service vprn interface ipv6 dhcp6-relay python-policy

python-policy

Syntax **python-policy** *policy-name*
no python-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if>pppoe python-policy)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe python-policy)

Full Context configure service ies subscriber-interface group-interface pppoe python-policy
configure service vprn subscriber-interface group-interface pppoe python-policy

Description This command specifies the Python policy for PPPoE packets sent/received on the group interface.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies an existing Python policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** *name*
no python-policy

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile python-policy)

Full Context configure subscriber-mgmt gtp peer-profile python-policy

Description This command specifies the Python policy for MGW profile packets sent/received on the group interface.

The **no** form of this command removes the policy name from the configuration.

Default no python-policy

Parameters *name* — Specifies an existing Python policy name up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** [*policy-name*]
no python-policy

Context **[Tree]** (config>aaa>diam-peer-plcy python-policy)
[Tree] (config>aaa>diam>node python-policy)

Full Context configure aaa diameter node python-policy
configure aaa diameter-peer-policy python-policy

Description This command specified the python-policy for Diameter messages received or transmitted on the diameter peers defined in the **diameter-peer-policy**.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the name of the Python policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** *name* [**create**] [**wlan-gw-group** *wlan-gw-group-id*] [**nat-group** *nat-group-id*]
no python-policy *name*

Context **[Tree]** (config>python python-policy)

Full Context configure python python-policy

Description This command creates a new Python policy or enables an existing Python policy configuration context.

There are two types of Python policies: centralized and distributed. A centralized Python policy runs on a CPM, while a distributed Python policy runs on an ISA. With the distributed Python policy, a **wlan-gw-group** *wlan-gw-group-id* or a **nat-group** *nat-group-id* command must specified.

The **no** form of this command removes the Python policy from the configuration.

Parameters *name* — Specifies the Python policy name up to 32 characters.

create — This keyword is required when first creating the Python policy. Once the context is created, it is possible to navigate into the context without the **create** keyword.

wlan-gw-group *wlan-gw-group-id* — Specifies the ID of the WLAN GW group that the distributed python-policy installs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

nat-group *nat-group-id* — Specifies the ID of the NAT group that the distributed python-policy installs.

Platforms All

python-policy

Syntax **python-policy** *policy-name*
no python-policy

Context **[Tree]** (config>aaa>isa-radius-policy python-policy)

Full Context configure aaa isa-radius-policy python-policy

Description This command specifies the Python policy for the ISA RADIUS proxy server. This is the python policy for RADIUS packets to/from the client.

The **no** form of this command removes the Python policy from the configuration.

Parameters *name* — Specifies the Python policy name, up to 32 characters

create — This keyword is required when first creating the Python policy. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

python-policy

Syntax **python-policy** *name*
no python-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv4>dhcp4 python-policy)
[Tree] (config>service>ies>sub-if>grp-if>ipv4>dhcp4 python-policy)

Full Context configure service ies subscriber-interface group-interface ipv4 dhcp4 python-policy
configure service vprn subscriber-interface group-interface ipv4 dhcp4 python-policy

Description This command specified the Python policy for DHCPv4 packets sent/received on the group interface.

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — Specifies an existing Python policy name, up to 32 characters.

python-policy

Syntax **python-policy** *name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no python-policy

Context [Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 python-policy)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 python-policy)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 python-policy
configure service vprn subscriber-interface group-interface ipv6 dhcp6 python-policy

Description This command specified the Python policy for DHCPv6 packets sent/received on the group interface.

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — Specifies an existing Python policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** *name*
no python-policy

Context [Tree] (config>aaa>radius-srv-plcy python-policy)

Full Context configure aaa radius-server-policy python-policy

Description This command specifies the Python policy for RADIUS packets to/from the RADIUS servers defined in the specified **radius-server-policy**.

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — Specifies the name of the Python policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** *name*
no python-policy

Context [Tree] (config>router>radius-proxy>server python-policy)
[Tree] (config>service>vprn>radius-proxy>server python-policy)

Full Context configure router radius-proxy server python-policy
configure service vprn radius-proxy server python-policy

Description This command specifies the Python policy for RADIUS packets sent/received on the client side of the RADIUS proxy server.

This command supports RADIUS proxy on both CPMs and ISAs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — Specifies the name of the Python policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** *name*
no python-policy

Context **[Tree]** (config>subscr-mgmt>pppoe-client-policy python-policy)

Full Context configure subscriber-mgmt pppoe-client-policy python-policy

Description This command applies a Python policy to all messages sent and received by the PPPoE client.

The **no** form of this command removes the associated Python policy from the PPPoE client.

Parameters *name* — The name of a preconfigured Python policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

python-policy

Syntax **python-policy** *name*
no python-policy

Context **[Tree]** (config>service>vprn>if>ipv6 python-policy)

Full Context configure service vprn interface ipv6 python-policy

Description This command specifies a python policy. Python policies are configured in the **config>python> python-policy** *name* context.

Parameters *name* — Specifies the name of an existing python script, up to 32 characters in length.

python-policy

Syntax **python-policy** *python-policy-name*
no python-policy

Context **[Tree]** (config>router>if>dhcp python-policy)

Full Context configure router interface dhcp python-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a python policy. Python policies are configured in the **config>python>python-policy** *name* context.

Default no python-policy

Parameters *python-policy-name* — Specifies the name of an existing python script, up to 32 characters in length.

Platforms All

python-policy

Syntax **python-policy** *policy-name*
no python-policy

Context **[Tree]** (config>log>log-id python-policy)

Full Context configure log log-id python-policy

Description This command associates the Python script with the events sent to this log ID. The Python policy can be associated with the log only if the destination in the log ID is set **to syslog**.

For information about Python policy configuration, refer to the Python Script Support for ESM in the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*.

The **no** form of this command disables Python processing of the events in this log ID.

Default no python-policy

Parameters *policy-name* — Specifies a Python policy name, up to 32 characters.

Platforms All

20.412 python-policy-cache

python-policy-cache

Syntax **python-policy-cache**

Context **[Tree]** (config>system>persistence python-policy-cache)

Full Context configure system persistence python-policy-cache

Description This command configures Python policy cache persistency parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

20.413 python-script

python-script

Syntax **python-script** *name* [**create**]
no python-script *name*

Context **[Tree]** (config>python python-script)

Full Context configure python python-script

Description Commands in this context configure Python scripts to modify messages of different protocols.

The **no** form of this command removes the Python script name from the configuration.

Parameters **name** — Specifies the name of this Python script policy.

create — This keyword is required when first creating the Python script. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms All

python-script

Syntax **python-script** *script-name*

Context **[Tree]** (debug>python python-script)

Full Context debug python python-script

Description Commands in this context debug the specified Python script.

Parameters *policy-name* — Specifies the Python script name, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21 q Commands

21.1 q-tag-range

q-tag-range

Syntax **q-tag-range** *qtag1* [**to** *qtag1*]
no q-tag-range *qtag1*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>dot1q q-tag-range)

Full Context configure service system bgp-evpn ethernet-segment dot1q q-tag-range

Description This command determines the VIDs associated with the virtual Ethernet Segment on a specific dot1q port or LAG based on the following considerations:

- Values *, 0 to 4094 are allowed.
- Any SAP for which the service-delimiting qtag matches the range is associated with the virtual ES, and only those, for example, SAP 1/1/1:0 will not match port 1/1/1, qtag-range 100.
- Maximum 8 ranges are allowed in the dot1q context.
- A range can be comprised of a single qtag.
- Shutting down the ES is not required prior to changing the q-tag-range.

The **no** form of the command removes the configured range. Only the first qtag1 value is required to remove the range.

Parameters *qtag1* — Specifies the VID. When configuring a range of qtags (and not a single value), the second qtag1 value must be greater than the first qtag1.

Values *, 0 to 4094

Platforms All

21.2 qci

qci

Syntax **qci** *qci-value*
no qci

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>gtp>peer-profile>pgw>qos qci)
[Tree] (config>subscr-mgmt>gtp>peer-profile>mme>qos qci)

Full Context configure subscriber-mgmt gtp peer-profile mme qos qci
configure subscriber-mgmt gtp peer-profile pgw qos qci

Description This command configures the QoS Class Identifier (QCI) to send in the Bearer Level QoS IE in GTPv2 messages.

The **no** form of this command reverts to the default.

Default qci 8

Parameters *qci-value* — Specifies the QCI value to send.

Values 1 to 9

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

21.3 qinq

qinq

Syntax **qinq**

Context [Tree] (config>service>system>bgp-evpn>eth-seg qinq)

Full Context configure service system bgp-evpn ethernet-segment qinq

Description Commands in this context configure q-tag and s-tag additions to the port or LAG virtual Ethernet Segments.

Platforms All

21.4 qinq-etype

qinq-etype

Syntax **qinq-etype** *qinq-etype-value*
no qinq-etype

Context [Tree] (config>port>ethernet qinq-etype)

Full Context configure port ethernet qinq-etype

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Ethertype used for Q-in-Q encapsulation.

The **no** form of this command reverts the qinq-etype value to the default.

Default no qinq-etype

Parameters *qinq-etype-value* — Specifies the qinq-etype to expect in the form of 0x600 to 0xfff.

Values 1536 to 65535 in decimal or hex formats

Platforms All

qinq-etype

Syntax **qinq-etype** *qinq-etype*
no qinq-etype

Context **[Tree]** (config>pw-port qinq-etype)

Full Context configure pw-port qinq-etype

Description This command configures the QinQ Ethertype on the PW port. The PW port is used to extract a customer's Ethernet traffic that is transported in a tunnel over an IP/MPLS network. The **qinq-etype** represents the first two bytes (TPID) in the outer 801.1Q header of the double-tagged Ethernet frame inside the tunnel.

The **no** form of this command removes the configuration.

Parameters *qinq-etype* — The value for the **qinq-etype** field, in hexadecimal format.

Values 0x0600..0xFFFF

Default 0x8100

Platforms All

21.5 qinq-mark-top-only

qinq-mark-top-only

Syntax [**no**] **qinq-mark-top-only**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress qinq-mark-top-only)
[Tree] (config>service>vprn>if>sap>egress qinq-mark-top-only)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress qinq-mark-top-only)

Full Context configure service ies subscriber-interface group-interface sap egress qinq-mark-top-only
configure service vprn interface sap egress qinq-mark-top-only

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap egress qinq-mark-top-only

Description When the encapsulation type is qinq for the access port for the specified SAP, enabling this command specifies which P-bits or DEI bit to mark during packet egress. Only the P-bits or DEI bit in the top Q tag are marked. When this command is disabled, both sets of P-bits and the DEI bit are marked.

Default no qinq-mark-top-only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap egress qinq-mark-top-only
- configure service vprn subscriber-interface group-interface sap egress qinq-mark-top-only

All

- configure service vprn interface sap egress qinq-mark-top-only

qinq-mark-top-only

Syntax [**no**] **qinq-mark-top-only**

Context **[Tree]** (config>service>apipe>sap>egress qinq-mark-top-only)
[Tree] (config>service>epipe>sap>egress qinq-mark-top-only)
[Tree] (config>service>fpipe>sap>egress qinq-mark-top-only)
[Tree] (config>service>ipipe>sap>egress qinq-mark-top-only)

Full Context configure service apipe sap egress qinq-mark-top-only
configure service epipe sap egress qinq-mark-top-only
configure service fpipe sap egress qinq-mark-top-only
configure service ipipe sap egress qinq-mark-top-only

Description When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the **qinq-mark-top-only** command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When the enabled, only the P-bits/DEI bit in the top Q-tag are marked.

Default no qinq-mark-top-only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress qinq-mark-top-only

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress qinq-mark-top-only

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap egress qinq-mark-top-only
- configure service ipipe sap egress qinq-mark-top-only

qinq-mark-top-only

Syntax [**no**] **qinq-mark-top-only**

Context **[Tree]** (config>service>vpls>sap>egress qinq-mark-top-only)

Full Context configure service vpls sap egress qinq-mark-top-only

Description When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the **qinq-mark-top-only** command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When enabled, only the P-bits/DEI bit in the top Q-tag are marked.

The **no** form of this command disables the command.

Default no qinq-mark-top-only

Platforms All

qinq-mark-top-only

Syntax [**no**] **qinq-mark-top-only**

Context **[Tree]** (config>service>ies>if>sap>egress qinq-mark-top-only)

Full Context configure service ies interface sap egress qinq-mark-top-only

Description When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the **qinq-mark-top-only** command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When the enabled, only the P-bits/DEI bit in the top Q-tag are marked.

Default no qinq-mark-top-only

Platforms All

21.6 qinq-vlan-translation

qinq-vlan-translation

Syntax **qinq-vlan-translation** *s-tag.c-tag*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no qinq-vlan-translation

Context [Tree] (config>service>epipe>sap>ingress qinq-vlan-translation)

Full Context configure service epipe sap ingress qinq-vlan-translation

Description This command provides ingress VLAN translation for two service-delimiting VLAN values, as opposed to the **vlan-translation** command that provides translation for only one service-delimiting VLAN value. This command is used with the **force-qinq-vc-forwarding** command so that the VLAN values that are pushed on SDP bindings or EVPN-MPLS can be normalized (translated). The command has no effect without the configuration of **force-qinq-vc-forwarding** and cannot be used in non-QinQ SAPs.

The **no** version of the command disables QinQ VLAN translation.

Default no qinq-vlan-translation

Parameters *s-tag.c-tag* — These are the VLAN tag values that are pushed on SDP bindings and EVPN-MPLS destinations when **force-qinq-vc-forwarding s-tag-c-tag** is configured. When **force-qinq-vc-forwarding c-tag-c-tag** is configured, only the c-tag value in qinq-vlan-translation s-tag.c-tag is pushed.

Values *s-tag*: 0 to 4094
c-tag: 0 to 4094

Platforms All

21.7 ql-minimum

ql-minimum

Syntax **ql-minimum** {**prs** | **stu** | **st2** | **tnc** | **st3e** | **st3** | **prc** | **ssua** | **ssub** | **sec** | **eec1** | **eec2**}
no ql-minimum

Context [Tree] (config>system>sync-if-timing>bits>output ql-minimum)

Full Context configure system sync-if-timing bits output ql-minimum

Description This command configures the minimum acceptable QL value that a signal must have in order to be selected for the BITSout port. This ensures that the signal has traceability to a source with at least this quality level so that attached equipment can function properly.

The **no** form of this command disables this check.

Default no ql-minimum

Parameters **prs** — Specifies the SONET Primary Reference Source.

stu — Specifies the SONET Synchronous Traceability Unknown.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

st2 — Specifies the SONET Stratum 2.

tnc — Specifies the SONET Transit Node Clock.

st3e — Specifies the SONET Stratum 3E.

st3 — Specifies the SONET Stratum 3.

prc — Specifies the SDH Primary Reference Clock.

ssua — Specifies the SDH Primary Level Synchronization Supply Unit.

ssub — Specifies the SDH Second Level Synchronization Supply Unit.

sec — Specifies the SDH Synchronous Equipment Clock.

eec1 — Specifies the Ethernet Equipment Clock Option 1 (sdh).

eec2 — Specifies the Ethernet Equipment Clock Option 2 (sonet).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ql-minimum

Syntax **ql-minimum** {**prs** | **stu** | **st2** | **tnc** | **st3e** | **st3** | **prc** | **ssua** | **ssub** | **sec** | **eec1** | **eec2**}
no ql-minimum

Context **[Tree]** (config>system>sync-if-timing ql-minimum)

Full Context configure system sync-if-timing ql-minimum

Description This command configures the minimum acceptable QL value that a signal must have in order to be considered for selection by the system timing module.

The **no** form of this command disables this check.

Default no ql-minimum

Parameters **prs** — Specifies the SONET Primary Reference Source.

stu — Specifies the SONET Synchronous Traceability Unknown.

st2 — Specifies the SONET Stratum 2.

tnc — Specifies the SONET Transit Node Clock.

st3e — Specifies the SONET Stratum 3E.

st3 — Specifies the SONET Stratum 3.

prc — Specifies the SDH Primary Reference Clock.

ssua — Specifies the SDH Primary Level Synchronization Supply Unit.

ssub — Specifies the SDH Second Level Synchronization Supply Unit.

sec — Specifies the SDH Synchronous Equipment Clock.

eec1 — Specifies the Ethernet Equipment Clock Option 1 (sdh).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

eec2 — Specifies the Ethernet Equipment Clock Option 2 (sonet).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

21.8 ql-override

ql-override

Syntax **ql-override** {**prs** | **stu** | **st2** | **tnc** | **st3e** | **st3** | **prc** | **ssua** | **ssub** | **sec**}
no ql-override

Context **[Tree]** (config>system>sync-if-timing>bits ql-override)
[Tree] (config>system>sync-if-timing>ptp ql-override)
[Tree] (config>system>sync-if-timing>synce ql-override)

Full Context configure system sync-if-timing bits ql-override
configure system sync-if-timing ptp ql-override
configure system sync-if-timing synce ql-override

Description This command configures the QL value to be used for the reference for SETS input selection and BITS output selection. This value overrides any value received by that reference's SSM process.

Default no ql-override

Parameters **prs** — Specifies the SONET Primary Reference Source Traceable.

stu — Specifies the SONET Synchronous Traceability Unknown.

st2 — Specifies the SONET Stratum 2 Traceable.

tnc — Specifies the SONET Transit Node Clock Traceable.

st3e — Specifies the SONET Stratum 3E Traceable.

st3 — Specifies the SONET Stratum 3 Traceable.

prc — Specifies the SDH Primary Reference Clock Traceable.

ssua — Specifies the SDH Primary Level Synchronization Supply Unit Traceable.

ssub — Specifies the SDH Second Level Synchronization Supply Unit Traceable.

sec — Specifies the SDH Synchronous Equipment Clock Traceable.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ql-override

Syntax **ql-override** {**prs** | **stu** | **st2** | **tnc** | **st3e** | **st3** | **prc** | **ssua** | **ssub** | **sec** | **eec1** | **eec2**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ql-override

Context [Tree] (config>system>sync-if-timing>ref1 ql-override)
[Tree] (config>system>sync-if-timing>ref2 ql-override)

Full Context configure system sync-if-timing ref1 ql-override
configure system sync-if-timing ref2 ql-override

Description This command configures the QL value to be used for the reference for SETS input selection and BITS output. This value overrides any value received by that reference's SSM process.

Default no ql-override

Parameters **prs** — Specifies the SONET Primary Reference Source Traceable.

stu — Specifies the SONET Synchronous Traceability Unknown.

st2 — Specifies the SONET Stratum 2 Traceable.

tnc — Specifies the SONET Transit Node Clock Traceable.

st3e — Specifies the SONET Stratum 3E Traceable.

st3 — Specifies the SONET Stratum 3 Traceable.

prc — Specifies the SDH Primary Reference Clock Traceable.

ssua — Specifies the SDH Primary Level Synchronization Supply Unit Traceable.

ssub — Specifies the SDH Second Level Synchronization Supply Unit Traceable.

sec — Specifies the SDH Synchronous Equipment Clock Traceable.

eec1 — Specifies the Ethernet Equipment Clock Option 1 Traceable (sdh).

eec2 — Specifies the Ethernet Equipment Clock Option 2 Traceable (sonet).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

21.9 ql-selection

ql-selection

Syntax [**no**] **ql-selection**

Context [Tree] (config>system>sync-if-timing ql-selection)

Full Context configure system sync-if-timing ql-selection

Description When enabled, the selection of system timing reference and BITS output timing reference takes into account quality level. Quality level is conveyed via the SSM or forced using the **ql-override** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no ql-selection

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

21.10 qos

qos

Syntax **qos**

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile>ggsn qos)
[Tree] (config>subscr-mgmt>gtp>peer-profile>mme qos)
[Tree] (config>subscr-mgmt>gtp>peer-profile>pgw qos)

Full Context configure subscriber-mgmt gtp peer-profile ggsn qos
configure subscriber-mgmt gtp peer-profile mme qos
configure subscriber-mgmt gtp peer-profile pgw qos

Description Commands in this context configure QoS for a GGSN Mobile Gateway.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id*
qos *policy-id* [**multipoint-shared** | **service-queuing**]
qos *policy-id* [**shared-queuing** | **service-queuing**]
no qos

Context **[Tree]** (config>subscr-mgmt>msap-policy>ies-vprn>egress qos)
[Tree] (config>subscr-mgmt>msap-policy>ies-vprn>ingress qos)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>egress qos)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>ingress qos)

Full Context configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters egress qos
configure subscriber-mgmt msap-policy ies-vprn-only-sap-parameters ingress qos
configure subscriber-mgmt msap-policy vpls-only-sap-parameters egress qos
configure subscriber-mgmt msap-policy vpls-only-sap-parameters ingress qos

Description This command specifies the ingress or egress Quality of Service (QoS) policy that is associated with a Managed SAP (MSAP). Only QoS policies with scope template can be associated with MSAPs.

The **no** form of this command resets the default value. The system default QoS policy is used in that case.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default qos 1 — For egress parameters.

qos 1 multipoint-shared — For ingress vpls-only-sap-parameters.

qos 1 shared-queuing — For ingress ies-vprn-only-sap-parameters.

Parameters *policy-id* — Specifies the QoS policy ID or name to associate with the MSAPs. The policy ID or name must already exist.

Values id: 1 to 65535
name: policy name up to 64 characters.

multipoint-shared — Ingress unicast MSAP queues are mapped one-for-one with hardware queues. Multipoint MSAP queues are not instantiated. Unicast and BUM packets traverse the ingress forwarding plane twice: in the first pass, both unicast and BUM traffic use the unicast MSAP queues, while in the second pass shared unicast and multipoint queues are used towards the egress line card. Multipoint-shared queuing greatly reduces ingress queue consumption. This keyword can only be specified for ingress **vpls-only-sap-parameters**.

shared-queuing — Ingress unicast MSAP queues are mapped one-for-one with hardware queues. Unicast packets traverse the ingress forwarding plane twice: in the first pass the MSAP queues are used, while in the second pass shared queues are used towards the egress line card. Shared-queuing greatly reduces ingress queue consumption. This keyword can only be specified for ingress **ies-vprn-only-sap-parameters**.

service-queuing — Ingress MSAP queues are mapped to multiple hardware queues, per egress line card destination. For scaled environments such as in subscriber management, this could lead to a high number of queue resources being used. Therefore, service-queuing for MSAPs should only be enabled for specific use cases. This keyword can only be specified for ingress parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id* [**vport-scheduler** | **port-scheduler**] [**force**]
no qos

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress qos)

Full Context configure subscriber-mgmt sla-profile egress qos

Description This command specifies the egress QoS policy applicable to this SLA profile. The policy must already be defined in the **config>qos>sap-egress** context.

The **no** form of this command reverts to the default.

Default qos 1 port-scheduler

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-id* — Specifies the egress policy to be applied to the egress SLA profile.

Values 1 to 65535

vport-scheduler | port-scheduler — Specifies if a host queue with the port-parent option enabled should be scheduled within the context of a Vport port scheduler policy or at the port's port scheduler policy.

force — Forces a policy change

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id* [**shared-queuing** | **multipoint-shared** | **service-queuing**] [**force**]
no qos

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress qos)

Full Context configure subscriber-mgmt sla-profile ingress qos

Description This command specifies the ingress QoS policy applicable to this SLA profile. The policy must already be defined in the **config>qos>sap-ingress** context.

The **no** form of this command reverts to the default.

Default qos 1

Parameters *policy-id* — Specifies the policy to be applied to the ingress SLA profile.

Values 1 to 65535

shared-queuing — Specifies the policy used by this SAP. When the value of this object is null it means that the SAP will use individual ingress QoS queues, instead of the shared ones.

multipoint-shared — This keyword is mutually exclusive with the **shared-queuing** and **service-queuing** keywords. When multipoint-shared is specified, the ingress forwarding plane will conserve hardware queues by performing two tier queuing on ingress unicast and multipoint packets through the SAP. Unicast service queues defined in the SAP ingress QoS policy are created for the SAP on the ingress forwarding plane without regard for the switch fabric destinations to which the SAP may need to forward (other destinations in the VPLS context). The multipoint queues defined in the SAP ingress QoS policy are not created for the SAP. Instead, all multipoint traffic is mapped to the unicast queues based on forwarding class in the first pass. In the second pass the unicast packets is mapped to the unicast shared queues while the multipoint traffic is mapped to the multipoint shared queues.

service-queuing — This keyword is mutually exclusive with the **multipoint-shared** and **shared-queuing** keywords to state that service queuing is needed.

force — Forces a policy change.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos

Syntax **qos** *policy-id*
no qos [policy-id]

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress qos)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress qos)
[Tree] (config>service>vprn>sub-if>grp-if>sap>ingress qos)

Full Context configure service ies subscriber-interface group-interface sap egress qos
configure service vprn subscriber-interface group-interface sap egress qos
configure service vprn subscriber-interface group-interface sap ingress qos

Description Associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP) or IP interface.

QoS egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the *policy-id* does not exist, an error are returned.

The **qos** command is used to associate egress QoS policies. The **qos** command only allows egress policies on SAP or IP interface egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type returns an error.

By default, no specific QoS policy is associated with the SAP or IP interface for egress, so the default QoS policy is used.

The normal behavior is for queues to be created per destination.

The **no** form of this command removes the QoS policy association from the SAP or IP interface, and the QoS policy reverts to the default.

Parameters *policy-id* — The egress policy ID to associate with SAP or IP interface on egress. The policy ID must already exist.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id*
qos *policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*
no qos [**policy-id**]

Context **[Tree]** (config>service>ies>if>sap>egress qos)
[Tree] (config>service>vpls>sap>egress qos)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>if>sap>egress qos)

Full Context configure service ies interface sap egress qos
configure service vpls sap egress qos
configure service vprn interface sap egress qos

Description This command associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP) or IP interface.

QoS egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the policy ID does not exist, an error is returned.

The **qos** command associates both ingress and egress QoS policies. The **qos** command only allows ingress policies to be associated on SAP or IP interface ingress and egress policies on SAP or IP interface egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type returns an error.

By default, no specific QoS policy is associated with the SAP or IP interface for ingress or egress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP or IP interface, and the QoS policy reverts to the default.

Parameters *policy-id* — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.

Values 1 to 65535

port-redirect-group — This keyword associates a SAP egress with an instance of a named queue group template on the egress port of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.

queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under config>port>ethernet>access>egress.

instance *instance-id* — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.

Values 1 to 40960

Default 1

Platforms All

qos

Syntax **qos policy-id** [**port-redirect-group** *queue-group-name* **instance** *instance-id*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no qos

Context **[Tree]** (config>service>vpls>sap>egress qos)

Full Context configure service vpls sap egress qos

Description This command associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a specified type will return an error.

When an egress QoS policy is associated with an IES IP interface that has been bound to a VPLS, the policy becomes associated with every SAP on the VPLS and augments the egress QoS policy that is defined on each SAP. Packets that are bridged will be processed using the policy defined on the VPLS SAP; packets that are routed will be processed using the policy defined in the IES IP interface- binding context.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters *port-redirect-group* — Associates a SAP egress with an instance of a named queue group template on the egress port of a specified IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.

queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under *config>port>ethernet>access>egress*.

instance *instance-id* — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA

Values 1 to 40960

Default 1

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos

Syntax **qos** *policy-id* [**shared-queuing**]
no qos

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>ingress qos)

Full Context configure service ies subscriber-interface group-interface sap ingress qos

Description Associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP) or IP interface.

QoS ingress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the *policy-id* does not exist, an error is returned.

This **qos** command is used to associate ingress QoS policies. The **qos** command only allows ingress policies to be associated on SAP or IP interface ingress.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type returns an error.

By default, no specific QoS policy is associated with the SAP or IP interface for ingress so the default QoS policy is used.

The normal behavior is for queues to be created per destination. Shared and multipoint shared change this behavior creating either unicast or unicast and mcast shared queues.

The **no** form of this command removes the QoS policy association from the SAP or IP interface, and the QoS policy reverts to the default.

Parameters *policy-id* — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.

Values 1 to 65535

shared-queuing — Specifies the ingress shared queue policy a SAP uses. When the value of this object is null, the SAP uses individual ingress QoS queues, instead of the shared ones. This keyword only applies on the SAP ingress.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id* [**shared-queuing** | **multipoint-shared**] [**fp-redirect-group** *queue-group-name* **instance** *instance-id*]
qos *policy-id* [**shared-queuing** | **multipoint-shared**]
no qos [*policy-id*]

Context **[Tree]** (config>service>ies>if>sap>ingress qos)
[Tree] (config>service>vprn>if>sap>ingress qos)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface sap ingress qos
configure service vprn interface sap ingress qos

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy ID does not exist, an error is returned.

The **qos** command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type returns an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

The **no** form of this command removes the QoS policy association from the SAP or IP interface, and the QoS policy reverts to the default.

Parameters *policy-id* — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.

1 to 65535

shared-queuing — Specifies the ingress shared queue policy used by this SAP. When the value of this object is null it means that the SAP uses individual ingress QoS queues instead of the shared ones.

multipoint-shared — Specifies that this queue-id is for multipoint forwarded traffic only. This queue-id can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. Attempting to map forwarding class unicast traffic to a multipoint queue generates an error; no changes are made to the current unicast traffic queue mapping.

A queue must be created as multipoint. The multipoint designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the multipoint keyword, an error is generated and the command is not executed.

The multipoint keyword can be entered in the command line on a preexisting multipoint queue to edit queue ID parameters.

Default Present (the queue is created as non-multipoint).

Values **Multipoint** or not present.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fp-redirect-group — Creates an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command. The named queue group template can contain only policers. If it contains queues, then the command fails.

queue-group-name — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM/XMA, up to 32 characters. The queue-group-name must correspond to a valid ingress queue group template name, configured in the **config>qos>queue-group-templates** context.

instance-id — Specifies the instance of the named queue group to be created on the IOM/IMM/XMA ingress forwarding plane.

Platforms All

qos

Syntax **qos** *policy-id*
no qos

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>egress qos)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress qos

Description This command configures the identifier of the egress QoS policy associated with each wlan-gw tunnel of this interface.

The **no** form of this command removes the policy ID from the configuration.

Default qos 1

Parameters *policy-id* — Specifies to apply the specified sap-*egress-policy-id*.

Values 1 to 65535
name: A string up to 64 characters

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*
qos *policy-id*
no qos [*policy-id*]

Context **[Tree]** (config>service>apipe>sap>egress qos)
[Tree] (config>service>cpipe>sap>egress qos)
[Tree] (config>service>epipe>sap>egress qos)
[Tree] (config>service>fpipe>sap>egress qos)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ipipe>sap>egress qos)

Full Context
configure service apipe sap egress qos
configure service cpipe sap egress qos
configure service epipe sap egress qos
configure service fpipe sap egress qos
configure service ipipe sap egress qos

Description
This command associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the *policy-id* does not exist, an error will be returned.

The **qos** command, when used under the egress context, is used to associate egress QoS policies.

The **qos** command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a specified type will return an error.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters
policy-id — The egress policy ID to associate with SAP on egress. The policy ID must already exist.

Values 1 to 65535

queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under *config>port>ethernet>access>egress*.

instance-id — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.

Values 1 to 40960

Default 1

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress qos
- configure service fpipe sap egress qos

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe sap egress qos

All

- configure service ipipe sap egress qos
- configure service epipe sap egress qos

qos

Syntax **qos** *policy-id* [**shared-queuing**] [**fp-redirect-group** *queue-group-name* **instance** *instance-id*]
no qos

Context **[Tree]** (config>service>apipe>sap>ingress qos)
[Tree] (config>service>cpipe>sap>ingress qos)
[Tree] (config>service>epipe>sap>ingress qos)
[Tree] (config>service>fpipe>sap>ingress qos)
[Tree] (config>service>ipipe>sap>ingress qos)

Full Context configure service apipe sap ingress qos
configure service cpipe sap ingress qos
configure service epipe sap ingress qos
configure service fpipe sap ingress qos
configure service ipipe sap ingress qos

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The **qos** command, when used under the ingress context, is used to associate ingress QoS policies. The **qos** command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a specified type will return an error.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters *policy-id* — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shared-queuing — This keyword can only be specified on SAP ingress. The shared-queuing keyword specifies the shared queue policy will be used by this SAP. When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

fp-redirect-group — This keyword can only be used on SAP ingress and associates a SAP ingress with an instance of a named queue group template on the ingress forwarding plane of a specified IOM/IMM/XMA. The queue-group-name and **instance** *instance-id* are mandatory parameters when executing the command.

queue-group-name — Specifies the name of the queue group to be instance on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The *queue-group-name* must correspond to a valid ingress forwarding plane queue group, created under **config**>**card**>**fp**>**ingress**>**access**.

instance-id — Specifies the instance of the named queue group on the IOM/IMM/XMA ingress forwarding plane.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap ingress qos
- configure service cpipe sap ingress qos

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap ingress qos

All

- configure service ipipe sap ingress qos
- configure service epipe sap ingress qos

qos

Syntax **qos** *network-policy-id* **port-redirect-group** *queue-group-name* [**instance** *instance-id*]
no qos

Context **[Tree]** (config>service>apipe>spoke-sdp>egress qos)
[Tree] (config>service>cpipe>spoke-sdp>egress qos)
[Tree] (config>service>epipe>spoke-sdp>egress qos)
[Tree] (config>service>fpipe>spoke-sdp>egress qos)
[Tree] (config>service>ipipe>spoke-sdp>egress qos)
[Tree] (config>service>vpls>mesh-sdp>egress qos)
[Tree] (config>service>vpls>spoke-sdp>egress qos)

Full Context configure service apipe spoke-sdp egress qos
configure service cpipe spoke-sdp egress qos
configure service epipe spoke-sdp egress qos
configure service fpipe spoke-sdp egress qos
configure service ipipe spoke-sdp egress qos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp egress qos
configure service vpls spoke-sdp egress qos

Description This command is used to redirect pseudowire (PW) packets to an egress port queue-group for the purpose of shaping.

The egress PW shaping provisioning model allows the mapping of one or more PWs to the same instance of queues, or policers and queues, that are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only, or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface that the PW packets can be forwarded on. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different PWs to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-sdp inside a service, or to the egress context of a PW template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use queues only, or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-sdp to the named queue-group. In such a case, the PW packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on. This queue can be a queue-group queue or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a PW packet.
2. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-sdp to the named queue-group. In such a case, the PW packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on.
3. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports that have network IP interfaces. The handling of this is dealt with in the data path as follows:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- When a PW packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
- When a PW packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the PW packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

4. If a network QoS policy is applied to the egress context of a PW, any PW FC that is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the PW is redirected to exists and the redirection succeeds, the marking of the packet's DEI/dot1p/DSCP and the tunnel's DEI/dot1p/DSCP/EXP is performed according to the relevant mappings of the {FC, profile} in the egress context of the network QoS policy applied to the PW. This is true regardless of whether an instance of the queue-group exists or not on the egress port the PW packet is forwarded to. If the packet's profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet's DEI/dot1p and the tunnel's DEI/dot1p/EXP, and the DSCP/prec will be remarked if **enable-dscp-prec-marking** is enabled under the policer.

When the queue-group name the PW is redirected does not exist, the redirection command is failed. In this case, the marking of the packet's DEI/dot1p/DSCP and the tunnel's DEI/dot1p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the PW packet is forwarded.

The **no** version of this command removes the redirection of the PW to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

queue-group-name — Specifies the name of the queue group template up to 32 characters in length.

instance-id — Specifies the optional identification of a specific instance of the queue-group.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe spoke-sdp egress qos
- configure service cpipe spoke-sdp egress qos

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp egress qos

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls mesh-sdp egress qos
- configure service vpls spoke-sdp egress qos
- configure service epipe spoke-sdp egress qos
- configure service ipipe spoke-sdp egress qos

qos

Syntax **qos** *network-policy-id* **port-redirect-group** *queue-group-name* [**instance** *instance-id*]
no qos [*network-policy-id*]

Context **[Tree]** (config>service>ies>if>spoke-sdp>egress qos)
[Tree] (config>service>vprn>if>spoke-sdp>egress qos)

Full Context configure service ies interface spoke-sdp egress qos
configure service vprn interface spoke-sdp egress qos

Description This command is used to redirect pseudowire packets to an egress port queue-group for the purpose of shaping.

The egress pseudowire shaping provisioning model allows the mapping of one or more pseudowires to the same instance of queues, or policers and queues, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

Step 1. Create an egress queue-group template and configure queues only or policers and queues for each FC that needs to be redirected.

Step 2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface on which the pseudowire packets can be forwarded. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.

Step 3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.

Step 4. Apply this network QoS policy to the egress context of a spoke-SDP inside a service or to the egress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-SDPs can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Step 1. When a pseudowire FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface on which the pseudowire packet is forwarded. This queue can be a queue-group queue, or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a pseudowire packet.

Step 2. When a pseudowire FC is redirected to use a queue or a policer, and a queue in a queue-group and the queue-group name exists, but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the pseudowire packet is forwarded on.

Step 3. When a pseudowire FC is redirected to use a queue, or a policer and a queue in a queue-group, and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:

a. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.

b. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the pseudowire packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

Step 4. If a network QoS policy is applied to the egress context of a pseudowire, any pseudowire FC, which is not explicitly redirected in the network QoS policy, will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the pseudowire is redirected to exists and the redirection succeeds, the marking of the packet DEI/dot1p/DSCP and the tunnel DEI/dot1p/DSCP/EXP is performed; according to the relevant mappings of the (FC, profile) in the egress context of the network QoS policy applied to the pseudowire. This is true regardless, whether an instance of the queue-group exists or not on the egress port to which the pseudowire packet is forwarded. If the packet profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet DEI/dot1p and the tunnel DEI/dot1p/EXP, and the DSCP/prec will be remarked if e**nable-dscp-prec-marking** is enabled under the policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the marking of the packet DEI/dot1p/DSCP and the tunnel DEI/dot1p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the pseudowire packet is forwarded.

The **no** version of this command removes the redirection of the pseudowire to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

port-redirect-group *queue-group-name* — This optional parameter specifies that the *queue-group-name* will be used for all egress forwarding class redirections within the network QoS policy ID. The specified *queue-group-name* must exist as a port egress queue group on the port associated with the IP interface.

egress-instance *instance-id* — Specifies the identification of a specific instance of the queue-group.

Values 1 to 16384

Platforms All

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*
no qos [*network-policy-id*]

Context **[Tree]** (config>service>vprn>if>spoke-sdp>ingress qos)
[Tree] (config>service>ies>if>spoke-sdp>ingress qos)

Full Context configure service ies interface spoke-sdp ingress qos
configure service vprn interface spoke-sdp ingress qos

Description This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers, which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

Step 1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally, for each traffic type (unicast, broadcast, unknown, or multicast).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Step 2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface to which the pseudowire packets can be received. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.

Step 3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.

Step 4. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service, or to the ingress context of a pseudowire template, and specify the redirect queue-group name.

Step 5. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

Step 1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

Step 2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

Step 3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:

When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as *policer-output-queues*.

When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

- If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:

the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the FP. This is the default behavior.

a queue-group policer followed by the per-FP ingress shared queues referred to as *policer-output-queues* if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group (csc-policing). The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from an R-VPLS spoke-SDP, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the FP is used.

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless of whether an instance of the named policer queue-group exists on the ingress FP on which the pseudowire packet is received. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload IP header if the user enabled the **ler-use-dscp** option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface on which the pseudowire packet is received.

The **no** version of this command removes the redirection of the pseudowire to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

fp- redirect-group *queue-group-name* — Specifies the name of the queue group template up to 32 characters in length.

ingress-instance *instance-id* — Specifies the identification of a specific instance of the queue-group.

Values 1 to 16384

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

qos

Syntax **qos** *network-policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos name *network-policy-name* **port-redirect-group** *queue-group-name* **instance** *instance-id*

no qos [*network-policy-id*]

Context **[Tree]** (config>service>pw-template>egress qos)

Full Context configure service pw-template egress qos

Description This command is used to redirect PW packets to an egress port queue-group for the purpose of shaping.

The egress PW shaping provisioning model allows the mapping of one or more PWs to the same instance of queues, or policers and queues, that are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only, or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface that the PW packets can be forwarded on. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different PWs to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-SDP inside a service, or to the egress context of a PW template and specify the redirect queue-group name.

One or more spoke-SDPs can have their FCs redirected to use queues only, or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model.

1. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SDP to the named queue-group. In such a case, the PW packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on. This queue can be a queue-group queue or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a PW packet.
2. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SDP to the named queue-group. In such a case, the PW packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports that have network IP interfaces. The handling of this is dealt with in the data path as follows:
   - When a PW packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
   - When a PW packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the PW packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.
4. If a network QoS policy is applied to the egress context of a PW, any PW FC that is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the PW is redirected to exists and the redirection succeeds, the marking of the packet's DEI/dot1p/DSCP and the tunnel's DEI/dot1p/DSCP/EXP is performed according to the relevant mappings of the {FC, profile} in the egress context of the network QoS policy applied to the PW. This is true regardless of whether an instance of the queue-group exists or not on the egress port the PW packet is forwarded to. If the packet's profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet's DEI/dot1p and the tunnel's DEI/dot1p/EXP, and the DSCP/prec will be remarked if **enable-dscp-prec-marking** is enabled under the policer.

When the queue-group name the PW is redirected does not exist, the redirection command is failed. In this case, the marking of the packet's DEI/dot1p/DSCP and the tunnel's DEI/dot1p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface the PW packet is forwarded to.

The **no** version of this command removes the redirection of the PW to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **qos name** *network-policy-name* variant can be used in all configuration modes.

Values 1 to 65535

queue-group-name — Specifies the name of the queue group template up to 32 characters in length.

instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

name *network-policy-name* — Specifies the network policy name. The value uniquely identifies the policy on the system, up to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*]
no qos

Context **[Tree]** (config>service>apipe>spoke-sdp>ingress qos)
[Tree] (config>service>cpipe>spoke-sdp>ingress qos)
[Tree] (config>service>epipe>spoke-sdp>ingress qos)
[Tree] (config>service>fpipe>spoke-sdp>ingress qos)
[Tree] (config>service>ipipe>spoke-sdp>ingress qos)
[Tree] (config>service>vpls>spoke-sdp>ingress qos)
[Tree] (config>service>vpls>mesh-sdp>ingress qos)

Full Context configure service apipe spoke-sdp ingress qos
configure service cpipe spoke-sdp ingress qos
configure service epipe spoke-sdp ingress qos
configure service fpipe spoke-sdp ingress qos
configure service ipipe spoke-sdp ingress qos
configure service vpls mesh-sdp ingress qos
configure service vpls spoke-sdp ingress qos

Description This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers, which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

Step 1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally, for each traffic type (unicast or multicast).

Step 2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface to which the pseudowire packets can be received. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.

Step 3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.

Step 4. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service, or to the ingress context of a pseudowire template, and specify the redirect queue-group name.

Step 5. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

Step 1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

Step 2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

Step 3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:

When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as *policer-output-queues*.

When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

- If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.
- If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:
  - the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the FP. This is the default behavior.
  - a queue-group policer followed by the per-FP ingress shared queues referred to as *policer-output-queues* if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group. The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from an R-VPLS spoke-SDP, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the FP is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless of whether an instance of the named policer queue-group exists on the ingress FP on which the pseudowire packet is received. The user can apply a QoS filter matching the dot1-p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload IP header if the user enabled the **ler-use-dscp** option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface on which the pseudowire packet is received.

The **no** version of this command removes the redirection of the pseudowire to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

queue-group-name — Specifies the name of the queue group template up to 32 characters in length

instance-id — Specifies the identification of a specific instance of the queue-group

Values 1 to 16384

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp ingress qos
- configure service fpipe spoke-sdp ingress qos

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe spoke-sdp ingress qos
- configure service vpls mesh-sdp ingress qos
- configure service vpls spoke-sdp ingress qos
- configure service epipe spoke-sdp ingress qos

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp ingress qos

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos name *network-policy-name* **fp-redirect-group** *queue-group-name* **instance** *instance-id*
no qos [*network-policy-id*]

Context **[Tree]** (config>service>pw-template>ingress qos)

Full Context configure service pw-template ingress qos

Description This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC which needs to be redirected and optionally for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface which the pseudowire packets can be received on. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the ingress context of a spoke-sdp inside a service or to the ingress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-sdp to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.
2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-sdp to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   - When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as “policer-output-queues”.
   - When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.
4. If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the FP.
5. If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:
   - the ingress network shared queue for the packet’s FC defined in the network-queue policy applied to the ingress of the FP. This is the default behavior.
   - a queue-group policer followed by the per-FP ingress shared queues referred to as “policer-output-queues” Good received is redirected to a queue-group. The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from a R-VPLS spoke-sdp which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet’s FC defined in the network-queue policy applied to the ingress of the FP is used. When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless if an instance of the named policer queue-group exists on the ingress FP the pseudowire packet is received on. The user can apply a QoS filter matching the dot1p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload’s IP header if the user enabled the ler-use-dscp option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface the pseudowire packet is received on.

The no version of this command removes the redirection of the pseudowire to the queue-group.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **qos name** *network-policy-name* variant can be used in all configuration modes.

Values 1 to 65535

queue-group-name — Specifies the name of the queue group template up to 32 characters in length.

instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

name *network-policy-name* — Specifies the network policy name. The value uniquely identifies the policy on the system, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

qos

Syntax **qos** *policy-id*
qos name *sap-egress-policy-name*
no qos

Context **[Tree]** (config>service>template>epipe-sap-template>egress qos)

Full Context configure service template epipe-sap-template egress qos

Description This command associates an existing QoS policy with the template.

Parameters *policy-id* — The egress policy ID to associate with SAP or IP interface on egress. The policy ID must already exist.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **qos name** *sap-egress-policy-name* variant can be used in all configuration modes.

Values 1 to 65535

sap-egress-policy-name — The SAP egress QoS policy name to associate with the SAP on egress, up to 64 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos name** *sap-ingress-policy-name* [**shared-queuing**]
qos *policy-id* [**shared-queuing**]
no qos

Context **[Tree]** (config>service>template>epipe-sap-template>ingress qos)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service template epipe-sap-template ingress qos

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP) for the Epipe SAP template.

Parameters *sap-ingress-policy-name* — The SAP ingress QoS policy name to associate with the SAP on ingress.

policy-id — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **qos name** *sap-ingress-policy-name* variant can be used in all configuration modes.

Values 1 to 65535

shared-queuing — This keyword can only be specified on SAP ingress. Specify the ingress shared queue policy used by this SAP. When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*
no qos

Context **[Tree]** (config>service>vpls>vxlan>network>ingress qos)

Full Context configure service vpls vxlan network ingress qos

Description This command is used to redirect traffic arriving on VXLAN tunnels in an EVPN VXLAN service as a single entity (per forwarding class) to policers in an ingress forwarding plane queue group for the purpose of rate-limiting.

For the policer to be used, the following must be true:

- The configured queue group template name must be applied to the forwarding plane on which the ingress traffic arrives using the instance id specified.
- The policer referenced in the FC-to-policer mappings in the ingress context of a network QoS policy must be present in the specified queue group template.

The command will fail if the queue group template name does not exist or if the policer specified in the network QoS policy does not exist in the queue group template. If the queue group template name with the specified instance is not applied to the forwarding plane on which the VXLAN traffic arrives, then this traffic will use the ingress network queues related to the network interface; however, the ingress classification is still based on the applied network QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The unicast traffic can be redirected to a policer under the forwarding class **fp-redirect-group** command in the ingress section of a network QoS policy. Similarly, broadcast, unknown and multicast traffic can be redirected to a **broadcast-policer**, **unknown-policer** or **mcast-policer**, respectively, also under the forwarding class **fp-redirect-group** command in the ingress section of a network QoS policy.

Ingress classification is based on the configuration of the ingress section of the specified network QoS policy, noting that the dot1p and DSCP classification is based on the outer Ethernet header and IP header, and the use of **ler-use-dscp**, **ip-criteria** and **ipv6-criteria** statements are ignored.

When this command is applied, it overrides the QoS applied to the related network interfaces for traffic arriving on VXLAN tunnels in that service but does not affect traffic received on a spoke-SDP in the same service.

The **no** version of this command removes the redirection of VXLAN tunnel traffic from the queue group policers.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

queue-group-name — Specifies the name of the queue group template up to 32 characters in length

instance-id — Specifies the identification of a specific instance of the queue-group

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name* **instance** *instance-id*
no qos [*network-policy-id*]

Context **[Tree]** (config>service>vpls>sap>egress>encap-defined-qos>encap-group qos)

Full Context configure service vpls sap egress encap-defined-qos encap-group qos

Description This command configures the QoS ID.

Platforms All

qos

Syntax **qos** *policy-id* [**shared-queuing** | **multipoint-shared**]
qos name *sap-ingress-policy-name* [**shared-queuing** | **multipoint-shared**]
no qos [*policy-id*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>template>vpls-sap-template>ingress qos)

Full Context configure service template vpls-sap-template ingress qos

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP) for the Epipe SAP template.

Parameters *policy-id* — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **qos name** *sap-ingress-policy-name* variant can be used in all configuration modes.

Values 1 to 65535

shared-queuing — This keyword can only be specified on SAP ingress. Specify the ingress shared queue policy used by this SAP. When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

multipoint-shared — This keyword can only be specified on SAP ingress. Multipoint shared queuing is a superset of shared queuing. When multipoint shared queuing keyword is set, as well as the unicast packets, multipoint packets also used shared queues.

Ingress unicast service queues are mapped one-for-one with hardware queues and unicast packets traverse the ingress forwarding plane twice, similar to the shared-queuing option. In addition, the multipoint queues defined in the ingress SAP QoS policy are not created. Instead, multipoint packets (broadcast, multicast and unknown unicast destined) are treated to the same dual pass ingress forwarding plane processing as unicast packets.

When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

Values Multipoint or not present

Default Present (the queue is created as non-multipoint)

sap-ingress-policy-name — The SAP ingress QoS policy name to associate with the SAP on ingress, up to 64 characters.

Platforms All

qos

Syntax **qos** *sap-egress-policy-id*
qos name *sap-egress-policy-name*
no qos

Context [Tree] (config>service>template>vpls-sap-template>egress qos)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service template vpls-sap-template egress qos

Description This command associates an existing QoS policy with the template.

Parameters *sap-egress-policy-id* — The egress policy ID to associate with SAP or IP interface on egress. The policy ID must already exist.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **qos name** *sap-egress-policy-name* variant can be used in all configuration modes.

Values 1 to 65535

sap-egress-policy-name — The SAP egress QoS policy name to associate with the SAP on egress, up to 64 characters.

Platforms All

qos

Syntax **qos** *policy-id* [**shared-queuing** | **multipoint-shared**] [**fp-redirect-group** *queue-group-name* **instance** *instance-id*]

no qos

Context **[Tree]** (config>service>vpls>sap>ingress qos)

Full Context configure service vpls sap ingress qos

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a specified type will return an error.

When an ingress QoS policy is defined on IES ingress IP interface that is bound to a VPLS, the policy becomes associated with every SAP on the VPLS and augments the QoS policy that is defined on each SAP. Packets that are bridged will be processed using the policy defined on the VPLS SAP; packets that are routed will be processed using the policy defined in the IES IP interface-binding context.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, the default QoS policy is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters *policy-id* — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.

Values 1 to 65535

shared-queuing — This keyword can only be specified on SAP ingress. Specify the ingress shared queue policy used by this SAP. When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

multipoint-shared — This keyword can only be specified on SAP ingress. Multipoint shared queuing is a superset of shared queuing. When multipoint shared queuing keyword is set, as well as the unicast packets, multipoint packets also used shared queues.

Ingress unicast service queues are mapped one-for-one with hardware queues and unicast packets traverse the ingress forwarding plane twice, similar to the shared-queuing option. In addition, the multipoint queues defined in the ingress SAP QoS policy are not created. Instead, multipoint packets (broadcast, multicast and unknown unicast destined) are treated to the same dual pass ingress forwarding plane processing as unicast packets.

When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

Values Multipoint or not present

Default Present (the queue is created as non-multipoint)

fp-redirect-group — Creates an instance of a named queue group template on the ingress forwarding plane of a specified IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command. The named queue group template can contain only policers. If it contains queues, then the command will fail.

queue-group-name — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid ingress queue group template name, configured under config>qos>queue- group-templates.

instance-id — Specifies the instance of the named queue group to be created on the IOM/IMM/XMA ingress forwarding plane.

Platforms All

qos

Syntax **qos** *network-policy-id*
qos *network-policy-id* **egress-port-redirect-group** *queue-group-name* **egress-instance**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

instance-id **ingress-fp-redirect-group** *queue-group-name* **ingress-instance** *instance-id*

qos *network-policy-id* **egress-port-redirect-group** *queue-group-name* **egress-instance** *instance-id*

qos *network-policy-id* **ingress-fp-redirect-group** *queue-group-name* **ingress-instance** *instance-id*

no qos

Context **[Tree]** (config>service>vprn>nw-if qos)

Full Context configure service vprn network-interface qos

Description This command associates a network Quality of Service (QoS) policy with a network IP interface. Only one network QoS policy can be associated with an IP interface at one time. Attempts to associate a second QoS policy return an error.

Associating a network QoS policy with a network interface is useful for the following purposes:

- To apply classification rules for determining the forwarding-class and profile of ingress packets on the interface.
- To associate ingress packets on the interface with a queue-group instance applied to the ingress context of the interface's forwarding plane (FP). (This is only applicable to interfaces on IOM3 and later cards.) The referenced ingress queue-group instance may have policers defined in order to rate limit ingress traffic on a per-forwarding class (and forwarding type: unicast vs. multicast) basis.
- To perform 802.1p, DSCP, IP precedence and/or MPLS EXP re-marking of egress packets on the interface.
- To associate egress packets on the interface with a queue-group instance applied to the egress context of the interface's port. The referenced egress queue-group instance may have policers and/or queues defined in order to rate limit egress traffic on a per-forwarding class basis.

The **no** form of this command removes the network QoS policy association from the network IP interface, and the QoS policy reverts to the default.

Default no qos

Parameters *network-policy-id* — An existing network policy ID to associate with the IP interface.

Values 1 to 65535

port-redirect-group *queue-group-name* — This optional parameter specifies the egress queue-group used for all egress forwarding-class redirections specified within the network QoS policy ID. The specified *queue-group-name* must exist as an egress queue group applied to the egress context of the port associated with the IP interface.

egress-instance *instance-id* — Since multiple instances of the same egress queue-group can be applied to the same port this optional parameter is used to specify which particular instance to associate with this particular network IP interface.

Values 1 to 16384

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fp- redirect-group *queue-group-name* — This optional parameter specifies the ingress queue-group used for all ingress forwarding-class redirections specified within the network QoS policy ID. The specified queue-group-name must exist as an ingress queue group applied to the ingress context of the forwarding plane associated with the IP interface.

ingress-instance *instance-id* — Since multiple instances of the same ingress queue-group can be applied to the same forwarding plane this parameter is required to specify which particular instance to associate with this particular network IP interface.

Values 1 to 16384

Platforms All

qos

Syntax **qos** *network-policy-id* **fp-redirect-group** *queue-group-name instance instance-id*
no qos

Context **[Tree]** (config>service>vprn>network>ingress qos)

Full Context configure service vprn network ingress qos

Description This command is used to redirect unicast packets arriving on an automatically (using the **auto-bind-tunnel** command) or manually configured (using a **spoke-sdp** command, but not the **spoke-sdp** command under the VPRN IP interface) binding in a VPRN to a policer in an ingress forwarding plane queue-group for the purpose of rate-limiting.

For the policer to be used, the following must be true:

Step 1. The configured queue group template name must be applied to the forwarding plane on which the ingress traffic arrives using the instance id specified.

Step 2. The policer referenced in the FC-to-policer mappings in the ingress context of a network QoS policy must be present in the specified queue group template.

The command fails if the queue group template name does not exist or if the policer specified in the network QoS policy does not exist in the queue group template. If the queue group template name with the specified instance is not applied to the forwarding plane on which the VPRN binding unicast traffic arrives then this traffic uses the ingress network queues related to the network interface, however, the ingress classification is still based on the applied network QoS policy.

The unicast traffic can be redirected to a policer under the forwarding class **fp-redirect-group** command in the ingress section of a network QoS policy; any **fp-redirect-group multicast-policer, broadcast-policer** or **unknown-policer** commands are ignored for this traffic. Multicast traffic would use the ingress network queues or queue group related to the network interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Ingress classification is based on the configuration of the ingress section of the specified network QoS policy, noting that the dot1p and exp classification is based on the outer Ethernet header and MPLS label whereas the DSCP applies to the outer IP header if the tunnel encapsulation is GRE, or the DSCP in the first IP header in the payload if **ler-use-dscp** is enabled in the ingress section of the referenced network QoS policy.

When this command is applied, it overrides the QoS applied to the related network interfaces for unicast traffic arriving on bindings in that VPRN.

The **no** version of this command removes the redirection of VPRN binding traffic to the queue-group policers.

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

fp-redirect-group *queue-group-name* — Specifies the name of the queue group template up to 32 characters in length.

instance *instance-id* — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

qos

Syntax **qos** *policy-id*
no qos [*policy-id*]

Context **[Tree]** (config>service>ies>aa-if>sap>egress qos)
[Tree] (config>service>ies>aa-if>sap>ingress qos)
[Tree] (config>service>vprn>aa-if>sap>egress qos)
[Tree] (config>service>vprn>aa-if>sap>ingress qos)

Full Context configure service ies aa-interface sap egress qos
configure service ies aa-interface sap ingress qos
configure service vprn aa-interface sap egress qos
configure service vprn aa-interface sap ingress qos

Description This command applies an QoS policy to the SAP.

Default qos 1

Parameters *policy-id* — Specifies an existing QoS policy ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos

Syntax **qos**

Context **[Tree]** (config>isa>aa-grp qos)

Full Context configure isa application-assurance-group qos

Description Commands in this context configure Quality of Service for this application assurance group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

qos

Syntax **qos** *policy-id*
no qos

Context **[Tree]** (config>service>ies>video-interface>video-sap>egress qos)
[Tree] (config>service>vpls>video-interface>video-sap>egress qos)
[Tree] (config>service>vprn>video-interface>video-sap>egress qos)
[Tree] (config>service>ies>video-interface>video-sap>ingress qos)
[Tree] (config>service>vpls>video-interface>video-sap>ingress qos)
[Tree] (config>service>vprn>video-interface>video-sap>ingress qos)

Full Context configure service ies video-interface video-sap egress qos
configure service ies video-interface video-sap ingress qos
configure service vpls video-interface video-sap egress qos
configure service vpls video-interface video-sap ingress qos
configure service vprn video-interface video-sap egress qos
configure service vprn video-interface video-sap ingress qos

Description This command associates an existing egress or ingress QoS policy to a video interface. If the policy-id does not exist, an error will be returned. Attempts to associate a QoS policy of the wrong type returns an error. Only one QoS policy can be associated with a video interface at one time in the ingress and egress contexts. Attempts to associate a second QoS policy of a given type will return an error.

The **no** form of the command removes the QoS policy association from the video interface, and the QoS policy reverts to the default.

Default default QoS policy

Parameters *policy-id* — The sap-egress or sap-ingress policy ID to associate with the video interface on ingress or egress. The policy ID must already exist.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos

Syntax **qos** *policy-id*
qos *policy-id* **port-redirect-group** *queue-group-name* **instance** *instance-id*
no qos

Context **[Tree]** (config>mirror>mirror-dest>sap>egress qos)

Full Context configure mirror mirror-dest sap egress qos

Description This command associates a QoS policy with an egress SAP for a mirrored service.

By default, no specific QoS policy is associated with the SAP for egress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Default qos 1

Parameters *policy-id* — Specifies the QoS policy ID to associate with SAP for the mirrored service. The policy ID must already exist.

Values 1 to 65535

queue-group-name — Specifies the queue group redirect list policy name.

instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

Platforms All

qos

Syntax **qos** *network-policy-id*
qos *network-policy-id* **egress-port-redirect-group** *queue-group-name* **egress-instance** *instance-id* **ingress-fp-redirect-group** *queue-group-name* **ingress-instance** *instance-id*
qos *network-policy-id* **egress-port-redirect-group** *queue-group-name* **egress-instance** *instance-id*
qos *network-policy-id* **ingress-fp-redirect-group** *queue-group-name* **ingress-instance** *instance-id*
no qos

Context **[Tree]** (config>router>if qos)

Full Context configure router interface qos

Description This command associates a network Quality of Service (QoS) policy with a network IP interface. Only one network QoS policy can be associated with an IP interface at one time. Attempts to associate a second QoS policy return an error.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Associating a network QoS policy with a network interface is useful for the following purposes:

- To apply classification rules for determining the forwarding-class and profile of ingress packets on the interface.
- To associate ingress packets on the interface with a queue-group instance applied to the ingress context of the interface's forwarding plane (FP). The referenced ingress queue-group instance may have policers defined in order to rate limit ingress traffic on a per-forwarding class (and forwarding type: unicast vs. multicast) basis.
- To perform 802.1p, DSCP, IP precedence and/or MPLS EXP re-marking of egress packets on the interface.
- To associate egress packets on the interface with a queue-group instance applied to the egress context of the interface's port. The referenced egress queue-group instance may have policers and/or queues defined in order to rate limit egress traffic on a per-forwarding class basis.

The **no** form of this command removes the network QoS policy association from the network IP interface, and the QoS policy reverts to the default.

Default no qos

Parameters *network-policy-id* — Specifies an existing network policy ID to associate with the IP interface.

Values 1 to 65535

egress-port-redirect-group *queue-group-name* — This optional parameter specifies the egress queue-group used for all egress forwarding-class redirections specified within the network QoS policy ID. The specified *queue-group-name* must exist as an egress queue group applied to the egress context of the port associated with the IP interface.

egress-instance *instance-id* — Since multiple instances of the same egress queue-group can be applied to the same port this optional parameter is used to specify which instance to associate with this specific network IP interface.

Values 1 to 16384

ingress-fp- redirect-group *queue-group-name* — This optional parameter specifies the ingress queue-group used for all ingress forwarding-class redirections specified within the network QoS policy ID. The specified queue-group-name must exist as an ingress queue group applied to the ingress context of the forwarding plane associated with the IP interface.

ingress-instance *instance-id* — Since multiple instances of the same ingress queue-group can be applied to the same forwarding plane this parameter is required to specify which instance to associate with this specific network IP interface.

Values 1 to 16384

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos

Syntax **qos** *network-policy-id*
no qos

Context **[Tree]** (config>fwd-path-ext>fpe>srv6>interface-a qos)
[Tree] (config>fwd-path-ext>fpe>srv6>interface-b qos)

Full Context configure fwd-path-ext fpe srv6 interface-a qos
configure fwd-path-ext fpe srv6 interface-b qos

Description This command configures the network QoS policy that is applied to the SRv6 FPE network interface-a or interface-b.

Default no qos

Parameters *network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

21.11 qos-marking-from-sap

qos-marking-from-sap

Syntax [**no**] **qos-marking-from-sap**

Context **[Tree]** (config>subscr-mgmt>sla-profile>egress qos-marking-from-sap)

Full Context configure subscriber-mgmt sla-profile egress qos-marking-from-sap

Description This command sets the QoS policy from which the egress QoS marking rules are applied.

Note: If applied to a managed SAP, the default s-egress qos-policy (sap-egress 1) cannot be changed.

The **no** form of this command reverts to the egress QoS marking defined in SAP-egress policy defined at sla-profile level.

Default qos-marking-from-sap

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.12 qos-policy-id-range

qos-policy-id-range

Syntax **qos-policy-id-range start** *policy-id* **end** *policy-id*
no qos-policy-id-range

Context **[Tree]** (config>qos>md-auto-id qos-policy-id-range)

Full Context configure qos md-auto-id qos-policy-id-range

Description This command specifies the range of IDs used by SR OS to automatically assign an ID to QoS policies that are created in model-driven interfaces without an ID explicitly specified by the user or client.

A QoS policy created with an explicitly-specified ID cannot use an ID in this range. In classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed which will cause any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **config>eth-cfm md-auto-id** command for further details.

Default no qos-policy-id-range

Parameters **start** *policy-id* — Specifies the lower value of the ID range. The value must be less than or equal to the **end** value.

Values 1 to 65535

end *policy-id* — Specifies the upper value of the ID range. The value must be greater than or equal to the **start** value.

Values 1 to 65535

Platforms All

21.13 qos-profile

qos-profile

Syntax **qos-profile** *profile-id*
no qos-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>ml-bundle>mlfr>ingress qos-profile)
[Tree] (config>port>ml-bundle>mlfr>egress qos-profile)

Full Context configure port multilink-bundle mlfr egress qos-profile
configure port multilink-bundle mlfr ingress qos-profile

Description This command specifies the ingress or egress QoS profile to be used for the configuration of the ingress or egress QoS parameters of an MLFR bundle or a Frame Relay port with FRF.12 UNI/NNI fragmentation enabled. Note that qos-profile on ingress is only applicable to MLFR.

The no form of this command removes the parameters from the configuration.

Parameters *profile-id* — Specifies the profile number. The value can only be modified if the MLFR bundle or FR port is shut down.

Values 1 to 128

Platforms 7450 ESS, 7750 SR-7/12/12e

qos-profile

Syntax **qos-profile** *profile-id*
no qos-profile

Context [Tree] (config>port>sonet-sdh>path>frame-relay>egress qos-profile)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay>frf-12>egress qos-profile)
[Tree] (config>port>tdm>ds3>frame-relay>frf-12>egress qos-profile)
[Tree] (config>port>tdm>e1>channel-group>frame-relay>frf-12>egress qos-profile)
[Tree] (config>port>tdm>e3>frame-relay>frf-12>egress qos-profile)
[Tree] (config>port>tdm>channel-group>frame-relay>egress qos-profile)
[Tree] (config>port>sonet-sdh>path>frame-relay>egress qos-profile)

Full Context configure port sonet-sdh path frame-relay egress qos-profile
configure port tdm channel-group frame-relay egress qos-profile
configure port tdm ds1 channel-group frame-relay frf-12 egress qos-profile
configure port tdm ds3 frame-relay frf-12 egress qos-profile
configure port tdm e1 channel-group frame-relay frf-12 egress qos-profile
configure port tdm e3 frame-relay frf-12 egress qos-profile

Description This command specifies the ingress or egress QoS profile to be used for the configuration of the egress QoS parameters of a Frame Relay port with FRF.12 UNI/NNI fragmentation enabled.

The **no** form of this command removes the parameters from the configuration.

Parameters *profile-id* — Specifies the profile number. The value can only be modified if the FR port is shut down.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos-profile

Syntax **qos-profile** *profile-id*
no qos-profile

Context **[Tree]** (config>port>ml-bundle>mlppp>egress qos-profile)

Full Context configure port multilink-bundle mlppp egress qos-profile

Description This command specifies the egress QoS profile to be used for the outgoing traffic over this MLPPP bundle.

The **no** form of this command removes the parameters from the configuration.

Parameters *profile-id* — Specifies the egress QoS profile to be used for the outgoing traffic over this MLPPP bundle. The value can only be modified if the bundle is shutdown.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR-7/12/12e

qos-profile

Syntax **qos-profile** *profile-id*
no qos-profile

Context **[Tree]** (config>port>ml-bundle>mlppp>ingress qos-profile)

Full Context configure port multilink-bundle mlppp ingress qos-profile

Description This command specifies the ingress QoS profile to be used for the incoming traffic over this MLPPP bundle.

Parameters *profile-id* — Specifies the ingress QoS profile to be used for the incoming traffic over this MLPPP bundle. The value can only be modified if the bundle is shutdown.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR-7/12/12e

21.14 qos-route-lookup

qos-route-lookup

Syntax **qos-route-lookup** [**source** | **destination**]
no qos-route-lookup

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if qos-route-lookup)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 qos-route-lookup)
[Tree] (config>service>vprn>sub-if>grp-if qos-route-lookup)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 qos-route-lookup)

Full Context configure service ies subscriber-interface group-interface ipv6 qos-route-lookup
configure service ies subscriber-interface group-interface qos-route-lookup
configure service vprn subscriber-interface group-interface ipv6 qos-route-lookup
configure service vprn subscriber-interface group-interface qos-route-lookup

Description This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional **destination** parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If the optional **source** parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If neither the optional **source** or **destination** parameter is present, then the default is **destination** address matching.

The functionality enabled by the qos-route-lookup command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the interface>ipv6 context (applies to IPv6). The ability to specify source address based QoS lookup is not supported for IPv6. For the 7740 ESS, subscriber management group interfaces also do not support the source QPPB option.

The **no** form of this command reverts to the default.

Default destination

Parameters **source** — Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

destination — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos-route-lookup

Syntax **qos-route-lookup** [**source** | **destination**]
no qos-route-lookup

Context **[Tree]** (config>service>ies>if qos-route-lookup)
[Tree] (config>service>ies>if>ipv6 qos-route-lookup)

Full Context configure service ies interface ipv6 qos-route-lookup
configure service ies interface qos-route-lookup

Description This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional **destination** parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the forwarding class (fc) and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

If the optional **source** parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

If neither the optional **source** or **destination** parameter is present, then the default is **destination** address matching.

The functionality enabled by the qos-route-lookup command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the interface>ipv6 context (applies to IPv6). Subscriber management group interfaces also do not support the source QPPB option.

The **no** form of this command reverts to the default destination address matching mode.

Default no qos-route-lookup

Parameters **source** — Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

destination — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos-route-lookup

Syntax **qos-route-lookup** [**source** | **destination**]
no qos-route-lookup

Context **[Tree]** (config>service>vprn>if qos-route-lookup)
[Tree] (config>service>vprn>if>ipv6 qos-route-lookup)

Full Context configure service vprn interface ipv6 qos-route-lookup
configure service vprn interface qos-route-lookup

Description This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional **destination** parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If the optional **source** parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If neither the optional **source** nor **destination** parameter is present, then the default is **destination** address matching.

The functionality enabled by the qos-route-lookup command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the interface>ipv6 context (applies to IPv6). The ability to specify source address based QoS lookup is not supported for IPv6. Subscriber management group interfaces also do not support the source QPPB option.

The **no** form of this command reverts to the default destination address matching mode.

Default no qos-route-lookup

Parameters **source** — Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

destination — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

qos-route-lookup

Syntax **qos-route-lookup** [{**source** | **destination**}]
no qos-route-lookup

Context **[Tree]** (config>router>if qos-route-lookup)
[Tree] (config>router>if>ipv6 qos-route-lookup)

Full Context configure router interface ipv6 qos-route-lookup
configure router interface qos-route-lookup

Description This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional **destination** parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

If the optional **source** parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

If neither the optional **source** or **destination** parameter is present, then the default is **destination** address matching.

The functionality enabled by the qos-route-lookup command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the interface>ipv6 context (applies to IPv6). Subscriber management group interfaces for the 7750 SR and 7450 ESS also do not support the source QPPB option.

The **no** form of this command reverts to the default.

Default no qos-route-lookup

Parameters **source** — Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

destination — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.15 query-interval

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>service>vpls>igmp-snooping query-interval)
[Tree] (config>service>vpls>sap>igmp-snooping query-interval)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping query-interval)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping query-interval)
[Tree] (config>service>vpls>mld-snooping query-interval)
[Tree] (config>service>vpls>sap>mld-snooping query-interval)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping query-interval)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping query-interval)

Full Context configure service vpls igmp-snooping query-interval
configure service vpls mesh-sdp igmp-snooping query-interval
configure service vpls mesh-sdp mld-snooping query-interval
configure service vpls mld-snooping query-interval
configure service vpls sap igmp-snooping query-interval
configure service vpls sap mld-snooping query-interval
configure service vpls spoke-sdp igmp-snooping query-interval
configure service vpls spoke-sdp mld-snooping query-interval

Description This command configures the IGMP query interval. If the **send-queries** command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on this SAP or SDP.

The configured query-interval must be greater than the configured query-response-interval.

If send-queries is not enabled on this SAP or SDP, the configured query-interval value is ignored.

Default query-interval 125

Parameters *seconds* — Specifies the time interval, in seconds, that the router transmits general host-query messages

Values 2 to 1024

Values **config>service>vpls>igmp-snooping**: 1 - 65535
config>service>vpls>sap>igmp-snooping: 2 - 1024

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>router>igmp>group-interface query-interval)
[Tree] (config>router>mld>group-interface query-interval)
[Tree] (config>service>vprn>igmp>group-interface query-interval)
[Tree] (config>service>vprn>mld>group-interface query-interval)

Full Context configure router igmp group-interface query-interval
configure router mld group-interface query-interval
configure service vprn igmp group-interface query-interval
configure service vprn mld group-interface query-interval

Description This command configures the query interval when the group interface is configured with **no sub-hosts-only**. If nothing is configured, by default, the **query-interval** takes the value defined in the **config>router>igmp** (or **mld**) context or in the **config>service>vprn>igmp** (or **mld**) context.

The **no** form of this command reverts to the default value.

Default query-interval 125

Parameters *seconds* — Specifies the frequency, in seconds, at which the router transmits general host-query messages.

Values 2 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>router>mld query-interval)
[Tree] (config>router>mld>if query-interval)

Full Context configure router mld interface query-interval
configure router mld query-interval

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

The **no** form of this command reverts to the default value.

Default query-interval 125

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 to 1024

Platforms All

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>subscr-mgmt>igmp-policy query-interval)

Full Context configure subscriber-mgmt igmp-policy query-interval

Description This command specifies the frequency at which the querier router transmits general host-query messages. Host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1. If nothing is configured, by default, the **query-interval** takes the value defined in the **config>router>igmp** context or in the **config>service>vprn>igmp** context. It is highly recommended that all three query intervals be configured together on each IGMP policy.

The **no** form of this command reverts to the default value.

Parameters *seconds* — Specifies the frequency, in seconds, at which the router transmits general host-query messages.

Values 2 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp query-interval)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping query-interval

Description This command configures the IGMP query interval. If the **send-queries** command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on an MSAP or SDP.

The configured query interval must be greater than the configured **query-response** interval.

If **send-queries** is not enabled on an MSAP or SDP, the configured query interval value is ignored.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default query-interval 125

Parameters *seconds* — Specifies the time interval, in seconds, that the router transmits general host-query messages.

Values 2 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>subscr-mgmt>mld-policy query-interval)

Full Context configure subscriber-mgmt mld-policy query-interval

Description This command specifies the frequency at which the querier router transmits general host-query messages. Host-query messages solicit group membership information and are sent to the link-scope all-node address, FF02::1. If nothing is configured, by default, the **query-interval** takes the value defined in the **config>router>mld** context or in the **config>service>vprn>mld** context. It is highly recommended that all three query intervals be configured together on each MLD policy.

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the frequency, in seconds, at which the router transmits general host-query messages.

Values 2 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>service>vprn>igmp query-interval)

Full Context configure service vprn igmp query-interval

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default query-interval 125

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 to 1024

Platforms All

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>service>vprn>mld query-interval)
[Tree] (config>service>vprn>mld>if query-interval)

Full Context configure service vprn mld interface query-interval
configure service vprn mld query-interval

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default query-interval 125

Parameters *seconds* — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 to 1024

Platforms All

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>router>igmp>if query-interval)

Full Context configure router igmp interface query-interval

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default query-interval 125

Parameters *seconds* — Specifies the frequency, in seconds, that the router transmits general host-query messages.

Values 2 to 1024

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context **[Tree]** (config>service>pw-template>igmp-snooping query-interval)

Full Context configure service pw-template igmp-snooping query-interval

Description This command configures the IGMP query interval. If the **send-queries** command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on this SAP or SDP.

The configured query-interval must be greater than the configured query-response-interval.

If send-queries is not enabled on this SAP or SDP, the configured query-interval value is ignored.

Default query-interval 125

Parameters *seconds* — Specifies the time interval, in seconds, that the router transmits general host-query messages.

Values 2 to 1024

Platforms All

21.16 query-last-listener-interval

query-last-listener-interval

Syntax **query-last-listener-interval** *seconds*
no query-last-listener-interval

Context **[Tree]** (config>router>mld>group-interface query-last-listener-interval)
[Tree] (config>service>vprn>mld>group-interface query-last-listener-interval)
[Tree] (config>router>mld>if query-last-listener-interval)
[Tree] (config>router>mld>group-interface query-last-listener-interval)

Full Context configure router mld group-interface query-last-listener-interval
configure router mld interface query-last-listener-interval
configure service vprn mld group-interface query-last-listener-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the frequency at which the querier router sends a group-specific query messages, including the messages sent in response to leave-group messages and is only applicable when the group interface is configured with the **no sub-hosts-only** command. The shorter the interval, the faster the loss of the last listener of a group can be detected. If nothing is configured, by default, the **query-last-listener-interval** takes the value defined in the **config>router>mld** context or in the **config>service>vprn>mld** context.

The **no** form of this command reverts to the default value.

Default query-last-listener-interval 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn mld group-interface query-last-listener-interval
- configure router mld group-interface query-last-listener-interval

All

- configure router mld interface query-last-listener-interval

query-last-listener-interval

Syntax **query-last-listener-interval** *seconds*
no query-last-listener-interval

Context **[Tree]** (config>subscr-mgmt>mld-policy query-last-listener-interval)

Full Context configure subscriber-mgmt mld-policy query-last-listener-interval

Description This command configures the frequency at which the querier router sends a group-specific query messages, including the messages sent in response to leave-group messages. The shorter the interval, the faster the loss of the last member of a group can be detected. If nothing is configured, by default, the **query-last-listener-interval** takes the value defined in the **config>router>mld** context or in the **config>service>vprn>mld** context. It is highly recommended that all three query intervals be configured together on each MLD policy.

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

query-last-listener-interval

Syntax **query-last-listener-interval** *seconds*
no query-last-listener-interval

Context **[Tree]** (config>service>vprn>mld query-last-listener-interval)
[Tree] (config>service>vprn>mld>if query-last-listener-interval)

Full Context configure service vprn mld interface query-last-listener-interval
configure service vprn mld query-last-listener-interval

Description This command specifies the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

The **no** form of this command reverts to the default value.

Default query-last-listener-interval 1

Parameters *seconds* — Specifies the frequency, in seconds, at which Group-Specific-Query packets are transmitted.

Values 1 to 1023

Platforms All

21.17 query-last-member-interval

query-last-member-interval

Syntax **query-last-member-interval** *seconds*
no query-last-member-interval

Context **[Tree]** (config>router>igmp>group-interface query-last-member-interval)

Full Context configure router igmp group-interface query-last-member-interval

Description This command configures the frequency at which the querier router sends group-specific query messages, including the messages sent in response to leave-group messages and is only applicable when the group interface is configured with **no sub-hosts-only**. The shorter the interval, the faster the loss of the last member of a group can be detected. If nothing is configured, by default, the **query-last-member-interval** takes the value defined in the **config>router>igmp** context.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default query-last-member-interval 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-last-member-interval

Syntax **query-last-member-interval** *seconds*
no query-last-member-interval

Context **[Tree]** (config>router>igmp query-last-member-interval)
[Tree] (config>router>igmp>if query-last-member-interval)

Full Context configure router igmp interface query-last-member-interval
configure router igmp query-last-member-interval

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default query-last-member-interval 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1023

Platforms All

query-last-member-interval

Syntax **query-last-member-interval** *seconds*
no query-last-member-interval

Context **[Tree]** (config>subscr-mgmt>igmp-policy query-last-member-interval)

Full Context configure subscriber-mgmt igmp-policy query-last-member-interval

Description This command configures the frequency at which the querier router sends group-specific query messages, including the messages sent in response to leave-group messages. The shorter the interval, the faster a loss of the last member of a group can be detected. If nothing is configured, by default, the **query-last-member-interval** takes the value defined in the **config>router>igmp** context or the **config>service>vprn>igmp** context. It is highly recommended that all three query intervals be configured together on each IGMP policy.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-last-member-interval

Syntax **query-last-member-interval** *seconds*

Context **[Tree]** (config>service>vprn>igmp query-last-member-interval)
[Tree] (config>service>vprn>igmp>grp-if query-last-member-interval)

Full Context configure service vprn igmp group-interface query-last-member-interval
configure service vprn igmp query-last-member-interval

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default query-last-member-interval 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface query-last-member-interval

All

- configure service vprn igmp query-last-member-interval

query-last-member-interval

Syntax **query-last-member-interval** *seconds*

Context **[Tree]** (config>service>vprn>mld query-last-member-interval)
[Tree] (config>service>vprn>mld>if query-last-member-interval)

Full Context configure service vprn mld interface query-last-member-interval
configure service vprn mld query-last-member-interval

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default query-last-member-interval 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 to 1024

21.18 query-response-interval

query-response-interval

Syntax **query-response-interval** *seconds*

Context **[Tree]** (config>service>vpls>sap>igmp-snooping query-response-interval)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping query-response-interval)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping query-response-interval)
[Tree] (config>service>vpls>sap>mld-snooping query-response-interval)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping query-response-interval)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping query-response-interval)

Full Context configure service vpls mesh-sdp igmp-snooping query-response-interval
configure service vpls mesh-sdp mld-snooping query-response-interval
configure service vpls sap igmp-snooping query-response-interval
configure service vpls sap mld-snooping query-response-interval
configure service vpls spoke-sdp igmp-snooping query-response-interval
configure service vpls spoke-sdp mld-snooping query-response-interval

Description This command configures the IGMP query response interval. If the **send-queries** command is enabled, this parameter specifies the maximum response time advertised in IGMPv2 or IGMPv3 queries.

The configured query response interval must be smaller than the configured query interval.

If **send-queries** is not enabled on this SAP or SDP, the configured query response interval value is ignored.

The **no** form of this command reverts to the default value.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 to 1023

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

query-response-interval

Syntax **query-response-interval** *seconds*
no query-response-interval

Context **[Tree]** (config>router>igmp>group-interface query-response-interval)
[Tree] (config>router>mld>group-interface query-response-interval)
[Tree] (config>service>vprn>igmp>group-interface query-response-interval)
[Tree] (config>service>vprn>mld>group-interface query-response-interval)
[Tree] (config>service>vprn>igmp query-response-interval)

Full Context configure router igmp group-interface query-response-interval
configure router mld group-interface query-response-interval
configure service vprn igmp group-interface query-response-interval
configure service vprn igmp query-response-interval
configure service vprn mld group-interface query-response-interval

Description This command configures the query response interval on when the group interface is configured with the **no sub-hosts-only** command. If nothing is configured, by default, the **query-response-interval** takes the value defined in the **config>router>igmp** (or **mld**) context or in the **config>service>vprn>igmp** (or **mld**) context.

The **no** form of this command reverts to the default value.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time to wait to receive a host-query message response from the host.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface query-response-interval
- configure service vprn mld group-interface query-response-interval
- configure router igmp group-interface query-response-interval
- configure router mld group-interface query-response-interval

All

- configure service vprn igmp query-response-interval

query-response-interval

Syntax **query-response-interval** *seconds*
no query-response-interval

Context **[Tree]** (config>router>mld query-response-interval)
[Tree] (config>router>mld>if query-response-interval)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mld interface query-response-interval
configure router mld query-response-interval

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

The **no** form of this command reverts to the default value.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 to 1023

Platforms All

query-response-interval

Syntax **query-response-interval** *seconds*
no query-response-interval

Context **[Tree]** (config>router>igmp query-response-interval)
[Tree] (config>router>igmp>if query-response-interval)

Full Context configure router igmp interface query-response-interval
configure router igmp query-response-interval

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 to 1023

Platforms All

query-response-interval

Syntax **query-response-interval** *seconds*
no query-response-interval

Context **[Tree]** (config>subscr-mgmt>igmp-policy query-response-interval)

Full Context configure subscriber-mgmt igmp-policy query-response-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the query response interval. If nothing is configured, by default, the **query-response-interval** takes the value defined in the **config>router>igmp** context or in the **config>service>vprn>igmp** context. It is highly recommended that all three query intervals be configured together on each IGMP policy.

The **no** form of this command reverts to the default value.

Parameters *seconds* — Specifies the length of time, in seconds, that the querier router waits to receive a response to from the host.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-response-interval

Syntax **query-response-interval** *seconds*

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp query-response-interval)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping query-response-interval

Description This command configures the IGMP query response interval. If the **send-queries** command is enabled, this parameter specifies the maximum response time advertised in IGMPv2/v3 queries.

The configured query-response-interval must be smaller than the configured **query-interval**.

If **send-queries** is not enabled on an MSAP or SDP, the configured query-response-interval value is ignored.

The **no** form of this command reverts to the default.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time, in seconds, to wait to receive a response to the host-query message from the host.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-response-interval

Syntax **query-response-interval** *seconds*
no query-response-interval

Context **[Tree]** (config>subscr-mgmt>mld-policy query-response-interval)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt mld-policy query-response-interval

Description This command configures the query response interval. If nothing is configured, by default, the **query-response-interval** takes the value defined in the **config>router>mld** context or in the **config>service>vprn>mld** context. It is highly recommended that all three query intervals be configured together on each MLD policy.

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the length of time that the querier router waits to receive a response to from the host.

Values 1 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-response-interval

Syntax **query-response-interval** *seconds*

Context **[Tree]** (config>service>vprn>mld query-response-interval)
[Tree] (config>service>vprn>mld>if query-response-interval)

Full Context configure service vprn mld interface query-response-interval
configure service vprn mld query-response-interval

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 to 1023

Platforms All

query-response-interval

Syntax **query-response-interval** *seconds*
no query-response-interval

Context **[Tree]** (config>service>pw-template>igmp-snooping query-response-interval)

Full Context configure service pw-template igmp-snooping query-response-interval

Description This command configures the IGMP query response interval. If the **send-queries** command is enabled, this parameter specifies the maximum response time advertised in IGMPv2/v3 queries.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured **query-response-interval** must be smaller than the configured **query-interval**.

If **send-queries** is not enabled on this SAP or SDP, the configured **query-response-interval** value is ignored.

Default query-response-interval 10

Parameters *seconds* — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 to 1023

Platforms All

21.19 query-src-ip

query-src-ip

Syntax **query-src-ip** *ip-address*
no query-src-ip

Context **[Tree]** (config>service>vpls>igmp-snooping query-src-ip)

Full Context configure service vpls igmp-snooping query-src-ip

Description This command configures the IP source address used in IGMP or MLD queries.

The **no** form of this command removes the IP address from this configuration.

Parameters *ip-address* — Specifies an IPv4 address in the form of a.b.c.d or an IPv6 address in the following form:

x:x:x:x:x:x:x:x:x:x:x:x:d.d.d.d
where:
x - [0 to FF]
d - [0 to 255]

Platforms All

query-src-ip

Syntax **query-src-ip** *ipv6-address*
no query-src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>mld-snooping query-src-ip)

Full Context configure service vpls mld-snooping query-src-ip

Description This command configures the IP source address used in MLD queries.

Parameters *ipv6-address* — Specifies an IPv6 address in the following form:

x:x:x:x:x:x:x:x (eight 16-bit pieces)

Platforms All

query-src-ip

Syntax **query-src-ip** *ip-address*
no query-src-ip

Context [Tree] (config>service>vprn>igmp>grp-if query-src-ip)

Full Context configure service vprn igmp group-interface query-src-ip

Description This command configures the query source IP address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of this command removes the IP address.

Parameters *ip-address* — Sets the source IPv4 address for all subscriber's IGMP queries.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

query-src-ip

Syntax **query-src-ip** *ip-address*
no query-src-ip

Context [Tree] (config>router>igmp>group-interface query-src-ip)

Full Context configure router igmp group-interface query-src-ip

Description This command configures the query source IP address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of the command removes the IP address.

Parameters *ip-address* — Sets the source IPv4 address for all subscriber's IGMP queries.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

query-src-ip

Syntax **query-src-ip** *ipv6-address*
no query-src-ip

Context **[Tree]** (config>router>mld>group-interface query-src-ip)

Full Context configure router mld group-interface query-src-ip

Description This command configures the query source IPv6 address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of this command removes the IPv6 address.

Parameters *ipv6-address* — Sets the source IPv6 address for all subscriber's MLD queries.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

21.20 queue

queue

Syntax **queue** *queue-id* {**ingress-only** | **egress-only** | **ingress-egress**}
no queue *queue-id*

Context **[Tree]** (config>subscr-mgmt>cat-map>category queue)

Full Context configure subscriber-mgmt category-map category queue

Description This command configures a queue in this category.

The **no** form of this command reverts to the default.

Parameters *queue-id* — Specifies the queue ID for this instances. Each queue nominated in the category map is monitored for activity (over a period of approximately 60 seconds), should the activity fall below the threshold value then a time is started. Whenever this timer exceeds the configured timeout under the idle-timeout the action (currently disconnect) is executed for that subscriber and all hosts under that given SLA-profile-instance.

Values 1 to 32

ingress-only — Specifies that ingress queues are defined in this category.

egress-only — Specifies that egress queues are defined in this category.

ingress-egress — Specifies that ingress and egress queues are defined in this category.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr queue)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue

Description This command specifies the queue-id for which counters are collected in this custom record. The counters that are collected are defined in egress and ingress counters.

The **no** form of this command reverts to the default value.

Parameters *queue-id* — Specifies the queue-id for which counters are collected in this custom record.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

queue

Syntax [**no**] **queue** *queue-id*

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos queue)
[Tree] (config>subscr-mgmt>sla-prof>ingress>qos queue)

Full Context configure subscriber-mgmt sla-profile egress qos queue
configure subscriber-mgmt sla-profile ingress qos queue

Description Commands in this context configure egress or ingress queue parameters. Parameters defined in the **config>qos>sap-egress** *policy-id* or the **config>qos>sap-ingress** *policy-id* context are overridden by parameters specified in the subscriber management SLA profile context.

The classification and the queue mapping are shared by all the hosts on the same complex that use the same QoS policy (specified in the **sla-profile** SAP egress and SAP ingress policy IDs).

The queues are shared by all the hosts (of the same subscriber) on the same SAP that are using the same SLA profile. Queues are instantiated when, on a given SAP, a host of a subscriber is the first to use a certain SLA profile. This instantiation is referred to as an SLA profile instance.

The **no** form of this command removes the *queue-id* from the SLA profile.

Parameters *queue-id* — Specifies the queue ID for the SAP egress or ingress queue, expressed as a decimal integer. The ID uniquely identifies the queue within the profile.

Values 1 to 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override queue)
[Tree] (config>service>ies>if>sap>ingress>queue-override queue)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress>queue-override queue)
[Tree] (config>service>vpls>sap>egress>queue-override queue)
[Tree] (config>service>vpls>sap>ingress>queue-override queue)

Full Context configure service ies interface sap egress queue-override queue
configure service ies interface sap ingress queue-override queue
configure service ies subscriber-interface group-interface sap egress queue-override queue
configure service vpls sap egress queue-override queue
configure service vpls sap ingress queue-override queue

Description This command specifies the ID of the queue whose parameters are to be overridden.

The **no** form of this command removes the queue ID from the configuration.

Parameters *queue-id* — Specifies the queue ID whose parameters are to be overridden.

Values 1 to 8 for SAP egress
1 to 32 for SAP ingress

create — Keyword used to create the queue ID. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover queue)
[Tree] (config>port>eth>network>egr>qgrp>qover queue)

Full Context configure port ethernet network egress queue-group queue-overrides queue
configure port ethernet access egress queue-group queue-overrides queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command associates a queue for use in a queue group template. The defined queue-id acts as a repository for the default parameters for the queue. The template queue is created on each queue-group object which is created with the queue group template name. Each queue is identified within the template by a queue-id number. The template ensures that all queue groups created with the template's name will have the same queue-ids providing a uniform structure for the forwarding class redirection commands in the SAP egress QoS policies. The parameters within the template queue will be used as the default settings for each queue in the actual queue group. The queue parameters may be individually changed for each queue in each queue group using per queue overrides.

The **no** form of this command removes the queue-id from the configuration.

Parameters *queue-id* — Specifies the queue ID.

Values 1 to 8

create — Mandatory when creating an entry.

Platforms All

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>port>ethernet>access>ing>qgrp>qover queue)

Full Context configure port ethernet access ingress queue-group queue-overrides queue

Description This command associates a queue for use in a queue group template. The defined queue-id acts as a repository for the default parameters for the queue. The template queue is created on each queue-group object which is created with the queue group template name. Each queue is identified within the template by a queue-id number. The template ensures that all queue groups created with the template's name will have the same queue-ids providing a uniform structure for the forwarding class redirection commands in the SAP egress QoS policies. The parameters within the template queue will be used as the default settings for each queue in the actual queue group. The queue parameters may be individually changed for each queue in each queue group using per queue overrides.

The **no** form of this command removes the queue-id from the configuration.

Parameters *queue-id* — Specifies the queue ID.

Values 1 to 32

create — Mandatory when creating an entry.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>service>apipe>sap>egress>queue-override queue)
[Tree] (config>service>apipe>sap>ingress>queue-override queue)
[Tree] (config>service>cpipe>sap>egress>queue-override queue)
[Tree] (config>service>cpipe>sap>ingress>queue-override queue)
[Tree] (config>service>epipe>sap>egress>queue-override queue)
[Tree] (config>service>epipe>sap>ingress>queue-override queue)
[Tree] (config>service>fpipe>sap>egress>queue-override queue)
[Tree] (config>service>fpipe>sap>ingress>queue-override queue)
[Tree] (config>service>ipipe>sap>egress>queue-override queue)
[Tree] (config>service>ipipe>sap>ingress>queue-override queue)

Full Context configure service apipe sap egress queue-override queue
configure service apipe sap ingress queue-override queue
configure service cpipe sap egress queue-override queue
configure service cpipe sap ingress queue-override queue
configure service epipe sap egress queue-override queue
configure service epipe sap ingress queue-override queue
configure service fpipe sap egress queue-override queue
configure service fpipe sap ingress queue-override queue
configure service ipipe sap egress queue-override queue
configure service ipipe sap ingress queue-override queue

Description This command specifies the ID of the queue whose parameters are to be overridden.

Parameters *queue-id* — The queue ID whose parameters are to be overridden.

Values 1 to 32

create — This keyword is mandatory when creating a queue.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress queue-override queue
- configure service cpipe sap ingress queue-override queue
- configure service fpipe sap ingress queue-override queue
- configure service cpipe sap egress queue-override queue

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue
- configure service apipe sap ingress queue-override queue

All

- configure service ipipe sap egress queue-override queue
- configure service ipipe sap ingress queue-override queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap egress queue-override queue
- configure service epipe sap ingress queue-override queue

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override queue)
[Tree] (config>service>vprn>if>sap>ingress>queue-override queue)

Full Context configure service vprn interface sap egress queue-override queue
configure service vprn interface sap ingress queue-override queue

Description This command specifies the ID of the queue whose parameters are to be overridden.

Parameters *queue-id* — Specifies the queue ID whose parameters are to be overridden.

Values 1 to 32

create — Keyword used to create the group override instance.

Platforms All

queue

Syntax **queue** *queue-id* [**group** *queue-group-name*]
no queue

Context **[Tree]** (config>qos>sap-ingress>fc queue)

Full Context configure qos sap-ingress fc queue

Description This command overrides the default queue mapping for **fc** fc-name. The specified queue-id must exist within the policy before the mapping can be made. When the forwarding class mapping is executed, all traffic classified to fc-name on a SAP using this policy.

The **no** form of this command sets the queue-id back to the default queue for the forwarding class.

Default queue 1

Parameters *queue-id* — Specifies the SAP egress queue-id to be associated with the forwarding class. The queue-id must be an existing queue defined in sap-egress policy-id.

Values 1 — 8

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

group *queue-group-name* — This optional parameter is used to redirect the forwarding type within the forwarding class to the specified *queue-id* within the *queue-group-name*. When the policy is applied, all packets matching the forwarding class and forwarding type will be redirected to the queue within the specified queue group. The queue-group-name are configured in the **config>qos>queue-group-templates** egress and ingress contexts. This parameter is used when policy-based queue group redirection is desired. That is, the specific queue group to redirect to is named in the QoS policy.

Platforms All

queue

Syntax **queue** *queue-id* [**multipoint**] [*queue-type*] [*queue-mode*] [**create**]
no queue *queue-id*

Context **[Tree]** (config>qos>sap-ingress queue)

Full Context configure qos sap-ingress queue

Description This command creates the context to configure an ingress SAP QoS policy queue.

Explicit definition of an ingress queue's type is supported. A single ingress queue allows support for multiple forwarding classes. The default behavior automatically chooses the expedited or best effort nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any best effort forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort (be) by the hardware schedulers. The queue type must be defined at the time of queue creation within the policy.

The **queue** command allows the creation of multipoint queues. Only multipoint queues can receive ingress packets that need flooding to multiple destinations. By separating the unicast for multipoint traffic at service ingress and handling the traffic on separate multipoint queues, special handling of the multipoint traffic is possible. Each queue acts as an accounting and (optionally) shaping device offering precise control over potentially expensive multicast, broadcast, and unknown unicast traffic. Only the back-end support of multipoint traffic (between the forwarding class and the queue based on forwarding type) needs to be defined. The individual classification rules used to place traffic into forwarding classes are not affected. Queues must be defined as multipoint at the time of creation within the policy.

The multipoint queues are for multipoint-destined service traffic. Within non-multipoint services, such as Epipe services, all traffic is considered unicast due to the nature of the service type. Multicast and broadcast-destined traffic in an Epipe service will not be mapped to a multipoint service queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an ingress SAP QoS policy with multipoint queues is applied to an Epipe SAP, the multipoint queues are not created. When an ingress SAP QoS policy with multipoint queues is applied to an IES SAP, a multipoint queue will be created when PIM is enabled on the IES interface.

Any billing or statistical queries about a multipoint queue on a non-multipoint service returns zero values. Any queue parameter information requested about a multipoint queue on a non-multipoint service returns the queue parameters in the policy. Buffers will not be allocated for multipoint queues on non-multipoint services. Buffer pool queries return zero values for actual buffers allocated and current buffer utilization.

The **no** form of this command removes the *queue-id* from the SAP ingress QoS policy and from any existing SAPs using the policy. If any forwarding class forwarding types are mapped to the queue, they revert to their default queues. When a queue is removed, any pending accounting information for each SAP queue created due to the definition of the queue in the policy is discarded.

Parameters *queue-id* — The *queue-id* for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 32

queue-type — The **expedite**, **best-effort**, and **auto-expedite** queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. A keyword can be specified at the time the queue is created. If an attempt to change the keyword after the queue is initially defined, an error is generated.

Values expedite, best-effort, auto-expedite

expedite — This keyword ensures that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

best-effort — This keyword ensures that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

auto-expedite — This keyword allows the system to auto-define the way the queue is serviced by the hardware. When **auto-expedite** is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types nc, ef, h1 or h2. When a single non-expedited forwarding class is mapped to the queue (be, af, l1, and l2), the queue automatically falls back to non-expedited status.

Default auto-expedite

multipoint — This optional keyword specifies that this *queue-id* is for multipoint forwarded traffic only. This *queue-id* can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. If forwarding class unicast traffic is mapped to a multipoint queue, an error is generated and no changes are made to the current unicast traffic queue mapping.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A queue must be created as multipoint. The **multipoint** designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the **multipoint** keyword, an error is generated and the command will not execute.

The **multipoint** keyword can be entered in the command line on a preexisting multipoint queue to edit *queue-id* parameters.

Default non-multipoint (unicast queue)

queue-mode — Specifies the mode in which the queue is operating. This attribute is associated with the queue at the time of creation and cannot be modified thereafter.

Values **profile-mode**: When the queue is operating in the profile mode (or the color aware mode), the queue tries to provide the appropriate bandwidth to the packets with different profiles. The profiles are assigned according to the configuration of the forwarding class or the sub-forwarding class.

priority-mode: The queue is capable of handling traffic differently with two distinct priorities. These priorities are assigned by the stages preceding the queueing framework in the system. In priority mode, the queue does not have the functionality to support the profiled traffic and in such cases the queue will have a degraded performance. However, the converse is not valid and a queue in-profile mode should be capable of supporting the different priorities of traffic.

Default priority-mode

create — Keyword creates an ingress SAP QoS policy queue.

Platforms All

queue

Syntax **queue** *queue-id* [{**group** *queue-group-name* [**instance** *instance-id*] | **port-redirect-group-queue**}]
no queue

Context **[Tree]** (config>qos>sap-egress>fc queue)

Full Context configure qos sap-egress fc queue

Description This command overrides the default queue mapping for **fc** fc-name. The specified queue ID must exist within the policy before the mapping can be made. When the forwarding class mapping is executed, all traffic is classified to fc-name on a SAP using this policy.

The **no** form of this command sets the queue-id back to the default queue for the forwarding class (queue 1).

Default no queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *queue-id* — Specifies the SAP egress queue-id to be associated with the forwarding class. The queue-id must be an existing queue defined in sap-egress policy-id.

Values 1 to 8

Default 1

queue-group-name — This optional parameter is used to redirect the forwarding type within the forwarding class to the specified *queue-id* within the *queue-group-name*. When the policy is applied, all packets matching the forwarding class and forwarding type will be redirected to the queue within the specified queue group. The queue-group-name are configured in the **config>qos>queue-group-templates** egress and ingress contexts. This parameter is used when policy-based queue group redirection is desired. That is, the specific queue group to redirect to is named in the QoS policy.

instance-id — This parameter is used to specify the specific instance of a queue group with template queue-group-name to which this queue should be redirected. This parameter is only valid for queue groups on egress ports where policy-based redirection is required.

Values 1 to 40960

Default 1

port-redirect-group-queue — This keyword is used to mark a given forwarding class queue for redirection to an egress queue group queue. This is only used when the specific queue group instance is assigned at the time the QoS policy is applied to the SAP. This redirection model is known as SAP-based redirection.

Platforms All

queue

Syntax **queue** *queue-id* [*queue-type*] [**create**]
no queue *queue-id*

Context **[Tree]** (config>qos>sap-egress queue)

Full Context configure qos sap-egress queue

Description This command creates the context to configure an egress service access point (SAP) QoS policy queue.

Explicit definition of an egress queue's type is supported. A single egress queue allows support for multiple forwarding classes. The default behavior automatically chooses the expedited or best effort nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any best effort forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort by the hardware schedulers. The queue type must be defined at the time of queue creation within the policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the *queue-id* from the SAP egress QoS policy and from any existing SAPs using the policy. If any forwarding class forwarding types are mapped to the queue, they revert to their default queues. When a queue is removed, any pending accounting information for each SAP queue created due to the definition of the queue in the policy is discarded.

Parameters *queue-id* — The ID for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 32

queue-type — Specifies the method that system uses to service the queue from a hardware perspective. A keyword can be specified at the time the queue is created. If an attempt is made to change the keyword after the queue is initially defined, an error is generated.

Values **expedite** - Specifies that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

best-effort - Specifies that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

auto-expedite - Allows the system to auto-define the way the queue is serviced by the hardware. When **auto-expedite** is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types nc, ef, h1, or h2. When a single non-expedited forwarding class is mapped to the queue (be, af, l1, and l2), the queue automatically falls back to non-expedited status.

Default auto-expedite

create — Creates an entry for the queue.

Platforms All

queue

Syntax **queue** *queue-id* **sched-class** *class-id*
queue *queue-id* **unattached**
queue *queue-id* **wrr-group** *wrr-group-id*
no queue *queue-id*

Context **[Tree]** (config>qos>hs-attachment-policy queue)

Full Context configure qos hs-attachment-policy queue

Description This command defines how the specified queue-id is attached to the scheduler. A queue may have one of four attachment states:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- directly attached to a scheduler class
- attached to a WRR group which is attached to a scheduler class
- attached to a WRR group which is unattached
- unattached

The following items are rules for attachment:

- Only one queue or WRR group can be attached to a given scheduling class. If another queue or a WRR group is currently attached to the specified scheduling class, the queue's attachment command fails and the current attachment for the *queue-id* is unchanged.
- Queues must be attached to scheduler classes (directly or indirectly through a WRR group) in an ascending order.

  For example, if queue 3 is attached to scheduler class 2, queues 1 and 2 cannot be attached to scheduling classes 3 through 6 (or attached to a WRR group that is attached to scheduling classes 3 through 6).
- Up to six queues can be placed in any WRR group. These queues can all be in one WRR group or be spread between both WRR groups. Attempting to execute the **wrr-group** keyword on a seventh queue within the attachment policy fails.
- Queues must attach to WRR groups in contiguous order.
- WRR group 1 must have lower queue ID members than WRR group 2. Attempting to attach a queue ID to group 1 that is higher than any queue ID currently attached to group 2 fails with no change to the current attachment state for that queue ID. Attempting to attach a queue ID to group 2 that is lower than any queue ID currently attached to group 1 fails with no change to the current attachment state for that queue ID.
- WRR group 1 must have at least one attached member queue before queues can be attached to WRR group 2.
- Queues and WRR groups can be unattached at any time.
  - Unattached queues, or queues attached to an unattached WRR group, discard all received packets. Normal discard accounting is maintained.
  - The unattached state for an in-service queue or WRR group is intended for **hs-attachment-policy** editing purposes and is expected to be an intermediate state in this case.

When an **hs-attachment-policy** is initially created, all queues and both WRR groups default to the unattached state. Each queue and WRR group attachment state must be explicitly configured.

The **no** form of the command reverts to the default unattached attachment state for queue ID. The command fails if the specified *queue-id* is currently in a WRR group and removing the queue from that group causes the queue IDs for that group to become discontinuous.

Default queue *queue-id* unattached

Parameters *queue-id* — Specifies the queue identifier for the HS attachment policy queue. This parameter is required when executing the command.

Values 1 to 8

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sched-class — Specifies a direct attachment between the *queue-id* and one of the six scheduling classes. A value of 1 through 6 must accompany the **sched-class** keyword representing the queue's attached scheduling class. The **sched-class**, **group**, and **unattached** keywords are mutually exclusive. One of the keywords must be specified when the **queue** attachment command is executed.

class-id — Specifies the scheduling class that is associated with this *queue-id*.

Values 1 to 6

wrr-group — Specifies the inclusion of the *queue-id* in either WRR group 1 or WRR group 2. A value of 1 or 2 must accompany the **wrr-group** keyword representing the queue's attached WRR group number. Queues placed in a WRR group must have contiguous queue IDs. The **sched-class**, **group**, and **unattached** keywords are mutually exclusive. One of the keywords must be specified when the **queue** attachment command is executed.

wrr-group-id — Specifies the WRR group to which the queue-id is to be attached.

Values 1, 2

unattached — Indicates that the *queue-id* is not attached to any scheduling class or WRR group. An unattached queue does not forward any packets. The **sched-class**, **group**, and **unattached** keywords are mutually exclusive. One of the keywords must be specified when the **queue** attachment command is executed.

Platforms 7750 SR-7/12/12e

queue

Syntax **queue** *queue-id* [**multipoint**] [*queue-type*] [**create**]
no queue *queue-id*

Context **[Tree]** (config>qos>network-queue>fc queue)

Full Context configure qos network-queue fc queue

Description Commands in this context configure a QoS network-queue policy queue.

Explicit definition of an ingress queue's type status is supported. A single ingress queue allows support for multiple forwarding classes. The default behavior automatically chooses the expedited or best effort nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any best effort forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort (be) by the hardware schedulers. The queue type must be defined at the time of queue creation within the policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **queue** command allows the creation of multipoint queues. Only multipoint queues can receive ingress packets that need flooding to multiple destinations. By separating the unicast for multipoint traffic at service ingress and handling the traffic on separate multipoint queues, special handling of the multipoint traffic is possible. Each queue acts as an accounting and (optionally) shaping device offering precise control over potentially expensive multicast, broadcast, and unknown unicast traffic. Only the back-end support of multipoint traffic (between the forwarding class and the queue based on forwarding type) needs to be defined. The individual classification rules used to place traffic into forwarding classes are not affected. Queues must be defined as multipoint at the time of creation within the policy.

The multipoint queues are for multipoint traffic.

The multipoint queues are for multipoint-destined service traffic. Within non-multipoint services, such as Epipe services, all traffic is considered unicast due to the nature of the service type. Multicast and broadcast-destined traffic in an Epipe service will not be mapped to a multipoint service queue.

When a QoS policy with multipoint queues is applied to an Epipe or IES SAP, the multipoint queues are not created. Any billing or statistical queries about a multipoint queue on a non-multipoint service returns zero values. Any queue parameter information requested about a multipoint queue on a non-multipoint service returns the queue parameters in the policy. Buffers will not be allocated for multipoint queues on non-multipoint services. Buffer pool queries return zero values for actual buffers allocated and current buffer utilization.

The **no** form of this command removes the *queue-id* from the network-queue policy and from any existing SAPs using the policy. If any forwarding class forwarding types are mapped to the queue, they revert to their default queues. When a queue is removed, any pending accounting information for each SAP queue created due to the definition of the queue in the policy is discarded.

Parameters *queue-id* — The *queue-id* for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 32

multipoint — This optional keyword specifies that this *queue-id* is for multipoint forwarded traffic only. This *queue-id* can only be used to forward multicast, broadcast, or unknown unicast ingress traffic.

A queue must be created as multipoint. The **multipoint** designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the **multipoint** keyword, an error is generated, and the command will not execute.

The **multipoint** keyword can be entered in the command line on a preexisting multipoint queue to edit *queue-id* parameters.

Default Non-multipoint (unicast queue)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue-type — The **expedite**, **best-effort**, and **auto-expedite** queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. While parental virtual schedulers can be defined for the queue, they only enforce how the queue interacts for bandwidth with other queues associated with the same scheduler hierarchy. An internal mechanism that provides access rules when the queue is vying for bandwidth with queues in other virtual schedulers is also needed. A keyword must be specified at the time the queue is created in the network-queue policy. If an attempt is made to change the keyword after the queue is initially defined, an error is generated.

Values expedite, best-effort, auto-expedite

expedite — This keyword ensures that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

best-effort — This keyword ensures that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

auto-expedite — This keyword allows the system to auto-define the way the queue is serviced by the hardware. When **auto-expedite** is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types nc, ef, h1 or h2. When a single non-expedited forwarding class is mapped to the queue (be, af, l1, and l2), the queue automatically falls back to non-expedited status.

Default auto-expedite

Platforms All

queue

Syntax **queue** *queue-id* [**multipoint**] [*queue-type*] [*queue-mode*] [**create**]
no queue *queue-id*

Context **[Tree]** (config>qos>qgrps>ing>queue-group queue)

Full Context configure qos queue-group-templates ingress queue-group queue

Description This command creates a queue for use in a queue group template. When created, the defined queue-id acts as a repository for the default parameters for the queue. The template queue is created on each queue-group object that is created with the queue group template name. Each queue is identified within the template by a queue-id number. The template ensures that all queue groups created with the template name will have the same queue-ids providing a uniform structure for the forwarding class redirection commands in the SAP ingress QoS policies. The parameters within the template queue will be used as the default settings for each queue in the actual queue group. The queue parameters may be individually changed for each queue in each queue group using per queue overrides.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a queue within a template is mapped by a forwarding class on any object, the queue may be edited, but not deleted.

The **no** form of this command removes a template queue from the queue group template. If the queue is specified as a forwarding class redirection target in any SAP ingress QoS policy, the command will fail.

Parameters *queue-id* — This required parameter identifies the queue that will either be created or edited within the queue group template.

Values 1 to 32

multipoint — This optional keyword creates an ingress multipoint queue. Multipoint queues in a queue group may be used by ingress VPLS for forwarding types multicast, broadcast or unknown within a forwarding class. For ingress IES and VPRN access SAPs, only multicast is supported. Multipoint queues are only supported on ingress queue group templates.

Default non-multipoint (unicast queue)

queue-type — The queue types are mutually exclusive.

Values **expedite —** This keyword ensures that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

best-effort — This keyword ensures that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

Default best-effort

queue-mode — These keywords are optional and mutually exclusive when creating a new template queue. The keywords specify how the queue manages ingress explicitly profiled packets.

Values **profile-mode** — Overrides the default priority mode of the queue and allows the adoption of color aware profiling within the queue. Forwarding classes and subclasses may be explicitly defined as in-profile or out-of-profile. Out-of-profile classified packets bypass the CIR rate associated with the queue, reserving it for the undefined or in-profile classified packets. If the template queue is not defined as profile-mode and the packet redirected to the queue is explicitly out-of-profile based on the classification rules, the queues within-CIR bandwidth may be consumed by the packet.

priority-mode — Defines that the SAP ingress QoS policy priority classification result will be honored by the queue. Priority mode is the default mode of the queue. High-priority packets are allowed into the queue up to the MBS defined for the queue. Low-priority packets are discarded at the low-priority MBS threshold that is derived from applying the low drop-tail percentage to the queue's MBS.

create — Keyword used to create the queue ID instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue

Syntax **queue** *queue-id*
no queue

Context **[Tree]** (config>qos>qgrps>egr>queue-group-template>fc queue)

Full Context configure qos queue-group-templates egress queue-group-template fc queue

Description This command is used to map the forwarding class to the specified *queue-id*. The specified *queue-id* must exist within the egress queue group template. When a queue is defined in a forwarding class mapping, that queue cannot be deleted unless the forwarding class mapping is moved to another queue within the template. Other criteria may also exist preventing the queue from being deleted from the template such as an applied SAP egress QoS policy mapping to the queue.

Parameters *queue-id* — The specified *queue-id* must exist within the egress queue group template.

Values 1 to 8

queue

Syntax **queue** *queue-id* [*queue-type*] [**create**]
no queue *queue-id*

Context **[Tree]** (cfg>qos>qgrps>egr>queue-group queue)

Full Context configure qos queue-group-templates egress queue-group queue

Description This command creates a queue for use in a queue group template. When created, the defined *queue-id* acts as a repository for the default parameters for the queue. The template queue is created on each queue group object that is created with the queue group template name. Each queue is identified within the template by a queue ID. The template ensures that all queue groups created with the template name will have the same queue-ids providing a uniform structure for the forwarding class redirection commands in the SAP egress QoS policies. The parameters within the template queue will be used as the default settings for each queue in the actual queue group. The queue parameters may be individually changed for each queue in each queue group using per queue overrides.

Parameters *queue-id* — Specifies the queue ID. The specified *queue-id* must exist within the egress queue group template.

Values 1 to 8

queue-type — Specifies the method that the system uses to service the queue from a hardware perspective.

Values expedite, best-effort

expedite — This keyword ensures that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

best-effort — This keyword ensures that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

Default best-effort

Platforms All

queue

Syntax **queue** *queue-id*
no queue

Context **[Tree]** (config>qos>shared-queue>fc queue)

Full Context configure qos shared-queue fc queue

Description This command overrides the default unicast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a non-multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all unicast traffic (this includes all traffic, even broadcast and multicast for services) on a SAP using this policy is forwarded using the *queue-id*.

The **no** form of this command sets the unicast (point-to-point) *queue-id* back to the default queue for the forwarding class (queue 1).

Parameters *queue-id* — The *queue-id* parameter specified must be an existing non-multipoint queue defined in the **config>qos>sap-ingress** context. For the 7950 XRS, this is not configurable in the policer-output-queues profile.

Values Any valid non-multipoint *queue-id* in the policy including 1 and 3 through 32.

Default 1

Platforms All

queue

Syntax **queue** *queue-id* [*queue-type*] [**multipoint**] [**create**]
no queue *queue-id*

Context **[Tree]** (config>qos>shared-queue queue)

Full Context configure qos shared-queue queue

Description This command creates the context to configure a shared queue QoS policy queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Explicit definition of an ingress queue's type is supported. A single ingress queue allows support for multiple forwarding classes. The default behavior automatically chooses the expedited or best effort nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any best effort forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort by the hardware schedulers. The queue type can be overridden within the policy.

On the 7450 ESS, the expedited hardware schedulers are used to enforce expedited access to internal switch fabric destinations. The hardware status of the queue must be defined at the time of queue creation within the policy.

Parameters *queue-id* — The *queue-id* for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 32

queue-type — The **expedite**, **best-effort**, and **auto-expedite** queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. While parental virtual schedulers can be defined for the queue, they only enforce how the queue interacts for bandwidth with other queues associated with the same scheduler hierarchy. An internal mechanism that provides access rules when the queue is vying for bandwidth with queues in other virtual schedulers is also needed. A keyword must be specified at the time the queue is created in the SAP ingress policy. If an attempt to change the keyword after the queue is initially defined, an error is generated.

expedite — This keyword ensures that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

best-effort — This keyword ensures that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

auto-expedite — This keyword allows the system to auto-define the way the queue is serviced by the hardware. When auto-expedite is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types nc, ef, h1, or h2. When a single non-expedited forwarding class is mapped to the queue (be, af, l1, and l2) the queue automatically falls back to non-expedited status.

Default **auto-expedite**

multipoint — This keyword specifies that this *queue-id* is for multipoint forwarded traffic only. This *queue-id* can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. If forwarding class unicast traffic is mapped to a multipoint queue, an error is generated and no changes are made to the current unicast traffic queue mapping.

A queue must be created as multipoint. The **multipoint** designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the **multipoint** keyword, an error is generated and the command will not execute.

The **multipoint** keyword can be entered in the command line on a preexisting multipoint queue to edit *queue-id* parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

queue

Syntax [**no**] **queue** *queue-id*

Context **[Tree]** (config>log>acct-policy>cr queue)

Full Context configure log accounting-policy custom-record queue

Description This command specifies the queue-id for which counters will be collected in this custom record. The counters that will be collected are defined in egress and ingress counters.

The **no** form of this command reverts to the default value.

Parameters *queue-id* — Specifies the queue-id for which counters will be collected in this custom record.

Platforms All

queue

Syntax **queue** *queue-id* [**create**]

Context **[Tree]** (config>system>security>cpm-queue queue)

Full Context configure system security cpm-queue queue

Description This command allows users to allocate dedicated CPM. The first available queue is 33.

Parameters *queue-id* — 33 to 2000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

queue

Syntax **queue** *queue-id* [**create**]
no queue *queue-id*

Context **[Tree]** (config>port>ethernet>network>egress-port-queue-overrides queue)

Full Context configure port ethernet network egress-port-queue-overrides queue

Description This command configures an Ethernet network queue ID.

The **no** form of this command removes the Ethernet network queue ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *queue-id* — Specifies the Ethernet network queue ID.

Values 1 to 16

create — Keyword used to create an entry.

Platforms All

queue

Syntax **queue** *queue-id* [**multipoint**] [*queue-type*] [**create**]
no queue *queue-id*

Context **[Tree]** (config>qos>network-queue queue)

Full Context configure qos network-queue queue

Description This command enters the context to configure a QoS network-queue policy queue.

Explicit definition of an ingress queue's type status is supported. A single ingress queue allows support for multiple forwarding classes. The default behavior automatically chooses the expedited or best effort nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any best effort forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort (be) by the hardware schedulers. The queue type must be defined at the time of queue creation within the policy.

The **queue** command allows the creation of multipoint queues. Only multipoint queues can receive ingress packets that need flooding to multiple destinations. By separating the unicast for multipoint traffic at service ingress and handling the traffic on separate multipoint queues, special handling of the multipoint traffic is possible. Each queue acts as an accounting and (optionally) shaping device offering precise control over potentially expensive multicast, broadcast, and unknown unicast traffic. Only the back-end support of multipoint traffic (between the forwarding class and the queue based on forwarding type) needs to be defined. The individual classification rules used to place traffic into forwarding classes are not affected. Queues must be defined as multipoint at the time of creation within the policy.

The multipoint queues are for multipoint traffic.

The multipoint queues are for multipoint-destined service traffic. Within non-multipoint services, such as Epipe services, all traffic is considered unicast due to the nature of the service type. Multicast and broadcast-destined traffic in an Epipe service will not be mapped to a multipoint service queue.

When a QoS policy with multipoint queues is applied to an Epipe or IES SAP, the multipoint queues are not created. Any billing or statistical queries about a multipoint queue on a non-multipoint service returns zero values. Any queue parameter information requested about a multipoint queue on a non-multipoint service returns the queue parameters in the policy. Buffers will not be allocated for multipoint queues on non-multipoint services. Buffer pool queries return zero values for actual buffers allocated and current buffer utilization.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the *queue-id* from the network-queue policy and from any existing SAPs using the policy. If any forwarding class forwarding types are mapped to the queue, they revert to their default queues. When a queue is removed, any pending accounting information for each SAP queue created due to the definition of the queue in the policy is discarded.

Parameters *queue-id* — The *queue-id* for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 32

multipoint — This optional keyword specifies that this *queue-id* is for multipoint forwarded traffic only. This *queue-id* can only be used to forward multicast, broadcast, or unknown unicast ingress traffic.

A queue must be created as multipoint. The **multipoint** designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the **multipoint** keyword, an error is generated, and the command will not execute.

The **multipoint** keyword can be entered in the command line on a preexisting multipoint queue to edit *queue-id* parameters.

Default Non-multipoint (unicast queue)

queue-type — The **expedite**, **best-effort**, and **auto-expedite** queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. While parental virtual schedulers can be defined for the queue, they only enforce how the queue interacts for bandwidth with other queues associated with the same scheduler hierarchy. An internal mechanism that provides access rules when the queue is vying for bandwidth with queues in other virtual schedulers is also needed. A keyword must be specified at the time the queue is created in the network-queue policy. If an attempt is made to change the keyword after the queue is initially defined, an error is generated.

Values expedite, best-effort, auto-expedite

expedite — This keyword ensures that the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue.

best-effort — This keyword ensures that the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue.

auto-expedite — This keyword allows the system to auto-define the way the queue is serviced by the hardware. When **auto-expedite** is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types nc, ef, h1 or h2. When a single non-expedited forwarding class is mapped to the queue (be, af, l1, and l2), the queue automatically falls back to non-expedited status.

Default auto-expedite

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.21 queue-delay

queue-delay

Syntax **queue-delay** *delay*
no queue-delay

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue queue-delay)

Full Context configure qos queue-group-templates egress queue-group queue queue-delay

Description This command configures the target queue delay for packets forwarded through the queue. It is used to determine the related queue parameters based on the administrative PIR of the queue. This command and the **mbs** command are mutually exclusive.

In order to change between the **mbs** and **queue-delay** parameters, the current parameter must be removed before adding the new parameter; that is, changing from **mbs** to **queue-delay** requires a **no mbs** before the **queue-delay** is configured and changing from **queue-delay** to **mbs** requires a **no queue-delay** before the **mbs** is configured.

If **queue-delay** is configured for an egress queue group queue, it is not possible to override the MBS for that queue.

The **no** form of this command disables the determination of the queue parameters based on the queue delay.

Default no queue-delay

Parameters *delay* — Specifies the target queue delay in ms.

Values 0 to 5000 (decimal)

Platforms All

21.22 queue-frame-based-accounting

queue-frame-based-accounting

Syntax [**no**] **queue-frame-based-accounting**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>sap>egress>agg-rate queue-frame-based-accounting)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress>agg-rate queue-frame-based-accounting)
[Tree] (config>service>ies>if>sap>egress>agg-rate queue-frame-based-accounting)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface sap egress agg-rate queue-frame-based-accounting
configure service ies subscriber-interface group-interface sap egress agg-rate queue-frame-based-accounting
configure service vprn subscriber-interface group-interface sap egress agg-rate queue-frame-based-accounting

Description This command enables frame-based accounting on all queues associated with the **agg-rate** context. Only supported on Ethernet ports. Packet byte offset settings are not included in the applied rate when queue frame based accounting is configured, however the offsets are applied to the statistics.

The **no** form of this command disables frame-based accounting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap egress agg-rate queue-frame-based-accounting
- configure service vprn subscriber-interface group-interface sap egress agg-rate queue-frame-based-accounting

All

- configure service ies interface sap egress agg-rate queue-frame-based-accounting

queue-frame-based-accounting

Syntax [**no**] **queue-frame-based-accounting**

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>agg-rate queue-frame-based-accounting)
[Tree] (config>port>ethernet>access>egr>vport>agg-rate queue-frame-based-accounting)
[Tree] (config>port>ethernet>network>egr>qgrp>agg-rate queue-frame-based-accounting)
[Tree] (config>port>sonet-sdh>path>access>egress>vport queue-frame-based-accounting)

Full Context configure port ethernet access egress queue-group agg-rate queue-frame-based-accounting
configure port ethernet access egress vport agg-rate queue-frame-based-accounting
configure port ethernet network egress queue-group agg-rate queue-frame-based-accounting
configure port sonet-sdh path access egress vport queue-frame-based-accounting

Description This command enables frame based accounting on all policers and queues associated with the agg-rate context. It is only supported on Ethernet ports. Packet byte offset settings are not included in the applied rate when queue frame-based accounting is configured, regardless of how offsets are applied to the statistics.

The **no** form of this command disables frame based accounting on all policers and queues associated with the agg-rate context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue-frame-based-accounting

Syntax [**no**] **queue-frame-based-accounting**

Context **[Tree]** (config>service>epipe>sap>egress>agg-rate queue-frame-based-accounting)

Full Context configure service epipe sap egress agg-rate queue-frame-based-accounting

Description This command is used to enable (or disable) frame based accounting on all policers and queues associated with the agg-rate context.

The command is supported on Ethernet ports only.

Packet byte offset settings are not included in the applied rate when queue frame based accounting is configured; however the offsets are applied to the statistics.

Platforms All

queue-frame-based-accounting

Syntax [**no**] **queue-frame-based-accounting**

Context **[Tree]** (config>service>vpls>sap>egress>agg-rate queue-frame-based-accounting)
[Tree] (config>service>template>vpls-sap-template>egress>agg-rate queue-frame-based-accounting)

Full Context configure service template vpls-sap-template egress agg-rate queue-frame-based-accounting
configure service vpls sap egress agg-rate queue-frame-based-accounting

Description This command is used to enabled frame-based accounting on all policers and queues associated with the agg-rate context. Only supported on Ethernet ports. Packet byte offset settings are not included in the applied rate when queue frame based accounting is configured; however the offsets are applied to the statistics.

The **no** form of this command disables the-frame based accounting.

Platforms All

queue-frame-based-accounting

Syntax [**no**] **queue-frame-based-accounting**

Context **[Tree]** (config>service>vprn>if>sap>egress>agg-rate queue-frame-based-accounting)

Full Context configure service vprn interface sap egress agg-rate queue-frame-based-accounting

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to enabled (or disable) frame based accounting on all policers and queues associated with the agg-rate context. Only supported on Ethernet ports. Packet byte offset settings are not included in the applied rate when queue frame-based accounting is configured; the offsets are applied to the statistics.

Platforms All

queue-frame-based-accounting

Syntax [**no**] **queue-frame-based-accounting**

Context **[Tree]** (config>service>cust>multi-service-site>egress>agg-rate queue-frame-based-accounting)

Full Context configure service customer multi-service-site egress agg-rate queue-frame-based-accounting

Description This command enables frame based accounting on all policers and queues associated with the agg-rate context. Only supported on Ethernet ports. Packet byte offset settings are not included in the applied rate when queue frame based accounting is configured, however the offsets are applied to the statistics.

The **no** form of the command disables frame based accounting.

Default no queue-frame-based-accounting

Platforms All

21.23 queue-group

queue-group

Syntax **queue-group** *queue-group-name* **instance** *instance-id* [**create**]
no queue-group *queue-group-name* **instance** *instance-id*

Context **[Tree]** (config>card>fp>ingress>access queue-group)

Full Context configure card fp ingress access queue-group

Description This command creates an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM. The queue-group-name and **instance** *instance-id* are mandatory parameters when executing the command.

The named queue group template can contain only policers. If it contains queues, then the command will fail.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes a specific instance of a queue group.

Parameters *queue-group-name* — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM, up to 32 characters. The queue-group-name must correspond to a valid ingress queue group template name, configured under **config>qos>queue-group-templates**.

instance-id — Specifies the instance of the named queue group to be created on the IOM/IMM ingress forwarding plane.

Values 1 to 65535

create — Keyword used to associate the queue group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

queue-group

Syntax **queue-group** *queue-group-name* **instance** *instance-id* [**create**]
no queue-group *queue-group-name* **instance** *instance-id*

Context **[Tree]** (config>card>fp>ingress>network queue-group)

Full Context configure card fp ingress network queue-group

Description This command creates a queue-group instance in the network ingress context of a forwarding plane.

Only a queue-group containing policers can be instantiated. If the queue-group template contains policers and queues, the queues are not instantiated. If the queue-group contains queues only, the instantiation in the data path is failed.

One or more instances of the same policer queue-group name and/or a different policer queue-group name can be created on the network ingress context of a forwarding plane.

The queue-group-name must be unique within all network ingress and access ingress queue groups in the system. The queue-group instance-id must be unique within the context of the forwarding plane.

The **no** form of this command deletes the queue-group instance from the network ingress context of the forwarding plane.

Parameters *queue-group-name* — Specifies the name of the queue group template up to 32 characters.

instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

create — Keyword used to create the queue-group instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue-group

Syntax **queue-group** *queue-group-name* **instance** *instance-id*
no queue-group

Context **[Tree]** (config>port>ethernet>network>egress queue-group)

Full Context configure port ethernet network egress queue-group

Description This command configures a queue-group instance in the network egress context of a port.

Queue-groups containing queues only or policers and queues can be instantiated. When a port is a LAG, one instance of the queue-group is instantiated on each member link.

One or more instances of the same queue-group name and/or a different queue-group name can be created in the network egress context of a port.

The queue-group-name must be unique within all network egress and access egress queue groups in the system. The queue-group instance-id must be unique within the context of the port.

The **no** version of this command deletes the queue-group instance from the network egress context of the port.

Parameters *queue-group-name* — Specifies the name of the queue group template up to 32 characters.

instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

Platforms All

queue-group

Syntax [**no**] **queue-group** *queue-group-name* [**instance** *instance-id*] [**create**]

Context **[Tree]** (config>port>ethernet>access>egr queue-group)
[Tree] (config>port>ethernet>access>ing queue-group)

Full Context configure port ethernet access egress queue-group
configure port ethernet access ingress queue-group

Description This command creates an ingress or egress queue group on an Ethernet port. A queue group is a collection of queues identified by a group name. Queue groups created on access ports are used as an alternative queue destination for SAPs.

Within a SAP, a forwarding class may be redirected from the local SAP queue to a port queue group queue. The forwarding classes from multiple SAPs may be redirected to the same queue group which can be used to minimize the number of per-SAP queues.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Queue groups may be created on both access and network oriented ports. When the port is in access mode, the queue groups must be created within the port access node.

Within the access node, queue groups are also configured as ingress or egress. Access ingress queue groups can only be used by ingress SAP forwarding classes and only a single ingress queue group per port is supported. Multiple access egress queue groups may be created on a single port and are used by egress SAP forwarding classes. The instance-id parameter identifies different instances of the same queue group template. Creating multiple queue groups with a different instance ID but the same queue group name results in separate queue groups being created on the port. The instance-id parameter is only valid for egress queue groups on access ports.

When the queue group is created in an ingress port context, the group-name must be an existing ingress queue group template. Similarly, queue groups created in an egress port context must have a group-name of an existing egress queue group template. Two ingress queue groups with the same name cannot be created on the same port. Two egress queue groups can only be created on the same port with the same queue group template name if they have different instance-id values.

The queues defined in the template are created on the queue group. The queue parameters within the template are used as the default queue parameters for each queue in the queue group. The default queue parameters for each queue may be overridden on the queue group with specific queue parameters.

Each queue group supports the application of a scheduler-policy for the purpose of managing the queues within the group into an aggregate SLA. The queues defined within the template may be configured with parent scheduler defining the mapping of a queue to one of the schedulers within the scheduler policy. Egress queue groups also support the **agg-rate** parameter and the queues in the egress template support the port-parent command. Each command is used for configuring egress port virtual scheduling behavior.

Each queue group allows the application of an accounting policy and the ability to enable and disable collecting statistics. The statistics are derived from the queue counters on each queue within the queue group. The accounting policy defines which queue counters are collected and to which accounting file they will be written.

A queue group does not have an administrative shutdown or no shutdown command. A queue group is considered to be always on once created.

When creating a queue group, the system will attempt to allocate queue resources based on the queues defined in the queue group template. If the appropriate queue resources do not currently exist, the queue group will not be created. Ingress port queue groups do not support the shared-queuing or multipoint-shared queuing behavior.

When the queue group is created on a LAG (Link Aggregation Group), it must be created on the primary port member. The primary port member is the port with the lowest port ID based on the slot, MDA position and port number on the MDA. A queue group created on the primary LAG port will be automatically created on all other port members. If a new port is being added to a LAG with an existing queue group, the queue group must first be created on the port prior to adding the port to the LAG. If the LAG queue group has queue overrides, the queue overrides must also be defined on the port queue group prior to adding the port to the LAG.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A port queue group cannot be removed from the port when a forwarding class is currently redirected to the group. All forwarding class redirections must first be removed prior to removing the queue group.

Parameters *queue-group-name* — The group-name parameter is required when executing the port queue-group command. The specified group-name must exist as an ingress or egress queue group template depending on the ingress or egress context of the port queue group. Only a single queue group may be created on an ingress port. Multiple queue groups may be created on an egress port.

instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 to 65535

create — Keyword used to associate the queue group. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms All

queue-group

Syntax **queue-group** *queue-group-name* [**create**]
no queue-group *queue-group-name*

Context **[Tree]** (config>qos>qgrps>egress queue-group)
[Tree] (config>qos>qgrps>ingress queue-group)

Full Context configure qos queue-group-templates egress queue-group
configure qos queue-group-templates ingress queue-group

Description This command creates a queue group template. The system does not maintain default queue groups or queue group templates. Each queue group template used in the system must be explicitly created.

The **no** form of this command removes the specified queue group template from the system. If the queue group template is currently in use by an ingress port, the command will fail. If *queue-group-name* does not exist, the command has no effect and does not return an error.

Parameters *queue-group-name* — Specifies the name of the queue group template up to 32 characters. Each ingress queue group template must be uniquely named within the system. Multiple ingress queue group templates may not share the same name. An ingress and egress queue group template may share the same name.

create — Keyword used to create the queue group instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.24 queue-group-egress

queue-group-egress

Syntax **queue-group-egress** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy queue-group-egress)

Full Context configure qos copy queue-group-egress

Description This command copies an existing **queue-group-egress** *queue-group-name* to another **queue-group-egress** *queue-group-name*. The **copy** command is a configuration level maintenance tool used to create new entries using an existing mapping policy name. If **overwrite** is not specified, an error occurs if the destination policy exists.

Parameters *src-name* — Specifies the existing source **queue-group-egress** *queue-group-name*, up to 32 characters, from which the **copy** command attempts to copy.

dst-name — Specifies the destination **queue-group-ingress** *queue-group-name*, up to 32 characters, to which the copy command attempts to copy.

overwrite — Use this parameter when the **queue-group-egress** *dst-name* already exists. If it does, everything in the existing destination **queue-group-egress** *dst-name* is completely overwritten with the contents of the **queue-group-egress** *src-name*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI Destination "qge2" exists - use {overwrite}.
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms All

21.25 queue-group-ingress

queue-group-ingress

Syntax **queue-group-ingress** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy queue-group-ingress)

Full Context configure qos copy queue-group-ingress

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command copies an existing **queue-group-ingress** to another **queue-group-ingress**. The **copy** command is a configuration level maintenance tool used to create new entries using an existing mapping policy name. If **overwrite** is not specified, an error occurs if the destination policy exists.

Parameters *src-name* — Specifies the existing source **queue-group-ingress**, up to 32 characters, from which the **copy** command attempts to copy.

dst-name — Specifies the destination **queue-group-ingress**, up to 32 characters, to which the copy command attempts to copy.

overwrite — Use this parameter when the **queue-group-ingress** *dst-name* already exists. If it does, everything in the existing destination **queue-group-ingress** *dst-name* is completely overwritten with the contents of the **queue-group-ingress** *src-name*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI Destination "qgitest2" exists - use {overwrite}.
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms All

21.26 queue-group-redirect-list

queue-group-redirect-list

Syntax **queue-group-redirect-list** *redirect-list-name*
no queue-group-redirect-list

Context **[Tree]** (config>service>ies>if>sap>egress queue-group-redirect-list)
[Tree] (config>service>ies>if>sap>ingress queue-group-redirect-list)

Full Context configure service ies interface sap egress queue-group-redirect-list
configure service ies interface sap ingress queue-group-redirect-list

Description This command applies a queue group redirect list to the ingress or egress of an interface SAP within an IES or VPRN service. The redirect list is used to redirect traffic to different instances of the default queue group. This command requires the prior configuration of a default queue group instance, this being the queue group instance specified with the QoS policy under the SAP ingress or egress.

The **no** version of this command removes the queue group redirect list from the SAP.

Parameters *redirect-list-name* — Specifies the name of the queue group redirect list up to 32 characters in length.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

queue-group-redirect-list

Syntax **queue-group-redirect-list** *redirect-list-name*
no queue-group-redirect-list

Context **[Tree]** (config>service>vprn>if>sap>egress queue-group-redirect-list)
[Tree] (config>service>vprn>if>sap>ingress queue-group-redirect-list)

Full Context configure service vprn interface sap egress queue-group-redirect-list
configure service vprn interface sap ingress queue-group-redirect-list

Description This command applies a queue group redirect list to the ingress or egress of an interface SAP within a VPRN service. The redirect list is used to redirect traffic to different instances of the default queue group.

This command requires the prior configuration of a default queue group instance, which is the queue group instance specified with the QoS policy under the SAP ingress or egress.

The **no** version of this command removes the queue group redirect list from the SAP.

Parameters *redirect-list-name* — Specifies the name of the queue group redirect list, up to 32 characters in length.

Platforms All

queue-group-redirect-list

Syntax **queue-group-redirect-list** *redirect-list-name* [**create**]
no queue-group-redirect-list *redirect-list-name*

Context **[Tree]** (config>qos queue-group-redirect-list)

Full Context configure qos queue-group-redirect-list

Description This command configures a queue group redirect list that is used to redirect traffic to different instances of a queue group.

The **no** form of this command deletes the queue group redirect list. A list can only be deleted when there no references to it.

Parameters *redirect-list-name* — Specifies the name of the queue group redirect list, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.27 queue-group-templates

queue-group-templates

Syntax **queue-group-templates**

Context **[Tree]** (config>qos queue-group-templates)

Full Context configure qos queue-group-templates

Description Commands in this context define ingress and egress queue group templates.

Platforms All

21.28 queue-instance-accounting

queue-instance-accounting

Syntax **queue-instance-accounting** [**interim-update**]
no queue-instance-accounting

Context **[Tree]** (config>subscr-mgmt>acct-plcy queue-instance-accounting)

Full Context configure subscriber-mgmt radius-accounting-policy queue-instance-accounting

Description This command enables per queue-instance-accounting. A stream of accounting messages (START/INTERIM-UPDATE/STOP) is generated per queuing instance. A queuing instance is equivalent to an sla-profile instance. Accounting session id is generated per queuing instance and this accounting session id cannot be included in RADIUS Access-Request message. Queue instance counters represent volume based aggregation for all hosts sharing the queuing instance.

CoA and LI is supported based on the acct-session-id of the queuing instance.

The **no** form of this command reverts to the default.

Default queue-instance-accounting interim-update

Parameters **interim-update** — Specifies whether accounting messages are sent for the queue-instance. The queue-instance is the SLA profile instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.29 queue-override

queue-override

Syntax [**no**] **queue-override**

Context **[Tree]** (config>service>ies>if>sap>egress queue-override)
[Tree] (config>service>ies>if>sap>ingress queue-override)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress queue-override)
[Tree] (config>service>vpls>sap>egress queue-override)
[Tree] (config>service>vpls>sap>ingress queue-override)
[Tree] (config>service>vprn>if>sap>egress queue-override)
[Tree] (config>service>vprn>if>sap>ingress queue-override)

Full Context configure service ies interface sap egress queue-override
configure service ies interface sap ingress queue-override
configure service ies subscriber-interface group-interface sap egress queue-override
configure service vpls sap egress queue-override
configure service vpls sap ingress queue-override
configure service vprn interface sap egress queue-override
configure service vprn interface sap ingress queue-override

Description Commands in this context configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress QoS policy.

Platforms All

queue-override

Syntax [**no**] **queue-override**

Context **[Tree]** (config>service>apipe>sap>egress queue-override)
[Tree] (config>service>apipe>sap>ingress queue-override)
[Tree] (config>service>cpipe>sap>egress queue-override)
[Tree] (config>service>cpipe>sap>ingress queue-override)
[Tree] (config>service>epipe>sap>egress queue-override)
[Tree] (config>service>epipe>sap>ingress queue-override)
[Tree] (config>service>fpipe>sap>egress queue-override)
[Tree] (config>service>fpipe>sap>ingress queue-override)
[Tree] (config>service>ipipe>sap>egress queue-override)
[Tree] (config>service>ipipe>sap>ingress queue-override)

Full Context configure service apipe sap egress queue-override
configure service apipe sap ingress queue-override
configure service cpipe sap egress queue-override
configure service cpipe sap ingress queue-override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe sap egress queue-override
configure service epipe sap ingress queue-override
configure service fpipe sap egress queue-override
configure service fpipe sap ingress queue-override
configure service ipipe sap egress queue-override
configure service ipipe sap ingress queue-override

Description Commands in this context configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy. If the policy was created as a template policy, this command overrides the parameter and its description and queue parameters in the policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap ingress queue-override
- configure service fpipe sap egress queue-override
- configure service cpipe sap ingress queue-override
- configure service cpipe sap egress queue-override

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override
- configure service apipe sap ingress queue-override

All

- configure service epipe sap egress queue-override
- configure service ipipe sap egress queue-override
- configure service epipe sap ingress queue-override
- configure service ipipe sap ingress queue-override

21.30 queue-overrides

queue-overrides

Syntax **queue-overrides**

Context **[Tree]** (config>port>ethernet>access>egr>qgrp queue-overrides)
[Tree] (config>port>ethernet>access>ing>qgrp queue-overrides)
[Tree] (config>port>ethernet>network>egr>qgrp queue-overrides)

Full Context configure port ethernet access egress queue-group queue-overrides
configure port ethernet access ingress queue-group queue-overrides
configure port ethernet network egress queue-group queue-overrides

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context define optional queue parameter overrides for each queue within the queue group.

Platforms All

21.31 queue-parameters

queue-parameters

Syntax **queue-parameters**

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2-paths>primary-path queue-parameters)
[Tree] (config>mcast-mgmt>bw-plcy>t2-paths>secondary-path queue-parameters)

Full Context configure mcast-management bandwidth-policy t2-paths primary-path queue-parameters
configure mcast-management bandwidth-policy t2-paths secondary-path queue-parameters

Description Commands in this context configure queue parameters. This command defines the individual parameters for the queues through which multicast packets are forwarded into the switch fabric on each path.

The individual path queues may be viewed as shared queues. All multicast packets forwarded through the switch fabric associated with one of the paths traverses bypass the normal queuing behavior. Instead of being forwarded through the normal service or network multicast queue, a single queue associated with the multicast path is used. To retain billing and diagnostic information, the forwarding and discard statistics for the service or network queue the packet would have traversed without ingress multicast management is used to account for each packet's behavior.

Note: Any ingress scheduling policy functions attempting to manage the service or network multicast queues is only able to read the statistics of the multicast queues and not able to manage the queues dynamic rate since the packets are flowing through different, non-managed queues. Since this is the case, multicast queues parented to a scheduling policy should be parented to the root scheduler at the highest priority without any rate limitation. Any ingress rate limiting for multicast traffic is performed by the multicast path bandwidth manger based on each records priority and a possible "black-hole" rate threshold.

All queues created for ingress multicast path management are automatically created by the system out of the system reserved queue space. Each queue is created as an expedited queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When forwarding through the queues, each packets forwarding class is ignored. However, the forwarding class is retained for proper egress processing. The packets expressed or implied profile is also ignored within the ingress path queues. A packets congestion priority is derived from the records cong-priority-threshold evaluation result as indicated by the policy or multicast-info-policy. The **cong-priority-threshold** sets the high or low congestion priority of a record based on the records preference value. Within each multicast information policy bundle the **cong-priority-threshold** *preference-level* is set with a value from 0 to 7 and defines the threshold at which all records with a preference equal to or higher than the defined preference is treated as congestion priority high. Multicast records with a preference lower than the defined class threshold is treated as congestion priority low. Low-priority packets use the low drop-tail threshold of the queue, while high-priority packets use the standard MBS value. In the event of path congestion, low-priority packets are discarded first, leaving room for the higher priority packets.

For the primary and secondary paths, a single queue exists for each path and every packet forwarded through the path by the bandwidth manager uses that queue.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

21.32 queue-policy

queue-policy

Syntax **queue-policy** *name*
no queue-policy

Context **[Tree]** (config>card>fp>ingress>network queue-policy)

Full Context configure card fp ingress network queue-policy

Description This command specifies the network-queue policy which defines queue parameters such as CBS, high priority only burst size, MBS, CIR and PIR rates, as well as forwarding-class to queue mappings. The network-queue policy is defined in the **config>qos>network-queue** context.

Default queue-policy default

Parameters *name* — Specifies an existing network-queue policy name, up to 32 characters long.

Platforms All

queue-policy

Syntax **queue-policy** *name*
no queue-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>ethernet>network queue-policy)
[Tree] (config>port>sonet-sdh>path>network queue-policy)
[Tree] (config>port>tdm>ds1>channel-group>network queue-policy)
[Tree] (config>port>tdm>ds3>network queue-policy)
[Tree] (config>port>tdm>e1>channel-group>network queue-policy)
[Tree] (config>port>tdm>e3>network queue-policy)

Full Context configure port ethernet network queue-policy
configure port sonet-sdh path network queue-policy
configure port tdm ds1 channel-group network queue-policy
configure port tdm ds3 network queue-policy
configure port tdm e1 channel-group network queue-policy
configure port tdm e3 network queue-policy

Description This command specifies the existing network queue policy which defines queue parameters such as CBS, high priority only burst size, MBS, CIR and PIR rates, as well as forwarding-class to queue mappings. The network-queue policy is defined in the **config>qos>network-queue** context.

Default queue-policy default

Parameters *name* — Specifies an existing network-queue policy name. The name can be up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path network queue-policy

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group network queue-policy
- configure port tdm ds1 channel-group network queue-policy
- configure port tdm ds3 network queue-policy
- configure port tdm e3 network queue-policy

All

- configure port ethernet network queue-policy

queue-policy

Syntax **queue-policy** *network-queue-policy-name*
no queue-policy

Context [Tree] (config>isa>aa-grp>qos>egress>from-subscriber queue-policy)
[Tree] (config>isa>aa-grp>qos>egress>to-subscriber queue-policy)

Full Context configure isa application-assurance-group qos egress from-subscriber queue-policy
configure isa application-assurance-group qos egress to-subscriber queue-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command assigns an IOM network queue policy as applicable to specific application assurance group traffic.

Default queue-policy “default”

Parameters *network-queue-policy-name* — Specifies the name of the network queue policy defined in the system.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

21.33 queues

queues

Syntax **queues**

Context **[Tree]** (config>qos>fp-resource-policy queues)

Full Context configure qos fp-resource-policy queues

Description Commands in this context modify the FP resource policy information for the queues.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

21.34 queues-hqos-manageable

queues-hqos-manageable

Syntax [**no**] **queues-hqos-manageable**

Context **[Tree]** (config>qos>qgrps>egr>qgrp queues-hqos-manageable)

Full Context configure qos queue-group-templates egress queue-group queues-hqos-manageable

Description This command specifies that the queues within this egress queue group template are to be managed by the Hierarchical QoS (HQoS) process when the template is applied to an Ethernet access egress or network egress context. It is applicable to all egress queue group templates, including the default **policer-output-queues** template.

The **no queues-hqos-manageable** command must be configured for access egress queue groups that are used for post-policer traffic in order to prevent HQoS from measuring the traffic through a policer managed by HQoS then again through a post-policer access egress queue group queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Avoid scenarios that result in traffic being either not being measured or being measured twice by HQoS as they will cause the HQoS result to be inaccurate.

A template configured for **no queues-hqos-manageable** cannot be applied to an Ethernet network egress context. Any egress queue group templates applied to an Ethernet network egress context cannot be configured as **no queues-hqos-manageable**. The configuration of **no queues-hqos-manageable** and the configuration of policers and queue **packet-byte-offset** within the egress queue group template are mutually exclusive.

When a queue group template with **no queues-hqos-manageable** is configured under a port's Ethernet access egress context, the configuration of an aggregate rate or scheduler policy is not permitted under that context, nor are parent overrides for any of the queues in the queue group. If a port scheduler is configured on the port, the queue group queues are not parented to the port scheduler.

The **no** form of this command specifies that queues within this egress queue group are not managed by HQoS.

Default queues-hqos-manageable

Platforms 7450 ESS, 7750 SR, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-e, VSR

21.35 quiet-period

quiet-period

Syntax **quiet-period** *seconds*

Context **[Tree]** (config>port>ethernet>dot1x quiet-period)

Full Context configure port ethernet dot1x quiet-period

Description This command configures the period between two authentication sessions during which no EAPOL frames are sent by the router.

The **no** form of this command returns the value to the default.

Default quiet-period 60

Parameters *seconds* — Specifies the quiet period in seconds.

Values 1 to 3600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

21.36 quit

quit

Syntax **quit**

Context **[Tree]** (candidate quit)

Full Context candidate quit

Description This command exits the **edit-cfg** mode. The contents of the current candidate will not be deleted and the operator can continue editing the candidate later.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22 r Commands

22.1 radius

radius

Syntax **radius** *type* **direction** {**ingress** | **egress**} **script** *script*
no radius *type* **direction** {**ingress** | **egress**}

Context **[Tree]** (config>python>py-policy radius)

Full Context configure python python-policy radius

Description This command specifies the Python script for the specified RADIUS packet type in the specified direction.

Multiple **radius** command configurations are allowed in the same Python policy.

The **no** form of this command reverts to the default.

Parameters *type* — Specifies the message type of the event.

Values access-request, access-accept, access-reject, accounting-request, accounting-response, access-challenge, disconnect-request, change-of-authorization-request

direction {**ingress** | **egress**} — Specifies whether the event is incoming or outgoing.

script — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

radius

Syntax [**no**] **radius**

Context **[Tree]** (debug>router radius)

Full Context debug router radius

Description This command enables the debug router RADIUS context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

radius

Syntax **radius** [**create**]
no radius

Context **[Tree]** (config>service>vprn>aaa>remote-servers radius)

Full Context configure service vprn aaa remote-servers radius

Description This command creates the context to configure RADIUS authentication on the VPRN.

Implement redundancy by configuring multiple server addresses for each VPRN.

The **no** form of this command removes the RADIUS configuration.

Parameters **create** — Keyword used to create the RADIUS context.

Platforms All

radius

Syntax **radius**

Context **[Tree]** (config>app-assure>group>transit-ip-policy radius)

Full Context configure application-assurance group transit-ip-policy radius

Description This command enables dynamic radius based management of transit aa-subs for the transit-ip-policy. This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

radius

Syntax **radius**

Context **[Tree]** (config>li radius)

Full Context configure li radius

Description This command configures RADIUS for Lawful Intercept.

Platforms All

radius

Syntax **radius** [**detail**] [**hex**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no radius

Context [Tree] (debug radius)

Full Context debug radius

Description This command enables debugging for RADIUS connections.

The **no** form of the command disables the debug output.

Parameters **detail** — Displays detailed output.

hex — Displays the packet dump in hex format.

Platforms All

radius

Syntax [**no**] **radius**

Context [Tree] (config>system>security radius)

Full Context configure system security radius

Description This command creates the context to configure RADIUS authentication on the router.

Implement redundancy by configuring multiple server addresses for each router.

The **no** form of this command removes the RADIUS configuration.

Platforms All

22.2 radius-accounting

radius-accounting

Syntax **radius-accounting**

Context [Tree] (config>subscr-mgmt>sub-prof radius-accounting)

Full Context configure subscriber-mgmt sub-profile radius-accounting

Description Commands in this context configure RADIUS accounting subscriber profile parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.3 radius-accounting-policy

radius-accounting-policy

Syntax **radius-accounting-policy** *policy-name*
no radius-accounting-policy

Context **[Tree]** (config>router>l2tp radius-accounting-policy)
[Tree] (config>router>l2tp>group radius-accounting-policy)
[Tree] (config>router>l2tp>group>tunnel radius-accounting-policy)
[Tree] (config>service>ies>if>sap>ipsec-gw radius-accounting-policy)
[Tree] (config>service>vprn>if>sap>ipsec-gw radius-accounting-policy)
[Tree] (config>service>vprn>l2tp>group radius-accounting-policy)
[Tree] (config>service>vprn>l2tp>group>tunnel radius-accounting-policy)
[Tree] (config>service>vprn>l2tp radius-accounting-policy)

Full Context configure router l2tp group radius-accounting-policy
configure router l2tp group tunnel radius-accounting-policy
configure router l2tp radius-accounting-policy
configure service ies interface sap ipsec-gw radius-accounting-policy
configure service vprn interface sap ipsec-gw radius-accounting-policy
configure service vprn l2tp group radius-accounting-policy
configure service vprn l2tp group tunnel radius-accounting-policy
configure service vprn l2tp radius-accounting-policy

Description This command configures the RADIUS accounting policy.

The **no** form of this command reverts to the default value.

Default no radius-accounting-policy

Parameters *policy-name* — Specifies the policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn l2tp radius-accounting-policy
- configure router l2tp radius-accounting-policy
- configure service vprn l2tp group radius-accounting-policy
- configure router l2tp group radius-accounting-policy
- configure service vprn l2tp group tunnel radius-accounting-policy
- configure router l2tp group tunnel radius-accounting-policy

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ipsec-gw radius-accounting-policy
- configure service vprn interface sap ipsec-gw radius-accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

radius-accounting-policy

Syntax **radius-accounting-policy** *name* [**create**]
no radius-accounting-policy

Context **[Tree]** (config>subscr-mgmt radius-accounting-policy)

Full Context configure subscriber-mgmt radius-accounting-policy

Description This command specifies a subscriber RADIUS based accounting policy.

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — The name of the policy. The string is case-sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

create — Keyword used to create a RADIUS accounting policy instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

radius-accounting-policy

Syntax **radius-accounting-policy** *nat-accounting-policy*
no radius-accounting-policy

Context **[Tree]** (config>isa>wlan-gw-group>nat radius-accounting-policy)

Full Context configure isa wlan-gw-group nat radius-accounting-policy

Description This command configures the RADIUS accounting policy to use for each MDA in this ISA group.

The **no** form of this command removes the accounting policy from the configuration.

Parameters *nat-accounting-policy* — Specifies the RADIUS accounting policy up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

radius-accounting-policy

Syntax **radius-accounting-policy** *rad-acct-plcy-name*
no radius-accounting-policy

Context **[Tree]** (config>app-assure>group>statistics>aa-sub radius-accounting-policy)

Full Context configure application-assurance group statistics aa-sub radius-accounting-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies an existing subscriber RADIUS based accounting policy to use for AA. RADIUS Accounting policies are configured in the **config>app-assure>radius-accounting-policy** context.

Default no radius-accounting-policy

Parameters *rad-acct-plcy-name* — Specifies the name of the policy. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

radius-accounting-policy

Syntax **radius-accounting-policy** *rad-acct-plcy-name* [**create**]
no radius-accounting-policy *rad-acct-plcy-name*

Context **[Tree]** (config>app-assure radius-accounting-policy)

Full Context configure application-assurance radius-accounting-policy

Description This command specifies an existing subscriber RADIUS-based accounting policy to use for AA. RADIUS accounting policies are configured in the **config>app-assure>radius-accounting-policy** context.

Default no radius-accounting-policy

Parameters *rad-acct-plcy-name* — Specifies the policy name. The string is case sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

create — Keyword used to create the policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

radius-accounting-policy

Syntax **radius-accounting-policy** *name* [**create**]
no radius-accounting-policy *name*

Context **[Tree]** (config>ipsec radius-accounting-policy)

Full Context configure ipsec radius-accounting-policy

Description This command specifies an existing RADIUS accounting policy to use to collect accounting statistics on this subscriber profile by RADIUS. This command is used independently of the **collect-stats** command.

Parameters *name* — Specifies an existing RADIUS based accounting policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

radius-accounting-policy

Syntax **radius-accounting-policy** *nat-accounting-policy*
no radius-accounting-policy

Context **[Tree]** (config>isa>nat-group radius-accounting-policy)

Full Context configure isa nat-group radius-accounting-policy

Description This command specifies the RADIUS accounting policy to use for each MDA in this ISA group.

The **no** form of the command removes the policy ID from the configuration.

Default no radius-accounting-policy

Parameters *nat-accounting-policy* — Reference to the nat-accounting-policy which defines:
Source IP addresses that are assigned to BB-ISA cards.
Parameters related to RADIUS server itself.
List of RADIUS attributes that are included in accounting messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.4 radius-accounting-server

radius-accounting-server

Syntax **radius-accounting-server**

Context **[Tree]** (config>aaa>l2tp-acct-plcy>include-radius-attribute radius-accounting-server)

Full Context configure aaa l2tp-accounting-policy include-radius-attribute radius-accounting-server

Description Commands in this context configure RADIUS accounting server attributes under a given session authentication policy.

radius-accounting-server

Syntax **radius-accounting-server**

Context **[Tree]** (config>app-assure>rad-acct-plcy radius-accounting-server)
[Tree] (config>aaa>l2tp-acct-plcy radius-accounting-server)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server
configure application-assurance radius-accounting-policy radius-accounting-server

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates the context for defining RADIUS accounting server attributes under a given session authentication policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure aaa l2tp-accounting-policy radius-accounting-server

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure application-assurance radius-accounting-policy radius-accounting-server

22.5 radius-attr

radius-attr

Syntax **radius-attr type** *attribute-type* [**extended-type** *attribute-ext-type*] [**transaction**]
radius-attr type *attribute-type* [**transaction**] {**address** | **hex** | **integer** | **string**} **value** *attribute-value*
radius-attr vendor *vendor-id* **type** *attribute-type* [**extended-type** *attribute-ext-type*] [**transaction**] [**encoding** *encoding-type*]
radius-attr vendor *vendor-id* **type** *attribute-type* [**extended-type** *attribute-ext-type*] [**transaction**] [**encoding** *encoding-type*] {**address** | **hex** | **integer** | **string**} **value** *attribute-value*
no radius-attr type *attribute-type* [**extended-type** *attribute-ext-type*]
no radius-attr type *attribute-type* [**extended-type** *attribute-ext-type*] {**address** | **hex** | **integer** | **string**} **value** *attribute-value*
no radius-attr vendor *vendor-id* **type** *attribute-type* [**extended-type** *attribute-ext-type*]
no radius-attr vendor *vendor-id* **type** *attribute-type* [**extended-type** *attribute-ext-type*] {**address** | **hex** | **integer** | **string**} [**value**] *attribute-value*

Context **[Tree]** (debug>router>radius radius-attr)

Full Context debug router radius radius-attr

Description This command specifies the RADIUS attribute filter of command **debug router radius**.

Parameters *attribute-type* — Specifies the RADIUS attribute type.

Values 1 to 255

attribute-ext-type — Specifies the RADIUS attribute extended type (RFC 6929).

Values 1 to 255

address — Specifies the value is a IPv4 or IPv6 address/prefix/subnet.

string — Specifies the value is a ASCII string.

integer — Specifies the value is a integer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hex — Specifies the value is a binary string in hex format, such as "\0xAB01FE".

attribute-value — Specifies the value of the RADIUS attribute.

Values		
address	<ipv4-address> | <ipv6-address> | <ipv6-prefix/prefix-length>	
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D
	ipv6-prefix-length [0 to 128]	
	hex	[0x0 to 0xFFFFFFFF (up to 506 hex nibbles)]
	integer	[0 to 4294967295]
	string	ascii-string (up to 253 characters)

transaction — Specifies that the system outputs both request and response packets in the same session even if the response packet does not include the filter attribute.

vendor-id — Specifies the vendor id for the vendor specific attribute.

Values 0 to 16777215

encoding-type — Specifies the size of the vendor-type and vendor-length in bytes. It is a two digitals string: "xy", x is the size of vendor-type, range from 1 to 4; y is the size of vendor-length, range from 0 to 2; it is "11" by default.

Values type-size:1 to 4, length-size: 0 to 2

Platforms All

22.6 radius-auth-policy

radius-auth-policy

Syntax **radius-auth-policy** *radius-authentication-policy-name*
no radius-auth-policy

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn radius-auth-policy)

Full Context configure subscriber-mgmt gtp apn-policy apn radius-auth-policy

Description This command configures the RADIUS authentication policy with which the GTP connection is authenticated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the authentication policy. Only new session setups are affected.

Default no radius-auth-policy

Parameters *radius-authentication-policy-name* — Specifies the name of the authentication policy to be used, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.7 radius-authentication

radius-authentication

Syntax **radius-authentication**

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile radius-authentication)

Full Context configure subscriber-mgmt vrgw brg brg-profile radius-authentication

Description Commands in this context configure parameters related to RADIUS authentication performed for the BRG.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.8 radius-authentication-policy

radius-authentication-policy

Syntax **radius-authentication-policy** *name*
no radius-authentication-policy

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw radius-authentication-policy)
[Tree] (config>service>vprn>if>sap>ipsec-gw radius-authentication-policy)

Full Context configure service ies interface sap ipsec-gw radius-authentication-policy
configure service vprn interface sap ipsec-gw radius-authentication-policy

Description This command specifies the policy to be used for the IKEv2 remote-access tunnels terminated on the IPsec GW. The **radius-authentication-policy** is defined under **config>ipsec** context.

Parameters *name* — Specifies the name of an existing RADIUS authentication policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

radius-authentication-policy

Syntax **radius-authentication-policy** *name* [**create**]
no radius-authentication-policy *name*

Context **[Tree]** (config>ipsec radius-authentication-policy)

Full Context configure ipsec radius-authentication-policy

Description This command specifies the RADIUS authentication policy associated with this IPsec gateway.

Parameters *name* — Specifies an existing RADIUS authentication policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.9 radius-authentication-server

radius-authentication-server

Syntax **radius-authentication-server**

Context **[Tree]** (config>subscr-mgmt>auth-plcy radius-authentication-server)

Full Context configure subscriber-mgmt authentication-policy radius-authentication-server

Description Commands in this context define RADIUS authentication server attributes under a given session authentication policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.10 radius-coa-port

radius-coa-port

Syntax **radius-coa-port** {*port-number*}
no radius-coa-port

Context **[Tree]** (config>aaa radius-coa-port)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa radius-coa-port

Description This command configures the system-wide UDP port number that RADIUS is listening on for CoA and Disconnect messages.

The **no** form of this command reverts to the default.

Default radius-coa-port 3799

Parameters *port-number* — Specifies the UDP port number for RADIUS CoA and disconnect messages.

Values 1647, 1700, 1812, 3799

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.11 radius-plcy

radius-plcy

Syntax **radius-plcy** *name*
no radius-plcy

Context **[Tree]** (config>port>ethernet>dot1x radius-plcy)

Full Context configure port ethernet dot1x radius-plcy

Description This command references the RADIUS policy to be used for 802.1x authentication. An 802.1x RADIUS policy must be configured (**config**>**system**>**security**>**dot1x**) before it can be associated to a port. If the RADIUS policy-id does not exist, an error is returned. Only one 802.1x RADIUS policy can be associated with a port at a time.

The **no** form of this command removes the RADIUS policy association.

Default no radius-plcy

Parameters *name* — Specifies an existing 802.1x RADIUS policy name, up to 32 characters.

Platforms All

radius-plcy

Syntax **radius-plcy** *name* [**create**]

Context **[Tree]** (config>system>security>dot1x radius-plcy)

Full Context configure system security dot1x radius-plcy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates the context to configure RADIUS server parameters for 802.1x network access control on the router.

Note: The RADIUS server configured under the config>system>security>dot1x>radius-plcy context authenticates clients who get access to the data plane of the router as opposed to the RADIUS server configured under the **config>system>radius** context which authenticates CLI login users who get access to the management plane of the router.

The **no** form of this command removes the RADIUS server configuration for 802.1x.

Platforms All

22.12 radius-proxy

radius-proxy

Syntax **radius-proxy**

Context **[Tree]** (config>router radius-proxy)
[Tree] (config>service>vprn radius-proxy)

Full Context configure router radius-proxy
configure service vprn radius-proxy

Description This command context to configure RADIUS proxy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.13 radius-proxy-cache

radius-proxy-cache

Syntax **radius-proxy-cache router** *router-instance* **server** *server-name*
no radius-proxy-cache

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>track-mobility radius-proxy-cache)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>track-mobility radius-proxy-cache)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range track-mobility radius-proxy-cache
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range track-mobility radius-proxy-cache

Description This command specifies the RADIUS-proxy server to allow subscribers created via data-triggered authentication to create an entry. This RADIUS proxy cache entry allows efficient handling of UE mobility.

Parameters *router-instance* — Specifies the router instance.

Values

router-name	Base
service-id	1 to 2147483647

server-name — Specifies the server name up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.14 radius-proxy-server

radius-proxy-server

Syntax [**no**] **radius-proxy-server router** *router-instance* **name** *server-name*

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile radius-proxy-server)

Full Context configure subscriber-mgmt vrgw brg brg-profile radius-proxy-server

Description This command enables BRG processing on the specified RADIUS proxy server. Whenever an Access-Accept message is received with the attribute Alc-BRG-Id present, this will trigger the creation of a BRG. The BRG will use the **brg-profile** specified in the Access-Accept message or fall back to this BRG profile. When the specified **radius-proxy-server** has a cache enabled, no cache entries will be created for a transaction identified as BRG. A RADIUS proxy server can only be listed in one BRG profile.

This command can be executed multiple times.

The **no** form of this command removes BRG processing for the specified **radius-proxy server**.

Parameters *router-instance* — Specifies the ID of the VRF where the proxy server is located.

server-name — Specifies the name of the RADIUS proxy server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

radius-proxy-server

Syntax **radius-proxy-server router** *router-instance* **name** *server-name*
no radius-proxy-server

Context **[Tree]** (config>router>nat>inside>subscriber-identification radius-proxy-server)
[Tree] (config>service>vprn>nat>inside>subscriber-identification radius-proxy-server)

Full Context configure router nat inside subscriber-identification radius-proxy-server
configure service vprn nat inside subscriber-identification radius-proxy-server

Description This command configures RADIUS proxy server parameters. This is a reference to a RADIUS accounting proxy server in Subscriber Aware Large Scale NAT44 application. RADIUS accounting proxy server will cache attributes related to a BNG subscriber as they are received in standard accounting messages (RFC 2866). Radius accounting proxy server can be configured in any routing instance within 7750 SR.

Default none

Parameters **router** *router-instance* — Specifies the routing instance in which the RADIUS accounting proxy is configured.

name *server-name* — Specifies the name reference to the RADIUS accounting proxy server that is instantiated in 7750 SR.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.15 radius-script-policy

radius-script-policy

Syntax **radius-script-policy** *policy-name* [**create**]
no radius-script-policy *policy-name*

Context **[Tree]** (config>aaa radius-script-policy)

Full Context configure aaa radius-script-policy

Description This command configures a RADIUS script policy.

The **no** form of this command removes the script policy from the configuration.

Parameters *policy-name* — Configures Python scripts to modify RADIUS messages.

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the **create** keyword.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.16 radius-server

radius-server

Syntax **radius-server**

Context **[Tree]** (config>router radius-server)
[Tree] (config>service>vprn radius-server)

Full Context configure router radius-server
configure service vprn radius-server

Description Commands in this context configure the RADIUS server under router or VPRN service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.17 radius-server-policy

radius-server-policy

Syntax **radius-server-policy** *policy-name*
no radius-server-policy

Context **[Tree]** (config>aaa>l2tp-acct-plcy radius-server-policy)

Full Context configure aaa l2tp-accounting-policy radius-server-policy

Description This command references an existing **radius-server-policy** (available under the **config>aaa** context) for use in subscriber management authentication and accounting.

When configured in an authentication-policy, following CLI commands are ignored in the policy to avoid conflicts:

- all commands in the radius-authentication-server context
- accept-authorization-change
- coa-script-policy
- accept-script-policy
- request-script-policy

When configured in a radius-accounting-policy, following CLI commands are ignored in the policy to avoid conflicts:

- all commands in the radius-accounting-server context
- acct-request-script-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the radius-server-policy reference from the configuration.

Default no radius-server-policy

Parameters *policy-name* — Specifies the RADIUS server policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

radius-server-policy

Syntax **radius-server-policy** *policy-name* [**create**]
no radius-server-policy *policy-name*

Context **[Tree]** (config>aaa radius-server-policy)

Full Context configure aaa radius-server-policy

Description This command creates a radius-server-policy.

A RADIUS server policy can be used in

- radius-proxy, for application like EAP authentication for WIFI access
- authentication policy, for Enhanced Subscriber Management authentication
- radius accounting policy, for Enhanced Subscriber Management accounting
- dynamic data service RADIUS accounting
- AAA route downloader

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the name of the radius-server-policy up to 32 characters.

create — Keyword used to create a radius-server-policy name. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

radius-server-policy

Syntax **radius-server-policy** *radius-server-policy-name*
no radius-server-policy

Context **[Tree]** (config>subscr-mgmt>auth-plcy radius-server-policy)
[Tree] (config>subscr-mgmt>acct-plcy radius-server-policy)

Full Context configure subscriber-mgmt radius-accounting-policy radius-server-policy
configure subscriber-mgmt authentication-policy radius-server-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command references an existing radius-server-policy (available under the config>aaa context) for use in subscriber management authentication and accounting.

When configured in an authentication-policy, following CLI commands are ignored in the policy to avoid conflicts:

- all commands in the radius-authentication-server context
- accept-authorization-change
- coa-script-policy
- accept-script-policy
- request-script-policy

When configured in a radius-accounting-policy, following CLI commands are ignored in the policy to avoid conflicts:

- all commands in the radius-accounting-server context
- acct-request-script-policy

The **no** form of this command removes the radius-server-policy reference from the configuration

Parameters *radius-server-policy-name* — Specifies the RADIUS server policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

radius-server-policy

Syntax **radius-server-policy** *policy-name*
no radius-server-policy

Context **[Tree]** (config>aaa>route-downloader radius-server-policy)

Full Context configure aaa route-downloader radius-server-policy

Description This command references an existing radius-server-policy (available under the **config>aaa** context). The server (or servers) referenced by the policy is used as the targets for the access-request message.

The **no** form of this command removes the policy name from the route-downloader configuration.

Parameters *policy-name* — Specifies the RADIUS server policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

radius-server-policy

Syntax **radius-server-policy** *policy-name*
no radius-server-policy

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile>radius-authentication radius-server-policy)

Full Context configure subscriber-mgmt vrgw brg brg-profile radius-authentication radius-server-policy

Description This command is used if the BRG needs to be authenticated to the controller/PCMP by the vRGW. This is required if the BRG does not perform RADIUS authentication via the proxy server. The vRGW will originate a valid Access Request using the BRG ID as the username.

The **no** form of this command removes the **radius-server-policy** from the configuration. Setup of an unauthenticated BRG will now fail.

Parameters *policy-name* — Specifies the RADIUS server policy, up to 32 characters, to be applied to this subscriber authentication policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

radius-server-policy

Syntax **radius-server-policy** *radius-server-policy-name*
no radius-server-policy

Context **[Tree]** (config>ipsec>rad-acct-plcy radius-server-policy)
[Tree] (config>ipsec>rad-auth-plcy radius-server-policy)

Full Context configure ipsec radius-accounting-policy radius-server-policy
configure ipsec radius-authentication-policy radius-server-policy

Description This command references an existing **radius-server-policy** (available under the **config>aaa** context) for use in subscriber management authentication and accounting.

When configured in an authentication-policy, following CLI commands are ignored in the policy to avoid conflicts:

- all commands in the radius-authentication-server context
- accept-authorization-change
- coa-script-policy
- accept-script-policy
- request-script-policy

When configured in a radius-accounting-policy, following CLI commands are ignored in the policy to avoid conflicts:

- all commands in the radius-accounting-server context

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- acct-request-script-policy

The **no** form of this command removes the radius-server-policy reference from the configuration.

Default no radius-server-policy

Parameters *radius-server-policy-name* — Specifies the RADIUS server policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

radius-server-policy

Syntax **radius-server-policy** *policy-name*
no radius-server-policy

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile radius-server-policy)

Full Context configure subscriber-mgmt vrgw brg brg-profile radius-server-policy

Description This command allows the vRGW to authenticate on the BRG's behalf. This is required if the BRG does not perform authentication itself using the radius proxy. The vRGW originates a valid Access Request using the BRG ID as a username.

The **no** form of this command removes the RADIUS server policy from the configuration. Setting up of an unauthenticated BRG will now fail.

Default no radius-server-policy

Parameters *policy-name* — Specifies the RADIUS server policy, up to 32 characters, to apply in this subscriber authentication policy.

radius-server-policy

Syntax **radius-server-policy** *policy-name*
radius-server-policy auth *policy-name-auth*
radius-server-policy acct *policy-name-acct*
radius-server-policy auth *policy-name-auth* **acct** *policy-name-acct*
no radius-server-policy

Context **[Tree]** (config>port>ethernet>dot1x radius-server-policy)

Full Context configure port ethernet dot1x radius-server-policy

Description This command configures the RADIUS policy with IPv4/IPv6 in base routing and VPRN. The current RADIUS policy can be found under the **configure>aaa>radius-server-policy** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The RADIUS servers for the policy are configured under **configure>router>radius-server** or **configure>service>vprn>radius-server** context.

The RADIUS policy is assigned under dot1x using the **radius-server-policy** command. When the RADIUS policy is configured, both authorization and accounting are performed via the same server.

The **no** form of this command allows authorization and accounting via different servers.

Default no radius-server-policy

Parameters *policy-name* — Specifies the RADIUS server policy, up to 32 characters.

The policy is configured under **configure>aaa>radius-server-policy**. When the policy name is configured, both authorization and accounting are done via this server.

policy-name-auth — Specifies the AAA RADIUS server policy for dot1x authorization only; up to 32 characters.

The policy is configured under **configure>aaa>radius-server-policy**. The policy name authorization is used if the user needs a different server for authorization.

policy-name-acct — Specifies the AAA RADIUS server policy for dot1x accounting only; up to 32 characters.

The policy is configured under **configure>aaa>radius-server-policy**. The policy name accounting is used if the user needs a different server for accounting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.18 radius-session-timeout

radius-session-timeout

Syntax **radius-session-timeout** {**backwards-compatible** | **ignore** | **absolute**}
no radius-session-timeout

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipoe-session radius-session-timeout)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session radius-session-timeout)

Full Context configure service ies subscriber-interface group-interface ipoe-session radius-session-timeout
configure service vprn subscriber-interface group-interface ipoe-session radius-session-timeout

Description This command specifies how to interpret the session-timeout coming from a RADIUS VSA in an Access-Accept or CoA message.

The value of this command can only be changed on wlan-gw group interfaces.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command to resets the default behavior.

Default radius-session-timeout absolute (backward compatible on wlan-gw group interfaces)

Parameters **backwards-compatible** — Specifies that the VSA is interpreted as an IPv4 lease time if the Alc-Lease-Time attribute is not present and an absolute timeout otherwise. The VSA is treated the same as for non-ipoe session DHCP hosts.

ignore — Specifies that the VSA meaning is irrelevant for IPoE session and should be ignored.

absolute — Specifies that the VSA would be treated as a timeout starting from the moment the IPoE session is set up.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.19 radius-user-name

radius-user-name

Syntax [**no**] **radius-user-name**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>include-avp radius-user-name)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp radius-user-name

Description This command includes the RADIUS user name AVP in the Diameter Gy messages.

The **no** form of this command returns the command to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.20 rai

rai

Syntax [**no**] **rai**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp rai)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp rai

Description This command enables the inclusion of the RAI AVP as signaled in the incoming GTP setup message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the inclusion of the AVP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.21 range

range

Syntax **range** *encap-range* **sync-tag** *sync-tag*
no range *encap-range*

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync>port range)

Full Context configure redundancy multi-chassis peer sync port range

Description This command configures a range of encapsulation values.

Parameters *encap-range* — Specifies a range of encapsulation values on a port to be synchronized with a multi-chassis peer.

Values

Dot1Q	start-tag-end-tag
start-tag	0 to 4094
end-tag	0 to 4094
QinQ	qtag1.start-qtag2-qtag1.end-qtag2-start-qtag1.*-end-qtag1.*
qtag1	1 to 4094
start-qtag1	1 to 4094
en-qtag1	1 to 4094
start-qtag2	0 to 4094
end-qtag2	0 to 4094

sync-tag — Specifies a synchronization tag up to 32 characters to be used while synchronizing this encapsulation value range with the multi-chassis peer.

Platforms All

range

Syntax **range** *vc-id-range* [**sync-tag** *sync-tag*]
no range *vc-id-range*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>redundancy>multi-chassis>peer>sync>sdp range)

Full Context configure redundancy multi-chassis peer sync sdp range

Description This command specifies a range of VC IDs for manually configured spoke SDPs to be synchronized with the multi-chassis peer and a synchronization tag to be used while synchronizing each range with the multi-chassis peer. The **range** command and the configuration of a synchronization tag on the parent **sdp** command are mutually exclusive.

To synchronize a single spoke SDP, the *start-vc-id* should be the same as the *end-vc-id*. If the configured *end-vc-id* is lower than the *start-vc-id*, the **range** command fails.

The synchronization tag can be changed by entering the same command with a different synchronization tag. Changing the synchronization tag removes all states relating to the previous synchronization tag for the SDP and a new synchronization tag state is created.

Multiple **range** commands can be configured, however, overlapping ranges for the same SDP (*sdp-id*) are not permitted.

The synchronization of PIM snooping is only supported for manually configured spoke SDPs but is not supported for spoke SDPs configured within an endpoint. See PIM Snooping for IPv4 Synchronization for service support.

The synchronization of the PIM snooping state is not supported on any of the following when used with the configured *sdp-id*:

- mesh SDPs
- spoke SDPs in non-VPLS services
- BGP-AD/BGP-VPLS (FEC 129) spoke SDPs
- spoke SDPs configured in endpoints
- pseudowire SAPs
- ESM-over-MPLS pseudowires

Non-existent spoke SDPs may be specified. If these spoke SDPs are created at a later time, then all states on the spoke SDPs are synchronized according to the synchronization tag and the synchronization protocols enabled. The **sync-tag** can be changed by entering the same command with a different **sync-tag** value. If the synchronization tag is changed, then all states for the previous **sync-tag** are removed for the SDP configured in the command and the state is then built for the new synchronization tag.

Parameters *vc-id-range* — Specifies a non-overlapping range of VC IDs for the spoke SDPs of the SDP to be synchronized with the multi-chassis peer.

Values *start-vc-id-end-vc-id*
start-vc-id: 1 to 4294967295
end-vc-id: 1 to 4294967295

sync-tag — Specifies a synchronization tag, up to 32 characters, to be used when synchronizing with the multi-chassis peer.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

range

Syntax [**no**] **range** *vlan-range*

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring>path-b range)
[Tree] (config>redundancy>mc>peer>mcr>ring>path-excl range)

Full Context configure redundancy multi-chassis peer mc-ring ring path-b range
configure redundancy multi-chassis peer mc-ring ring path-excl range

Description This command configures a Layer 2 MC-Ring path-b or path-excl VLAN range.

By default, all customer VLANs participating in an L2 MC-Ring are on path-a. For load balancing purposes, a range of customer VLANs can be configured to use path-b which is set up in the opposite direction than path-a.The range of VLANs that are not participating in L2 MC-Ring are configured using the **path-excl** command.

Parameters *vlan-range* — Specifies the VLAN range.

Values [0 to 4094] - [0 to 4094]
[0 to 4094] - *
* - *

Platforms All

range

Syntax [**no**] **range** *vlan-range*

Context **[Tree]** (config>service>vpls>sap>managed-vlan-list range)

Full Context configure service vpls sap managed-vlan-list range

Description This command configures a range of VLANs on an access port that are to be managed by an existing management VPLS.

This command is only valid when the VPLS in which it is entered was created as a management VPLS, and when the SAP in which it was entered was created on an Ethernet port with encapsulation type of dot1q or qinq, or on a SONET/SDH port with encapsulation type of bcp-dot1q.

To modify the range of VLANs, first the new range should be entered and afterwards the old range removed.

The **no** form of this command removes the VLAN range from this configuration.

Parameters *vlan-range* — Specifies the VLAN start value and VLAN end value. The end-vlan must be greater than start-vlan. The format is <start-vlan>-<end-vlan>.

Values start-vlan: 1 to 4094
end-vlan: 1 to 4094

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

range

Syntax **range start** [*value*] **end** [*value*]
range default
no range start [*value*] **end** [*value*]

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges range)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges range)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range

Description This command creates a VLAN range or enters the context of the specified VLAN ranges for configuration applicable to that range of VLANs.

Parameters **start** — Specifies the start of the VLAN range.

Values 0 to 4096

Default 200

end — Specifies the end of VLAN range.

Values 0 to 4096

Default 400

default — Specifies to use defaults for the interface.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

range

Syntax **range** *isid* [**to** *isid*]
no range

Context **[Tree]** (config>service>vpls>isid-policy>entry range)

Full Context configure service vpls isid-policy entry range

Description This command specifies an ISID or a Range of ISIDs in a B-VPLS. One range is allowed per entry.

Default no range

Parameters *isid* — Specifies the ISID value in 24 bits. When singular, ISID identifies a particular ISID to be used for matching

Values 0 to 16777215

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

to *isid* — Identifies upper value in a range of ISIDs to be used as matching criteria

Platforms All

range

Syntax **range** *range-id* **isid** *isid-value* [**to** *isid-value*] [**create**]
no range *range-id*

Context **[Tree]** (config>service>vpls>sap>static-isid range)
[Tree] (config>service>vpls>spoke-sdp>static-isid range)

Full Context configure service vpls sap static-isid range
configure service vpls spoke-sdp static-isid range

Description This command identifies a set of ISIDs for I-VPLS services that are external to SPBM. These ISIDs are advertised as supported locally on this node unless an altered by an isid-policy. This allows communication from I-VPLS services external to SPBM through this node. The SAP may be a regular SAP or MC-LAG SAP. The spoke-SDP may be an active/standby spoke. When used with MC-LAG or active/stand-by PWs the conditional static-mac must be configured. ISIDs declared this way become part of the ISID multicast and consume MFIBs. Multiple SPBM static-isid ranges are allowed under a SAP/spoke-SDP.

The static-isids are associated with a remote B-MAC that must be declared as a static-mac for unicast traffic. ISIDs are advertised as if they were attached to the local B-MAC. Only remote I-VPLS ISIDs need to be defined. In the MFIB, the group MACs are then associated with the active SAP or spoke-SDP. An ISID policy may be defined to suppress the advertisement of an ISID if the ISID is primary used for unicast services. The following rules govern the usage of multiple ISID statements:

- overlapping values are allowed:
  - isid from 301 to 310
  - isid from 305 to 315
  - isid 316
- the minimum and maximum values from overlapping ranges are considered and displayed. The above entries will be equivalent with “ISID from 301 to 316” statement.
- there is no consistency check with the content of ISID statements from other entries. The entries will be evaluated in the order of their IDs and the first match will cause the implementation to execute the associated action for that entry.

The **no** form of this command removes all the previous statements under one interface

no isid value | from value to higher-value - removes a specific ISID value or range. Must match a previously used positive statement: for example if the command “isid 316 to 400” was used using “no isid 316 to 350” will not work but “no isid 316 to 400 will be successful.

Parameters *range-id* — Sets context for specified entry ID for the static-isids

Values 1— 8191

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

isid-value — Configures the ISID or the start of an ISID range. Specifies the ISID value in 24 bits. When just one present identifies a particular ISID to be used for matching.

Values 0 to 16777215

to isid — Identifies upper value in a range of ISIDs to be used as matching criteria

Values 0 to 16777215

create — This keyword is mandatory when creating a range instance.

Platforms All

range

Syntax **range start-entry** *policer-id* **count** *count*
no range

Context **[Tree]** (config>qos>sap-egress>dyn-policer range)
[Tree] (config>qos>sap-ingress>dyn-policer range)

Full Context configure qos sap-egress dynamic-policer range
configure qos sap-ingress dynamic-policer range

Description This command defines the range of ids for dynamic policers that are created using a Gx interface.

The **no** form of this command disables creation of dynamic policers using a Gx interface, resulting in a Gx rule instantiation failure, which is the default.

Default no range

Parameters **start-entry** *policer-id* — Specifies the lowest entry in the range.

Values 1 to 63

count *count* — Specifies the number of entries in the range.

Values 1 to 63

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.22 rapid-psc-timer

rapid-psc-timer

Syntax **rapid-psc-timer** *interval*
no rapid-psc-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>mpls>mpls-tp>protection-template rapid-psc-timer)

Full Context configure router mpls mpls-tp protection-template rapid-psc-timer

Description This command configures the rapid timer value to be used for protection switching coordination (PSC) packets for MPLS-TP linear protection (RFC 6378).

Default rapid-psc-timer 10

Parameters *interval* — Specifies the rapid timer interval in milliseconds.

Values [10, 100, 1000]

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.23 rapid-retransmit-time

rapid-retransmit-time

Syntax **rapid-retransmit-time** *hundred-milliseconds*
no rapid-retransmit-time

Context [Tree] (config>router>gmpls rapid-retransmit-time)

Full Context configure router gmpls rapid-retransmit-time

Description This command configures the value of the Rapid Retransmission Interval. It is used in the re-transmission mechanism to handle unacknowledged message_id objects and is based on an exponential back-off timer.

Re-transmission interval of a RSVP message with the same message_id = 2 * rapid-retransmit-time interval of time.

The node stops re-transmission of unacknowledged RSVP messages:

- if the updated back-off interval exceeds the value of the regular refresh interval, or
- if the number of re-transmissions reaches the value of the **rapid-retry-limit** parameter, whichever comes first

The Rapid Retransmission Interval must be smaller than the regular refresh interval configured in **config>router>gmpls>refresh-time**.

The **no** form of this command resets the configuration to the default value.

Default rapid-retransmit-time 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hundred-milliseconds* — Specifies the Rapid Retransmission Interval, in units of 100 ms (for example, enter “6” for a 600 ms retransmit time).

Values 1 to 100

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rapid-retransmit-time

Syntax **rapid-retransmit-time** *hundred-milliseconds*
no rapid-retransmit-time

Context **[Tree]** (config>router>rsvp rapid-retransmit-time)

Full Context configure router rsvp rapid-retransmit-time

Description This command defines the value of the Rapid Retransmission Interval. It is used in the re-transmission mechanism to handle unacknowledged message_id objects and is based on an exponential back-off timer.

Re-transmission interval of a RSVP message with the same message_id = 2 * rapid-retransmit-time interval of time.

The node stops re-transmission of unacknowledged RSVP messages:

- If the updated back-off interval exceeds the value of the regular refresh interval.
- If the number of re-transmissions reaches the value of the **rapid-retry-limit** parameter, whichever comes first.

The Rapid Retransmission Interval must be smaller than the regular refresh interval configured in **config>router>rsvp>refresh-time**.

The **no** form of this command reverts to the default value.

Default rapid-retransmit-time 5

Parameters *hundred-milliseconds* — Specifies the rapid retransmission interval, in hundred-milliseconds (for example, enter “6” for a 600 millisecond retransmit time).

Values 1 to 100, in units of 100 ms.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.24 rapid-retry-limit

rapid-retry-limit

Syntax **rapid-retry-limit** *limit*
no rapid-retry-limit

Context **[Tree]** (config>router>gmpls rapid-retry-limit)

Full Context configure router gmpls rapid-retry-limit

Description This command configures the value of the Rapid Retry Limit. This is used in the retransmission mechanism based on an exponential backoff timer in order to handle unacknowledged message_id objects. The RSVP message with the same message_id is retransmitted every 2 * rapid-retransmit-time interval of time. The node will stop retransmission of unacknowledged RSVP messages whenever the updated backoff interval exceeds the value of the regular refresh interval, or the number of retransmissions reaches the value of the **rapid-retry-limit** parameter, whichever comes first.

The **no** form of this command resets the configuration to the default value.

Default rapid-retry-limit 3

Parameters *limit* — Specifies the rapid retry limit.

Values 1 to 6

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rapid-retry-limit

Syntax **rapid-retry-limit** *number*
no rapid-retry-limit

Context **[Tree]** (config>router>rsvp rapid-retry-limit)

Full Context configure router rsvp rapid-retry-limit

Description This command is used to define the value of the Rapid Retry Limit. This is used in the retransmission mechanism based on an exponential backoff timer in order to handle unacknowledged message_id objects. The RSVP message with the same message_id is retransmitted every 2 * rapid-retransmit-time interval of time. The node will stop retransmission of unacknowledged RSVP messages whenever the updated backoff interval exceeds the value of the regular refresh interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default rapid-retry-limit 3

Parameters *number* — Specifies the value of the Rapid Retry Limit.

Values 1 to 6, integer values

Platforms All

22.25 rapid-update

rapid-update

Syntax **rapid-update** [**l2-vpn**] [**mvpn-ipv4**] [**mvpn-ipv6**] [**mdt-safi**] [**evpn**] [**label-ipv4**] [**label-ipv6**] [**vpn-ipv4**] [**vpn-ipv6**] [**mcast-vpn-ipv4**] [**mcast-vpn-ipv6**]
no rapid-update

Context **[Tree]** (config>router>bgp rapid-update)

Full Context configure router bgp rapid-update

Description This command enables and disables BGP rapid update for specified address families.

If rapid update is enabled for a set of address families, and a route belonging to a family in that set is received by the router and chosen for propagation to certain BGP peers, the remaining time on the MRAI timer of these peers is ignored and the route is transmitted immediately, along with all other pending routes for these peers (including routes of address families not specified in the **rapid-update** command).

The **rapid-update** command overrides the peer-level **min-route-advertisement** (**config>router>bgp min-route-advertisement**, **config>router>bgp>group min-route-advertisement**, **config>router>bgp>group>neighbor min-route-advertisement**) time and applies the minimum setting (0 seconds) to routes belonging to specified address families; routes of other address families continue to be advertised according to the session-level MRAI setting.

The **no** form of this command disables rapid update for all address families.

Default no rapid-update

Parameters **l2-vpn** — Specifies the BGP rapid update for the 12-byte Virtual Switch Instance identifier (VSI-ID) value consisting of the 8-byte route distinguisher (RD) followed by a 4-byte value.

mvpn-ipv4 — Specifies BGP rapid update for the mvpn-ipv4 address family. The mvpn-pv4 address is a variable size value consisting of the 1-byte route type, 1-byte length and variable size that is route type specific. Route type defines encoding for the route type specific field. Length indicates the length in octets of the route type specific field.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mdt-safi — Specifies BGP rapid update for the mdt-safi address family. The address is a 16-byte value consisting of 12-byte route distinguisher (RD) followed by a 4-byte group address.

mvpn-ipv6 — Specifies BGP rapid update for the mvpn-ipv6 address family.

evpn — Specifies BGP rapid update for the evpn address family by including or removing EVPN routes from the set of routes that can trigger rapid update.

label-ipv4 — Includes or removes label-ipv4 routes from the set of routes that can trigger rapid update.

label-ipv6 — Includes or removes label-ipv6 routes from the set of routes that can trigger rapid update.

vpn-ipv4 — Includes or removes vpn-ipv4 routes from the set of routes that can trigger rapid update.

vpn-ipv6 — Includes or removes vpn-ipv6 routes from the set of routes that can trigger rapid update.

mcast-vpn-ipv4 — Includes or removes mcast-vpn-ipv4 routes from the set of routes that can trigger rapid update.

mcast-vpn-ipv6 — Includes or removes mcast-vpn-ipv6 routes from the set of routes that can trigger rapid update.

Platforms All

22.26 rapid-withdrawal

rapid-withdrawal

Syntax [**no**] **rapid-withdrawal**

Context **[Tree]** (config>service>vprn>bgp rapid-withdrawal)

Full Context configure service vprn bgp rapid-withdrawal

Description This command disables the delay (Minimum Route Advertisement) on sending BGP withdrawals. Normal route withdrawals may be delayed up to the minimum route advertisement to allow for efficient packing of BGP updates.

The **no** form of this command removes this command from the configuration and returns withdrawal processing to the normal behavior.

Default no rapid-withdrawal

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rapid-withdrawal

Syntax [**no**] **rapid-withdrawal**

Context **[Tree]** (config>router>bgp rapid-withdrawal)

Full Context configure router bgp rapid-withdrawal

Description This command disables the delay (Minimum Route Advertisement) on sending BGP withdrawals. Normal route withdrawals may be delayed up to the minimum route advertisement to allow for efficient packing of BGP updates.

The **no** form of this command removes this command from the configuration and returns withdrawal processing to the normal behavior.

Default no rapid-withdrawal

Platforms All

22.27 rat-type

rat-type

Syntax **rat-type** {**utran** | **geran** | **wlan** | **gan** | **hspa** | **eutran** | **virtual** | *id*}
no rat-type

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile rat-type)

Full Context configure subscriber-mgmt gtp peer-profile rat-type

Description This command configures the default Radio Access Type (RAT) signaled during GTP setup. RAT is the underlying physical connection method for a radio-based communication network. This can be overridden by RADIUS.

The **no** form of this command reverts to the default value.

Default rat-type wlan

Parameters **utran** — Specifies the signaled RAT type is UTRAN (1).

geran — Specifies the signaled RAT type is GERAN (2).

wlan — Specifies the signaled RAT type is WLAN (3).

gan — Specifies the signaled RAT type is GAN (4).

hspa — Specifies the signaled RAT type is HSPA Evolution (5).

eutran — Specifies the signaled RAT type is EUTRAN (6).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

virtual — Specifies the signaled RAT type is virtual (7).

id — Specifies the numeric RAT type value.

Values 0 to 255

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

rat-type

Syntax [**no**] **rat-type**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute rat-type)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute rat-type

Description This command enables the inclusion of the Radio Access Type in AAA protocols as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

rat-type

Syntax [**no**] **rat-type**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp rat-type)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp rat-type)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp rat-type
configure subscriber-mgmt diameter-application-policy nasreq include-avp rat-type

Description This command includes the RAT type.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt diameter-application-policy gx include-avp rat-type

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt diameter-application-policy nasreq include-avp rat-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.28 rate

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>hs-wrr-grp rate)

Full Context configure subscriber-mgmt sla-profile egress qos hs-wrr-group rate

Description This command configures the rate (PIR) override for the WRR group.

The **no** form of this command removes the rate from the configuration.

Parameters *rate* — Specifies the PIR expressed as a percentage of line rate in kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress>qos>queue rate)

Full Context configure subscriber-mgmt sla-profile egress qos queue rate

Description This command defines the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile then out-of-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent command's *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Parameters *pir-rate* — Defines the administrative PIR rate, in kb/s, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queues **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 2000000000, max

Default max

cir-rate — Defines the administrative CIR rate, kb/s, for the queue. The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer.

Values 0 to 2000000000, max

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>queue rate)

Full Context configure subscriber-mgmt sla-profile ingress qos queue rate

Description This command defines the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets through the switch fabric (for SAP ingress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. For SAP ingress, the CIR also defines the rate that packets are considered in-profile by the system. In-profile then out-of-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The CIR can be used by the queue's parent command's *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP ingress or SAP egress QoS policy with the *queue-id*.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queues **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 2000000000, max

Default max

cir-rate — Specifies the **cir** parameter used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer.

Values 0 to 2000000000, max

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

rate

Syntax **rate** {**max** | *rate*} [**cir** {**max** | *rate*}]

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>policer rate)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>policer rate)

Full Context configure subscriber-mgmt sla-profile egress qos policer rate
configure subscriber-mgmt sla-profile ingress qos policer rate

Description This command is used to configure the policer's metering and optional profiling rates. The metering rate is used by the system to configure the policer's PIR leaky bucket's decrement rate while the profiling rate configures the policer's CIR leaky bucket's decrement rate. The decrement function empties the bucket while packets applied to the bucket attempt to fill it based on each packets size. If the bucket fills faster than how much is decremented per packet, the bucket's depth eventually reaches it's exceed (CIR) or violate (PIR) threshold. The **cbs**, **mbs**, and **high-prio-only** commands are used to configure the policer's PIR and CIR thresholds.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a packet arrives at the policer while the bucket's depth is less than the threshold associated with the packet, the packet is considered to be conforming to the bucket's rate. If the bucket depth is equal to or greater than the threshold, the packet is considered to be in the exception state. For the CIR bucket, the exception state is exceeding the CIR rate while the PIR bucket's exception state is violating the PIR bucket rate. If the packet is violating the PIR, the packet is marked red and is discarded. If the packet is not red, it may be green or yellow based on the conforming or exceeding state from the CIR bucket.

When a packet is red neither the PIR or CIR bucket depths are incremented by the packets size. When the packet is yellow the PIR bucket is incremented by the packet size, but the CIR bucket is not. When the packet is green, both the PIR and CIR buckets are incremented by the packet size. This ensures that conforming packets impact the bucket depth while exceeding or violating packets do not.

The policer's **adaptation-rule** command settings are used by the system to convert the specified rates into hardware timers and decrement values for the policer's buckets.

By default, the policer's metering rate is **max** and the profiling rate is 0 kb/s (all packets out-of-profile).

The **rate** settings defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command restores the default metering and profiling rate to a policer.

Parameters {**max** | *rate*} — Specifies the packet byte offset. Specifying the keyword **max** or an explicit **rate** (in kilobits per second) parameter directly following the rate command is required and identifies the policer's metering rate for the PIR leaky bucket. When the policer is first created, the metering rate defaults to max. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used is equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to max.

Values max or 1 to 2000000000

cir {**max** | *rate*} — Specifies the packet byte offset. The optional **cir** keyword is used to override the default CIR rate of the policer. Specifying the keyword **max** or an explicit **rate** (in kilobits per second) parameter directly following the cir keyword is required and identifies the policer's profiling rate for the CIR leaky bucket. When the policer is first created, the profiling rate defaults to 0 kb/s. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used is equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to **max**.

Values max or 0 to 2000000000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate

Syntax **rate** *kilobits-per-second*
no rate

Context **[Tree]** (config>service>ies>if>sap>egress>agg-rate rate)
[Tree] (config>service>ies>sub-if>grp-if>sap>egress>agg-rate rate)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress>agg-rate rate)

Full Context configure service ies interface sap egress agg-rate rate
configure service ies subscriber-interface group-interface sap egress agg-rate rate
configure service vprn subscriber-interface group-interface sap egress agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object (SAP, subscriber, Vport, and so on).

The **no** form of this command removes an explicit rate value from the aggregate rate therefore returning it to its default value.

Parameters *kilobits-per-second* — Specifies the rate limit for the SAP, in kilobits per second.

Values 1 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap egress agg-rate rate
- configure service vprn subscriber-interface group-interface sap egress agg-rate rate

All

- configure service ies interface sap egress agg-rate rate

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>queue rate)
[Tree] (config>service>ies>if>sap>ingress>queue-override>queue rate)
[Tree] (config>service>vpls>sap>egress>queue-override>queue rate)
[Tree] (config>service>vpls>sap>ingress>queue-override>queue rate)

Full Context configure service ies interface sap egress queue-override queue rate
configure service ies interface sap ingress queue-override queue rate
configure service vpls sap egress queue-override queue rate
configure service vpls sap ingress queue-override queue rate

Description This command overrides specific attributes of the specified queue's Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile, then out-of-profile, packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (max, 0).

Default rate max cir 0

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 6400000000, **max**

Default max

cir-rate — Overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer.

Values 0 to 6400000000, **max**

Default 0

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap>egress>sched-override>scheduler rate)

Full Context configure service vpls sap egress scheduler-override scheduler rate

Description This command overrides specific attributes of the specified scheduler rate. The **rate** command defines the maximum bandwidth that the scheduler can offer its policers, child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler assumes that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's PIR and CIR parameters to the value configured in the applied scheduler policy.

Default rate max cir sum

Parameters *pir-rate* — Specifies the PIR rates. The **pir** parameter accepts a step multiplier value that specifies the multiplier used to determine the PIR rate at which the queue operates. A value of 0 to 100000000 or the keyword **max** is accepted. Any other value results in an error without modifying the current PIR rate.

To calculate the actual PIR rate, the rate described by the queue's **rate** is multiplied by the *pir-rate*.

The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default **pir** and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate at which the queue is allowed to forward packets in a given second, thus shaping the queue's output.

The PIR parameter for SAP ingress queues do not have a negate (**no**) function. To return the queue's PIR rate to the default value, that value must be specified as the PIR value.

Values 1 to 6400000000, max

Default max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-rate — Specifies the CIR rate. The **cir** parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue operate. A value of 0 to 250 or the keyword max is accepted. Any other value results in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the **rate pir** *pir-rate* is multiplied by the *cir-rate*. If the **cir** is set to max, then the CIR rate is set to infinity.

The context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a policer or queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods.

Values 0 to 6400000000, max, sum

Default sum

Platforms All

rate

Syntax **rate** *rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>subscr-mgmt>isa-policer rate)

Full Context configure subscriber-mgmt isa-policer rate

Description This command specifies at which rate the policer drains packets. The **cir** value is only supported on dual-bucket-bandwidth policers. If rate **max** is configured, no actual rate limitations are applied.

The **no** form of this command reverts to the default.

Parameters *rate* — Specifies the rate in kb/s.

Values 1 to 100000000, **max**

Default max

cir-rate — Specifies the CIR rate in kb/s.

Values 1 to 100000000, **max**

Default max

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

rate

Syntax **rate** {**max** | **rate**}
no rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>wlan-gw>egress>agg-rate rate)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>egress>agg-rate rate)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress agg-rate rate
configure service vprn subscriber-interface group-interface wlan-gw egress agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object (SAP, subscriber, Vport, and so on).

The **no** form of this command reverts to the default.

rate

Syntax **rate** {*rate* | **max**} [**cir** {**max** | *rate*}]
no rate

Context [Tree] (config>card>fp>ingress>access>qgrp>policer-over>plcr rate)
[Tree] (config>card>fp>ingress>network>qgrp>policer-over>plcr rate)

Full Context configure card fp ingress access queue-group policer-override policer rate
configure card fp ingress network queue-group policer-override policer rate

Description This command configures the policer's metering and optional profiling rates. The metering rate is used by the system to configure the policer's PIR leaky bucket's decrement rate while the profiling rate configures the policer's CIR leaky bucket's decrement rate. The decrement function empties the bucket while packets applied to the bucket attempt to fill it based on its packet size. If the bucket fills faster than how much is decremented per packet, the bucket's depth eventually reaches it's exceeded (CIR) or violate (PIR) threshold. The **cbs**, **mbs**, and **high-prio-only** commands are used to configure the policer's PIR and CIR thresholds.

If a packet arrives at the policer while the bucket's depth is less than the threshold associated with the packet, the packet is considered to be conforming to the bucket's rate. If the bucket depth is equal to or greater than the threshold, the packet is considered to be in the exception state. For the CIR bucket, the exception state is exceeding the CIR rate while the PIR bucket's exception state is violating the PIR bucket rate. If the packet is violating the PIR, the packet is marked red and will be discarded. If the packet is not red, it may be green or yellow based on the conforming or exceeding state from the CIR bucket.

When a packet is red neither the PIR nor the CIR bucket depths are incremented by the packets size. When the packet is yellow the PIR bucket is incremented by the packet size, but the CIR bucket is not. When the packet is green, both the PIR and CIR buckets are incremented by the packet size. This ensures that conforming packets impact the bucket depth while exceeding or violating packets do not.

The policer's **adaptation-rule** command settings are used by the system to convert the specified rates into hardware timers and decrement values for the policer's buckets.

By default, the policer's metering rate is **max** and the profiling rate is 0 kb/s (all packets out-of-profile).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **rate** settings defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command reverts to the default metering and profiling rate of a policer.

Parameters {*rate* | **max**} — Specifying the keyword **max** or an explicit *rate* parameter directly following the rate command is required and identifies the policer's metering rate for the PIR leaky bucket. When the policer is first created, the metering rate defaults to max. The *kilobits-per-second* value must be expressed as an integer and defines the rate in kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When max is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to max.

Values **max** or 1 to 2000000000

cir {**max** | *rate*} — The optional **cir** keyword is used to override the default CIR rate of the policer. Specifying the keyword max or an explicit *rate* parameter directly following the cir keyword is required and identifies the policer's profiling rate for the CIR leaky bucket. When the policer is first created, the profiling rate defaults to 0 kb/s. The *kilobits-per-second* value must be expressed as an integer and defines the rate in kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When max is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to max.

Values **max** or 0 to 2000000000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

rate

Syntax **rate** *kilobits-per-second*
no rate

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>agg-rate rate)
[Tree] (config>port>ethernet>network>egr>qgrp>agg-rate rate)

Full Context configure port ethernet access egress queue-group agg-rate rate
configure port ethernet network egress queue-group agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object.

The **no** form of this command removes an explicit rate value from the aggregate rate returning it to its default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *kilobits-per-second* — Specifies the rate limit for the queue group, in kilobits per second.

Values 1 to 3200000000, **max**

Platforms All

rate

Syntax **rate** *kilobits-per-second*
no rate

Context **[Tree]** (config>port>ethernet>access>egr>vport>agg-rate rate)
[Tree] (config>port>sonet-sdh>path>access>egr>vport>agg-rate rate)

Full Context configure port ethernet access egress vport agg-rate rate
configure port sonet-sdh path access egress vport agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object.

The **no** form of this command removes an explicit rate value from the aggregate rate returning it to its default value.

Parameters *kilobits-per-second* — Specifies the rate limit for the Vport, in kilobits per second.

Values 1 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path access egress vport agg-rate rate

All

- configure port ethernet access egress vport agg-rate rate

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>qover>q rate)
[Tree] (config>port>ethernet>access>ing>qgrp>qover>q rate)
[Tree] (config>port>ethernet>network>egr>qover>q rate)

Full Context configure port ethernet access egress queue-group queue-overrides queue rate
configure port ethernet access ingress queue-group queue-overrides queue rate
configure port ethernet network egress queue-overrides queue rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile then out-of-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **rate** is performed under the **hs-wrr-group** within the egress queue group template.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Default rate max cir 0 - The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the pir-rate value.

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits per second, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 200000000, max

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR used by the queue, in kilobits per second. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer.

Values 0 to 200000000, max

Default 0

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>sched-override>scheduler rate)
[Tree] (config>port>ethernet>access>ing>qgrp>sched-override>scheduler rate)

Full Context configure port ethernet access egress queue-group scheduler-override scheduler rate
configure port ethernet access ingress queue-group scheduler-override scheduler rate

Description This command can be used to override specific attributes of the specified scheduler rate. The rate command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is max. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child policers, queues, and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's PIR and CIR parameters to the value configured in the applied scheduler policy.

Parameters *pir-rate* — Specifies the PIR rate, in kilobits per second. Any other value will result in an error without modifying the current PIR rate.

Values 1 to 6400000000, **max**

cir-rate — Specifies the CIR rate, in kilobits per second. If the CIR is set to **max**, then the CIR rate is set to infinity. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers, policers, or queues.

Values 0 to 6400000000, **sum**, **max**

Platforms All

rate

Syntax **rate** *rate*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no rate

Context [Tree] (config>port>ethernet>egress>hs-sec-shaper>agg rate)
[Tree] (config>port>ethernet>egress>hs-sec-shaper>class rate)

Full Context configure port ethernet egress hs-secondary-shaper aggregate rate
configure port ethernet egress hs-secondary-shaper class rate

Description This command specifies the rate allowed for the HS secondary shaper's aggregate rate and per-class rates.

The **no** form of this command reverts to the default.

Default rate max

Parameters *rate* — Specifies the maximum rate in kilobits per second. When the **max** keyword follows the **rate** keyword, the bandwidth limitation is removed from the aggregate or class. The **max** keyword is mutually exclusive to the **rate** parameter. Either **max** or a rate value must follow the **rate** keyword.

Values 1 to 100000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** *kilobits-per-second*
no rate

Context [Tree] (config>service>apipe>sap>egress>agg-rate rate)
[Tree] (config>service>cpipe>sap>egress>agg-rate rate)
[Tree] (config>service>epipe>sap>egress>agg-rate rate)
[Tree] (config>service>fpipe>sap>egress>agg-rate rate)
[Tree] (config>service>ipipe>sap>egress>agg-rate rate)

Full Context configure service apipe sap egress agg-rate rate
configure service cpipe sap egress agg-rate rate
configure service epipe sap egress agg-rate rate
configure service fpipe sap egress agg-rate rate
configure service ipipe sap egress agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object (SAP, subscriber, Vport, and so on).

The **no** form of this command removes an explicit rate value from the aggregate rate returning it to its default value.

Parameters *kilobits-per-second* — The enforced aggregate rate for all queues associated with the agg-rate context, in kilobits per second.

Values 1 to 6400000000, **max**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress agg-rate rate
- configure service fpipe sap egress agg-rate rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress agg-rate rate

All

- configure service ipipe sap egress agg-rate rate
- configure service epipe sap egress agg-rate rate

rate

Syntax **rate** {*rate* | **max**} [**cir** {*rate* | **max**}]

Context **[Tree]** (config>service>apipe>sap>egress>policer-over>plcr rate)
[Tree] (config>service>apipe>sap>ingress>policer-over>plcr rate)
[Tree] (config>service>cpipe>sap>egress>policer-over>plcr rate)
[Tree] (config>service>cpipe>sap>ingress>policer-over>plcr rate)
[Tree] (config>service>epipe>sap>egress>policer-over>plcr rate)
[Tree] (config>service>epipe>sap>ingress>policer-over>plcr rate)
[Tree] (config>service>fpipe>sap>egress>policer-over>plcr rate)
[Tree] (config>service>fpipe>sap>ingress>policer-over>plcr rate)
[Tree] (config>service>ipipe>sap>egress>policer-over>plcr rate)
[Tree] (config>service>ipipe>sap>ingress>policer-over>plcr rate)

Full Context configure service apipe sap egress policer-override policer rate
configure service apipe sap ingress policer-override policer rate
configure service cpipe sap egress policer-override policer rate
configure service cpipe sap ingress policer-override policer rate
configure service epipe sap egress policer-override policer rate
configure service epipe sap ingress policer-override policer rate
configure service fpipe sap egress policer-override policer rate
configure service fpipe sap ingress policer-override policer rate
configure service ipipe sap egress policer-override policer rate
configure service ipipe sap ingress policer-override policer rate

Description This command within the SAP ingress and egress policer-overrides contexts is used to override the sap-ingress and sap-egress QoS policy configured rate parameters for the specified policer-id.

The **no** rate command is used to restore the policy defined metering and profiling rate to a policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **rate** *rate* — Specifies the policer instance metering rate for the PIR leaky bucket, in kilobits per second. The integer value is multiplied by 1000 to derive the actual rate in bits per second.

Values 1 to 6400000000

cir *rate* — Specifies the overriding value for the policy-derived profiling rate of the policer, in kilobits per second. The integer value is multiplied by 1000 to derive the actual rate in bits per second.

Values 0 to 6400000000

max — Uses the maximum policer rate, equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR or CIR used is equivalent to **max**.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress policer-override policer rate
- configure service fpipe sap egress policer-override policer rate
- configure service cpipe sap egress policer-override policer rate
- configure service fpipe sap ingress policer-override policer rate

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap egress policer-override policer rate
- configure service epipe sap ingress policer-override policer rate
- configure service ipipe sap ingress policer-override policer rate
- configure service epipe sap egress policer-override policer rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap egress policer-override policer rate
- configure service apipe sap ingress policer-override policer rate

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>service>epipe>sap>egress>queue-override>hs-wrr-group rate)
[Tree] (config>service>ipipe>sap>egress>queue-override>hs-wrr-group rate)

Full Context configure service epipe sap egress queue-override hs-wrr-group rate
configure service ipipe sap egress queue-override hs-wrr-group rate

Description This command overrides the scheduling rate applied to the HS WRR group in kb/s. A rate can be specified in kb/s or the keyword **max** can be used to remove the bandwidth limitation on the HS WRR group. The override rate type must match the corresponding rate type within the applied QoS policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the rate override value from the configuration.

Parameters *rate* — Specifies the scheduling rate of the HS WRR group in kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>service>apipe>sap>egress>queue-override>queue rate)
[Tree] (config>service>apipe>sap>ingress>queue-override>queue rate)
[Tree] (config>service>cpipe>sap>egress>queue-override>queue rate)
[Tree] (config>service>cpipe>sap>ingress>queue-override>queue rate)
[Tree] (config>service>epipe>sap>egress>queue-override>queue rate)
[Tree] (config>service>epipe>sap>ingress>queue-override>queue rate)
[Tree] (config>service>fpipe>sap>egress>queue-override>queue rate)
[Tree] (config>service>fpipe>sap>ingress>queue-override>queue rate)
[Tree] (config>service>ipipe>sap>egress>queue-override>queue rate)
[Tree] (config>service>ipipe>sap>ingress>queue-override>queue rate)

Full Context configure service apipe sap egress queue-override queue rate
configure service apipe sap ingress queue-override queue rate
configure service cpipe sap egress queue-override queue rate
configure service cpipe sap ingress queue-override queue rate
configure service epipe sap egress queue-override queue rate
configure service epipe sap ingress queue-override queue rate
configure service fpipe sap egress queue-override queue rate
configure service fpipe sap ingress queue-override queue rate
configure service ipipe sap egress queue-override queue rate
configure service ipipe sap ingress queue-override queue rate

Description This command can be used to override specific attributes of the specified queue's Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters.

The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile and then out-of-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the **rate** is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Default rate max cir 0

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits per second, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 6400000000, **max**

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers, policers, or queues.

Values 0 to 6400000000, **max**, **sum**

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress queue-override queue rate
- configure service fpipe sap ingress queue-override queue rate
- configure service cpipe sap egress queue-override queue rate
- configure service cpipe sap ingress queue-override queue rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress queue-override queue rate
- configure service apipe sap ingress queue-override queue rate

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ipipe sap egress queue-override queue rate
- configure service epipe sap ingress queue-override queue rate
- configure service epipe sap egress queue-override queue rate
- configure service ipipe sap ingress queue-override queue rate

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>service>apipe>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>apipe>sap>ingress>sched-override>scheduler rate)
[Tree] (config>service>cpipe>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>cpipe>sap>ingress>sched-override>scheduler rate)
[Tree] (config>service>fpipe>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>fpipe>sap>ingress>sched-override>scheduler rate)
[Tree] (config>service>ipipe>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>ipipe>sap>ingress>sched-override>scheduler rate)
[Tree] (config>service>epipe>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>epipe>sap>ingress>sched-override>scheduler rate)

Full Context configure service apipe sap egress scheduler-override scheduler rate
configure service apipe sap ingress scheduler-override scheduler rate
configure service cpipe sap egress scheduler-override scheduler rate
configure service cpipe sap ingress scheduler-override scheduler rate
configure service epipe sap egress scheduler-override scheduler rate
configure service epipe sap ingress scheduler-override scheduler rate
configure service fpipe sap egress scheduler-override scheduler rate
configure service fpipe sap ingress scheduler-override scheduler rate
configure service ipipe sap egress scheduler-override scheduler rate
configure service ipipe sap ingress scheduler-override scheduler rate

Description This command can be used to override specific attributes of the specified scheduler rate. The **rate** command defines the maximum bandwidth that the scheduler can offer its child policers, queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child policers or queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child policers, queues, and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's PIR and CIR parameters to the values configured in the applied scheduler policy.

Parameters *pir-rate* — The **pir** parameter accepts the **max** keyword or a value in kilobits per second. Any other value will result in an error without modifying the current PIR rate.

Values 1 to 6400000000, **max**

cir *cir-rate* — The **cir** parameter accepts a value in kilobits per second or the **max** keyword. Any other value will result in an error without modifying the current CIR rate.

If the **cir** parameter is set to **max**, then the CIR rate is set to infinity but bounded by the PIR rate.

The **sum** keyword specifies that the CIR will be used as the summed CIR values of the children schedulers, policers, or queues.

Values 0 to 6400000000, **max**, **sum**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress scheduler-override scheduler rate
- configure service fpipe sap ingress scheduler-override scheduler rate
- configure service cpipe sap egress scheduler-override scheduler rate
- configure service fpipe sap egress scheduler-override scheduler rate

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress scheduler-override scheduler rate
- configure service apipe sap ingress scheduler-override scheduler rate

All

- configure service epipe sap ingress scheduler-override scheduler rate
- configure service ipipe sap ingress scheduler-override scheduler rate
- configure service epipe sap egress scheduler-override scheduler rate
- configure service ipipe sap egress scheduler-override scheduler rate

rate

Syntax **rate** *kilobits-per-second*
no rate

Context **[Tree]** (config>service>vpls>sap>egress>agg-rate rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>template>vpls-sap-template>egress>agg-rate rate)
[Tree] (config>service>vpls>sap>egress>encap-defined-qos>encap-group>agg-rate rate)

Full Context configure service template vpls-sap-template egress agg-rate rate
configure service vpls sap egress agg-rate rate
configure service vpls sap egress encap-defined-qos encap-group agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the **agg-rate** context. A rate must be specified for the **agg-rate** context to be considered active on the context's object (SAP, subscriber, Vport, and so on.).

The **no** form of this command removes an explicit rate value from the aggregate rate returning it to its default value.

Parameters *kilobits-per-second* — The enforced aggregate rate for all queues associated with the **agg-rate** context, in kilobits per second.

Values 1 to 6400000000, **max**

Platforms All

rate

Syntax **rate** {*rate* | **max**} [**cir** {**max** | *rate*}]

Context [Tree] (config>service>vpls>sap>egress>policer-override>plcr rate)
[Tree] (config>service>vpls>sap>ingress>policer-override>plcr rate)

Full Context configure service vpls sap egress policer-override policer rate
configure service vpls sap ingress policer-override policer rate

Description This command within the SAP ingress and egress policer-overrides contexts is used to override the sap-ingress and sap-egress QoS policy configured rate parameters for the specified policer-id.

The **no** form of this command removes the **rate** override so that the **rate** configured for the policer in the applied SAP egress QoS policy is used.

Parameters {*rate* | **max**} — Specifying the keyword **max** or an explicit kilobits per second parameter directly following the rate override command is required and identifies the policer instance's metering rate for the PIR leaky bucket. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to **max**.

Values 1 to 6400000000, **max**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir {**max** | *rate*} — The optional **cir** keyword is used to override the policy derived profiling rate of the policer. Specifying the keyword **max** or an explicit kilobits per second parameter directly following the **cir** keyword is required. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to **max**.

Values 0 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>service>vpls>sap>egress>queue-override>hs-wrr-group rate)

Full Context configure service vpls sap egress queue-override hs-wrr-group rate

Description This command overrides the scheduling rate applied to the HS WRR group in kb/s. Alternatively, the keyword **max** can be specified which removes the bandwidth limitation on the HS WRR group. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the rate override value from the configuration.

Parameters *rate* — Specifies the scheduling rate of the HS WRR group in kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** {*rate* | **max**} [**cir** {**max** | *rate*}]

Context **[Tree]** (config>service>ies>if>sap>egress>policer-override>plcr rate)
[Tree] (config>service>ies>if>sap>ingress>policer-override>plcr rate)

Full Context configure service ies interface sap egress policer-override policer rate
configure service ies interface sap ingress policer-override policer rate

Description This command within the SAP ingress and egress policer-overrides contexts is used to override the sap-ingress and sap-egress QoS policy configured rate parameters for the specified policer-id.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the **rate** override so that the **rate** configured for the policer in the applied SAP egress QoS policy is used.

Parameters {*rate* | **max**} — Specifying the keyword **max** or an explicit kilobits per second parameter directly following the rate override command is required and identifies the policer instance's metering rate for the PIR leaky bucket. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to **max**.

Values 1 to 6400000000, **max**

cir {**max** | *rate*} — The optional **cir** keyword is used to override the policy derived profiling rate of the policer. Specifying the keyword **max** or an explicit kilobits per second parameter directly following the **cir** keyword is required. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to **max**.

Values 0 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>service>ies>if>sap>egress>queue-override>hs-wrr-group rate)

Full Context configure service ies interface sap egress queue-override hs-wrr-group rate

Description This command overrides the scheduling rate applied to the HS WRR group in Kb/s. Alternatively, the keyword **max** can be specified which removes the bandwidth limitation on the HS WRR group. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the rate override value from the configuration.

Parameters *rate* — Specifies the scheduling rate of the HS WRR group in Kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>service>ies>if>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>ies>if>sap>ingress>sched-override>scheduler rate)

Full Context configure service ies interface sap egress scheduler-override scheduler rate
configure service ies interface sap ingress scheduler-override scheduler rate

Description This command can be used to override specific attributes of the specified scheduler rate. The **rate** command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's PIR and CIR parameters to the value configured in the applied scheduler policy.

Parameters *pir-rate* — The **pir** parameter accepts a value in kilobits per second, or the keyword **max**. Any other value will result in an error without modifying the current PIR rate.

Values 1 to 6400000000, **max**

cir-rate — This parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value in kilobits per second or the keywords **max** or **sum** is accepted. Any other value will result in an error without modifying the current CIR rate.

If the **cir** is set to max, then the CIR rate is set to infinity but is restricted by the PIR rate.

The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers, policers, or queues.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For **egress>sched-override>scheduler** and **ingress>sched-override>scheduler**:

Values 0 to 6400000000, **max**, **sum**

Platforms All

rate

Syntax **rate** *kilobits-per-second*
no rate

Context **[Tree]** (config>service>vprn>if>sap>egress>agg-rate rate)

Full Context configure service vprn interface sap egress agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object.

The **no** form of this command removes an explicit rate value from the aggregate rate returning it to its default value.

Parameters *kilobits-per-second* — Specifies the rate limit for the SAP, in kilobits per second.

Values 1 to 6400000000, max

Platforms All

rate

Syntax **rate** {*rate* | **max**} [**cir** {**max** | *rate*}]

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-override>plcr rate)
[Tree] (config>service>vprn>if>sap>ingress>policer-override>plcr rate)

Full Context configure service vprn interface sap egress policer-override policer rate
configure service vprn interface sap ingress policer-override policer rate

Description This command within the SAP ingress and egress policer-overrides contexts is used to override the sap-ingress and sap-egress QoS policy configured rate parameters for the specified policer-id.

The **no** form of this command restores the policy defined metering and profiling rate to a policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters {*rate* | **max**} — Specifying the keyword **max** or an explicit kilobits per second parameter directly following the rate override command is required and identifies the policer instance's metering rate for the PIR leaky bucket. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to **max**.

Values 1 to 6400000000, **max**

cir {**max** | *rate*} — The optional **cir** keyword is used to override the policy derived profiling rate of the policer. Specifying the keyword **max** or an explicit kilobits per second parameter directly following the **cir** keyword is required. The kilobits per second value must be expressed as an integer and defines the rate in kilobits per second. The integer value is multiplied by 1,000 to derive the actual rate in bits per second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to **max**.

Values 0 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>service>vprn>if>sap>egress>queue-override>hs-wrr-group rate)

Full Context configure service vprn interface sap egress queue-override hs-wrr-group rate

Description This command overrides the scheduling rate applied to the HS WRR group in Kb/s. Alternatively, the keyword **max** can be specified which removes the bandwidth limitation on the HS WRR group. The override rate type must match the corresponding rate type within the applied QoS policy.

The **no** form of this command removes the rate override value from the configuration.

Parameters *rate* — Specifies the scheduling rate of the HS WRR group in Kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no rate

Context [Tree] (config>service>vprn>if>sap>egress>queue-override>queue rate)
[Tree] (config>service>vprn>if>sap>ingress>queue-override>queue rate)

Full Context configure service vprn interface sap egress queue-override queue rate
configure service vprn interface sap ingress queue-override queue rate

Description This command can be used to override specific attributes of the specified queue's Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the rate is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Default rate max cir 0

Parameters *pir-rate* — Defines the administrative PIR rate, in kb/s, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 6400000000, **max**

Default max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-rate — Defines the administrative CIR rate, in kb/s, for the queue. The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer.

Values 0 to 6400000000, **max**

Default 0

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>service>vprn>if>sap>egress>sched-override>scheduler rate)
[Tree] (config>service>vprn>if>sap>ingress>sched-override>scheduler rate)

Full Context configure service vprn interface sap egress scheduler-override scheduler rate
configure service vprn interface sap ingress scheduler-override scheduler rate

Description This command can be used to override specific attributes of the specified scheduler rate. The **rate** command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child policers and queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's PIR and CIR parameters to the value configured in the applied scheduler policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *pir-rate* — Specifies the PIR rate for the scheduler. The **pir** parameter accepts a value in kb/s, or the **max** keyword. Any other value will result in an error without modifying the current PIR rate.

Values 1 to 6400000000, **max**

cir-rate — Specifies the CIR rate for the scheduler. The **cir** parameter accepts a value in kb/s, or the **max** or **sum** keywords. Any other value will result in an error without modifying the current CIR rate.

If the **cir** is set to **max**, then the CIR rate is set to infinity, but is limited by the *pir-rate*.

If the **cir** is set to **sum**, then the CIR rate is set to the summed CIR values of the children schedulers, policers, or queues.

Values 0 to 6400000000, **max**, **sum**

Platforms All

rate

Syntax **rate** *sample-rate*
no rate

Context **[Tree]** (config>app-assure>group>cflowd>volume rate)

Full Context configure application-assurance group cflowd volume rate

Description This command configures the sampling rate of packets for the cflowd export of application assurance volume statistics.

The **no** form of this command reverts to the default value.

Parameters *sample-rate* — Specifies the rate at which to sample packets for the cflowd export of application assurance volume statistics.

Values 1 to 10000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>app-assure>group>policer rate)
[Tree] (config>app-assure>group>tod-override rate)

Full Context configure application-assurance group policer rate
configure application-assurance group policer tod-override rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the administrative PIR and CIR for bandwidth policers and flow setup rate limits for flow policers. The actual rate sustained by the flow can be limited by other policers that may be applied to that flow's traffic. This command does not apply to flow-count-limit policers.

The **cir** option is applicable only to dual-bucket bandwidth policers. It is recommended to configure flow setup rate subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

The **no** form of this command resets the values to defaults.

Default rate max cir 0

Parameters *pir-rate* — Specifies an integer for the PIR rate in kb/s for bandwidth policers.

Values 1 to 100000000, **max** or flows/sec

cir-rate — Specifies an integer for the CIR rate in kb/s.

Values 0 to 100000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

rate

Syntax **rate** *sample-rate*
no rate

Context **[Tree]** (debug>app-assure>group>http-host-recorder rate)
[Tree] (debug>app-assure>group>port-recorder rate)

Full Context debug application-assurance group http-host-recorder rate
debug application-assurance group port-recorder rate

Description This command configures the sampling rate for the recorded http host, a sampling rate of 10 will sample one out of 10 http-host.

Parameters *sample-rate* — Specifies the sample rate.

Values 1 to 10000

Default 100

Output The following configuration records http-host entries ending with ".com" as a result of the expression filter configuration. It will not record any other HTTP host values since the default-filter-action set to no-record. The http-host entries analyzed by the recorder in the first place are http-host-app-filter-candidates.

Sample Output

```
7750# show debug
debug
    application-assurance
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
            group 1:1
                http-host-recorder
                    filter
                        default-filter-action no-record
                        expression 1 http-host eq "*.com$" record
                        record http-host-app-filter-candidates
                    exit
                    rate 100
                    no shutdown
                exit
            exit
        exit
    exit
```

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>qos>plcr-ctrl-plcy>tier>arbiter rate)

Full Context configure qos policer-control-policy tier arbiter rate

Description This command is used to define the maximum bandwidth an instance of the arbiter can receive from its parent tier 1 arbiter or the root arbiter. The arbiter instance enforces this limit by calculating the bandwidth each of its child policers should receive relative to their offered loads, parenting parameters, and individual rate limits, and using that derived rate as a child PIR decrement rate override. The override will not exceed the child policer's administrative rate limit and the aggregate of all the child PIR decrement rates will not exceed the specified arbiter rate limit.

The arbiter's policy defined rate value may be overridden at the SAP or sub-profile where the **policer-control-policy** is applied. Specifying an override prevents the arbiter from being removed from the policer control policy until the override is removed.

The **no** form of this command is used to remove a rate limit from the arbiter at the policer control policy level. The policy level rate limit for the arbiter will return to the default value of **max**. The **no rate** command has no effect on instances of the arbiter where a rate limit override has been defined.

Default rate max

Parameters *rate* — Enter an integer representing the rate limit in kilobits per second.

Values 1 to 6400000000, **max**

max — When **max** is specified, the arbiter does not enforce a rate limit on its child policers or arbiters other than the individual rate limits enforced at the child level.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate

Syntax **rate** {**max** | *pir-rate*} [**cir** {**max** | *cir-rate*}]

Context **[Tree]** (config>qos>sap-ingress>policer rate)
[Tree] (config>qos>sap-egress>policer rate)

Full Context configure qos sap-egress policer rate
configure qos sap-ingress policer rate

Description This command is used to configure the policer's metering and optional profiling rates. The metering rate is used by the system to configure the policer's PIR leaky bucket's decrement rate while the profiling rate configures the policer's CIR leaky bucket's decrement rate. The decrement function empties the bucket while packets applied to the bucket attempt to fill it based on each packet's size. If the bucket fills faster than how much is decremented per packet, the bucket's depth eventually reaches its exceed (CIR) or violate (PIR) threshold. The **cbs**, **mbs**, and **high-prio-only** commands are used to configure the policer's PIR and CIR thresholds.

If a packet arrives at the policer while the bucket's depth is less than the threshold associated with the packet, the packet is considered to be conforming to the bucket's rate. If the bucket depth is equal to or greater than the threshold, the packet is considered to be in the exception state. For the CIR bucket, the exception state is exceeding the CIR rate while the PIR bucket's exception state is violating the PIR bucket rate. If the packet is violating the PIR, the packet is marked red and will be discarded. If the packet is not red, it may be green or yellow, based on the conforming or exceeding state from the CIR bucket.

When a packet is red, neither the PIR nor CIR bucket depths are incremented by the packets size. When the packet is yellow, the PIR bucket is incremented by the packet size, but the CIR bucket is not. When the packet is green, both the PIR and CIR buckets are incremented by the packet size. This ensures that conforming packets impact the bucket depth while exceeding or violating packets do not.

The policer's **adaptation-rule** command settings are used by the system to convert the specified rates into hardware timers and decrement values for the policer's buckets.

By default, the policer's metering rate is **max** and the profiling rate is 0 kb/s (all packets out-of-profile).

The **rate** settings defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied.

The **no** form of this command is used to restore the default metering and profiling rate to a policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **{max | *pir-rate*}** — Specifying the keyword **max** or an explicit *pir-rate* parameter directly following the rate command is required and identifies the policer's metering rate for the PIR leaky bucket. When the policer is first created, the metering rate defaults to max. The *pir-rate* value must be expressed as an integer and defines the rate in kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When max is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to max.

Values 1 to 6400000000, **max**

cir {max | *cir-rate*} — The optional **cir** keyword is used to override the default CIR rate of the policer. Specifying the keyword max or an explicit *cir-rate* parameter directly following the cir keyword is required and identifies the policer's profiling rate for the CIR leaky bucket. When the policer is first created, the profiling rate defaults to 0 kb/s. The *cir-rate* value must be expressed as an integer and defines the rate in kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to max.

Values 0 to 6400000000, **max**

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*] [**fir** *fir-rate*]
rate *pir-rate* **police**
no rate

Context **[Tree]** (config>qos>sap-ingress>queue rate)

Full Context configure qos sap-ingress queue rate

Description This command defines the administrative Peak Information Rate (PIR), the administrative Committed Information Rate (CIR), and the administrative Fair Information Rate (FIR) parameters for the queue.

The PIR defines the maximum rate that the queue can transmit packets through the switch fabric (for SAP ingress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. For SAP ingress, the CIR also defines the rate that packets are considered in-profile by the system, unless **cir-non-profiling** is configured. In-profile, then out-of-profile, packets are preferentially queued by the system at egress and at subsequent next-hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The FIR defines an additional rate at which the system prioritizes the queue over other queues competing for the same bandwidth above that used by the CIR.

The **rate** command can be executed at any time, altering the PIR, CIR, and FIR for all queues created through the association of the SAP ingress QoS policy with the *queue-id*.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0, 0).

Default rate max cir 0 fir 0

Parameters *pir-rate* — Defines the administrative PIR, in kilobits per second, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and the value must be given as a positive integer.

The actual PIR is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 6400000000, **max**

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR, in kilobits per second, used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and the value must be given as a positive integer. The actual CIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 0 to 6400000000, **max**

Default 0

fir-rate — The **fir** parameter overrides the default administrative FIR, in kilobits per second, used by the queue. When the **rate** command is executed, an FIR setting is optional. When the **rate** command has not been executed or the **fir** parameter is not explicitly specified, the default FIR (0) is assumed.

Fractional values are not allowed and the value must be given as a positive integer. The actual FIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

Values 0 to 6400000000, **max**

Default 0

police — Specifies that traffic feeding into the queue instance above the specified PIR rate will be dropped. When the **police** keyword is defined, only the PIR rate may be overridden.

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>qos>sap-egress>queue rate)

Full Context configure qos sap-egress queue rate

Description This command defines the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

When configured on an egress HSQ queue group queue, the **cir** keyword is ignored.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the rate is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default rate max cir 0

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits per second, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 6400000000, **max**

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR, in kilobits per second, used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer.

Values 0 to 6400000000, **max**

Default 0

Platforms All

rate

Syntax **rate** *percent*
no rate

Context **[Tree]** (config>qos>network-queue>hs-wrr-group rate)

Full Context configure qos network-queue hs-wrr-group rate

Description This command specifies the scheduling rate applied to the HS WRR group as a percentage of the port rate, which includes both the **egress-rate** and HS scheduler policy **max-rate**, if configured.

The **no** form of the command reverts to the default.

Default rate 100

Parameters *percent* — Specifies the scheduling rate of the HS WRR group as a percentage.

Values 1 to 100

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>qos>sap-egress>hs-wrr-group rate)

Full Context configure qos sap-egress hs-wrr-group rate

Description This command specifies the scheduling rate applied to the HS WRR group in kb/s. Alternatively, the keyword **max** can be specified, which removes the bandwidth limitation on the HS WRR group. The **rate** and **percent-rate** commands are mutually exclusive.

The **no** form of the command reverts to the default value.

Default rate max

Parameters *rate* — Specifies the scheduling rate of the HS WRR group in kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** *rate*
no rate

Context **[Tree]** (config>qos>qgrps>egr>qgrp>hs-wrr-group rate)

Full Context configure qos queue-group-templates egress queue-group hs-wrr-group rate

Description This command specifies the scheduling rate applied to the HS WRR group in kb/s. Alternatively, the keyword **max** can be specified, which removes the bandwidth limitation on the HS WRR group. The **rate** and **percent-rate** commands are mutually exclusive.

The **no** form of the command reverts to the **rate max**.

Default rate max

Parameters *rate* — Specifies the scheduling rates of the HS WRR group in kb/s.

Values 1 to 2000000000, max

Platforms 7750 SR-7/12/12e

rate

Syntax **rate** *percent* [**cir** *percent*] [**fir** *percent*]
no rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>qos>network-queue>queue rate)

Full Context configure qos network-queue queue rate

Description This command defines the administrative Peak Information Rate (PIR), the administrative Committed Information Rate (CIR), and the administrative Fair Information Rate (FIR) parameters for the queue.

The PIR defines the percentage that the queue can transmit packets through the switch fabric (for ingress queues) or out of an egress port (for egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available bandwidth.

The CIR defines the percentage at which the system prioritizes the queue over other queues competing for the same bandwidth.

The CIR can be used by the queue's **port-parent** commands **cir-level** and **cir-weight** parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent port scheduler.

The FIR defines an additional percentage at which the system prioritizes the queue over other queues competing for the same bandwidth above that used by the CIR percentage.

The **rate** command can be executed at any time, altering the PIR, CIR, and FIR for all queues created through the association of the network queue policy with the *queue-id*.

When configured on an egress HSQ queue group queue, the **cir** keyword is ignored.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the rate is performed under the **hs-wrr-group** within the network queue policy.

The **no** form of the command returns all queues created with the *queue-id* by association with the network queue policy to the default PIR, CIR, and FIR parameters.

Default rate 100 cir 0 fir 0

Parameters *percent* — Defines the percentage of the sum of the capacities of network and hybrid ports on that FP (taking into account any **ingress-rate** configuration) or egress port speed for the rate allowed for the queue. When the **rate** command is executed, a valid *percent* (PIR setting) must be explicitly defined. When the **rate** command has not been executed, the default PIR of **100** is assumed. Fractional values are not allowed, and the value must be given as a positive integer.

The actual PIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 100

Default 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir *percent* — Defines the percentage of the sum of the capacities of network and hybrid ports on that FP (taking into account any **ingress-rate** configuration) or egress port speed for the CIR allowed for the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed, and the value must be given as a positive integer. The actual CIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 0 to 100

Default 0

fir *percent* — Defines the percentage of the sum of the capacities of network and hybrid ports on that FP (taking into account any **ingress-rate** configuration) or egress port speed for the FIR allowed for the queue. When the **rate** command is executed, a FIR setting is optional. When the **rate** command has not been executed or the **fir** parameter is not explicitly specified, the default FIR (0) is assumed. Fractional values are not allowed, and the value must be given as a positive integer. The actual FIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

Values 0 to 100

Default 0

Platforms All

rate

Syntax **rate** {**max** | *pir-rate*} [**cir** {**max** | *cir-rate*}]
no rate

Context **[Tree]** (config>qos>qgrps>egr>qgrp>policer rate)
[Tree] (config>qos>qgrps>ing>qgrp>policer rate)

Full Context configure qos queue-group-templates egress queue-group policer rate
configure qos queue-group-templates ingress queue-group policer rate

Description This command is used to configure the policer's metering and optional profiling rates. The metering rate is used by the system to configure the policer's PIR leaky bucket's decrement rate while the profiling rate configures the policer's CIR leaky bucket's decrement rate. The decrement function empties the bucket while packets applied to the bucket attempt to fill it based on each packet's size. If the bucket fills faster than how much is decremented per packet, the bucket's depth eventually reaches its exceed (CIR) or violate (PIR) threshold. The **cbs**, **mbs**, and **high-prio-only** commands are used to configure the policer's PIR and CIR thresholds.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a packet arrives at the policer while the bucket's depth is less than the threshold associated with the packet, the packet is considered to be conforming to the bucket's rate. If the bucket depth is equal to or greater than the threshold, the packet is considered to be in the exception state. For the CIR bucket, the exception state is exceeding the CIR rate while the PIR bucket's exception state is violating the PIR bucket rate. If the packet is violating the PIR, the packet is marked red and will be discarded. If the packet is not red, it may be green or yellow, based on the conforming or exceeding state from the CIR bucket.

When a packet is red, neither the PIR nor CIR bucket depths are incremented by the packets size. When the packet is yellow, the PIR bucket is incremented by the packet size, but the CIR bucket is not. When the packet is green, both the PIR and CIR buckets are incremented by the packet size. This ensures that conforming packets impact the bucket depth while exceeding or violating packets do not.

The policer's **adaptation-rule** command settings are used by the system to convert the specified rates into hardware timers and decrement values for the policer's buckets.

By default, the policer's metering rate is **max** and the profiling rate is 0 kb/s (all packets out-of-profile).

The **no** form of this command is used to restore the default metering and profiling rate to a policer.

Parameters **{max |** *pir-rate***}** — Specifying the keyword **max** or an explicit *pir-rate* parameter directly following the rate command is required and identifies the policer's metering rate for the PIR leaky bucket. When the policer is first created, the metering rate defaults to max. The *pir-rate* value must be expressed as an integer and defines the rate in kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When max is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to max.

Values **max**, 1 to 2000000000

cir {max | *cir-rate***}** — The optional **cir** keyword is used to override the default CIR rate of the policer. Specifying the keyword max or an explicit *cir-rate* parameter directly following the cir keyword is required and identifies the policer's profiling rate for the CIR leaky bucket. When the policer is first created, the profiling rate defaults to 0 kb/s. The *cir-rate* value must be expressed as an integer and defines the rate in kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When **max** is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to max.

Values **max,** 0 to 2000000000

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*] [**fir** *fir-rate*]
rate *pir-rate* **police**
no rate

Context **[Tree]** (config>qos>queue-group-templates>ingress>queue-group>queue rate)

Full Context configure qos queue-group-templates ingress queue-group queue rate

Description This command defines the administrative Peak Information Rate (PIR), the administrative Committed Information Rate (CIR), and the administrative Fair Information Rate (FIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets through the switch fabric (for SAP ingress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. For SAP ingress, the CIR also defines the rate that packets are considered in-profile by the system, unless **cir-non-profiling** is configured. In-profile, then out-of-profile, packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The FIR defines an additional rate at which the system prioritizes the queue over other queues competing for the same bandwidth above that used by the CIR.

The **rate** command can be executed at any time, altering the PIR, CIR, and FIR for all queues created through the association of the ingress queue group template with the *queue-id*.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR, CIR, and FIR parameters (**max**, 0, 0).

Default rate max cir 0 fir 0

Parameters *pir-rate* — Defines the administrative PIR, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and the value must be given as a positive integer.

The actual PIR is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 2000000000 kb/s, **max**

Default max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cir-rate — The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and the value must be given as a positive integer. The actual CIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 2000000000 kb/s, **max**

Default 0

fir-rate — The **fir** parameter overrides the default administrative FIR used by the queue. When the rate command is executed, an FIR setting is optional. When the rate command has not been executed or the **fir** parameter is not explicitly specified, the default FIR (0) is assumed.

Fractional values are not allowed and the value must be given as a positive integer. The actual FIR used is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

Values 1 to 2000000000 kb/s, **max**

Default 0

police — Specifies that traffic feeding into the queue instance above the specified rate is dropped.

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>qos>queue-group-templates>egress>queue-group>queue rate)

Full Context configure qos queue-group-templates egress queue-group queue rate

Description This command defines the administrative PIR and the administrative CIR parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress port. Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The CIR can be used by the queue's parent commands *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR for all queues created through the association of the egress queue group template with the *queue-id*.

When configured on an egress HSQ queue group queue, the **cir** keyword is ignored.

This command is ignored for egress HSQ queue group queues which are attached to an HS WRR group within an associated HS attachment policy. In this case, the configuration of the rate is performed under the **hs-wrr-group** within the SAP egress QoS policy.

The **no** form of this command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Default rate max cir 0

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 1 to 200000000 kb/s, **max**

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer.

Values 0 to 200000000 kb/s, **max**

Default 0

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>qos>scheduler-policy>tier>scheduler rate)

Full Context configure qos scheduler-policy tier scheduler rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **rate** command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler's within-CIR distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's PIR and CIR parameters to the value configured in the applied scheduler policy.

Parameters **pir** *pir* — Specifies the PIR rate of the scheduler in kb/s or it can be set to the maximum using the max keyword.

Values 1 to 6400000000, **max**

Default max

cir *cir* — Specifies the CIR rate of the scheduler in kb/s or it can be set to the maximum using the max keyword. The sum keyword can also be used, which sets the CIR to the sum of child CIR values.

Values 0 to 6400000000, **max, sum**

Default sum

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>qos>port-scheduler-policy>group rate)

Full Context configure qos port-scheduler-policy group rate

Description This command specifies the total bandwidth and the within-CIR bandwidth allocated to a weighted scheduler group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns the rate to its default value of **max**.

Parameters *pir-rate* — Specifies PIR rates, in kilobits per second.

Values 1 to 6400000000, **max**

cir *cir-rate* — Specifies CIR rates, in kilobits per second.

Values 0 to 6400000000, **max**

Platforms All

rate

Syntax **rate** *percent* [**cir** *percent*] [**fir** *percent*]
no rate

Context **[Tree]** (config>qos>shared-queue>queue rate)

Full Context configure qos shared-queue queue rate

Description This command defines the administrative PIR, the administrative CIR, and the administrative FIR parameters for the queue.

The PIR defines the percentage that the queue can transmit packets through the switch fabric (for ingress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by over-subscription factors or available bandwidth.

The CIR defines the percentage at which the system prioritizes the queue over other queues competing for the same bandwidth.

The **rate** command can be executed at any time, altering the PIR, CIR, and FIR for the queue created with the *queue-id*.

Parameters *percent* — Defines the percentage of the FP ingress capacity for the max rate allowed for the queue. When the **rate** command is executed, a valid percent (PIR) setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and the value must be given as a positive integer.

Values 1 to 100, **max**

Default 100

cir *percent* — Defines the percentage of the FP ingress capacity for the CIR allowed for the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and the value must be given as a positive integer.

Values 0 to 100, **max**

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fir *percent* — Defines the percentage of the FP ingress capacity for the FIR allowed for the queue. When the **rate** command is executed, a FIR setting is optional. When the **rate** command has not been executed or the **fir** parameter is not explicitly specified, the default FIR (0) is assumed. Fractional values are not allowed and the value must be given as a positive integer. FIR is only supported on FP4 hardware and is ignored when the related policy is applied to FP2- or FP3-based hardware.

Values 0 to 100

Default 0

Platforms All

rate

Syntax **rate** *sample-rate*
no rate

Context **[Tree]** (config>cflowd rate)

Full Context configure cflowd rate

Description This command specifies the rate (N) at which traffic is sampled and sent for flow analysis. A packet is sampled every N packets; for example, when **sample-rate** is configured as 1, then all packets are sent to the cache. When **sample-rate** is configured as 100, then every 100th packet is sent to the cache.

The **no** form of this command resets the sample rate to the default value.

Default rate 1000

Parameters *sample-rate* — Specifies the rate at which traffic is sampled.

Values 1 to 10000

rate

Syntax **rate** *kilobits-per-second*
no rate

Context **[Tree]** (config>service>cust>multi-service-site>egress>agg-rate rate)

Full Context configure service customer multi-service-site egress agg-rate rate

Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context's object.

The **no** form of the command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *kilobits-per-second* — Specifies the rate limit for the multi-service site, in kilobits per second.

Values 1 to 6400000000, **max**

Platforms All

rate

Syntax **rate** *pir-rate* [**cir** *cir-rate*]
no rate

Context **[Tree]** (config>service>cust>multi-service-site>ingress>sched-override>scheduler rate)
[Tree] (config>service>cust>multi-service-site>egress>sched-override>scheduler rate)

Full Context configure service customer multi-service-site egress scheduler-override scheduler rate
configure service customer multi-service-site ingress scheduler-override scheduler rate

Description This command overrides specific attributes of the specified scheduler rate.

The **rate** command defines the maximum bandwidth that the scheduler can offer its child policers, queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the scheduler's amount of bandwidth to be considered during the parent schedulers 'within CIR' distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler's parent scheduler may not have the available bandwidth to meet the scheduler's needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child policers or queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns the scheduler's to the PIR and CIR parameters to the value configured in the applied scheduler policy.

Parameters *pir-rate* — Specifies the PIR rate.

Values 1 to 6400000000, **max**

Default **max**

cir-rate — Specifies the CIR rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the *cir-rate* is set to **max**, then the CIR rate is set to infinity. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers, policers or queues.

Values 0 to 6400000000, **max**, **sum**

Default **sum**

Platforms All

rate

Syntax **rate** *rate* [**cir** *cir*]
no rate

Context **[Tree]** (config>system>security>cpm-queue>queue rate)

Full Context configure system security cpm-queue queue rate

Description This command specifies the maximum bandwidth that will be made available to the queue in kilobits per second (kb/s).

Parameters *rate* — Specifies the administrative Peak Information Rate (PIR) for the queue.

cir — Specifies the amount of bandwidth committed to the queue.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rate

Syntax **rate kbps** {*kilobits-per-second* | **max**} [**mbs** *size*] [**bytes** | **kilobytes**]
rate packets {*ppi* | **max**} **within** *seconds* [**initial-delay** *packets*]
no rate

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>local-monitoring-policer rate)
[Tree] (config>sys>security>dist-cpu-protection>policy>protocol>dynamic-parameters rate)

Full Context configure system security dist-cpu-protection policy local-monitoring-policer rate
configure system security dist-cpu-protection policy protocol dynamic-parameters rate

Description This command configures the rate and burst tolerance for the policer in either a packet rate or a bit rate.

The actual hardware may not be able to perfectly rate limit to the exact configured parameters. In this case, the configured parameters will be adapted to the closest supported rate. The actual (operational) parameters can be seen in CLI, for example, **show service id** *33* **sap** 1/1/3:33 **dist-cpu-protection detail**.

If the *kilobits-per-second* parameter value is configured as max, then the policer is effectively disabled (always conforming).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the *size* parameter value is configured as 0, then all packets are considered as nonconforming.

Default rate packets max within 1 initial-delay 0

Parameters **packets | kbps** — specifies that the rate is either in units of packets per interval or in units of kilobits per second. The packets option would typically be used for lower rates (for example, for per-subscriber DHCP rate limiting) while the kbps option would typically be used for higher rates (for example, per-interface BGP rate limiting).

ppi — Specifies packets per interval.

Values 0 to 255, max
max = disable the policer (always conforming)
packets 0 = all packets considered nonconforming

seconds — Specifies the length of the ppi rate measurement interval.

Values 1 to 32767

packets — Specifies the number of packets allowed (even at line rate) in an initial burst (or a burst after the policer bucket has drained to zero) in addition to the normal *ppi*. This would typically be set to a value that is equal to the number of received packets in several full handshakes/negotiations of the particular protocol.

Values 0 to 255

kilobits-per-second — Specifies the kilobits per second.

Values 1 to 20000000, max

size — Specifies the tolerance for the kbps rate.

Values 0 to 4194304

Default 10

bytes | kilobytes — Specifies that the units of the mbs size parameter are either in bytes or kilobytes.

Platforms All

rate

Syntax **rate kbps** {*kilobits-per-second* | **max**} [**mbs** *size*] [**bytes** | **kilobytes**]
rate packets {*ppi* | **max**} **within** *seconds* [**initial-delay** *packets*]
no rate

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy>static-policer rate)

Full Context configure system security dist-cpu-protection policy static-policer rate

Description This command configures the rate and burst tolerance for the policer in either a packet rate or a bit rate.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The actual hardware may not be able to perfectly rate limit to the exact configured parameters. In this case, the configured parameters will be adapted to the closest supported rate. The actual (operational) parameters can be seen in CLI, for example, **show service id** *33* **sap** 1/1/3:33 **dist-cpu-protection detail**.

If the *kilobits-per-second* parameter value is configured as max, then the policer is effectively disabled (always conforming).

If the *size* parameter is configured as 0, then all packets are considered as nonconforming.

Default rate packets max within 1 initial-delay 0

Parameters **packets | kbps** — specifies that the rate is either in units of packets per interval or in units of kilobits per second. The packets option would typically be used for lower rates (for example, for per-subscriber DHCP rate limiting) while the kbps option would typically be used for higher rates (for example, per-interface BGP rate limiting).

ppi — Specifies packets per interval.

Values 0 to 8000, max
max = disable the policer (always conforming)
packets 0 = all packets considered nonconforming

seconds — Specifies the length of the ppi rate measurement interval.

Values 1 to 32767

packets — Specifies the number of packets allowed (even at line rate) in an initial burst (or a burst after the policer bucket has drained to zero) in addition to the normal *ppi*. This would typically be set to a value that is equal to the number of received packets in several full handshakes/negotiations of the particular protocol.

Values 0 to 255

kilobits-per-second — Specifies the kilobits per second.

Values 1 to 20000000, max

size — Specifies the tolerance for the kbps rate.

Values 0 to 4194304

Default 10

bytes | kilobytes — Specifies that the units of the mbs size parameter are either in bytes or kilobytes.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.29 rate-adjustment

rate-adjustment

Syntax **rate-adjustment** *adjusted-percent*
no rate-adjustment

Context [Tree] (config>subscr-mgmt>ancp>policy>ingress rate-adjustment)
[Tree] (config>subscr-mgmt>ancp>policy>egress rate-adjustment)

Full Context configure subscriber-mgmt ancp ancp-policy egress rate-adjustment
configure subscriber-mgmt ancp ancp-policy ingress rate-adjustment

Description This command configures a rate adjustment for the scheduler. The **rate-adjustment** command should be used when the rate returned by the DSLAM is calculated with different encapsulation than the 7450 ESS or 7750 SR. The node will adjust the rate by the percent specified as:

DSLAM_RATE*adjust-rate/100 — rate-reduction.

The **no** form of this command reverts to the default.

Parameters *adjusted-percent* — Specifies a rate adjustment for the scheduler.

Values 1 to 200

Default 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.30 rate-calc-min-int

rate-calc-min-int

Syntax **rate-calc-min-int** [**fast-queue** *percent-of-default*] [**slow-queue** *percent-of-default*]
no rate-calc-min-int

Context [Tree] (config>card>virt-sched-adj rate-calc-min-int)

Full Context configure card virtual-scheduler-adjustment rate-calc-min-int

Description This command overrides the default minimum time that must elapse before a policer or queue's offered rate may be recalculated. A minimum time between offered rate calculations is enforced to both prevent inaccurate estimation of the offered rate and excessive input to the virtual scheduler process.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In order to smooth out rapidly fluctuating offered rates, the system averages the measured offered rate with a window of previously measured offered traffic statistics and knowledge of the time between the samples.

The window size is defined by the “rate calculation minimum interval” with offered traffic statistics being read at most four times within the window. Any previous measured offered statistics within the window are used in the averaging function. Note that if there are large numbers of samples required, for example when a large number of queues are running HQoS, then it may be that a time greater than the “rate calculation minimum interval” passes before another sample of the offered statistics can be taken for a queue. In this case, in order to calculate an offered rate, HQoS will always use two samples, the current and the previous. In this case, using a smaller **rate-calc-min-int** will have no effect on the responsiveness of HQoS to queue rate changes.

The system separates policers and queues into fast and slow categories and maintains a separate “rate calculation minimum interval” for each type. The default for each type are as follows:

Slow Queue: 1.0 seconds

Fast Queue: 0.25 seconds

The actual minimum rate calculation interval may be increased or decreased by using the fast-queue and/or slow-queue keywords (which are also applicable for policers managed by HQoS) followed by a percent value which is applied to the default interval. The default slow-queue threshold rate is 1 Mb/s. Once a policer or queue is categorized as slow, its rate must rise to 1.5 Mb/s before being categorized as a fast policer or queue. The categorization threshold may be modified by using the **slow-queue-threshold** command.

The **no** form of this command restores the default fast queue and slow queue minimum rate calculation interval.

Default no rate-calc-min-int

Parameters *percent-of-default* — Specifies that the fast-queue percent-of-default parameter is optional and is used to modify the default minimum rate calculation time for “fast” queues. Defining 100.00 percent is equivalent to removing the override (restoring the default) on the fast queue minimum rate calculation time.

Values 0.01% to 1000.00%

Default 100.00%

percent-of-default — Specifies that the slow-queue percent-of-default parameter is optional and is used to modify the default minimum rate calculation time for “slow” queues. Defining 100.00 percent is equivalent to removing the override (restoring the default) on the slow queue minimum rate calculation time.

Values 0.01% to 1000.00%

Default 100.00%

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.31 rate-down

rate-down

Syntax **rate-down** *rate*
no rate-down

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>access-loop-encapsulation rate-down)

Full Context configure subscriber-mgmt local-user-db ppp host access-loop-encapsulation rate-down

Description This command is applicable to LAC and LNS. It provides the last mile link rate in the downstream direction that is needed for proper shaping and calculating the interleaving delay.

The rate information in the last mile will be taken from the following sources in the order of priority:

- Statically provisioned value in local user database (LUDB).
- RADIUS.
- PPPoE tags on LAC or ICRQ message (RFC 5515) /ICCN message (TX Connect Seed) on LNS.

Default no rate-down

Parameters *rate* — Specifies the last mile link downstream rate in the access loop

Values 1 to 100000 kb/s

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

22.32 rate-limit

rate-limit

Syntax **rate-limit** *packets-per-second*
no rate-limit

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy rate-limit)

Full Context configure service nat syslog syslog-export-policy rate-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum rate limit at which syslog messages are sent. Once the rate limit is exceeded, NAT flow logs will be buffered. Overload condition is characterized by exhaustion of this buffer space. This condition can occur due to imposed rate limit or the software speed limit. Once the buffer space is exhausted, new flow creation will be denied, and the teardown of the existing flows will be delayed until the buffer space becomes available.

The **no** form of the command removes the maximum rate limit from the configuration.

Parameters *packets-per-second* — Specifies the packet rate limit in seconds.

Values 10 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

rate-limit

Syntax **rate-limit** *value*
rate-limit *value* **extracted-traffic**
rate-limit *value* **packet-length** {**lt** | **gt** | **eq**} *packet-length-value*
rate-limit *value* **packet-length range** *packet-length-value packet-length-value*
rate-limit *value* **pattern expression** *expression* **mask** *mask* **offset-type** *offset-type* **offset-value** *offset-value*
rate-limit *value* **ttl** {**lt** | **gt** | **eq**} *ttl-value*
rate-limit *value* **ttl range** *ttl-value ttl-value*

Context **[Tree]** (config>filter>ip-filter>entry>action rate-limit)

Full Context configure filter ip-filter entry action rate-limit

Description This command configures the rate limit value for traffic matching this filter entry. Rate limit policers are configured with MBS equals CBS equals 10 ms of the rate and high-prio-only equals 0.

Traffic can also be rate-limited based on extracted-traffic, packet-length, packet-length range, ttl, ttl range, or a pattern of conditional match criteria.

Packets that match the filter entry match criteria, but do not match the conditional match criteria value, are implicitly forwarded with no further match in the following filter entries.

For pattern match:

- the expression is left-aligned for the odd number bytes, for example, the expression 0xABC is programmed 0x0ABC in the line card
- the 'data' offset requires protocol UDP or TCP to be selected in the filter entry match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the **rate-limit** *value* in kb/s. A rate of 0 results in all traffic being dropped. A rate of **max** results in all traffic being forwarded.

Values 0 to 2000000000 kb/s, max

extracted-traffic — Specifies rate-limit packets both extracted to the CPM and matching the filter entry match criteria.

packet-length — Specifies rate-limit packets matching both the filter entry match criteria and the *packet-length value* defined in the **rate-limit** action statement. Packets matching the filter entry match criteria and not matching the *packet-length* value, as defined in the **rate-limit** action statement, are implicitly forwarded with no further match in the following filter entries.

Values **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

packet-length-value — Specifies the packet length value for the rate limit action.

Values 0 to 65535

range — Specifies an inclusive range. When **range** is used, the start of the range (the first value entered) must be smaller than the end of the range (the second value entered).

expression — Specifies the hexadecimal pattern to match; up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

mask — Specifies the mask for the pattern expression, up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

offset-type — Specifies the starting point reference for the offset-value of this pattern.

Values layer-3, layer-4, data, dns-qtype

offset-value — Specifies the offset value for the pattern expression. Dns-qtype supports offset value of 0.

Values 0 to 255

ttl-value — Specifies rate-limit packets matching both the filter entry match criteria and the TTL value defined in the *rate-limit* action statement. Packets matching the filter entry match criteria and not matching the TTL value, as defined in the *rate-limit* action statement, are implicitly forwarded with no further match in the following filter entries.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rate-limit

Syntax **rate-limit** *value*

Context **[Tree]** (config>filter>mac-filter>entry>action rate-limit)

Full Context configure filter mac-filter entry action rate-limit

Description This command sets the rate limit for the traffic matching both the filter entry match criteria and the *packet-length-value* defined in the **rate-limit action** statement.

Packets matching the filter entry match criteria and not matching the *packet-length-value* defined in the **rate-limit action** statement are implicitly forwarded with no further match in subsequent filter entries.

Rate limit packets matching both the filter entry match criteria and the *ttl-value* are defined in the **action rate-limit** statement.

Packets matching the filter entry match criteria and not matching the *ttl-value* defined in the **rate-limit action** statement are implicitly forwarded with no further match in the following filter entries.

Parameters *value* — Specifies the **rate-limit** *value* in kb/s. A rate of 0 results in all traffic being dropped. A rate of **max** results in all traffic being forwarded.

Values 0 to 2000000000 kb/s | max

Platforms All

rate-limit

Syntax **rate-limit** *value*
rate-limit *value* **extracted-traffic**
rate-limit *value* **hop-limit** {**lt** | **gt** | **eq**} *hop-limit-value*
rate-limit *value* **hop-limit range** *hop-limit-value hop-limit-value*
rate-limit *value* **pattern expression** *expression* **mask** *mask* **offset-type** *offset-type* **offset-value** *offset-value*
rate-limit *value* **payload-length** {**lt** | **gt** | **eq**} *payload-length-value*
rate-limit *value* **payload-length range** *payload-length-value payload-length-value*

Context **[Tree]** (config>filter>ipv6-filter>entry>action rate-limit)

Full Context configure filter ipv6-filter entry action rate-limit

Description This command configures the rate limit value for traffic matching this filter entry.

Traffic can also be rate-limited based on extracted-traffic, payload-length, payload-length range, hop-limit, hop-limit range, or a pattern of conditional match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Packets that match the filter entry match criteria, but do not match the conditional match criteria value, are implicitly forwarded with no further match in the following filter entries.

For pattern match:

- the expression is left-aligned for the odd number bytes, for example, the expression 0xABC is programmed 0x0ABC in the line card.
- the 'data' offset requires protocol UDP or TCP to be selected in the filter entry match criteria.

Parameters *value* — Specifies the **rate-limit** *value* in kb/s. A rate of 0 results in all traffic being dropped. A rate of **max** results in all traffic being forwarded.

Values 0 to 2000000000 kb/s, max

extracted-traffic — Specifies packets extracted to the CPM.

hop-limit — Specifies the hop limit value for the rate limit action.

Values **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

hop-limit-value — Specifies the hop limit value for the rate limit action.

Values 0 to 255

range — Specifies an inclusive range. When the **range** parameter is used, the start of the range (the first value entered) must be smaller than the end of the range (the second value entered).

expression — Specifies the hexadecimal pattern to match; up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

mask — Specifies the mask for the pattern expression, up to eight bytes.

Values 0x0000000000000001 to 0xffffffffffffffff

offset-type — Specifies the starting point reference for the offset-value of this pattern.

Values layer-3, layer-4, data, dns-qtype

offset-value — Specifies the offset value for the pattern expression. Dns-qtype supports offset value of 0.

Values 0 to 255

payload-length — Specifies rate-limit packets matching both the filter entry match criteria and the *payload-length-value* defined in the **rate-limit** action statement. Packets matching the filter entry match criteria and not matching the *payload-length-value,* as defined in the **rate-limit** action statement, are implicitly forwarded with no further match in the following filter entries.

Values **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

payload-length-value — Specifies the payload length value for the rate limit action.

Values 0 to 65535

Platforms All

22.33 rate-modify

rate-modify

Syntax **rate-modify scheduler** *scheduler-name*
rate-modify agg-rate-limit
no rate-modify

Context **[Tree]** (config>subscr-mgmt>ancp>policy>egress rate-modify)
[Tree] (config>subscr-mgmt>ancp>policy>ingress rate-modify)

Full Context configure subscriber-mgmt ancp ancp-policy egress rate-modify
configure subscriber-mgmt ancp ancp-policy ingress rate-modify

Description This command configures rate modify scheduler parameters.

The **no** form of this command removes the scheduler name from the configuration.

Parameters **agg-rate-limit** — Specifies that the maximum total rate for all subscriber egress queues for each subscriber associated with the policy.

scheduler-name — Specifies a scheduler name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.34 rate-monitor

rate-monitor

Syntax **rate-monitor** *kilobit-per-second* [**alarm**]
no rate-monitor

Context **[Tree]** (config>subscr-mgmt>ancp>policy>ingress rate-monitor)
[Tree] (config>subscr-mgmt>ancp>policy>egress rate-monitor)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt ancp ancp-policy egress rate-monitor
configure subscriber-mgmt ancp ancp-policy ingress rate-monitor

Description This command configures the rate monitor level.

The **no** form of this command removes the value from the configuration.

Parameters *kilobit-per-second* — Specifies the rate below which the system generates an event.

Values 0 to 4294967295

alarm — When the monitored rate is below the configured value the system generates an alarm (trap) to the management system. The trap includes the rate as well as the ANCP policy name and the ANCP string.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.35 rate-percentage

rate-percentage

Syntax **rate-percentage** *rate-percentage*
no rate-percentage

Context **[Tree]** (config>app-assure>group>policer rate-percentage)

Full Context configure application-assurance group policer rate-percentage

Description This command indirectly configures the rate used by Access-Network-Location (ANL) policers. Because ANL total bandwidth is dynamically measured and estimated by AA, this command allows the operator to configure the ratio of that measured bandwidth to be used by the ANL policer as the policer rate.

The **no** form of this command resets the values to defaults.

Default no rate-percentage

Parameters *rate-percentage* — Specifies an integer value that specifies a percentage that is applied against the ANL estimate maximum bandwidth to produce the actual rate that is used by the policer when ANL congestion occurs.

Values 0 to 200 (0: means drop all traffic)

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.36 rate-percentage-stage2

rate-percentage-stage2

Syntax **rate-percentage-stage2** *rate-percentage*
no rate-percentage-stage2

Context **[Tree]** (config>app-assure>group>policer rate-percentage-stage2)

Full Context configure application-assurance group policer rate-percentage-stage2

Description This command indirectly configures the rate used by Access-Network-Location (ANL) policers. Because ANL stage2 total bandwidth is dynamically measured and estimated by AA, this command allows the operator to configure the ratio of that measured bandwidth to be used by the ANL stage2 policer as the policer rate.

The **no** form of this command reverts to the default.

Parameters *rate-percentage* — Specifies an integer value that specifies a percentage that is applied to the ANL estimated maximum bandwidth to produce the actual rate that is used by the policer when ANL stage2 congestion occurs. A value of 0 means that all traffic is dropped.

Values 0 to 200

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.37 rate-reduction

rate-reduction

Syntax **rate-reduction** *kilobit-per-second*
no rate-reduction

Context **[Tree]** (config>subscr-mgmt>ancp>policy>ingress rate-reduction)
[Tree] (config>subscr-mgmt>ancp>policy>egress rate-reduction)

Full Context configure subscriber-mgmt ancp ancp-policy egress rate-reduction
configure subscriber-mgmt ancp ancp-policy ingress rate-reduction

Description This command defines a constant rate reduction to the rate specified by the DSLAM. The **rate-reduction** command should be used if the node should adjust the rate to a value that is offset (for example by a fixed multicast dedicated bandwidth) compared to the total available on the DSLAM.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When set, the rate is:

DSLAM_RATE*adjust-rate/100 — rate-reduction

The **no** form of this command removes the value from the configuration.

Parameters *kilobits-per-second* — Specifies the rate reduction to be applied for this subscriber.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.38 rate-thresholds

rate-thresholds

Syntax **rate-thresholds high** *high-percentage* **low** *low-percentage*
no rate-thresholds

Context **[Tree]** (config>subscr-mgmt>sla-profile>egress>bonding-selection rate-thresholds)

Full Context configure subscriber-mgmt sla-profile egress bonding-selection rate-thresholds

Description This command configures the rate thresholds that are required before decreasing or increasing the preferred link's weight with the specified change percentage.

The low threshold value must be lower than the high threshold value.

The **no** form of this command reverts to the default.

Default rate-thresholds high 90 low 80

Parameters *high-percentage* — Specifies the high threshold, as a percentage of the reference rate.

Values 56 to 99

low-percentage — Specifies the low threshold, as a percentage of the reference rate.

Values 55 to 98

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.39 rating-group

rating-group

Syntax **rating-group** *rating-group-id*
no rating-group

Context **[Tree]** (config>subscr-mgmt>cat-map>category rating-group)

Full Context configure subscriber-mgmt category-map category rating-group

Description This command configures the rating group applicable for this category.

The **no** form of this command reverts to the default.

Parameters *rating-group-id* — Specifies the rating group applicable for this category.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.40 raw

raw

Syntax [**no**] **raw**

Context **[Tree]** (config>cflowd>collector>aggregation raw)

Full Context configure cflowd collector aggregation raw

Description This command configures raw (unaggregated) flow data to be sent in Version 5.

The **no** form of this command removes this type of aggregation from the collector configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.41 rd

rd

Syntax **rd** *file-url* **rf**
rd *file-url* [**force**]

Context **[Tree]** (file rd)

Full Context file rd

Description If the directory is empty, the **rd** command is used to remove it. The **force** option executes the command without prompting the user to confirm the action.

If the directory contains files and/or subdirectories, the **rf** parameter must be used to remove the directory.

Example:

```
A:nE1>file cf1:\ # rd test
Are you sure (y/n)? y
Deleting directory cf1:\test ..MINOR: CLI Cannot delete cf1:\test.
A:nE1>file cf1:\ # rd test force
Deleting directory cf1:\test .MINOR: CLI Cannot delete cf1:\test.


A:nE1>file cf1:\ # rd testbase rf
Deleting all subdirectories and files in specified directory. y/n ?y
Deleting directory cf1:\testbase\testbase1 ..OK
Deleting directory cf1:\test .OK
```

Parameters *file-url* — Specifies the directory to be removed.

Values

local-url	[*cflash-id*/][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

rf — Forces a recursive delete.

force — Forces an immediate deletion of the specified directory. The **rd** *file-url* **force** command executes the command without displaying a user prompt message.

Platforms All

22.42 rdi-alarms

rdi-alarms

Syntax **rdi-alarms** [**suppress** | **circuit**]

Context **[Tree]** (config>port>aps rdi-alarms)

Full Context configure port aps rdi-alarms

Description This command configures how RDI alarms (line, path, section) are generated on physical circuits of an APS ports. The command configuration changes are supported only for switching-mode set to uni_1plus1. The configuration can be changed only when no working and protecting circuit has been added. Options:

- circuit–RDI alarms are H/W-generated independently on each working and protect circuit based on RX failure of that circuit regardless of APS line status.
- suppress–RDI H/W generation on working and protect circuits is suppressed. No alarms are generated on RX failure of that circuit.

Default rdi-alarms circuit

22.43 rdnss-lifetime

rdnss-lifetime

Syntax **rdnss-lifetime** *seconds*
rdnss-lifetime infinite
no rdnss-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>rtr-adv-plcy>dns-opt rdnss-lifetime)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv rdnss-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 rdnss-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv rdnss-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 rdnss-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 rdnss-lifetime
configure service ies subscriber-interface ipv6 rtr-adv rdnss-lifetime
configure service vprn subscriber-interface group-interface ipv6 rdnss-lifetime
configure service vprn subscriber-interface ipv6 rtr-adv rdnss-lifetime
configure subscriber-mgmt router-advertisement-policy dns-options rdnss-lifetime

Description This command configures the maximum time that the RDNSS address may be used for name resolution.

The **no** form of this command returns the command to the default setting.

Default rdnss-lifetime 3600

Parameters *seconds* — Specifies the time, in seconds, that the RDNSS address is valid for this route.

Values 900 to 3600

infinite — Specifies that the RDNSS address can be used permanently.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

rdnss-lifetime

Syntax **rdnss-lifetime** *seconds*
rdnss-lifetime infinite
no rdnss-lifetime

Context [Tree] (config>service>ies>sub-if>ipv6>rtr-adv>dns-opt rdnss-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv>dns-opt rdnss-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv>dns-opt rdnss-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv>dns-opt rdnss-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements dns-options rdnss-lifetime
configure service ies subscriber-interface ipv6 router-advertisements dns-options rdnss-lifetime
configure service vprn subscriber-interface group-interface ipv6 router-advertisements dns-options rdnss-lifetime
configure service vprn subscriber-interface ipv6 router-advertisements dns-options rdnss-lifetime

Description This command configures the maximum time that the RDNSS address may be used for name resolution.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default rdnss-lifetime 3600

Parameters *seconds* — Specifies the time, in seconds, that the RDNSS address is valid for this route.

Values 900 to 3600

infinite — The RDNSS address can be used permanently.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

rdnss-lifetime

Syntax **rdnss-lifetime** {*seconds* | **infinite**}
no rdnss-lifetime

Context **[Tree]** (config>service>vprn>router-advert>dns-options rdnss-lifetime)
[Tree] (config>service>vprn>router-advert>if>dns-options rdnss-lifetime)

Full Context configure service vprn router-advertisement dns-options rdnss-lifetime
configure service vprn router-advertisement interface dns-options rdnss-lifetime

Description This command specifies the maximum time that the RDNSS address may be used for name resolution by the client. The RDNSS Lifetime must be no more than twice MaxRtrAdvLifetime with a maximum of 3600 seconds.

Default rdnss-lifetime infinite

Parameters *infinite* — Specifies an infinite RDNSS lifetime.

seconds — Specifies the time in seconds.

Values 4to 3600

Platforms All

rdnss-lifetime

Syntax **rdnss-lifetime** *seconds*
rdnss-lifetime infinite
no rdnss-lifetime

Context **[Tree]** (config>router>router-advert>dns-opt rdnss-lifetime)
[Tree] (config>router>router-advert>if>dns-opt rdnss-lifetime)

Full Context configure router router-advertisement dns-options rdnss-lifetime
configure router router-advertisement interface dns-options rdnss-lifetime

Description This command specifies the maximum time that the RDNSS address may be used for name resolution by the client.

Default rdnss-lifetime infinite

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the time in seconds.

Values 4 to 3600

infinite — Specifies an infinite RDNSS lifetime.

Platforms All

22.44 re-auth-period

re-auth-period

Syntax **re-auth-period** *seconds*
no re-auth-period

Context **[Tree]** (config>port>ethernet>dot1x re-auth-period)

Full Context configure port ethernet dot1x re-auth-period

Description This command configures the period after which re-authentication is performed. This value is only relevant if **re-authentication** is enabled.

The **no** form of this command returns the value to the default.

Default re-auth-period 3600

Parameters *seconds* — Specifies the re-authentication delay period in seconds.

Values 1 to 9000

Platforms All

22.45 re-authentication

re-authentication

Syntax [**no**] **re-authentication**

Context **[Tree]** (config>subscr-mgmt>auth-policy re-authentication)

Full Context configure subscriber-mgmt authentication-policy re-authentication

Description This command enables authentication process at every DHCP address lease renewal s only if RADIUS did not reply any special attributes (for example, authentication only, no authorization).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

re-authentication

Syntax [**no**] **re-authentication**

Context **[Tree]** (config>port>ethernet>dot1x re-authentication)

Full Context configure port ethernet dot1x re-authentication

Description This command enables/disables periodic 802.1x re-authentication.

When **re-authentication** is enabled, the router re-authenticates clients on the port every **re-auth-period**.

The **no** form of this command returns the value to the default.

Default no re-authentication

Platforms All

22.46 re-establish-session

re-establish-session

Syntax **re-establish-session padr**
no re-establish-session

Context **[Tree]** (config>subscr-mgmt>ppp-policy re-establish-session)

Full Context configure subscriber-mgmt ppp-policy re-establish-session

Description This command enables host to reconnect and override existing session.

If disabled and a subscriber abruptly terminates a PPP sessions without sending a PADT to the BNG, the BNG denies any reconnect attempts until the stale PPP session has expired. With this, enabled re-establish-session eliminates the waiting period by allowing immediate PPP reconnection attempts.

The **no** form of this command reverts to the default.

Parameters **padr** — Specifies that the existing session will be deleted upon reception of the PPPoE Active Discovery Request (PADR).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.47 reachable-time

reachable-time

Syntax **reachable-time** *milli-seconds*
no reachable-time

Context **[Tree]** (config>subscr-mgmt>rtr-adv-plcy reachable-time)

Full Context configure subscriber-mgmt router-advertisement-policy reachable-time

Description This command configures the reachable time for advertisements.

The **no** form of this command returns the command to the default setting.

Default reachable-time 0

Parameters *milli-seconds* — Specifies the time, in milliseconds, for the reachable time.

Values 0 to 3600000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

reachable-time

Syntax **reachable-time** *milli-seconds*
no reachable-time

Context **[Tree]** (config>router>router-advert>if reachable-time)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv reachable-time)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv reachable-time)
[Tree] (config>service>vprn>router-advert>if reachable-time)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv reachable-time)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv reachable-time)

Full Context configure router router-advertisement interface reachable-time
configure service ies subscriber-interface group-interface ipv6 router-advertisements reachable-time
configure service ies subscriber-interface ipv6 router-advertisements reachable-time
configure service vprn router-advertisement interface reachable-time
configure service vprn subscriber-interface group-interface ipv6 router-advertisements reachable-time
configure service vprn subscriber-interface ipv6 router-advertisements reachable-time

Description This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured value is placed in the reachable time field in router advertisement messages sent from this interface.

The **no** form of this command reverts to the default.

Default reachable-time 0

Parameters *milli-seconds* — Specifies the reachable time, in seconds, for advertisements from this interface.

Values 0 to 3600000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface ipv6 router-advertisements reachable-time
- configure service ies subscriber-interface group-interface ipv6 router-advertisements reachable-time
- configure service ies subscriber-interface ipv6 router-advertisements reachable-time
- configure service vprn subscriber-interface group-interface ipv6 router-advertisements reachable-time

All

- configure service vprn router-advertisement interface reachable-time
- configure router router-advertisement interface reachable-time

reachable-time

Syntax **reachable-time** *seconds*
no reachable-time

Context **[Tree]** (config>service>vprn>ipv6 reachable-time)
[Tree] (config>service>vprn>if>ipv6 reachable-time)

Full Context configure service vprn interface ipv6 reachable-time
configure service vprn ipv6 reachable-time

Description This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Default no reachable-time

Parameters *seconds* — Specifies the length of time, in seconds the router should be considered reachable.

Values 30 to 3600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

reachable-time

Syntax **reachable-time** *milliseconds*
no reachable-time

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>router-ad reachable-time)

Full Context configure service ies subscriber-interface group-interface ipv6 router-ad reachable-time

Description This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Parameters *milliseconds* — Specifies the length of time the router should be considered reachable for default router selection.

Values 0 to 3600000

reachable-time

Syntax **reachable-time** *seconds*
no reachable-time

Context **[Tree]** (config>router>ipv6 reachable-time)

Full Context configure router ipv6 reachable-time

Description This command configures the neighbor reachability detection timer.

The **no** form of this command reverts to the default value.

Default reachable-time 30

Parameters *seconds* — Specifies the length of time the router should be considered reachable.

Values 30 to 3600

Platforms All

reachable-time

Syntax **reachable-time** *seconds*
no reachable-time

Context **[Tree]** (config>router>if>ipv6 reachable-time)

Full Context configure router interface ipv6 reachable-time

Description This command configures the neighbor reachability detection timer.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no reachable-time

Parameters *seconds* — Specifies the length of time the router should be considered reachable.

Values 30 to 3600

Platforms All

22.48 reactivation-failure-threshold

reactivation-failure-threshold

Syntax **reactivation-failure-threshold** *number*
no reactivation-failure-threshold

Context **[Tree]** (config>test-oam>icmp>ping-template reactivation-failure-threshold)

Full Context configure test-oam icmp ping-template reactivation-failure-threshold

Description This command configures the number of consecutive failures, without previous successes, that must occur transmitting at the reactivation-interval (recovering phase) level before changing to the standard interval and subsequently waiting for the first success.

The **no** form of this command reverts to the default value.

Default reactivation-failure-threshold 4

Parameters *number* — Specifies the number of consecutive failures without previous successes.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.49 reactivation-interval

reactivation-interval

Syntax **reactivation-interval** *seconds*
no reactivation-interval

Context **[Tree]** (config>test-oam>icmp>ping-template reactivation-interval)

Full Context configure test-oam icmp ping-template reactivation-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the packet transmit interval used when the IP interface is operationally down because of a ping template failure and the previous ICMP echo request successfully received a response, recovering phase.

The **no** form of this command reverts to the default value.

Default reactivation-interval 1

Parameters *seconds* — Specifies the packet transmit interval used when IP interface is operational down

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.50 reactivation-threshold

reactivation-threshold

Syntax **reactivation-threshold** *number*
no reactivation-threshold

Context **[Tree]** (config>test-oam>icmp>ping-template reactivation-threshold)

Full Context configure test-oam icmp ping-template reactivation-threshold

Description This command configures the count, when reached, that causes the transition of the IP interface from operationally down to operationally up because of a ping template failure. This is used in the recovering phase.

The **no** form of this command reverts to the default value.

Default reactivation-threshold 3

Parameters *number* — Specifies a count that causes the transition of the IP interface from operationally up to operationally down because of ping-template failure.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.51 reactivation-timeout

reactivation-timeout

Syntax **reactivation-timeout** *seconds*
no reactivation-timeout

Context **[Tree]** (config>test-oam>icmp>ping-template reactivation-timeout)

Full Context configure test-oam icmp ping-template reactivation-timeout

Description This command configures the time that the function waits before declaring the packet as lost. This is the timer used to time out the **reactivation-interval** transmitted packets. The **reactivation-timeout** value can be equal to or lower than the **reactivation-interval** value but not higher.

The **no** form of this command reverts to the default value.

Default reactivation-timeout 1

Parameters *seconds* — Specifies the wait time, in seconds, before declaring the packet is lost.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.52 read-algorithm

read-algorithm

Syntax **read-algorithm** {**hash** | **hash2** | **custom**| **all-hash**}
no read-algorithm

Context **[Tree]** (config>system>security>management-interface>classic-cli read-algorithm)

Full Context configure system security management-interface classic-cli read-algorithm

Description This command specifies how encrypted configuration secrets are interpreted, and which encryption types are accepted, when secrets are input into the system or read from a configuration file (for example at system bootup time).

The **no** form of this command reverts to the default value.

Default read-algorithm all-hash

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **hash** — Specifies hash. Use this option to transport a phrase between modules and nodes. In this case the write-algorithm should be **hash** as well.

hash2 — Specifies hash2 which is module-specific.

custom — Specifies the custom encryption to management interface.

all-hash — Specifies that the system accepts hash or hash2.

Platforms All

22.53 reassemble

reassemble

Syntax **reassemble**

Context **[Tree]** (config>filter>ip-filter>entry>action reassemble)

Full Context configure filter ip-filter entry action reassemble

Description This command sets the filter entry action to reassemble.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.54 reassembly

reassembly

Syntax **reassembly** [*wait-msecs*]
no reassembly

Context **[Tree]** (config>service>ies>if>sap>ip-tunnel reassembly)
[Tree] (config>service>vprn>if>sap>ip-tunnel reassembly)

Full Context configure service ies interface sap ip-tunnel reassembly
configure service vprn interface sap ip-tunnel reassembly

Description This command configures the maximum number of seconds to wait to receive all fragments of a particular IPsec or GRE packet for reassembly.

The **no** form of this commands removes the wait time from the configuration.

Default no reassembly

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *wait-msecs* — Specifies the reassembly wait time in 100 increments.

Values 1 to 5000 ms

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

reassembly

Syntax **reassembly** [*wait-msecs*]
no reassembly

Context **[Tree]** (config>isa>tunnel-group reassembly)
[Tree] (config>service>ies>if>sap>gre-tunnel reassembly)
[Tree] (config>service>vprn>if>sap>gre-tunnel reassembly)

Full Context configure isa tunnel-group reassembly
configure service ies interface sap gre-tunnel reassembly
configure service vprn interface sap gre-tunnel reassembly

Description This command configures IP packet reassembly for IPsec and GRE tunnels supported by an MS-ISA. The **reassembly** command at the tunnel-group level configures IP packet reassembly for all IPsec and GRE tunnels associated with the tunnel-group. The **reassembly** command at the GRE tunnel level configures IP packet reassembly for that one specific GRE tunnel, overriding the tunnel-group configuration.

The **no** form of this command disables IP packet reassembly.

Default no reassembly (tunnel-group level)

reassembly (gre-tunnel level)

Parameters *wait* — Specifies the maximum number of milliseconds that the ISA tunnel application will wait to receive all fragments of a particular IPsec or GRE packet. If one or more fragments are still missing when this limit is reached the partially reassembled datagram is discarded and an ICMP time exceeded message is sent to the source host (if allowed by the ICMP configuration of the sending interface). Internally, the configured value is rounded up to the nearest multiple of 100 ms.

Values 1 to 5000

Default 2000 (tunnel-group level)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

reassembly

Syntax [**no**] **reassembly**

Context **[Tree]** (config>router>nat>inside>dual-stack-lit>address reassembly)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router nat inside dual-stack-lit address reassembly

Description This command enables reassembly of fragmented frames for DS-Lite. Reassembly is enabled in the upstream direction per AFTR address.

The **no** form of the command disables the reassembly.

22.55 reassembly-group

reassembly-group

Syntax **reassembly-group** *nat-group-id* [**to-base-network**]
no reassembly-group

Context **[Tree]** (config>router reassembly-group)
[Tree] (config>service>vprn reassembly-group)

Full Context configure router reassembly-group
configure service vprn reassembly-group

Description This command associates a reassembly-group consisting of multiple ISAs with the routing context in which the application requiring reassembly service resides.

Default no reassembly-group

Parameters *nat-group-id* — Specifies the NAT group ID; the NAT group contains up to 10 active ISAs.

Values 1 to 4

to-base-network — Enables the reassembly context to use network interfaces in the base routing context.

Platforms All

22.56 reassembly-timeout

reassembly-timeout

Syntax **reassembly-timeout** {*timeout*}
no reassembly-timeout

Context **[Tree]** (config>router>l2tp>group>mlppp reassembly-timeout)
[Tree] (config>router>l2tp>group>tunnel>mlppp reassembly-timeout)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>l2tp>group>mlppp reassembly-timeout)
[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp reassembly-timeout)

Full Context configure router l2tp group mlppp reassembly-timeout
configure router l2tp group tunnel mlppp reassembly-timeout
configure service vprn l2tp group mlppp reassembly-timeout
configure service vprn l2tp group tunnel mlppp reassembly-timeout

Description This command is applicable only to LNS. It determines the time during which the LNS keeps fragments of the same packet in the buffer before it discards them. The assumption is that if the fragments do not arrive within certain time, the chance is that they were lost somewhere in the network. In this case the partial packet cannot be reassembled and all fragments that has arrived up to this point and are stored in the buffer IS discarded to free up the buffer. Otherwise, a condition arises in which partial packets are held in the buffer until the buffer is exhausted.

The configuration under the tunnel hierarchy overrides the configuration under the group hierarchy.

The **no** form of this command reverts to the default.

Default reassembly-timeout 1000

Parameters *timeout* — Specifies the reassembly timeout value.

Values 100, 1000 milliseconds

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

reassembly-timeout

Syntax **reassembly-timeout** *timeout-value*
no reassembly-timeout

Context [Tree] (config>qos>mlppp-profile-ingress>class reassembly-timeout)

Full Context configure qos mlppp-profile-ingress class reassembly-timeout

Description This command configures the value of the MLPPP bundle ingress per class reassembly timer for this profile.

Parameters *timeout-value* — Specifies a reassembly timeout for this policy in ms.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

reassembly-timeout

Syntax **reassembly-timeout** *timeout-value*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no reassembly-timeout

Context [Tree] (config>qos>mc-fr-profile-ingress>class reassembly-timeout)

Full Context configure qos mc-fr-profile-ingress class reassembly-timeout

Description This command configures the value of the MLFR bundle ingress per-class reassembly timer for the profile.

Default reassembly-timeout 25 — class 0

reassembly-timeout 25 — class 1

reassembly-timeout 100 — class 2

reassembly-timeout 1000 — class 3

Parameters *timeout-value* — Specifies the timeout value, in ms.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.57 rebind-timer

rebind-timer

Syntax **rebind-timer** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no rebind-timer

Context [Tree] (config>router>dhcp6>server>defaults rebind-timer)
[Tree] (config>router>dhcp6>server>pool>prefix rebind-timer)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>ipv6-lease-times rebind-timer)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ipv6-lease-times rebind-timer)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy-server rebind-timer)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy rebind-timer)
[Tree] (config>service>vprn>dhcp6>defaults rebind-timer)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix rebind-timer)

Full Context configure router dhcp6 local-dhcp-server defaults rebind-timer
configure router dhcp6 local-dhcp-server pool prefix rebind-timer
configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server rebind-timer
configure service vprn dhcp6 defaults rebind-timer
configure service vprn dhcp6 local-dhcp-server pool prefix rebind-timer
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server rebind-timer
configure subscriber-mgmt local-user-db ipoe host ipv6-lease-times rebind-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt local-user-db ppp host ipv6-lease-times rebind-timer

Description This command configures the lease rebind timer (T2) via LUDB.

The T2 time is the time at which the client contacts any available addressing authority to extend the lifetimes of DHCPv6 leases. T2 is a time duration relative to the current time expressed in units of seconds.

The IP addressing authority controls the time at which the client contacts the addressing authority to extend the lifetimes on assigned addresses/prefixes through the T1 and T2 parameters assigned to an IA. At time T1 for an IA, the client initiates a Renew/Reply message exchange to extend the lifetimes on any addresses in the IA. The client includes an IA option with all addresses/prefixes currently assigned to the IA in its Renew message. Recommended values for T1 and T2 are .5 and .8 times the shortest preferred lifetime of the addresses/prefixes in the IA that the addressing authority is willing to extend, respectively.

The configured rebind timer should always be longer than or equal to the renew timer.

The T1 and T2 are carried in the IPv6 address option that is within the IA.

The **no** form of this command reverts to the default.

Default rebind-timer min 48

Parameters *rebind-timer* — Specifies the preferred lifetime.

Values

days *days*	0 to 14
hrs *hours*	0 to 23
min *minutes*	0 to 59
sec *seconds*	0 to 9

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt local-user-db ppp host ipv6-lease-times rebind-timer
- configure router dhcp6 local-dhcp-server pool prefix rebind-timer
- configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server rebind-timer
- configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server rebind-timer
- configure service vprn dhcp6 local-dhcp-server pool prefix rebind-timer
- configure subscriber-mgmt local-user-db ipoe host ipv6-lease-times rebind-timer

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure router dhcp6 local-dhcp-server defaults rebind-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.58 reboot

reboot

Syntax **reboot** [**active** | **standby** | **upgrade**] [**now**]

Context **[Tree]** (admin reboot)

Full Context admin reboot

Description This command reboots the router or one CPM and can also be used to force an upgrade of the system boot ROMs.

If no options are specified, the user is prompted to confirm the reboot operation. Answering yes (y) will result in both CPMs and all IOMs rebooting.

```
ALA-1>admin# reboot
Are you sure you want to reboot (y/n)?
```

Parameters **active** — Reboots the active CPM.

Default active

standby — Reboots the standby CPM.

Default active

upgrade — Forces card firmware to be upgraded during chassis reboot. This option should only be used if it has been indicated as required in the Release Notes or by Nokia technical support. Normally, the SR-series router OS automatically performs firmware upgrades on CPMs and XCM/IOM cards without the need for the **upgrade** keyword.

When the **upgrade** keyword is specified, a chassis flag is set for the BOOT Loader (boot.ldr) and on the subsequent boot of the OS on the chassis, firmware images on CPMs, XCMs, and IOMs will be upgraded automatically.

Firmware on CPMs, XCMs, or IOMs that are installed in a running chassis will be upgraded automatically. For example, if a card is inserted as the result of a hot swap, and the card has a firmware version that is no longer compatible with the SR OS image running on the chassis, then the firmware on the card will be automatically upgraded before the card is brought online.

If the card firmware is upgraded, a chassis cardUpgraded (event 2032) log event is generated. The corresponding SNMP trap for this log event is tmnxEqCardFirmwareUpgraded.

During any firmware upgrade, automatic or manual, it is imperative that during the upgrade procedure:

- Power must not be switched off or interrupted.
- The system must not be reset.
- No cards are inserted or removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Any of the above conditions may render cards inoperable requiring a return of the card for resolution.

The time required to upgrade the firmware on the cards in the chassis depends on the number of cards to be upgraded. The progress of a firmware upgrade can be monitored at the console.

now — Forces a reboot of the router immediately without an interactive confirmation.

Platforms All

reboot

Syntax **reboot** [**now**] **upgrade**

Context **[Tree]** (admin>satellite>eth-sat reboot)

Full Context admin satellite eth-sat reboot

Description The command initiates an administrative reboot of the specified Ethernet-satellite chassis.

Parameters **now** — Causes the satellite to reboot immediately without further prompts or interactive confirmation.

upgrade — Causes the satellite to update its firmware image during chassis reboot.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.59 receive

receive

Syntax [**no**] **receive**

Context **[Tree]** (config>port>ethernet>eth-cfm>mep>eth-bn receive)

Full Context configure port ethernet eth-cfm mep eth-bn receive

Description This command enables the reception and processing of **eth-bn** messages and the retrieval and processing of the current bandwidth field for inclusion in dynamic egress rate adjustments.

The received rate is an Layer 2 rate, and is expected to be in Mb/s. If this rate is a link rate (including preamble, start frame delimiter, and inter-frame gap), this would require the use of network egress queue groups (configured in the **configure qos queue-group-templates egress queue-group "qg1" queue 1 packet-byte-offset add** *20*). The **packet-byte-offset** is not supported for default network queues.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no receive

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

receive

Syntax **receive** {**both** | **none** | **version-1** | **version-2**}
no receive

Context **[Tree]** (config>service>vprn>rip receive)
[Tree] (config>service>vprn>rip>group receive)
[Tree] (config>service>vprn>rip>group>neighbor receive)
[Tree] (config>service>vprn>ripng receive)
[Tree] (config>service>vprn>ripng>group receive)
[Tree] (config>service>vprn>ripng>group>neighbor receive)

Full Context configure service vprn rip group neighbor receive
configure service vprn rip group receive
configure service vprn rip receive
configure service vprn ripng group neighbor receive
configure service vprn ripng group receive
configure service vprn ripng receive

Description This command configures the type(s) of RIP updates that will be accepted and processed.

If **both** or **version-2** is specified, the RIP instance listens for and accepts packets sent to the broadcast and multicast (224.0.0.9) addresses.

If **version-1** is specified, the router only listens for and accepts packets sent to the broadcast address.

This control can be issued at the global, group or interface level. The default behavior accepts and processes both RIPv1 and RIPv2 messages.

The **no** form of this command resets the type of messages accepted to both.

Default no receive

Parameters *both* — Accept RIP updates in either Version 1 or Version 2 format.

none — Do not accept and RIP updates.

version-1 — Router should only accept RIP updates in Version 1 format.

version-2 — Router should only accept RIP updates in Version 2 format.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

receive

Syntax **receive**

Context **[Tree]** (config>system>security>keychain>direction>uni receive)

Full Context configure system security keychain direction uni receive

Description This command enables the receive nodal context. Entries defined under this context are used to authenticate TCP segments that are being received by the router.

Platforms All

receive

Syntax **receive** *option-number*
no receive

Context **[Tree]** (config>system>security>keychain>tcp-option-number receive)

Full Context configure system security keychain tcp-option-number receive

Description This command configures the TCP option number accepted in TCP packets received.

The **no** form of this command reverts to the default value.

Default receive 254

Parameters *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

Values 253, 254, 253&254, tcp-ao

Platforms All

receive

Syntax **receive** {**both** | **none** | **version-1** | **version-2**}
no receive

Context **[Tree]** (config>router>rip receive)
[Tree] (config>router>rip>group receive)
[Tree] (config>router>rip>group>neighbor receive)
[Tree] (config>router>ripng receive)
[Tree] (config>router>ripng>group receive)
[Tree] (config>router>ripng>group>neighbor receive)

Full Context configure router rip group neighbor receive
configure router rip group receive

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router rip receive
configure router ripng group neighbor receive
configure router ripng group receive
configure router ripng receive

Description This command configures the types of RIP updates that will be accepted and processed.

If **both** or **version-2** is specified, the RIP instance listens for and accepts packets sent to the broadcast and multicast (224.0.0.9) addresses.

If **version-1** is specified, the router only listens for and accept packets sent to the broadcast address.

This control can be issued at the global, group or interface level. The default behavior is to accept and process both RIPv1 and RIPv2 messages.

The **no** form of the command reverts to the default value.

Default receive both – in the config>router>rip context

receive version-1 – in the config>router>ripng context

Parameters **both** — Specifies that RIP updates in either version 1 or version 2 format will be accepted.

none — Specifies that RIP updates will not be accepted.

version-1 — Specifies that RIP updates in version 1 format only will be accepted.

version-2 — Specifies that RIP updates in version 2 format only will be accepted.

Platforms All

22.60 receive-interval

receive-interval

Syntax **receive-interval** *receive-interval*
no receive-interval

Context **[Tree]** (config>lag>bfd>family receive-interval)

Full Context configure lag bfd family receive-interval

Description This command specifies the receive timer used for micro-BFD session over the associated LAG links.

The **no** form of this command removes the receive timer from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default receive-interval 100

Parameters *receive-interval* — Specifies the interval value, in milliseconds.

Values 10 to 100000

Default 100 for CPM3 or later, 1000 for all others

Platforms All

receive-interval

Syntax **receive-interval** *receive-interval*
no receive-interval

Context **[Tree]** (config>router>bfd>bfd-template receive-interval)

Full Context configure router bfd bfd-template receive-interval

Description This command specifies the receive timer used for BFD packets. If the template is used for a BFD session on an MPLS-TP LSP, then this timer is used for CC packets.

The **no** form of this command reverts to the default value.

Default receive-interval 100

Parameters *receive-interval* — Specifies the receive interval. The minimum interval that can be configured is hardware dependent.

Values 10 ms to 100,000 ms in 1 ms intervals

Default 10 ms for CPM3 or higher; 1 second for other hardware

Platforms All

22.61 receive-msdp-msg-rate

receive-msdp-msg-rate

Syntax **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
no receive-msdp-msg-rate

Context **[Tree]** (config>service>vprn>msdp receive-msdp-msg-rate)
[Tree] (config>service>vprn>msdp>group receive-msdp-msg-rate)
[Tree] (config>service>vprn>msdp>group>peer receive-msdp-msg-rate)
[Tree] (config>service>vprn>msdp>peer receive-msdp-msg-rate)

Full Context configure service vprn msdp group peer receive-msdp-msg-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn msdp group receive-msdp-msg-rate
configure service vprn msdp peer receive-msdp-msg-rate
configure service vprn msdp receive-msdp-msg-rate

Description This command limits the number of Multicast Source Discovery Protocol (MSDP) messages that are read from the TCP session. It is possible that an MSDP/ RP router may receive a large number of MSDP protocol message packets in a particular source active message.

After the number of MSDP packets (including source active messages) defined in the threshold have been processed, the rate of all other MSDP packets is rate limited by no longer accepting messages from the TCP session until the time (seconds) has elapsed.

The **no** form of this command reverts this active-source limit to default operation.

Default no receive-msdp-msg-rate

Parameters *number* — Defines the number of MSDP messages (including source active messages) that are read from the TCP session per the number of seconds.

Values 10 to 10000

Default 0

interval *seconds* — Defines the time that, together with the *number* parameter, defines the number of MSDP messages (including source active messages) that are read from the TCP session within the configured number of seconds.

Values 1 to 600

Default 0

threshold number — The number of MSDP messages can be processed before the MSDP message rate limiting function described above is activated; this is particularly of use during at system startup and initialization.

Values 1 to 1000000

Default 0

Platforms All

receive-msdp-msg-rate

Syntax **receive-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
no receive-msg-rate

Context **[Tree]** (config>router>msdp receive-msdp-msg-rate)
[Tree] (config>router>msdp>peer receive-msdp-msg-rate)
[Tree] (config>router>msdp>group receive-msdp-msg-rate)
[Tree] (config>router>msdp>group>peer receive-msdp-msg-rate)

Full Context configure router msdp group peer receive-msdp-msg-rate
configure router msdp group receive-msdp-msg-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router msdp peer receive-msdp-msg-rate
configure router msdp receive-msdp-msg-rate

Description This command limits the number of Multicast Source Discovery Protocol (MSDP) messages that are read from the TCP session. It is possible that an MSDP/ RP router may receive a large number of MSDP protocol message packets in a particular source active message.

After the number of MSDP packets (including source active messages) defined in the threshold have been processed, the rate of all other MSDP packets is rate limited by no longer accepting messages from the TCP session until the time (seconds) has elapsed.

The **no** form of this command sets no limit on the number of MSDP and source active limit messages that will be accepted.

Default no receive-msdp-msg-rate

Parameters *number* — Specifies the number of MSDP messages (including source active messages) that are read from the TCP session per the number of seconds.

Values 10 to 10000

Default 0

seconds — Specifies the time that, together with the *number* parameter, defines the number of MSDP messages (including source active messages) that are read from the TCP session within the configured number of seconds.

Values 1 to 600

Default 0

number — Specifies the number of MSDP messages can be processed before the MSDP message rate limiting function described above is activated; this is particularly of use during at system startup and initialization.

Values 1 to 1000000

Default 0

Platforms All

22.62 receive-window-size

receive-window-size

Syntax **receive-window-size** *window-size*
no receive-window-size

Context **[Tree]** (config>router>l2tp receive-window-size)
[Tree] (config>router>l2tp>group receive-window-size)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>l2tp>group>tunnel receive-window-size)
[Tree] (config>service>vprn>l2tp receive-window-size)
[Tree] (config>service>vprn>l2tp>group receive-window-size)
[Tree] (config>service>vprn>l2tp>group>tunnel receive-window-size)

Full Context configure router l2tp group receive-window-size
configure router l2tp group tunnel receive-window-size
configure router l2tp receive-window-size
configure service vprn l2tp group receive-window-size
configure service vprn l2tp group tunnel receive-window-size
configure service vprn l2tp receive-window-size

Description This command configures the L2TP receive window size.

Default receive-window-size 64

Parameters *window-size* — Specifies the window size.

Values 4 to 1024

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.63 receiver

receiver

Syntax **receiver** *receiver-name* [**create**]
no receiver

Context [Tree] (config>sflow receiver)

Full Context configure sflow receiver

Description This command creates an sFlow receiver context or enters existing sFlow receiver context for the sFlow agent.

The **no** form of this command deletes an existing sFlow receiver context.

Parameters *receiver-names* — String of up to 127 characters.

Platforms 7750 SR, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.64 reclassify-using-qos

reclassify-using-qos

Syntax **reclassify-using-qos** *policy-id*
no reclassify-using-qos

Context **[Tree]** (config>service>ies>if>vpls>egress reclassify-using-qos)

Full Context configure service ies interface vpls egress reclassify-using-qos

Description The reclassify-using-qos command is used to specify a sap-egress QoS policy that will be used to reclassify the forwarding class and profile of egress routed packets on the VPLS or I-VPLS service. When routed packets associated with the IP interface egress a VPLS SAP, the reclassification rules within the sap-egress QoS policy applied to the SAP are always ignored (even when reclassify-using-qos is not defined).

Any queues or policers defined within the specified QoS policy are ignored and are not created on the VPLS egress SAPs. Instead, the routed packets continue to use the forwarding class mappings, queues and policers from the sap-egress QoS policy applied to the egress VPLS SAP.

While the specified sap-egress policy ID is applied to an IP interface it cannot be deleted from the system.

The **no** form of this command removes the sap-egress QoS policy used for reclassification from the egress IP interface. When removed, IP routed packets will not be reclassified on the egress SAPs of the VPLS service attached to the IP interface.

Parameters *policy-id* — Specifies the SAP egress QoS policy ID. This parameter is required when executing the reclassify-using-qos command. The specified SAP egress QoS ID must exist within the system or the command fails.

Platforms All

reclassify-using-qos

Syntax **reclassify-using-qos** *policy-id*
no reclassify-using-qos

Context **[Tree]** (config>service>vprn>if>vpls>egress reclassify-using-qos)

Full Context configure service vprn interface vpls egress reclassify-using-qos

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a SAP egress QoS policy that is used to reclassify the forwarding class and profile of egress routed packets on the VPLS service. When routed packets associated with the IP interface egress a VPLS SAP, the reclassification rules within the sap-egress QoS policy applied to the SAP are always ignored (even when reclassify-using-qos is not defined).

Any queues or policers defined within the specified QoS policy are ignored and are not created on the VPLS egress SAPs. Instead, the routed packets continue to use the forwarding class mappings, queues and policers from the SAP egress QoS policy applied to the egress VPLS SAP.

While the specified SAP egress policy ID is applied to an IP interface it cannot be deleted from the system.

The **no** form of this command removes the SAP egress QoS policy used for reclassification from the egress IP interface. When removed, IP routed packets is not reclassified on the egress SAPs of the VPLS service attached to the IP interface.

Parameters *policy-id* — Specifies the SAP egress QoS policy ID This parameter is required when executing the **reclassify-using-qos** command. The specified SAP egress QoS ID must exist within the system or the command fails.

Platforms All

22.65 reconnect-timeout

reconnect-timeout

Syntax **reconnect-timeout** *reconnect-timeout*
reconnect-timeout infinite
no reconnect-timeout

Context **[Tree]** (config>router>l2tp>eth-tunnel reconnect-timeout)
[Tree] (config>router>l2tp>group>eth-tunnel reconnect-timeout)
[Tree] (config>service>vprn>l2tp reconnect-timeout)
[Tree] (config>service>vprn>l2tp>group reconnect-timeout)

Full Context configure router l2tp eth-tunnel reconnect-timeout
configure router l2tp group eth-tunnel reconnect-timeout
configure service vprn l2tp group reconnect-timeout
configure service vprn l2tp reconnect-timeout

Description This command configures the number of seconds that the Ethernet tunnel client of L2TPv3 waits before attempting to re-establish a new session after a session setup fails or a session closes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns **reconnect-timeout** to an infinite timeout value, meaning that reconnection is not attempted by the local client.

Default no reconnect-timeout (infinite timeout)

Parameters *reconnect-timeout* — Specifies the number of seconds before a session reconnection is attempted after a previous session or session setup fails.

Values 10 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

reconnect-timeout

Syntax **reconnect-timeout** *reconnect-timeout*
no reconnect-timeout

Context **[Tree]** (config>service>vprn>l2tp>eth-tunnel reconnect-timeout)

Full Context configure service vprn l2tp eth-tunnel reconnect-timeout

Description This command configures the number of seconds that the Ethernet tunnel client of L2TPv3 waits before attempting to re-establish a new session after a session setup fails or a session closes.

The **no** form of this command returns **reconnect-timeout** to an infinite timeout value, meaning that reconnection is not attempted by the local client.

Default no reconnect-timeout (infinite timeout)

Parameters *reconnect-timeout* — Specifies the timeout value for the next session setup retry.

Values 10 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

reconnect-timeout

Syntax **reconnect-timeout** *reconnect-timeout*
reconnect-timeout infinite
no reconnect-timeout

Context **[Tree]** (config>service>vprn>l2tp>group>eth-tunnel reconnect-timeout)

Full Context configure service vprn l2tp group eth-tunnel reconnect-timeout

Description This command configures the number of seconds that the Ethernet tunnel client of L2TPv3 waits before attempting to re-establish a new session after a session setup fails or a session closes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command returns **reconnect-timeout** to an infinite timeout value, meaning that reconnection is not attempted by the local client.

Default no reconnect-timeout (infinite timeout)

Parameters *reconnect-timeout* — Specifies the timeout value for the next session setup retry.

Values 10 to 3600

infinite — Specifies the timeout value for the next session setup retry.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.66 record

record

Syntax [**no**] **record**

Context **[Tree]** (config>router>mpls>lsp>primary record)
[Tree] (config>router>mpls>lsp>primary-p2mp-instance record)
[Tree] (config>router>mpls>lsp>secondary record)
[Tree] (config>router>mpls>lsp-template record)

Full Context configure router mpls lsp primary record
configure router mpls lsp primary-p2mp-instance record
configure router mpls lsp secondary record
configure router mpls lsp-template record

Description This command enables recording of all the hops that an LSP path traverses. Enabling **record** increases the size of the PATH and RESV refresh messages for the LSP since this information is carried end-to-end along the path of the LSP. The increase in control traffic per LSP may impact scalability.

The config>router>mpls>lsp>primary-p2mp-instance>record command is not supported on the 7450 ESS.

The **no** form of this command disables the recording of all the hops for the given LSP. There are no restrictions as to when the **no** command can be used. The **no** form of this command also disables the **record-label** command.

Default record

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

record

Syntax **record**

Context **[Tree]** (debug>app-assure>group>traffic-capture record)

Full Context debug application-assurance group traffic-capture record

Description This command configures traffic recording options.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

record

Syntax **record** {**all-hosts** | **http-host-app-filter-candidates**}

Context **[Tree]** (debug>app-assure>group>http-host>filter record)

Full Context debug application-assurance group http-host-recorder filter record

Description This command configures which http-host are selected for the http-host-recorder. It is either any http-host values going through the AA ISA or the http-host corresponding to flows not matching a string based app-filter.

For the feature to work it is required to configure at least one app-filter to catch the HTTP protocol signature.

Parameters **all-hosts | http-host-app-filter-candidates** — Specifies which hosts the recorder will record

Values all-hosts, http-host-app-filter-candidates

Default http-host-app-filter-candidates

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

record

Syntax [**no**] **record** *record-name*

Context **[Tree]** (config>log>accounting-policy record)

Full Context configure log accounting-policy record

Description This command adds the accounting record type to the accounting policy that is forwarded to the configured accounting file. A record name can only be used in one accounting policy. To obtain a list of all record types that can be configured, use the **show log accounting-records** command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: aa, video, and subscriber records are not applicable to the 7950 XRS.

To configure an accounting policy for access ports, select a service record (for example, service-ingress-octets). To change the record name to another service record, enter the **record** command with the new record name and it replaces the old record name.

When configuring an accounting policy for network ports, select a network record. To change the record name to another network record, enter the **record** command with the new record name and it replaces the old record name.

If the change required modifies the record from network to service or from service to network, then the old record name must be removed using the **no** form of this command.

Only one record can be configured in a single accounting policy. For example, if an accounting-policy is configured with an **access-egress-octets** record, to change it to a **service-ingress-octets** record, use the **no record** command under the accounting-policy to remove the old record first, and then enter the **service-ingress-octets** record.

Note: Collecting excessive statistics can adversely affect the CPU utilization and take up large amounts of storage space.

The **no** form of this command removes the record type from the policy.

Default no record

Parameters *record-name* — Specifies the accounting record name.

Platforms All

22.67 record-label

record-label

Syntax [**no**] **record-label**

Context **[Tree]** (config>router>mpls>lsp>primary record-label)
[Tree] (config>router>mpls>lsp>secondary record-label)
[Tree] (config>router>mpls>lsp-template record-label)

Full Context configure router mpls lsp primary record-label
configure router mpls lsp secondary record-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mpls lsp-template record-label

Description This command enables recording of all the labels at each node that an LSP path traverses. Enabling the **record-label** command will also enable the **record** command if it is not already enabled.

The **no** form of this command disables the recording of the hops that an LSP path traverses.

Default record-label

Platforms All

22.68 record-stats

record-stats

Syntax **record-stats** {**delay** | **loss** | **delay-and-loss**}
no record-stats

Context **[Tree]** (config>oam-pm>session>ip>twamp-light record-stats)

Full Context configure oam-pm session ip twamp-light record-stats

Description This option provides the ability to determine which statistics are recorded. The TWAMP-Light PDU can report on both delay and loss using a single packet. The operator may choose which statistics they would like to report. Only delay recording is on by default. All other metrics are ignored. In order to change what is being recorded and reported, the TWAMP-Light session must be shutdown. This is required because the single packet approach means the base statistics are shared between the various datasets. Issuing a **no shutdown** command clears previous all non-volatile memory for the session and allocate new memory blocks. All the parameters under this context are mutually exclusive.

The **no** version of the command restores the default “delay” only.

Default record-stats delay

Parameters **delay** — Specifies report on delay using a single packet..

loss — Specifies to report on loss using a single packet..

delay-and-loss — Specifies to report on both delay and loss using a single packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.69 recovery

recovery

Syntax [**no**] **recovery**

Context **[Tree]** (debug>router>l2tp>assignment-id>event recovery)
[Tree] (debug>router>l2tp>event recovery)
[Tree] (debug>router>l2tp>group>event recovery)
[Tree] (debug>router>l2tp>peer>event recovery)
[Tree] (debug>router>l2tp>tunnel>event recovery)

Full Context debug router l2tp assignment-id event recovery
debug router l2tp event recovery
debug router l2tp group event recovery
debug router l2tp peer event recovery
debug router l2tp tunnel event recovery

Description This command configures L2TP LAC state recovery event debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.70 recovery-failed

recovery-failed

Syntax [**no**] **recovery-failed**

Context **[Tree]** (debug>router>l2tp>assignment-id>event recovery-failed)
[Tree] (debug>router>l2tp>event recovery-failed)
[Tree] (debug>router>l2tp>group>event recovery-failed)
[Tree] (debug>router>l2tp>peer>event recovery-failed)
[Tree] (debug>router>l2tp>tunnel>event recovery-failed)

Full Context debug router l2tp assignment-id event recovery-failed
debug router l2tp event recovery-failed
debug router l2tp group event recovery-failed
debug router l2tp peer event recovery-failed
debug router l2tp tunnel event recovery-failed

Description This command configures L2TP LAC state recovery failed event debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.71 recovery-max-session-lifetime

recovery-max-session-lifetime

Syntax **recovery-max-session-lifetime** *minutes*
no recovery-max-session-lifetime

Context **[Tree]** (config>router>l2tp>failover recovery-max-session-lifetime)
[Tree] (config>service>vprn>l2tp>failover recovery-max-session-lifetime)

Full Context configure router l2tp failover recovery-max-session-lifetime
configure service vprn l2tp failover recovery-max-session-lifetime

Description This command configures the sub-set of sessions that this system attempts to synchronize in the Session State Synchronization phase as described in RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP)*.

The **no** form of this command reverts to the default.

Default recovery-max-session-lifetime 2

Parameters *minutes* — Specifies the sub-set of sessions to recover.

Values 2 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.72 recovery-method

recovery-method

Syntax **recovery-method** *method*
no recovery-method

Context **[Tree]** (config>router>l2tp>failover recovery-method)
[Tree] (config>service>vprn>l2tp>failover recovery-method)
[Tree] (config>router>l2tp>group>failover recovery-method)
[Tree] (config>service>vprn>l2tp>group>failover recovery-method)
[Tree] (config>router>l2tp>group>tunnel>failover recovery-method)
[Tree] (config>service>vprn>l2tp>group>tunnel>failover recovery-method)

Full Context configure router l2tp failover recovery-method
configure router l2tp group failover recovery-method
configure router l2tp group tunnel failover recovery-method
configure service vprn l2tp failover recovery-method

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn l2tp group failover recovery-method
configure service vprn l2tp group tunnel failover recovery-method

Description This command sets the recovery method to be used for newly created tunnels.

The **no** form of this command reverts to the default.

Default recovery-method mcs on config>router>l2tp>failover and config>service>vprn>l2tp>failover

recovery-method default on config>router>l2tp>group>failover

recovery-method default on config>router>l2tp>group>tunnel>failover

recovery-method default on config>service>vprn>l2tp>group>failover

recovery-method default on config>service>vprn>l2tp>group>tunnel>failover

Parameters *method* — Describes how a pair of redundant LAC peers recover tunnel and session state (sequence numbers, for example) immediately after a failover.

Note: While failover is enabled, the tunnels and sessions proper are always kept synchronized between the redundant pair, regardless of the recovery method for the sequence numbers when a failover really occurs.

Values **mcs** — Specifies that the stateful information is recovered from the failover peer directly, using Multi-Chassis Redundancy Synchronization (MCS).

recovery-tunnel — Specifies that the stateful information is recovered as described in RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP)*. This method uses a recovery tunnel to the L2TP peer to pass the stateful information.

default — Specifies that the actual value must be derived from another object of the same type with a wider scope. Takes the value of the next higher level (not available in **config>router>l2tp>failover** and **config>service>vprn>l2tp>failover**).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.73 recovery-time

recovery-time

Syntax **recovery-time** *seconds*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no recovery-time

Context [Tree] (config>router>l2tp>failover recovery-time)
[Tree] (config>service>vprn>l2tp>failover recovery-time)
[Tree] (config>router>l2tp>group>failover recovery-time)
[Tree] (config>service>vprn>l2tp>group>failover recovery-time)
[Tree] (config>router>l2tp>group>tunnel>failover recovery-time)
[Tree] (config>service>vprn>l2tp>group>tunnel>failover recovery-time)

Full Context configure router l2tp failover recovery-time
configure router l2tp group failover recovery-time
configure router l2tp group tunnel failover recovery-time
configure service vprn l2tp failover recovery-time
configure service vprn l2tp group failover recovery-time
configure service vprn l2tp group tunnel failover recovery-time

Description This command sets the recovery time to be negotiated via RFC 4951. It represents the extra time this L2TP peer (LAC or LNS) needs to recover all its tunnels.

The **no** form of this command reverts to the default.

Default recovery-time 0 on config>router>l2tp>failover and config>service>vprn>l2tp>failover

Parameters *seconds* — Specifies the period, expressed in seconds, an endpoint asks its peer to wait before assuming the recovery process has failed.

Values 0 to 900

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.74 recovery-timer

recovery-timer

Syntax **recovery-timer** *timer-value*
no recovery-timer

Context [Tree] (config>service>ipipe>eth-legacy-fault-notification recovery-timer)

Full Context configure service ipipe eth-legacy-fault-notification recovery-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This timer provides the legacy protocols PPP, MLPPP and HDLC time to establish after the Ethernet fault condition has cleared. The legacy protocol is afforded this amount of time to establish the connection before a fault is declared on the legacy side and propagated to the Ethernet segment. This timer is started as a result of a clearing Ethernet failure. Faults that may exist on the legacy side will not be detected until the expiration of this timer. Until the legacy side connection is established or the timer expires the traffic arriving on the Ethernet SAP from a peer will be discarded. The default value is unlikely to be a representative of all operator requirements and must be evaluated on a case by case basis.

Parameters *timer-value* — The value of the wait time in tenths of a second (100 ms). Granularity is in 500 ms increments, starting from 1 s and up to 30 s.

Values 10 to 300

Default 100

Platforms All

22.75 red

red

Syntax **red** [**detail**]
no red

Context **[Tree]** (debug>service>id>pim-snooping red)

Full Context debug service id pim-snooping red

Description This command enables or disables debugging for PIM messages sent to the standby CPM.

Parameters **detail** — Displays detailed debugging information

Platforms All

red

Syntax [**no**] **red** [**detail**]

Context **[Tree]** (debug>router>pim red)

Full Context debug router pim red

Description This command enables debugging for PIM redundancy messages to the standby CPM.

The **no** form of this command disables debugging for PIM redundancy messages to the standby CPM.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **detail** — Displays detailed redundancy information.

Platforms All

22.76 red-alarm-threshold

red-alarm-threshold

Syntax **red-alarm-threshold** *percentage*
no red-alarm-threshold

Context **[Tree]** (config>port>access>egress>pool red-alarm-threshold)
[Tree] (config>port>access>ingress>pool red-alarm-threshold)
[Tree] (config>port>network>egress>pool red-alarm-threshold)

Full Context configure port access egress pool red-alarm-threshold
configure port access ingress pool red-alarm-threshold
configure port network egress pool red-alarm-threshold

Description This command configures the threshold for the red alarm on the over-subscription allowed.

Users can selectively enable amber or red alarm thresholds. But if both are enabled (non-zero), the amber alarm threshold cannot be more than the red alarm threshold.

The **no** form of this command reverts to the default value.

Default no red-alarm-threshold

Parameters *percentage* — Specifies the red alarm threshold.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

red-alarm-threshold

Syntax **red-alarm-threshold** *percentage*
no red-alarm-threshold

Context **[Tree]** (config>card>fp>ingress>network>pool red-alarm-threshold)

Full Context configure card fp ingress network pool red-alarm-threshold

Description This command configures the threshold for the red alarm on the over-subscription allowed.

Users can selectively enable amber or red alarm thresholds. But if both are enabled (non-zero) then the red alarm threshold must be greater than the amber alarm threshold.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default no amber-alarm-threshold

Parameters *percentage* — Specifies the red alarm threshold.

Values 1 to 1000

Platforms All

22.77 red-differential-delay

red-differential-delay

Syntax **red-differential-delay** *red-diff-delay* [**down**]
no red-differential-delay

Context **[Tree]** (config>port>multilink-bundle red-differential-delay)

Full Context configure port multilink-bundle red-differential-delay

Description This command sets the maximum acceptable differential delay for individual links within a multilink bundle. The differential delay is calculated as the round-trip differential delay for MLPPP bundles, and as uni-directional differential delay for IMA bundles.

The **no** form of this command restores the red-differential-delay defaults.

Parameters *red-diff-delay* — Specify the maximum red differential delay value.

Values 0 to 50 milliseconds for IMA bundles 0 to 25 milliseconds for all other bundles

down — Transition the link that exceeded the differential delay to a down state (for example, remove it from the multilink bundle from an operational perspective).

Platforms 7450 ESS, 7750 SR-7/12/12e

22.78 red-source-list

red-source-list

Syntax **red-source-list**

Context **[Tree]** (config>service>vprn>mvpn red-source-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn mvpn red-source-list

Description This command enables context to configure list of redundant source prefixes for preferred source selection.

Platforms All

22.79 redelegation-timer

redelegation-timer

Syntax **redelegation-timer** *seconds*
no redelegation-timer

Context **[Tree]** (config>router>pcep>pcc redelegation-timer)

Full Context configure router pcep pcc redelegation-timer

Description This command configures the redelegation timer for PCE-initiated LSPs.

The **no** form of the command sets this value to the default.

Default redelegation-timer 90

Parameters *seconds* — Specifies the number of seconds before the redelegation timer expires.

Values 1 to 3600

Platforms All

22.80 redirect-https

redirect-https

Syntax **redirect-https**
no redirect-https

Context **[Tree]** (config>app-assure>group>http-redirect redirect-https)

Full Context configure application-assurance group http-redirect redirect-https

Description This command configures the http-redirect policy to redirect HTTPS sessions to the configured redirect-url.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the redirect-https.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.81 redirect-policy

redirect-policy

Syntax **redirect-policy** *redirect-policy-name* [**create**]
no redirect-policy *redirect-policy-name*

Context **[Tree]** (config>filter redirect-policy)

Full Context configure filter redirect-policy

Description This command, creates a configuration context for the specified redirect policy.

The **no** form of the command removes the redirect policy from the filter configuration only if the policy is not referenced in a filter and the filter is not in use (applied to a service or network interface).

Parameters *redirect-policy-name* — Specifies the redirect policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. There is no limit to the number of redirect policies that can be configured.

create — This keyword is required to create the configuration context. Once it is created, the context can be enabled with or without the **create** keyword.

Platforms All

redirect-policy

Syntax **redirect-policy** *redirect-policy-name* **destination** *ip-address*
no redirect-policy *redirect-policy-name* [**destination** *ip-address*]

Context **[Tree]** (config>filter>redirect-policy-binding redirect-policy)

Full Context configure filter redirect-policy-binding redirect-policy

Description This command adds the destination (specified by its IP address) of a redirect-policy (specified by its name) to the binding. An error is thrown if either the destination does not exist for the specified redirect-policy or if the redirect-policy does not exist.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes from the binding from all the destinations of the specified redirect-policy, or only the specified destination.

Parameters *redirect-policy-name* — Specifies the name of the redirect-policy (up to 32 characters) as the destination that is to be added to the binding.

ip-address — The IP address of the destination. This can be an IPv4 or IPv6 address.

Values

ipv4-address:	a.b.c.d.
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms All

22.82 redirect-policy-binding

redirect-policy-binding

Syntax **redirect-policy-binding** *name* [**create**]
no redirect-policy-binding *name*

Context **[Tree]** (config>filter redirect-policy-binding)

Full Context configure filter redirect-policy-binding

Description This command creates a redirect-policy binding (specified by its name) in case it does not exist and, enters the context associated with it. When a redirect-policy binding is created, no destination is associated to this binding by default and the binding operator is set to AND.

The **no** form of this command deletes the redirect-policy binding and all the associated configuration information.

Parameters *name* — Specifies the name of the binding. Possible values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotations.

create — This keyword is required to create the binding if it does not exist. This has no effect when used with an existing binding.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.83 redirect-url

redirect-url

Syntax **redirect-url** *redirect-url*
no redirect-hurl

Context **[Tree]** (config>app-assure>group>http-redirect redirect-url)

Full Context configure application-assurance group http-redirect redirect-url

Description This command configures the http redirect URL which is the URL (page) that the user is redirected to when an HTTP redirect takes effect.

The operator can select the URL arguments to include in the redirect-url using either a specific template-id or by configuring the redirect-url using any of the supported macro substitution keywords. Only ESM and ESM-MAC sub types support $MAC, $SAP, $CID, and $RID macro substitution.

The **no** form of this command removes the redirect-url field from the configuration.

Parameters *redirect-url* — Specifies the URL of the landing page

Values **macro substitutions**:

$CATID	The category ID.
$CATNAME	The category name of the URL.
$URL	The Request-URI in the HTTP GET Request received.
$SUB	A string that represents the subscriber ID.
$IP	A string that represents the IP address of the subscriber host.
$RTRID	A string that represents the router ID.
$URLPRM	The HTTP URL parameter associated with the subscriber.
$MAC	A string that represents the MAC address of the subscriber host.
$SAP	A string that represents a SAP ID.
$CID	A string that represents the circuit-id or interface-id of the subscriber host (hexadecimal format).
$RID	A string that represents the remote-id of the subscriber host (hexadecimal format).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.84 redirect-vprn

redirect-vprn

Syntax **redirect-vprn**

Context **[Tree]** (config>router>dns redirect-vprn)

Full Context configure router dns redirect-vprn

Description This command configures the DNS resolution to be resolved via VPRN. If configured, all packet URL resolution is done through a DNS server that is reachable in a VPRN. This includes packets in the global routing table.

Default redirect-vprn

Platforms All

22.85 redirection

redirection

Syntax **redirection** *level*
no redirection

Context **[Tree]** (config>system>file-trans-prof redirection)

Full Context configure system file-transmission-profile redirection

Description This command enables system to accept HTTP redirection response, along with the max level of redirection. The virtual router may send a new request to another server if the requested resources are not available (temporarily available to another server).

Default no redirection

Parameters *level* — Specifies the maximum level of redirection of the file transmission profile max level of HTTP redirection.

Values 1 to 8

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.86 redirection-policy

redirection-policy

Syntax **redirection-policy** *policy-name*
no redirection-policy

Context **[Tree]** (config>subscr-mgmt>igmp-policy redirection-policy)

Full Context configure subscriber-mgmt igmp-policy redirection-policy

Description This command will apply multicast redirection action to the subscriber. The redirection action along with the redirected interface (and possibly service id) is defined in the referenced policy-name. IGMP messages is redirected to an alternate interface if that alternate interface has IGMP enabled. The alternate interface does not have to have any multicast groups registered via IGMP. Currently all IGMP messages are redirected and there is no ability to selectively redirect IGMP messages based on match conditions (multicast-group address, source IP address, and so on). Multicast redirection is supported between VPRN services and also between interfaces within the Global Routing Context. Multicast Redirection is not supported between the VPRN services and the Global Routing Table (GRT).

IGMP state is maintained per subscriber host and per redirected interface. Traffic is however forwarded only on the redirected interface.

The **no** form of this command reverts to the default value.

Parameters *policy-name* — Specifies the redirection policy to be applied to this host IGMP policy up to 32 characters. This is a policy defined in the **config>router>policy-option>policy-statement** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

redirection-policy

Syntax **redirection-policy** *policy-name*
no redirection-policy

Context **[Tree]** (config>subscr-mgmt>mld-policy redirection-policy)

Full Context configure subscriber-mgmt mld-policy redirection-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command applies multicast redirection action to the subscriber. The redirection action along with the redirected interface (and possibly service id) is defined in the referenced policy-name. MLD messages is redirected to an alternate interface if that alternate interface has MLD enabled. The alternate interface does not have to have any multicast groups registered via MLD. Currently all MLD messages are redirected and there is no ability to selectively redirect MLD messages based on match conditions (multicast-group address, source IP address, and so on). Multicast redirection is supported between VPRN services and also between interfaces within the Global Routing Context. Multicast Redirection is not supported between the VPRN services and the Global Routing Table (GRT).

MLD state is maintained per subscriber host and per redirected interface. Traffic is however forwarded only on the redirected interface.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies a redirection policy name up to 32 characters. This is a regular policy defined under the **configure>router>policy-option>policy-statement** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.87 redirects

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context **[Tree]** (config>service>ies>if>icmp redirects)
[Tree] (config>service>ies>if>ipv6>icmp6 redirects)
[Tree] (config>service>ies>sub-if>grp-if>icmp redirects)
[Tree] (config>service>vprn>if>icmp redirects)
[Tree] (config>service>vprn>if>ipv6>icmp6 redirects)
[Tree] (config>service>vprn>if redirects)
[Tree] (config>service>vprn>nw-if>icmp redirects)

Full Context configure service ies interface icmp redirects
configure service ies interface ipv6 icmp6 redirects
configure service ies subscriber-interface group-interface icmp redirects
configure service vprn interface icmp redirects
configure service vprn interface ipv6 icmp6 redirects
configure service vprn interface redirects
configure service vprn network-interface icmp redirects

Description This command configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

The **no** form of this command disables the generation of ICMP redirects on the router interface.

Default redirects 100 10

Parameters *number* — Specifies the maximum number of ICMP redirect messages to send. This parameter must be specified with the *second* parameter.

Values 10 to 1000

seconds — Specifies the time frame in seconds used to limit the *number* of ICMP redirect messages that can be issued.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface icmp redirects

All

- configure service ies interface ipv6 icmp6 redirects
- configure service vprn interface icmp redirects
- configure service vprn network-interface icmp redirects
- configure service ies interface icmp redirects
- configure service vprn interface ipv6 icmp6 redirects

redirects

Syntax **redirects** [**number** *number*] [**seconds** *seconds*]
no redirects

Context **[Tree]** (config>subscr-mgmt>git>ipv4>icmp redirects)

Full Context configure subscriber-mgmt group-interface-template ipv4 icmp redirects

Description This command configures the ICMPv4 redirect messages that are generated when routes are not optimal on the router and the node needs to be alerted that another router on the same subnetwork has a better route available.

When disabled, ICMPv4 redirects are not generated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables generation of redirect messages.

Default redirects number 100 seconds 10

Parameters *number* — Specifies the number of ICMPv4 redirects that are issued in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds — Specifies the time, in seconds, that is used to limit the number of ICMPv4 redirects issued.

Values 1 to 60

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context **[Tree]** (config>router>if>icmp redirects)

Full Context configure router interface icmp redirects

Description This command enables and configures the rate for ICMP redirect messages issued on the router interface.

When routes are not optimal on this router, and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects are issued can be controlled with the optional *number* and *time* parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of ICMP redirects on the router interface.

Default redirects 100 10 — Maximum of 100 redirect messages in 10 seconds.

Parameters *number* — The maximum number of ICMP redirect messages to send, expressed as a decimal integer. This parameter must be specified with the *time* parameter.

Values 10 to 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

seconds — The time frame, in seconds, used to limit the *number* of ICMP redirect messages that can be issued, expressed as a decimal integer.

Values 1 to 60

Platforms All

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context **[Tree]** (config>router>if>ipv6>icmp6 redirects)

Full Context configure router interface ipv6 icmp6 redirects

Description This command configures the rate for ICMPv6 redirect messages. When configured, ICMPv6 redirects are generated when routes are not optimal on the router and another router on the same subnetwork has a better route to alert that node that a better route is available.

The **no** form of this command disables ICMPv6 redirects.

Default redirects 100 10 (when IPv6 is enabled on the interface)

Parameters *number* — Limits the number of redirects issued per the time frame specified in *seconds* parameter.

Values 10 to 1000

seconds — Determines the time frame, in seconds, that is used to limit the number of redirects issued per time frame.

Values 1 to 60

Platforms All

22.88 redistribute-delay

redistribute-delay

Syntax **redistribute-delay** *redistribute-delay*
no redistribute-delay

Context **[Tree]** (config>router>ospf>timers redistribute-delay)
[Tree] (config>router>ospf3>timers redistribute-delay)

Full Context configure router ospf timers redistribute-delay
configure router ospf3 timers redistribute-delay

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the internal OSPF hold down timer for external routes being redistributed into OSPF.

Shorting this delay can speed up the advertisement of external routes into OSPF but can result in additional OSPF messages if that source route is not yet stable.

The **no** form of this command resets the timer value back to the default value.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is greater than or equal to 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default redistribute-delay 1000

Parameters *redistribute-delay* — Specifies the OSPF redistribution hold down time in milliseconds for external routes being advertised into OSPF.

Values 0 to 1000

Platforms All

22.89 redistribute-external

redistribute-external

Syntax [**no**] **redistribute-external**

Context **[Tree]** (config>service>vprn>ospf>area>nssa redistribute-external)
[Tree] (config>service>vprn>ospf3>area>nssa redistribute-external)

Full Context configure service vprn ospf area nssa redistribute-external
configure service vprn ospf3 area nssa redistribute-external

Description This command enables the redistribution of external routes into the Not So Stubby Area (NSSA) or an NSSA area border router (ABR) that is exporting the routes into non-NSSA areas.

NSSA or Not So Stubby Areas are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that the NSSA has the capability to flood external routes that it learns (providing it is an ASBR) throughout its area and via an ABR to the entire OSPF domain.

The **no** form of this command disables the default behavior to automatically redistribute external routes into the NSSA area from the NSSA ABR.

Default redistribute-external — External routes are redistributed into the NSSA.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

redistribute-external

Syntax [**no**] **redistribute-external**

Context **[Tree]** (config>router>ospf>area>nssa redistribute-external)
[Tree] (config>router>ospf3>area>nssa redistribute-external)

Full Context configure router ospf area nssa redistribute-external
configure router ospf3 area nssa redistribute-external

Description This command enables the redistribution of external routes into the Not So Stubby Area (NSSA) or an NSSA area border router (ABR) that is exporting the routes into non-NSSA areas.

NSSA or Not So Stubby Areas are similar to stub areas in that no external routes are imported into the area from other OSPF or OSPF3 areas. The major difference between a stub area and an NSSA is that the NSSA has the capability to flood external routes that it learns (providing it is an ASBR) throughout its area and via an Area Border Router to the entire OSPF or OSPF3 domain.

The **no** form of this command disables the default behavior to automatically redistribute external routes into the NSSA area from the NSSA ABR.

Default redistribute-external

Platforms All

22.90 redo

redo

Syntax **redo** [*count*]

Context **[Tree]** (candidate redo)

Full Context candidate redo

Description This command reapplies the changes to the candidate that were removed using a previous undo. All undo or redo history is lost when the operator exits **edit-cfg** mode.

A **redo** command is blocked if another user has made changes in the same CLI branches that would be impacted during the redo.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **count** — Specifies the number of previous changes to reapply.

Values 1 to 50

Default 1

22.91 reduced-prompt

reduced-prompt

Syntax **reduced-prompt** [*no-of-nodes-in-prompt*]
no reduced-prompt

Context **[Tree]** (environment reduced-prompt)

Full Context environment reduced-prompt

Description This command configures the maximum number of higher CLI context levels to display in the CLI prompt for the current CLI session. This command is useful when configuring features that are several node levels deep, causing the CLI prompt to become too long. By default, the CLI prompt displays the system name and the complete context in the CLI.

The number of *nodes* specified indicates the number of higher-level contexts that can be displayed in the prompt. For example, if reduced prompt is set to 2, the two highest contexts from the present working context are displayed by name with the hidden (reduced) contexts compressed into a ellipsis ("…").

```
A:ALA-1>environment# reduced-prompt 2
A:ALA-1>config>router# interface to-103
A:ALA-1>...router>if#
```

The setting is not saved in the configuration. It must be reset for each CLI session or stored in an **exec** script file.

The **no** form of the command reverts to the default.

Default no reduced-prompt

Parameters *no-of-nodes-in-prompt* — Specifies the maximum number of higher-level nodes displayed by name in the prompt, expressed as a decimal integer.

Values 0 to 15

Default 2

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.92 redundancy

redundancy

Syntax **redundancy**

Context **[Tree]** (config redundancy)

Full Context configure redundancy

Description This command allows the user to perform redundancy operations.

Associated commands include the following in the **admin>redundancy** context:

- **force-switchover** - Forces a switchover to the standby CPM card.
- **now** - Switch to standby CPM.
  Switching to the standby displays the following message.
  ```
  WARNING: Configuration and/or Boot options may have changed since
  the last save.
  Are you sure you want to switchover (y/n)?
  ```
- **synchronize** - Synchronizes the secondary CPM.

Platforms All

redundancy

Syntax **redundancy**

Context **[Tree]** (admin redundancy)

Full Context admin redundancy

Description Commands in this context allow the user to perform redundancy operations.

Platforms All

redundancy

Syntax **redundancy**

Context **[Tree]** (config>service>ies>sub-if>wlan-gw redundancy)

Full Context configure service ies subscriber-interface wlan-gw redundancy

Description Commands in this context configure WLAN-GW redundancy-related parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

redundancy

Syntax **redundancy**

Context **[Tree]** (config>router>nat>inside redundancy)
[Tree] (config>service>vprn>nat>inside redundancy)
[Tree] (config>service>vprn>nat>outside>pool redundancy)

Full Context configure router nat inside redundancy
configure service vprn nat inside redundancy
configure service vprn nat outside pool redundancy

Description Commands in this context configure redundancy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

redundancy

Syntax **redundancy** {**active-active** | **active-standby** | **l2aware-bypass**}
no redundancy

Context **[Tree]** (config>isa>nat-group redundancy)

Full Context configure isa nat-group redundancy

Description This command configures intra-chassis redundancy mode for the NAT group.

Default redundancy active-standby

Parameters **active-active** — Specifies the mode in which all MS-ISAs in a NAT group are active. If one or two MS-ISAs in the system fail, the remaining active MS-ISA accepts the load from the failed MS-ISAs.

active-standby — Specifies the mode in which one or more MS-ISAs in the NAT group are in standby mode. While in standby mode, MS-ISAs do not process traffic. Traffic is diverted to the standby MS-ISA only when the active MS-ISA fails, at which point the standby becomes active.

l2-aware-bypass — Specifies that when an ISA MDA fails, NAT reroutes its traffic based on the regular destination address lookup. This resiliency mode is applicable only to L2-Aware NAT. When the MS-ISA fails, its traffic is routed via regular routing (destination-based lookup). The assumption is that traffic is sent to an external NAT device that serves as a backup NAT device.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

redundancy

Syntax **redundancy**

Context **[Tree]** (config>router>nat>outside>pool redundancy)

Full Context configure router nat outside pool redundancy

Description Commands in this context configure NAT pool redundancy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

redundancy

Syntax **redundancy**

Context **[Tree]** (config>eth-cfm redundancy)

Full Context configure eth-cfm redundancy

Description Commands in this context configure the ETH-CFM redundancy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.93 redundant-interface

redundant-interface

Syntax **redundant-interface** *red-ip-int-name*
no redundant-interface

Context **[Tree]** (config>service>ies>sub-if>grp-if redundant-interface)
[Tree] (config>service>vprn>sub-if>grp-if redundant-interface)

Full Context configure service ies subscriber-interface group-interface redundant-interface
configure service vprn subscriber-interface group-interface redundant-interface

Description This command configures a redundant interface used for dual homing.

Parameters *red-ip-int-name* — Specifies the redundant IP interface name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

redundant-interface

Syntax **redundant-interface** *ip-int-name* [**create**]
no redundant-interface *ip-int-name*

Context **[Tree]** (config>service>ies redundant-interface)
[Tree] (config>service>vprn redundant-interface)

Full Context configure service ies redundant-interface
configure service vprn redundant-interface

Description This command configures a redundant interface.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — Keyword used to create a redundant interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

redundant-interface

Syntax **redundant-interface service** *service-id* **name** *interface-name*
no redundant-interface

Context **[Tree]** (config>subscr-mgmt>up-resiliency>fsg-template redundant-interface)

Full Context configure subscriber-mgmt up-resiliency fate-sharing-group-template redundant-interface

Description This command configures downstream traffic shunting from a standby BNG UPF to an active BNG UPF. Downstream traffic that is received for standby sessions is sent over the redundant interface to the active BNG UPF. This requires the configuration of the **multi-chassis-shunt-id** in the service that receives the session traffic.

The **no** form of the command removes the configuration.

Parameters *service-id* — Specifies the name of the VPRN or IES service that contains the redundant interface, up to 64 characters. This can be different from the service where session traffic is terminated.

interface-name — Specifies the redundant interface name, up to 32 characters. It must exist within the configured *service-id*.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.94 redundant-mcast-capacity

redundant-mcast-capacity

Syntax **redundant-mcast-capacity** *primary-percentage* **secondary** *secondary-percentage*
no redundant-mcast-capacity

Context **[Tree]** (config>mcast-mgmt>chassis-level>plane-capacity redundant-mcast-capacity)

Full Context configure mcast-management chassis-level per-mcast-plane-capacity redundant-mcast-capacity

Description This command configures the primary and secondary multicast plane capacities used when the full complement of possible switch fabrics in the system are up. The rates are defined as a percentage of the total multicast plane capacity which is configured using the **total-capacity** command.

The **no** form of this command reverts to the default values.

Default redundant-mcast-capacity 87.50 secondary 87.50

Parameters *primary-percentage* — Specifies the percentage of the total multicast plane capacity to be used for primary multicast planes.

Values 0.01 to 100

secondary-percentage — Specifies the percentage of the total multicast plane capacity to be used for secondary multicast planes.

Values 0.01 to 100

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

22.95 redundant-multicast

redundant-multicast

Syntax [**no**] **redundant-multicast**

Context **[Tree]** (config>router>igmp>if redundant-multicast)

Full Context configure router igmp interface redundant-multicast

Description This command configures the interface as a member of a redundant pair for multicast traffic.

The **no** form of the command removes the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.96 ref-aa-specific-counter

ref-aa-specific-counter

Syntax **ref-aa-specific-counter any**
no ref-aa-specific-counter

Context **[Tree]** (config>log>acct-policy>cr ref-aa-specific-counter)

Full Context configure log accounting-policy custom-record ref-aa-specific-counter

Description This command enables the use of significant-change so only those aa-specific records which have changed in the last accounting interval are written.

The **no** form of this command disables the use of significant-change so all aa-specific records are written whether or not they have changed within the last accounting interval.

Parameters **any** — Indicates that a record is collected as long as any field records activity when non-zero significant-change value is configured.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.97 ref-order

ref-order

Syntax **ref-order** *first second* [*third* [*fourth*][fifth]]]
no ref-order

Context **[Tree]** (config>system>sync-if-timing ref-order)

Full Context configure system sync-if-timing ref-order

Description The synchronous equipment timing subsystem can lock to different timing reference inputs, those specified in the **ref1, ref2, bits, synce**, and **ptp** command configuration. This command organizes the priority order of the timing references.

If a reference source is disabled, then the clock from the next reference source as defined by **ref-order** is used. If all reference sources are disabled, then clocking is derived from a local oscillator.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a **sync-if-timing** reference is linked to a source port that is operationally down, the port is no longer qualified as a valid reference.

For 7450 ESS and 7750 SR systems with two CPM modules, the system distinguishes between the BITS inputs on the active and standby CPMs. The active CPM will use its BITS input port providing that port is qualified. If the local port is not qualified, then the active CPM will use the BITS input port from the standby CPM as the next priority reference. For example, the normal **ref-order** of **bits ref1 ref2** will actually be **bits** (active CPM), followed by **bits** (standby CPM), followed by **ref1**, followed by **ref2**.

For 7950 XRS systems with two CPMs and two CCMs, the system distinguishes between the BITS inputs on the CCMs associated with the active and standby CPMs. The active CPM will use the BITS input port on the associated CCM, provided that the port is qualified. If the local port is not qualified, then the active CPM will use the BITS input port from the CCM associated with the standby CPM as the next priority reference. For example, the normal ref-order of **bits ref1 ref2** will actually be **bits** (active CCM), followed by **bits** (standby CCM), followed by **ref1**, followed by **ref2**.

The **no** form of the command resets the reference order to the default values.

The SyncE/1588 port of the CPM or CCM can be used as a frequency input reference. It shares internal resources with the BITS input ports and so only one can be used at a time. The BITS port shall have priority, if BITS input is enabled, then the SyncE port cannot be enabled.

Similar to the BITS input ports, when the **synce** reference is enabled and in the **ref-order**, the system distinguishes between the **synce** inputs on the active and standby CPM/CCMs. The active CPM/CCM uses its **synce** input port if that port is qualified. If the local port is not qualified, the active CPM uses the synce input port from the standby CPM/CCM as the next priority reference. For example, the **ref-order** of **synce ref1 ref2** will actually be synce (active CPM/CCM), followed by **synce** (standby CPM/CCM), followed by **ref1**, followed by **ref2**.

Default bits synce ref1 ref2 ptp (7750 SR-7/12/12e with CPM-5, 7950 XRS-20/20e, SR-7s/14s, and 7450 ESS-7/12)

bits ref1 ref2 ptp (7750 SR-a4/8, SR-1e/2e/3e, SR-1, SR-1s/2s)

Parameters *first* — Specifies the first timing reference to use in the reference order sequence.

Values bits, synce, ref1, ref2, ptp

second — Specifies the second timing reference to use in the reference order sequence.

Values bits, synce, ref1, ref2, ptp

third — Specifies the third timing reference to use in the reference order sequence.

Values bits, synce, ref1, ref2, ptp

fourth — Specifies the fourth timing reference to use in the reference order sequence.

Values bits, synce, ref1, ref2, ptp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fifth — Specifies the fifth timing reference to use in the reference order sequence.

Values bits, synce, ref1, ref2, ptp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.98 ref-policer

ref-policer

Syntax **ref-policer** *policer-id*
ref-policer all
no ref-policer

Context **[Tree]** (config>log>acct-policy>cr ref-policer)

Full Context configure log accounting-policy custom-record ref-policer

Description This command creates a policer context to configure reference policer counters for significant change only reporting. The custom record is only generated when the change in the sum of all queue and policer reference counters equals or exceeds the configured (non-zero) significant change value.

The **no** form of this command deletes all policer reference counters.

Default no ref-policer

Parameters *policer-id* — Specifies the policer for which reference counters are configured and to which **significant-change** is applied.

Values 1 to 63

all — Applies the **significant-change** to the specified counters for all policers.

Platforms All

22.99 ref-queue

ref-queue

Syntax **ref-queue** *queue-id*
ref-queue all
no ref-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>acct-plcy>cr ref-queue)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record ref-queue

Description This command configures a reference queue.

The **no** form of this command reverts to the default value.

Parameters *queue-id* — Specifies the reference queue ID.

Values 1 to 32

all — Includes all reference queue IDs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ref-queue

Syntax **ref-queue** *queue-id*
ref-queue all
no ref-queue

Context [Tree] (config>log>acct-policy>cr ref-queue)

Full Context configure log accounting-policy custom-record ref-queue

Description This command creates a queue context to configure reference queue counters for significant change only reporting. The custom record is only generated when the change in the sum of all queue and policer reference counters equals or exceeds the configured (non-zero) significant change value.

The **no** form of this command deletes all queue reference counters.

Default no ref-queue

Parameters *queue-id* — Specifies the queue for which reference counters are configured and to which the **significant-change** is applied.

Values 1 to 32

all — Applies the **significant-change** to the specified counters for all queues.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.100 ref1

ref1

Syntax **ref1**

Context **[Tree]** (config>system>sync-if-timing ref1)

Full Context configure system sync-if-timing ref1

Description Commands in this context configure parameters for the first timing reference.

The restrictions on the location for the source port or source bits for **ref1** and **ref2** are listed in Ref1 and Ref2 Timing References.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.101 ref2

ref2

Syntax **ref2**

Context **[Tree]** (config>system>sync-if-timing ref2)

Full Context configure system sync-if-timing ref2

Description Commands in this context configure parameters for the second timing reference. There are restrictions on the source-port and source-bits locations for **ref2** based on the platform. The restrictions on the location for the source-port or source-bits for **ref1** and **ref2** are listed in Revertive, non-Revertive Timing Reference Switching Operation.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.102 reference-bandwidth

reference-bandwidth

Syntax **reference-bandwidth** *bandwidth-in-kbps*
reference-bandwidth [**zbps** *Zetta-bps*] [**ebps** *Exa-bps*] [**pbps** *Peta-bps*] [**tbps** *Tera-bps*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[**gbps** *Giga-bps*] [**mbps** *Mega-bps*] [**kbps** *Kilo-bps*]
no reference-bandwidth

Context **[Tree]** (config>service>vprn>isis reference-bandwidth)

Full Context configure service vprn isis reference-bandwidth

Description This command configures the reference bandwidth that provides the basis of bandwidth relative costing.

In order to calculate the lowest cost to reach a specific destination, each configured level on each interface must have a cost. If the reference bandwidth is defined, then the cost is calculated using the following formula:

cost = reference – bandwidth ÷ bandwidth

If the reference bandwidth is configured as 10 Gigabits (10,000,000,000), a 100 M/bps interface has a default metric of 100. In order for metrics in excess of 63 to be configured, wide metrics must be deployed. (See **wide-metrics-only** in the **config>router>isis** context.)

If the reference bandwidth is not configured, all interfaces have a default metric of 10.

The **no** form of this command reverts to the default value.

Default no reference-bandwidth — No reference bandwidth is defined. All interfaces have a metric of 10.

Parameters *Zetta-bps* — Specifies the reference bandwidth in zettabits per second, expressed as a decimal integer.

Values 1 to 18

Exa-bps — Specifies the reference bandwidth in exabits per second, expressed as a decimal integer.

Values 1 to 999

Peta-bps — Specifies the reference bandwidth in petabits per second, expressed as a decimal integer.

Values 1 to 999

bandwidth-in-kbps — Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 18446744073709551615

Tera-bps — Specifies the reference bandwidth in terabits per second, expressed as a decimal integer.

Values 1 to 999

Giga-bps — Specifies the reference bandwidth in gigabits per second, expressed as a decimal integer.

Values 1 to 999

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Mega-bps — Specifies the reference bandwidth in megabits per second, expressed as a decimal integer.

Values 1 to 999

Kilo-bps — Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 999

Platforms All

reference-bandwidth

Syntax **reference-bandwidth** *bandwidth-inkbps*
reference-bandwidth [**zbps** *Zetta-bps*] [**ebps** *Exa-bps*] [**pbps** *Peta-bps*] [**tbps** *Tera-bps*] [**gbps** *Giga-bps*] [**mbps** *Mega-bps*] [**kbps** *Kilo-bps*]
no reference-bandwidth

Context **[Tree]** (config>service>vprn>ospf reference-bandwidth)
[Tree] (config>service>vprn>ospf3 reference-bandwidth)

Full Context configure service vprn ospf reference-bandwidth
configure service vprn ospf3 reference-bandwidth

Description This command configures the reference bandwidth in kilobits per second (kb/s) that provides the reference for the default costing of interfaces based on their underlying link speed.

The default interface cost is calculated as follows:

cost = reference–bandwidth ÷ bandwidth

The default *reference-bandwidth* is 100,000,000 kb/s or 100 Gb/s, so the default auto-cost metrics for various link speeds are as follows:

- 10 Mb/s link default cost of 10000
- 100 Mb/s link default cost of 1000
- 1 Gb/s link default cost of 100
- 10 Gb/s link default cost of 10
- 40 Gb/s link default cost of 2
- 100 Gb/s link default cost of 1
- 400 Gb/s link default cost of 1

Note: The default **reference-bandwidth** value must be manually configured to a higher value if interface speeds are greater than 100 Gb/s, and metrics based on link speed are used. When the default **reference-bandwidth** value is used, a metric of 1 is set on all interface speeds ≥ 100 Gb/s. For example, 100 GE, 100 GE LAG, 400 GE, and 400 GE LAG interfaces will all have a metric of 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the reference bandwidth is configured as 10 Gb (reference-bandwidth 10000000000), a 100 Mb/s interface has a default metric of 100.

When a very large reference bandwidth value is configured, a metric calculation may result in a value higher than the supported protocol cost value. If this occurs, OSPF automatically reverts to the maximum configurable cost metric.

The reference-bandwidth command assigns a default cost to the interface based on the interface speed. To override this default cost on a particular interface, use the **metric** *metric* command configured in the **config>router>ospf>area>if** *ip-int-name* context.

The **no** form of this command reverts the reference bandwidth to the default value.

Default reference-bandwidth 100000000

Parameters *bandwidth-in-kbps* — Specifies the reference bandwidth in kilobits per second expressed as a decimal integer.

Values 1 to 4000000000

tbps *Tera-bps* — Specifies the reference bandwidth in terabits per second expressed as a decimal integer.

Values 1 to 4

gbps *Giga-bps* — Specifies the reference bandwidth in gigabits per second expressed as a decimal integer.

Values 1 to 999

mbps *Mega-bps* — Specifies the reference bandwidth in megabits per second expressed as a decimal integer.

Values 1 to 999

kbps *Kilo-bps* — Specifies the reference bandwidth in kilobits per second expressed as a decimal integer.

Values 1 to 999

Platforms All

reference-bandwidth

Syntax **reference-bandwidth** *bandwidth-in-kbps*
reference-bandwidth [**zbps** *Zetta-bps*] [**ebps** *Exa-bps*] [**pbps** *Peta-bps*] [**tbps** *Tera-bps*] [**gbps** *Giga-bps*] [**mbps** *Mega-bps*] [**kbps** *Kilo-bps*]
no reference-bandwidth

Context **[Tree]** (config>router>isis reference-bandwidth)

Full Context configure router isis reference-bandwidth

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the reference bandwidth that provides the basis of bandwidth relative costing.

To calculate the lowest cost to reach a specific destination, each configured level on each interface must have a cost. If the reference bandwidth is defined, then the cost is calculated using the following formula:

cost = reference-bandwidth ÷ bandwidth

If the reference bandwidth is configured as 10 Gb (**reference-bandwidth** 10000000000), a 100 Mb/s interface has a default metric of 100. To configure metrics in excess of 63, wide metrics must be deployed (see **wide-metrics-only** in the **config>router>isis** context).

When a large **reference-bandwidth** value is configured, a metric calculation may result in a value higher than the supported protocol cost value. If this occurs, IS-IS automatically reverts to the maximum configurable cost metric.

If the reference bandwidth is not configured, then all interfaces have a default metric of 10.

The **no** form of this command reverts to the default value.

Default no reference-bandwidth

Parameters *bandwidth-in-kbps* — Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 18446744073709551615

Zetta-bps — Specifies the reference bandwidth in zettabits per second, expressed as a decimal integer.

Values 1 to 18

Exa-bps — Specifies the reference bandwidth in exabits per second, expressed as a decimal integer.

Values 1 to 999

Peta-bps — Specifies the reference bandwidth in petabits per second, expressed as a decimal integer.

Values 1 to 999

Tera-bps — Specifies the reference bandwidth in terabits per second, expressed as a decimal integer.

Values 1 to 999

Giga-bps — Specifies the reference bandwidth in gigabits per second, expressed as a decimal integer.

Values 1 to 999

Mega-bps — Specifies the reference bandwidth in megabits per second, expressed as a decimal integer.

Values 1 to 999

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Kilo-bps — Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 999

Platforms All

reference-bandwidth

Syntax **reference-bandwidth** *bandwidth-in-kbps*
reference-bandwidth [**zbps** *Zetta-bps*] [**ebps** *Exa-bps*] [**pbps** *Peta-bps*] [**tbps** *Tera-bps*] [**gbps** *Giga-bps*] [**mbps** *Mega-bps*] [**kbps** *Kilo-bps*]
no reference-bandwidth

Context **[Tree]** (config>router>ospf reference-bandwidth)
[Tree] (config>router>ospf3 reference-bandwidth)

Full Context configure router ospf reference-bandwidth
configure router ospf3 reference-bandwidth

Description This command configures the reference bandwidth in kilobits per second (kb/s) that provides the reference for the default costing of interfaces based on their underlying link speed.

The default interface cost is calculated as follows:

cost = reference-bandwidth ÷ bandwidth

The default *reference-bandwidth* is 100,000,000 kb/s or 100 Gb/s, the default auto-cost metrics for various link speeds are as follows:

- 10 Mb/s link default cost of 10000
- 100 Mb/s link default cost of 1000
- 1 Gb/s link default cost of 100
- 10 Gb/s link default cost of 10
- 100 Gb/s link default cost of 1
- 400 Gb/s link default cost of 1

Note: The default reference-bandwidth must be manually configured to a higher value if interface speeds are greater than 100 Gb/s, and metrics based on link speed are used. When the default reference-bandwidth is used, a metric of 1 is set on all interface speeds ≥ 100 Gb/s. For example, 100 GE, 100 GE LAG, 400 GE, and 400 GE LAG interfaces will all have a metric of 1.

If the reference bandwidth is configured as 10 Gb (reference-bandwidth 10000000000), a 100 Mb/s interface has a default metric of 100.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a very large reference bandwidth value is configured, a metric calculation may result in a value higher than the supported protocol cost value. If this occurs, OSPF automatically reverts to the maximum configurable cost metric.

The **reference-bandwidth** command assigns a default cost to the interface based on the interface speed. To override this default cost on a particular interface, use the **metric** *metric* command configured in the **config>router>ospf>area>interface** *ip-int-name* context.

The **no** form of this command reverts to the default value.

Default reference-bandwidth 100000000

Parameters *bandwidth-in-kbps* — Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 18446744073709551615

Zetta-bps — Specifies the reference bandwidth in zettabits per second, expressed as a decimal integer.

Values 1 to 18

Exa-bps — Specifies the reference bandwidth in exabits per second, expressed as a decimal integer.

Values 1 to 999

Peta-bps — Specifies the reference bandwidth in petabits per second, expressed as a decimal integer.

Values 1 to 999

Tera-bps — Specifies the reference bandwidth in terabits per second, expressed as a decimal integer.

Values 1 to 999

Giga-bps — Specifies the reference bandwidth in gigabits per second, expressed as a decimal integer.

Values 1 to 999

Mega-bps — Specifies the reference bandwidth in megabits per second, expressed as a decimal integer.

Values 1 to 999

Kilo-bps — Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 999

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.103 reflect-pad

reflect-pad

Syntax [**no**] **reflect-pad**

Context **[Tree]** (config>oam-pm>session>mpls>dm reflect-pad)

Full Context configure oam-pm session mpls dm reflect-pad

Description This command enables copying the padding in each MPLS-DM query to the response.

When padding is included in the DM frame the option exists to reflect the padding back in the direction of the source or remove the padding. The removal of the pad-tlv is good practice when using unidirectional tunnels such as RSVP.

This command uses the mandatory TLV type 0, instructing the responder to include the pad TLV from the response. The no form of this command uses the optional TVL type 128, instructing the responder to remove the pad TLV from the response.

The **no** form of this command disables copying the padding in each MPLS-DM query to the response.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.104 reflector

reflector

Syntax **reflector** [**udp-port** *udp-port-number*] [**create**]
no reflector

Context **[Tree]** (config>router>twamp-light reflector)
[Tree] (config>service>vprn>twamp-light reflector)

Full Context configure router twamp-light reflector
configure service vprn twamp-light reflector

Description This command configures a TWAMP Light session reflector parameters and to enable TWAMP Light functionality with the **no shutdow**n command. The **udp-port** keyword and value must be specified with the **create** keyword. An error message is generated if the specific UDP port is unavailable.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *udp-port-number* — Specifies the UDP port number. A strictly enforced restricted range has been introduced. The TWAMP Light session reflector must be brought in line with this new restriction prior upgrading or rebooting from any previous release if there is an active TWAMP Light session reflector configured. Failure to do so prevents an ISSU operation from proceeding and fails to activate any reflector outside of the enforced range.

Note that in the Two-Way Active Measurement Protocol Light (TWAMP Light) section for a complete description. This parameter is required and specifies the destination udp-port that the session reflector uses to listen for TWAMP Light packets. The session controller launching the TWAMP Light packets must be configured with the same destination UDP port as part of the TWAMP Light test. The IES service uses the destination UDP port that is configured under the **router** context. Only one UDP port can be configured per unique context.

Values 862, 64364 to 64373

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

reflector

Syntax [**no**] **reflector** *reflector-name*

Context **[Tree]** (config>bfd>seamless-bfd reflector)

Full Context configure bfd seamless-bfd reflector

Description This command specifies the seamless BFD reflector.

The **no** form of this command removes the context.

Parameters *reflector-name* — Specifies the reflector name, up to 32 characters.

Platforms All

22.105 refresh-reduction

refresh-reduction

Syntax [**no**] **refresh-reduction**

Context **[Tree]** (config>router>rsvp>interface refresh-reduction)

Full Context configure router rsvp interface refresh-reduction

Description This command enables the use of the RSVP overhead refresh reduction capabilities on this RSVP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this option is enabled, a node will enable support for three capabilities. It will accept bundles RSVP messages from its peer over this interface, it will attempt to perform reliable RSVP message delivery to its peer, and will use summary refresh messages to refresh path and resv states. The reliable message delivery must be explicitly enabled by the user after refresh reduction is enabled. The other two capabilities are enabled immediately.

A bundle message is intended to reduce overall message handling load. A bundle message consists of a bundle header followed by one or more bundle sub-messages. A sub-message can be any regular RSVP message except another bundle message. A node will only process received bundled RSVP messages but will not generate them.

When reliable message delivery is supported by both the node and its peer over the RSVP interface, an RSVP message is sent with a message_id object. A message_id object can be added to any RSVP message when sent individually or as a sub-message of a bundled message.

if the sender sets the ack_desired flag in the message_id object, the receiver acknowledges the receipt of the RSVP message by piggy-backing a message_ack object to the next RSVP message it sends to its peer. Alternatively, an ACK message can also be used to send the message_ack object. In both cases, one or many message_ack objects could be included in the same message.

The router supports the sending of separate ACK messages only but is capable of processing received message_ack objects piggy-backed to hop-by-hop RSVP messages, such as path and resv.

The router sets the ack_desired flag only in non-refresh RSVP messages and in refresh messages which contain new state information.

A retransmission mechanism based on an exponential backoff timer is supported in order to handle unacknowledged message_id objects. The RSVP message with the same message_id is retransmitted every 2 * rapid-retransmit-time interval of time. The rapid-retransmit-time is referred to as the rapid retransmission interval as it must be smaller than the regular refresh interval configured in the **config>router>rsvp>refresh-time** context. There is also a maximum number of retransmissions of an unacknowledged RSVP message rapid-retry-limit. The node will stop retransmission of unacknowledged RSVP messages whenever the updated backoff interval exceeds the value of the regular refresh interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first. These two parameters are configurable globally on a system in the **config>router>rsvp** context.

Refresh summary consists of sending a summary refresh message containing a message_id list object. The fields of this object are populated each with the value of the message_identifier field in the message_id object of a previously sent individual path or resv message. The summary refresh message is sent every refresh regular interval as configured by the user using the refresh-time command in the **config>router>rsvp** context. The receiver checks each message_id object against the saved path and resv states. If a match is found, the state is updated as if a regular path or resv refresh message was received from the peer. If a specific message_identifier field does not match, then the node sends a message_id_nack object to the originator of the message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The above capabilities are referred to collectively as “refresh overhead reduction extensions”. When the refresh-reduction is enabled on an RSVP interface, the node indicates this to its peer by setting a “refresh-reduction-capable” bit in the flags field of the common RSVP header. If both peers of an RSVP interface set this bit, all the above three capabilities can be used. Furthermore, the node monitors the settings of this bit in received RSVP messages from the peer on the interface. As soon as this bit is cleared, the router stops sending summary refresh messages. If a peer did not set the “refresh-reduction-capable” bit, a node does not attempt to send summary refresh messages.

However, if the peer did not set the “refresh-reduction-capable” bit, a node, with refresh reduction enabled and reliable message delivery enabled, will still attempt to perform reliable message delivery with this peer. If the peer does not support the message_id object, it returns an error message “unknown object class”. In this case, the node retransmits the RSVP message without the message_id object and reverts to using this method for future messages destined to this peer. The RSVP Overhead Refresh Reduction is supported with both RSVP P2P LSP path and the S2L path of an RSVP P2MP LSP instance over the same RSVP instance.

The **no** form of this command reverts to the default value.

Default no refresh-reduction

Platforms All

22.106 refresh-reduction-over-bypass

refresh-reduction-over-bypass

Syntax **refresh-reduction-over-bypass** [**enable** | **disable**]

Context **[Tree]** (config>router>rsvp refresh-reduction-over-bypass)

Full Context configure router rsvp refresh-reduction-over-bypass

Description This command enables the refresh reduction capabilities over all bypass tunnels originating on this PLR node or terminating on this Merge Point (MP) node.

By default, this is disabled. Since a bypass tunnel may merge with the primary LSP path in a node downstream of the next-hop, there is no direct interface between the PLR and the MP node and it is possible the latter will not accept summary refresh messages received over the bypass.

When disabled, the node as a PLR or MP will not set the “Refresh-Reduction-Capable” bit on RSVP messages pertaining to LSP paths tunneled over the bypass. It will also not send Message-ID in RSVP messages. This effectively disables summary refresh.

Default refresh-reduction-over-bypass disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.107 refresh-time

refresh-time

Syntax **refresh-time** *seconds*
no refresh-time

Context **[Tree]** (config>router>gmpls refresh-time)

Full Context configure router gmpls refresh-time

Description This command configures the interval (in s), between the successive Path and Resv refresh messages. RSVP declares the session down after it misses a consecutive number of refresh messages equal to the configured **keep-multiplier** number.

The **no** form of this command resets the command to the default value.

Default refresh-time 30

Parameters *seconds* — Specifies the interval (in seconds), between successive Path and Resv refresh messages.

Values 1 to 65535

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

refresh-time

Syntax **refresh-time** *seconds*
no refresh-time

Context **[Tree]** (config>router>rsvp refresh-time)

Full Context configure router rsvp refresh-time

Description The **refresh-time** controls the interval (in s), between the successive Path and Resv refresh messages. RSVP declares the session down after it misses **keep-multiplier** *number* consecutive refresh messages.

The **no** form of this command reverts to the default value.

Default refresh-time 30

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — The refresh time in s.

Values 1 to 65535

Platforms All

refresh-time

Syntax **refresh-time** *seconds* **hold-time** *seconds*
no refresh-time

Context **[Tree]** (config>router>origin-validation>rpki-session refresh-time)

Full Context configure router origin-validation rpki-session refresh-time

Description This command is used to configure the **refresh-time** and **hold-time** intervals that are used for liveness detection of the RPKI-Router session. The **refresh-time** defaults to 300 seconds and is reset whenever a Reset Query PDU or Serial Query PDU is sent to the cache server. When the timer expires, a new Serial Query PDU is sent with the last known serial number.

The **hold-time** specifies the length of time in seconds that the session is to be considered UP without any indication that the cache server is alive and reachable. The timer defaults to 600 seconds and must be at least 2x the refresh-time (otherwise the CLI command is not accepted). Reception of any PDU from the cache server resets the hold timer. When the **hold-time** expires, the session is considered to be DOWN and the stale timer is started.

Default no refresh-time

Parameters *seconds* — Specifies a time in seconds.

Values 30 to 32767

seconds — Specifies a time in seconds.

Values 60 to 65535

Platforms All

22.108 refresh-timer

refresh-timer

Syntax **refresh-timer** *value*
no refresh-timer

Context **[Tree]** (config>service>apipe>spoke-sdp>control-channel-status refresh-timer)
[Tree] (config>service>cpipe>spoke-sdp>control-channel-status refresh-timer)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>epipe>spoke-sdp>control-channel-status refresh-timer)
[Tree] (config>service>vpls>spoke-sdp>control-channel-status refresh-timer)

Full Context configure service apipe spoke-sdp control-channel-status refresh-timer
configure service cpipe spoke-sdp control-channel-status refresh-timer
configure service epipe spoke-sdp control-channel-status refresh-timer
configure service vpls spoke-sdp control-channel-status refresh-timer

Description This command configures the refresh timer for control channel status signaling packets. By default, no refresh packets are sent.

Default no refresh-timer

Parameters *value* — Specifies the refresh timer value, in seconds.

Values 10 to 65535

Default 0 (off)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp control-channel-status refresh-timer

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp control-channel-status refresh-timer

All

- configure service epipe spoke-sdp control-channel-status refresh-timer
- configure service vpls spoke-sdp control-channel-status refresh-timer

refresh-timer

Syntax **refresh-timer** *value*
no refresh-timer

Context [Tree] (config>service>ies>if>spoke-sdp>control-channel-status refresh-timer)

Full Context configure service ies interface spoke-sdp control-channel-status refresh-timer

Description This command configures the refresh timer for control channel status signaling packets. By default, no refresh packets are sent.

Default no refresh-timer

Parameters *value* — Specifies the refresh timer value.

Values 10 to 65535 seconds

Default 0 (off)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

refresh-timer

Syntax **refresh-timer** *value*
no refresh-timer

Context **[Tree]** (config>service>vprn>if>spoke-sdp>control-channel-status refresh-timer)
[Tree] (config>service>vprn>red-if>spoke-sdp>control-channel-status refresh-timer)

Full Context configure service vprn interface spoke-sdp control-channel-status refresh-timer
configure service vprn redundant-interface spoke-sdp control-channel-status refresh-timer

Description This command configures the refresh timer for control channel status signaling packets. By default, no refresh packets are sent.

Default no refresh-timer

Parameters *value* — Specifies the refresh timer value.

Values 10 to 65535 seconds

Default 0 (off)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp control-channel-status refresh-timer

All

- configure service vprn interface spoke-sdp control-channel-status refresh-timer

refresh-timer

Syntax **refresh-timer** *seconds*
no refresh-timer

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp>control-channel-status refresh-timer)
[Tree] (config>mirror>mirror-dest>spoke-sdp>control-channel-status refresh-timer)

Full Context configure mirror mirror-dest remote-source spoke-sdp control-channel-status refresh-timer
configure mirror mirror-dest spoke-sdp control-channel-status refresh-timer

Description This command configures the refresh timer for control channel status signaling packets. By default, no refresh packets are sent.

Parameters *seconds* — Specifies the refresh timer value.

Values 10 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.109 register

register

Syntax **register** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no register

Context **[Tree]** (debug>router>pim register)

Full Context debug router pim register

Description This command enables debugging for PIM register mechanism.

The **no** form of this command disables debugging for PIM register mechanism.

Parameters *grp-ip-address* — Debugs information associated with the specified PIM register.

Values multicast group address (ipv4, ipv6)

ip-address — Debugs information associated with the specified PIM register.

Values source address (ipv4, ipv6)

detail — Debugs detailed register information.

Platforms All

22.110 registrant-sm

registrant-sm

Syntax [**no**] **registrant-sm**

Context **[Tree]** (debug>service>id>mrp registrant-sm)

Full Context debug service id mrp registrant-sm

Description This command enables debugging of the registrant state machine.

The **no** form of this command disables debugging of the registrant state machine.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.111 reinit-delay

reinit-delay

Syntax **reinit-delay** *time*
no reinit-delay

Context **[Tree]** (config>system>lldp reinit-delay)

Full Context configure system lldp reinit-delay

Description This command configures the time before re-initializing LLDP on a port.

The **no** form of this command reverts to the default value.

Default no reinit-delay

Parameters *time* — Specifies the time, in seconds, before re-initializing LLDP on a port.

Values 1 to 10

Default 2

Platforms All

22.112 reject-disabled-ncp

reject-disabled-ncp

Syntax [**no**] **reject-disabled-ncp**

Context **[Tree]** (config>router>l2tp>group>ppp reject-disabled-ncp)
[Tree] (config>router>l2tp>group>tunnel>ppp reject-disabled-ncp)
[Tree] (config>service>vprn>l2tp>group>ppp reject-disabled-ncp)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp reject-disabled-ncp)

Full Context configure router l2tp group ppp reject-disabled-ncp
configure router l2tp group tunnel ppp reject-disabled-ncp
configure service vprn l2tp group ppp reject-disabled-ncp
configure service vprn l2tp group tunnel ppp reject-disabled-ncp

Description This command forces an LCP Protocol Reject when receiving an IPv6CP Configure Request message whenIPv6 is not configured.

By default, an IPv6CP Configure Request message is silently ignored when IPv6 is not configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

reject-disabled-ncp

Syntax [**no**] **reject-disabled-ncp**

Context **[Tree]** (config>subscr-mgmt>ppp-policy reject-disabled-ncp)

Full Context configure subscriber-mgmt ppp-policy reject-disabled-ncp

Description This command forces an LCP Protocol Reject when receiving an IPv6CP Configure Request message while IPv6 is not configured or when receiving an IPv4CP Configure Request message and no local IPv4 address is assigned.

By default, an IPv4CP/IPv6CP Configure Request message is silently ignored when IPv4/IPv6 is not configured.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.113 relative

relative

Syntax **relative** *percent*
no relative

Context **[Tree]** (config>test-oam>link-meas>template>sw>thr relative)
[Tree] (config>test-oam>link-meas>template>asw>thr relative)

Full Context configure test-oam link-measurement measurement-template aggregate-sample-window threshold relative
configure test-oam link-measurement measurement-template sample-window threshold relative

Description This command configures the percentage value of change, positive or negative, compared to the previously reported measurement. If this percentage value is reached in either direction, the new value is conveyed to the routing engine for further handling and stored as the delay measurement last reported. If the percentage value is not configured, this threshold is disabled.

The **no** form of this command reverts to the default value.

Default relative 0

Parameters *percent* — Specifies the percentage of change.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A value of 0 (zero) indicates no relative thresholding is performed when considering report to the routing engine.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.114 relay

relay

Syntax [**no**] **relay**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 relay)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 relay)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6 relay)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6 relay)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay
configure service ies subscriber-interface ipv6 dhcp6 relay
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay
configure service vprn subscriber-interface ipv6 dhcp6 relay

Description Commands in this context configure DHCPv6 relay parameters for this interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.115 relay-plain-bootp

relay-plain-bootp

Syntax [**no**] **relay-plain-bootp**

Context **[Tree]** (config>service>ies>if>dhcp relay-plain-bootp)
[Tree] (config>service>vprn>if>dhcp relay-plain-bootp)

Full Context configure service ies interface dhcp relay-plain-bootp
configure service vprn interface dhcp relay-plain-bootp

Description This command enables the relaying of plain BOOTP packets.

The **no** form of this command disables the relaying of plain BOOTP packets.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

relay-plain-bootp

Syntax [**no**] **relay-plain-bootp**

Context **[Tree]** (config>router>if>dhcp relay-plain-bootp)

Full Context configure router interface dhcp relay-plain-bootp

Description This command enables the relaying of plain BOOTP packets.

The **no** form of this command disables the relaying of plain BOOTP packets.

Default no relay-plain-bootp

Platforms All

22.116 relay-proxy

relay-proxy

Syntax **relay-proxy** [**release-update-src-ip**] [**siaddr-override** *ip-address*]
no relay-proxy

Context **[Tree]** (config>service>ies>if>dhcp relay-proxy)
[Tree] (config>service>ies>sub-if>dhcp relay-proxy)
[Tree] (config>service>ies>sub-if>grp-if>dhcp relay-proxy)
[Tree] (config>service>vprn>if>dhcp relay-proxy)
[Tree] (config>service>vprn>sub-if>dhcp relay-proxy)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp relay-proxy)

Full Context configure service ies interface dhcp relay-proxy
configure service ies subscriber-interface dhcp relay-proxy
configure service ies subscriber-interface group-interface dhcp relay-proxy
configure service vprn interface dhcp relay-proxy
configure service vprn subscriber-interface dhcp relay-proxy
configure service vprn subscriber-interface group-interface dhcp relay-proxy

Description This command enables the DHCPv4 relay proxy function on the interface. The command has no effect when no dhcp servers are configured (DHCPv4 relay not configured). By default, unicast DHCPv4 release messages are forwarded transparently.

A relay proxy enhances the relay such that it also relays unicast client DHCPv4 REQUEST messages (lease renewals).

- In the upstream direction, update the source IP address and add the gateway IP address (gi-address) field before sending the message to the intended DHCP server (the message is not broadcasted to all configured DHCP servers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- In the downstream direction, remove the gi-address and update the destination IP address to the address of the `yiaddr` (your IP address) field.

The optional **release-update-src-ip** parameter updates the source IP address of a DHCP RELEASE message with the address used for relayed DHCPv4 messages.

The optional **siaddr-override** *ip-address* parameter enables DHCP server IP address hiding towards the client. This parameter requires that **lease-populate** is enabled on the interface. The DHCP server ip address is required for the address hiding function and is stored in the lease state record. The client interacts with the relay proxy as if it is the DHCP server. In all DHCP messages to the client, the value of following header fields and DHCP options containing the DHCP server IP address is replaced with the configured <*ip-address*>:

- the “source IP address” field in the IP DHCPv4 packet header
- the “siaddr” field in the DHCPv4 header if not equal to zero in the message received from the server
- the Server Identification option (DHCPv4 option 54) if present in the original server message
- the source IP address field in the IP packet header

DHCP OFFER selection during initial binding is done in the relay-proxy. Only the first DHCP OFFER message is forwarded to the client. Subsequent DHCP OFFER messages from different servers are silently dropped.

Parameters **release-update-src-ip** — Updates the source IP address of a DHCP RELEASE message with the address used for relayed DHCPv4 messages.

ip-address — Enables DHCPv4 server address hiding towards the DHCPv4 client and activates DHCPv4 OFFER selection in case multiple DHCP servers are configured. The *ip-address* can be any local address in the same routing instance. If DHCP relay lease-split is enabled, **siaddr-override** *ip-address* has priority over the **emulated-server** *ip-address* configured in the proxy-server and is used as the source IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp relay-proxy
- configure service ies subscriber-interface dhcp relay-proxy
- configure service vprn subscriber-interface dhcp relay-proxy
- configure service ies subscriber-interface group-interface dhcp relay-proxy

All

- configure service ies interface dhcp relay-proxy
- configure service vprn interface dhcp relay-proxy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.117 relay-unsolicited-cfg-attribute

relay-unsolicited-cfg-attribute

Syntax **relay-unsolicited-cfg-attribute**

Context **[Tree]** (config>ipsec>ike-policy relay-unsolicited-cfg-attribute)

Full Context configure ipsec ike-policy relay-unsolicited-cfg-attribute

Description This command enters relay unsolicited configuration attributes context. With this configuration, the configured attributes returned from source (such as a RADIUS server) will be returned to IKEv2 remote-access tunnel client regardless if the client has requested it in the CFG_REQUEST payload.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.118 release-reason

release-reason

Syntax [**no**] **release-reason**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes release-reason)

Full Context configure aaa isa-radius-policy acct-include-attributes release-reason

Description This command enables the inclusion of the release reason attributes.

The **no** form of the command excludes release reason attributes.

Default no release-reason

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.119 release-timeout

release-timeout

Syntax **release-timeout** *seconds*
no release-timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>pfcp-association release-timeout)

Full Context configure subscriber-mgmt pfcp-association release-timeout

Description This command configures the time to wait to clean up the PFCP association after administratively disabling it and requesting a shutdown to the BNG CPF. If the BNG CPF does not gracefully remove the PFCP association before the timer expires, the full association and all related sessions are forcefully removed.

The **no** form of this command reverts to the default.

Default release-timeout 3600

Parameters *seconds* — Specifies the wait time, in seconds, for cleanup of the PFCP association.

Values 30 to 3600

Note: The PFCP protocol encoding does not allow the full range of configured values. The system automatically rounds up the configured value to the nearest value allowed by the protocol. For more information about the protocol encoding, see 3GPP TS 29.244 8.2.78.1.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.120 reliable-delivery

reliable-delivery

Syntax [**no**] **reliable-delivery**

Context [Tree] (config>router>rsvp>if>refresh-reduction reliable-delivery)

Full Context configure router rsvp interface refresh-reduction reliable-delivery

Description This command enables reliable delivery of RSVP messages over the RSVP interface. When refresh-reduction is enabled on an interface and reliable-delivery is disabled, the router will send a message_id and not set ACK desired in the RSVP messages over the interface. The router does not expect an ACK and but will accept it if received. The node will also accept message ID and reply with an ACK when requested. In this case, if the neighbor set the “refresh-reduction-capable” bit in the flags field of the common RSVP header, the node will enter summary refresh for a specific message_id it sent regardless if it received an ACK or not to this message from the neighbor.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Finally, when 'reliable-delivery' option is enabled on any interface, RSVP message pacing is disabled on all RSVP interfaces of the system, for example, the user cannot enable the **msg-pacing** option in the **config>router>rsvp** context, and error message is returned in CLI. Conversely, when the **msg-pacing** option is enabled, the user cannot enable the reliable delivery option on any interface on this system. An error message is also generated in CLI after such an attempt.

The **no** form of this command reverts to the default value.

Default no reliable-delivery

Platforms All

22.121 reload

reload

Syntax **reload type** {**cert** | **key** | **cert-key-pair**} *filename* **protocol** *protocol* [**key-file** *filename*]

Context **[Tree]** (admin>certificate reload)

Full Context admin certificate reload

Description This command reloads imported certificate or key file or both at the same time. This command is typically used to update certificate or key file without shutting down **ipsec-tunnel/ipsec-gw/cert-profile/ca-profile**. Note that **type cert** and **type key** is deprecated in a future release. Use **type cert-key-pair** instead. Instead of **type cert** use **type key** instead.

- If the new file exists and valid, then for each tunnel using it:
  - If the key matches the certificate, then the new file is downloaded to the MS-ISA to be used the next time. Tunnels currently up are not affected.
  - If the key does not match the certificate:
    - If **cert** and **key** configuration is used instead of **cert-profile** then the tunnel is brought down.
    - If **cert-profile** is used, then **cert-profile** is brought down. The next authentication fails while the established tunnels are not affected.

If the new file does not exists or somehow invalid (bad format, does not contain right extension, and so on), then this command will abort.

In the case of **type cert-key-pair**, if the new file does not exist or is invalid or **cert** and **key** do not match, then this command aborts with an error message.

Parameters **type** — Specifies what item will be reloaded.

cert — Specifies that a certificate cache will be reloaded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

key — Specifies that a key cache will be reloaded.

cert-key-pair — Specifies that a paired certificate and key cache will be reloaded.

filename — Up to 95 characters.

protocol — Specifies which protocol the certificate will be reloaded for.

Values ipsec, tls

Platforms All

22.122 rem-router-id

rem-router-id

Syntax **rem-router-id** *ip-addr*
no rem-router-id

Context **[Tree]** (config>service>vprn>l2tp>group>l2tpv3 rem-router-id)

Full Context configure service vprn l2tp group l2tpv3 rem-router-id

Description This command configures the IP address that should be used within the Remote Router-ID AVP.

The **no** form of this command removes the configured IP address.

Default no rem-router-id

Parameters *ip-addr* — Specifies an IP address to be used within the Remote Router-ID AVP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.123 remark

remark

Syntax **remark**

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action remark)

Full Context configure application-assurance group policy app-qos-policy entry action remark

Description This command configures remark action on flows matching this AQP entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

remark

Syntax **remark dscp** *dscp-name*

Context **[Tree]** (config>filter>ip-filter>entry>action remark)
[Tree] (config>filter>ipv6-filter>entry>action remark)
[Tree] (config>filter>ip-filter>entry>action>extended-action remark)
[Tree] (config>filter>ipv6-filter>entry>action>extended-action remark)

Full Context configure filter ip-filter entry action extended-action remark
configure filter ip-filter entry action remark
configure filter ipv6-filter entry action extended-action remark
configure filter ipv6-filter entry action remark

Description This command enables and configures the remarking of the DiffServ Code Points of packets matching the criteria of the IPv4/IPv6 filter policy entry, in conjunction with a PBR action. Packets are remarked regardless of QoS-based in-profile or out-of-profile classification. QoS-based DSCP remarking is overridden. If the status of the PBR target is tracked and it is down, the extended action will not be executed; otherwise, the extended action will be performed.

Parameters *dscp-name* — Specifies the DSCP value to write.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

Platforms All

22.124 remarking

remarking

Syntax **remarking** [**force**]
no remarking

Context **[Tree]** (config>qos>network>egress remarking)

Full Context configure qos network egress remarking

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command remarks both customer traffic and egress network IP interface traffic; VPRN customer traffic is not remarked. The remarking is based on the forwarding class to DSCP and LSP EXP bit mapping defined under the egress node of the network QoS policy.

Normally, packets that ingress on network ports have either the DSCP or, for MPLS packets, LSP EXP bit set by an upstream router. The packets are placed in the appropriate forwarding class based on the DSCP-to-forwarding class mapping or the LSP EXP-to-forwarding class mapping. The DSCP or LSP EXP bits of such packets are not altered as the packets egress this router, unless **remarking** is enabled.

Remarking can be required if this router is connected to a different DiffServ domain where the DSCP-to-forwarding class mapping is different.

Normally, no remarking is necessary when all router devices are in the same DiffServ domain.

The network QoS policy supports an egress flag that forces remarking of packets that were received on trusted IES and network IP interfaces. This provides the capability of remarking without regard to the ingress state of the IP interface on which a packet was received. The effect of the egress network remark trusted state on each type of ingress IP interface and trust state is listed in Table 118.

The remark trusted state has no effect on packets received on an ingress VPRN IP interface.

Table 118 **Ingress IP Interface Type and Trust State Effect on Egress Network Remarking**

Ingress IP Interface Type and Trust State	Egress Network IP Interface Trust Remark Disabled (Default)	Egress Network IP Interface Trust Remark Enabled
IES Non-Trusted (Default)	Egress Remarked	Egress Remarked
IES Trusted	Egress Not Remarked	Egress Remarked
VPRN Non-Trusted	Egress Remarked	Egress Remarked
VPRN Trusted (Default)	Egress Not Remarked	Egress Not Remarked
Network Non-Trusted	Egress Remarked	Egress Remarked
Network Trusted (Default)	Egress Not Remarked	Egress Remarked

The **no** form of this command resets the configuration to the default behavior.

Default no remarking — Remarking disabled in the Network QoS policy.

Parameters **force** — Specifies that all IP routed traffic egressing the associated network interface will have its EXP, DSCP, P-bit, and DE bit setting remarked as defined in the associated QoS policy. Only bit fields configured in the QoS policy will be remarked; all others will be left untouched or set based on the default if the fields were not present at ingress.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.125 remote

remote

Syntax **remote**

Context **[Tree]** (config>ipsec>ts-list remote)

Full Context configure ipsec ts-list remote

Description Commands in this context configure remote TS-list parameters. The TS-list is the traffic selector of the local system, such as TSi, when the system acts as an IKEv2 responder.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.126 remote-address

remote-address

Syntax **remote-address** *ip-address*
no remote-address

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query remote-address)

Full Context configure subscriber-mgmt wlan-gw tunnel-query remote-address

Description This command enables matching only on the tunnel that uses the specified source IP address.

The **no** form of this command disables matching on a tunnel's source IP address.

Default no remote-address

Parameters *ip-address* — Specifies the IPv4 or IPv6 remote address.

Values	
ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

d: [0 to 255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.127 remote-age

remote-age

Syntax **remote-age** *aging-timer*
no remote-age [*aging-timer*]

Context **[Tree]** (config>service>vpls remote-age)
[Tree] (config>service>template>vpls-template remote-age)

Full Context configure service template vpls-template remote-age
configure service vpls remote-age

Description This command specifies the aging time for remotely learned MAC addresses in the forwarding database (FDB) for the Virtual Private LAN Service (VPLS) instance.

In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the FDB. The **remote-age** timer specifies the aging time for remote learned MAC addresses. To reduce the amount of signaling required between switches configure this timer larger than the **local-age** timer.

The **no** form of this command returns the remote aging timer to the default value.

Default remote-age 900

Parameters *seconds* — Specifies the aging time for remote MACs expressed in seconds

Values 60 to 86400

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.128 remote-attachment-circuit

remote-attachment-circuit

Syntax **remote-attachment-circuit** *ac-name* [**endpoint** *endpoint-name*] [**create**]
no remote-attachment-circuit *ac-name*

Context **[Tree]** (config>service>epipe>bgp-evpn remote-attachment-circuit)

Full Context configure service epipe bgp-evpn remote-attachment-circuit

Description This command configures the remote attachment circuit.

The **no** form of this command disables the context.

Default no remote-attachment-circuit

Parameters *ac-name* — Specifies the name of the remote attachment circuit, up to 32 characters.

endpoint-name — Specifies the name of the endpoint, up to 32 characters.

create — Keyword used to create the remote AC.

Platforms All

22.129 remote-ecid

remote-ecid

Syntax **remote-ecid** *emulated circuit identifier*
no remote-ecid

Context **[Tree]** (config>service>epipe>sap>cem remote-ecid)

Full Context configure service epipe sap cem remote-ecid

Description This command defines the Emulated Circuit Identifiers (ECID) to be used for the remote (destination) end of the circuit emulation service.

Parameters *emulated circuit identifier* — Specifies the value to be used as the remote (destination) ECID for the circuit emulation service. Upon CES packet reception, the ECID in the packet will be compared to the configured local-ecid value. These must match for the packet payload to be used for the TDM circuit. The remote-ecid value is inserted into the MEF-8 CES packet to be transmitted.

Values 0 to 1048575

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

22.130 remote-gateway-address

remote-gateway-address

Syntax **remote-gateway-address** [*ip-address* | *ipv6-address*]
no remote-gateway-address

Context **[Tree]** (config>router>if>ipsec>ipsec-tunnel remote-gateway-address)

Full Context configure router interface ipsec ipsec-tunnel remote-gateway-address

Description This command configures the remote IPsec tunnel endpoint address.

Parameters *ip-address* — Specifies a remote unicast IPv4 address, up to 64 characters.

ipv6-address — Specifies a remote unicast global unicast IPv6 address, up to 64 characters.

Platforms VSR

22.131 remote-id

remote-id

Syntax **remote-id hex** *hex-string*
remote-id string *ascii-string*
no remote-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident remote-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-ident remote-id)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification remote-id
configure subscriber-mgmt local-user-db ppp host host-identification remote-id

Description This command specifies the remote ID to match for a host lookup. When the LUDB is accessed using a DHCPv4 server, the SAP-ID is matched against DHCP option 82.

Note: This command is used only when **remote-id** is configured as one of the **match-list** parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the remote ID from the configuration.

Parameters *hex-string* — Specifies the hexadecimal format for the remote ID.

Values 0x0 to 0xFFFFFFFF (maximum 254 hex nibbles)

ascii-string — Specifies the string format for the remote ID, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

remote-id

Syntax **remote-id mac**
remote-id string *ASCII string*
no remote-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>ali remote-id)

Full Context configure subscriber-mgmt local-user-db ppp host access-loop-information remote-id

Description This command specifies a remote-id for PPPoE hosts. A remote-id received in PPPoE tags has precedence over the LUDB specified remote ID.

The **no** form of this command reverts to the default.

Parameters **mac** — Specifies MAC address of the PPPoE session as the remote ID.

ASCII string — Specifies the circuit ID as a string, up to 63 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

remote-id

Syntax **remote-id**
remote-id mac
remote-id string [*string*]
no remote-id

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6>option remote-id)
[Tree] (config>service>vprn>if>ipv6>dhcp6>option remote-id)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>option remote-id)

Full Context configure service ies interface ipv6 dhcp6-relay option remote-id
configure service vprn interface ipv6 dhcp6-relay option remote-id
configure service vprn subscriber-interface group-interface ipv6 dhcp6 option remote-id

Description This command enables the sending of remote ID option in the DHCPv6 relay packet.

The client DHCP Unique Identifier (DUID) is used as the remote ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the sending of remote ID option in the DHCPv6 relay packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface ipv6 dhcp6 option remote-id

All

- configure service vprn interface ipv6 dhcp6-relay option remote-id
- configure service ies interface ipv6 dhcp6-relay option remote-id

remote-id

Syntax **remote-id**
remote-id hex [*hex-string*]
remote-id {**mac** | **string** *string*}
no remote-id

Context **[Tree]** (config>service>ies>if>dhcp>option remote-id)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option remote-id)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option remote-id)
[Tree] (config>service>vpls>sap>dhcp>option remote-id)
[Tree] (config>service>vprn>if>dhcp>option remote-id)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option remote-id)

Full Context configure service ies interface dhcp option remote-id
configure service ies subscriber-interface group-interface dhcp option remote-id
configure service vpls sap dhcp option remote-id
configure service vprn interface dhcp option remote-id
configure service vprn subscriber-interface group-interface dhcp option remote-id
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option remote-id

Description This command specifies what information goes into the remote-id sub-option in the DHCP relay packet.

If disabled, the **remote-id** sub-option of the DHCP packet is left empty. When the command is configured without any parameters, it equals to the remote-id mac option.

The **no** form of this command reverts to the default.

Parameters *string* — Specifies the remote-id, up to 32 characters.

hex-string — Specifies the hex value of this option.

Values 0x0 to 0xFFFFFFFF...(up to 64 hex nibbles)

mac — Specifies that the MAC address of the remote end is encoded in the sub-option.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies subscriber-interface group-interface dhcp option remote-id
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option remote-id
- configure service vprn subscriber-interface group-interface dhcp option remote-id

All

- configure service ies interface dhcp option remote-id
- configure service vprn interface dhcp option remote-id
- configure service vpls sap dhcp option remote-id

remote-id

Syntax [**no**] **remote-id**

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute remote-id)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute remote-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute remote-id
configure subscriber-mgmt authentication-policy include-radius-attribute remote-id

Description This command enables the generation of the Broad Band Forum Agent-Remote-Id VSA in RADIUS request messages.

The **no** form of this command disables the generation of the Broad Band Forum Agent-Remote-Id VSA.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

remote-id

Syntax [**no**] **remote-id**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp remote-id)

Full Context configure subscriber-mgmt diameter-application-policy nasreq include-avp remote-id

Description This command enables the generation of the Broad Band Forum Agent-Remote-Id Vendor Specific AVP in Diameter NASREQ AAR messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-id

Syntax [**no**] **remote-id** *remote-id*

Context **[Tree]** (debug>service>id>ppp remote-id)

Full Context debug service id ppp remote-id

Description This command enable PPP debug for the specified remote-id.

Multiple remote-id filters can be specified in the same debug command.

Parameters *remote-id* — Specifies the remote-id in PADI.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

remote-id

Syntax **remote-id** *remote-id*
no remote-id

Context **[Tree]** (config>router>lmp>te-link>data-bearer remote-id)

Full Context configure router lmp te-link data-bearer remote-id

Description This command configures the identifier assigned to the data-bearer at the LMP peer node. For a GMPLS UNI, this is the UNI-N node.

Default no remote-id

Parameters *remote-id* — Specifies the ID of the data-bearer at the LMP peer node.

Values 1 to 4294967295

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

remote-id

Syntax **remote-id** *id*
no remote-id

Context **[Tree]** (config>router>lmp>te-link remote-id)

Full Context configure router lmp te-link remote-id

Description This command configures the identifier assigned to the TE Link at the LMP peer node. For a GMPLS UNI, this is the UNI-N node.

Default no remote-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *id* — Specifies the identifier for the LMP peer node TE Link.

Values 1 to 4294967295

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

remote-id

Syntax [**no**] **remote-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes remote-id)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes remote-id)

Full Context configure aaa isa-radius-policy acct-include-attributes remote-id
configure aaa isa-radius-policy auth-include-attributes remote-id

Description This command enables the sending of remote ID option. The client DHCP Unique Identifier (DUID) is used as the remote ID.

The **no** form of the command disables the sending of remote ID option relay packet.

Default no remote-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

remote-id

Syntax **remote-id** [{**mac** | **string** *string*}]
no remote-id

Context **[Tree]** (config>router>if>dhcp>option remote-id)

Full Context configure router interface dhcp option remote-id

Description When enabled, the router sends the MAC address of the remote end (typically the DHCP client) in the **remote-id** suboption of the DHCP packet. This command identifies the host at the other end of the circuit. If disabled, the **remote-id** suboption of the DHCP packet will be left empty.

The **no** form of this command returns the system to the default.

Default no remote-id

Parameters **mac** — This keyword specifies the MAC address of the remote end is encoded in the suboption.

string — Specifies the remote ID.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.132 remote-ip

remote-ip

Syntax **remote-ip** *ip-address*
no remote-ip

Context **[Tree]** (config>service>ies>if>sap>ip-tunnel remote-ip)

Full Context configure service ies interface sap ip-tunnel remote-ip

Description This command configures the primary destination IPv4 or IPv6 address to use for an IP tunnel. This configuration applies to the outer IP header of the encapsulated packets. The **source** address, **remote-ip** address and **backup-remote-ip** address of a tunnel must all belong to the same address family (IPv4 or IPv6). When the remote-ip address contains an IPv6 address it must be a global unicast address.

Default no remote-ip

Parameters *ip-address* — An IPv4 address or an IPv6 address.

Platforms All

remote-ip

Syntax **remote-ip** *ip-address*
no remote-ip

Context **[Tree]** (config>service>vprn>if>sap>ip-tunnel remote-ip)

Full Context configure service vprn interface sap ip-tunnel remote-ip

Description This command sets the primary destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

The **no** form of this command deletes the destination address from the GRE tunnel configuration.

Parameters *ip-address* — Specifies the destination IPv4 address of the GRE tunnel.

Values 1.0.0.0 to 223.255.255.255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-ip

Syntax **remote-ip** {*ip-prefix/prefix-length* | *ip-prefix netmask* | **any**}

Context **[Tree]** (config>router>ipsec>sec-plcy>entry remote-ip)
[Tree] (config>service>vprn>ipsec>sec-plcy>entry remote-ip)

Full Context configure router ipsec security-policy entry remote-ip
configure service vprn ipsec security-policy entry remote-ip

Description This command configures the remote (from the tunnel) IP prefix/mask for the policy parameter entry.

Only one entry is necessary to describe a potential flow. The **local-ip** and **remote-ip** commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

Parameters *ip-prefix* — Specifies the destination address of the aggregate route in dotted decimal notation.

Values a.b.c.d (host bits must be 0)
prefix-length 1 to 32

netmask — Specifies the subnet mask in dotted decimal notation.

any — keyword to specify that it can be any address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec security-policy entry remote-ip

VSR

- configure router ipsec security-policy entry remote-ip

remote-ip

Syntax **remote-ip** *ip-address*
no remote-ip

Context **[Tree]** (config>router>if>ip-tunnel remote-ip)

Full Context configure router interface ip-tunnel remote-ip

Description This command configures the far-end IP address for an IP/GRE tunnel used by a **control-channel** loopback interface. The address refers to the “to” address of the outer IP header in the encapsulation.

Default no remote-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies an IPv4 address.

Values a.b.c.d

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.133 remote-ip-address

remote-ip-address

Syntax **remote-ip-address** *ip-address*
no remote-ip-address

Context **[Tree]** (config>lag>bfd>family remote-ip-address)

Full Context configure lag bfd family remote-ip-address

Description This command specifies the IPv4 or IPv6 address of the BFD destination.

The **no** form of this command removes this address from the configuration.

Default no remote-ip-address

Parameters *ip-address* — Specifies the IP address.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x:-[0 to FFFF]H
	d: [0 to 255]D

Platforms All

22.134 remote-ip-range-start

remote-ip-range-start

Syntax **remote-ip-range-start** *ip-address*
no remote-ip-range-start

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy remote-ip-range-start)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure isa nat-group inter-chassis-redundancy remote-ip-range-start

Description This command configures the first IPv4 address that is assigned to a first member ISA on the remote node. The remaining member ISAs on the remote node are assigned the consecutive IP addresses starting from the first IP address. These IP addresses are used to communicate between the ISAs on redundant nodes for the purpose of flow synchronization. Traffic from the first local IP address (member ISA), is sent to the first IP address from the remote IP range.

The **no** form of this command removes the ip-address from the configuration.

Default no remote-ip-range-start

Parameters *ip-address* — Specifies the first IPv4 address, in the a.b.c.d format, from the range assigned to the first member ISA on the remote node.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.135 remote-lfa

remote-lfa

Syntax **remote-lfa** [**max-pq-cost** *value*]
no remote-lfa

Context **[Tree]** (config>router>isis>loopfree-alternates remote-lfa)

Full Context configure router isis loopfree-alternates remote-lfa

Description This command enables the use of the Remote LFA algorithm in the LFA SPF calculation for this ISIS instance.

The **no** form of this command disables the use of the Remote LFA algorithm in the LFA SPF calculation for this ISIS instance.

Default no remote-lfa

Parameters *value* — Specifies the integer used to limit the search of candidate P and Q nodes in the remote LFA by setting the maximum IGP cost from the router performing the remote LFA calculation to the candidate P or Q node.

Values 0 to 4294967295

Default 4261412864

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-lfa

Syntax **remote-lfa** [**max-pq-cost** *value*]
no remote-lfa

Context **[Tree]** (config>router>ospf>loopfree-alternates remote-lfa)
[Tree] (config>router>ospf3>loopfree-alternates remote-lfa)

Full Context configure router ospf loopfree-alternates remote-lfa
configure router ospf3 loopfree-alternates remote-lfa

Description This command enables the use of the Remote LFA algorithm in the LFA SPF calculation in this OSPF or OSPF3 instance.

The **no** form of this command disables the use of the Remote LFA algorithm in the LFA SPF calculation in this OSPF or OSPF3 instance.

Default no remote-lfa

Parameters **max-pq-cost** *value* — Specifies the integer used to limit the search of candidate P and Q nodes in the remote LFA by setting the maximum IGP cost from the router performing the remote LFA calculation to the candidate P or Q node.

Values 0 to 4294967295

Default 4261412864

Platforms All

22.136 remote-loop-respond

remote-loop-respond

Syntax [**no**] **remote-loop-respond**

Context **[Tree]** (config>port>tdm>ds1 remote-loop-respond)

Full Context configure port tdm ds1 remote-loop-respond

Description When enabled, the channel responds to requests for remote loopbacks.

Default no remote-loop-respond — The port will not respond.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.137 remote-mac

remote-mac

Syntax **remote-mac** *ieee-address*
no remote-mac

Context **[Tree]** (config>service>epipe>sap>cem remote-mac)

Full Context configure service epipe sap cem remote-mac

Description This command defines the destination IEEE MAC address to be used to reach the remote end of the circuit emulation service.

Default remote-mac 00:00:00:00:00:00

Parameters *ieee-address* — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

22.138 remote-management

remote-management

Syntax **remote-management**

Context **[Tree]** (config>system>management-interface remote-management)

Full Context configure system management-interface remote-management

Description Commands in this context configure remote management features.

Platforms All

remote-management

Syntax **remote-management**
no remote-management
remote-management manager [*manager-name*]
no remote-management manager [*manager-name*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>system>management-interface remote-management)

Full Context debug system management-interface remote-management

Description This command configures the management interface to debug the **remote-management** managers.

The **no** form of this command removes the configuration.

Parameters **manager** *manager-name* — Specifies the name of the manager, up to 64 characters. If the parameter is not specified, all configured managers are debugged.

Platforms All

22.139 remote-max-checkpoints

remote-max-checkpoints

Syntax **remote-max-checkpoints** [*number-of-files*]
no remote-max-checkpoints

Context [Tree] (config>system>rollback remote-max-checkpoints)

Full Context configure system rollback remote-max-checkpoints

Description This command configures the maximum number of rollback checkpoint files when the rollback-location is remote (for example, ftp).

Default no remote-max-checkpoints

Parameters *number of files* — Specifies the maximum rollback files saved at a remote location.

Values 1 to 200

Platforms All

22.140 remote-mepid

remote-mepid

Syntax **remote-mepid** *mep-id* **remote-mac** {*unicast-da* | **default**}
no remote-mepid *mep-id*

Context [Tree] (config>eth-cfm>domain>assoc remote-mepid)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure eth-cfm domain association remote-mepid

Description This command configures the remote MEP ID. Optionally, the operator may configure a unicast MAC address associated with the remote MEP. This unicast value replaces the default Layer 2 class 1 multicast address that is typically associated with ETH-CC packets.

Note: This command is not supported with sub second CCM intervals. The *unicast-da* parameter may only be configured when a single remote MEP exists in the association.

The **no** form of this command removes the peer information.

Parameters *mep-id* — Specifies the peer MEP ID.

Values 1 to 8191

unicast-da — Specifies the unicast MAC destination address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx or default

default — Removes the remote MAC unicast address and reverts back to class 1 multicast address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

remote-mepid

Syntax **remote-mepid** *mep-id*
no remote-mepid

Context **[Tree]** (config>oam-pm>session>ethernet remote-mepid)

Full Context configure oam-pm session ethernet remote-mepid

Description This command specifies the remote MEP ID as an alternative to the static **dest-mac** *ieee-address*. When the **remote-mepid** option is configured as an alternative to the **dest-mac**, the domain and association information of the **source mep** within the session is used to check for a locally-stored unicast MAC address for the peer. The local MEP must be administratively enabled. Peer MEP MAC addresses are learned and maintained by the ETH-CC protocol.

The **no** form of this command removes this session parameter.

Parameters *mep-id* — Specifies the remote MEP ID of the peer within the association.

Values 1 to 8191

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.141 remote-name

remote-name

Syntax **remote-name** *host-name*
no remote-name

Context **[Tree]** (config>router>l2tp>group>tunnel remote-name)
[Tree] (config>service>vprn>l2tp>group>tunnel remote-name)

Full Context configure router l2tp group tunnel remote-name
configure service vprn l2tp group tunnel remote-name

Description This command configures a string to be compared to the host name used by the tunnel peer during the authentication phase of tunnel establishment.

Default no remote-name

Parameters *host-name* — Specifies a remote host name for the tunnel, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.142 remote-proxy-arp

remote-proxy-arp

Syntax [**no**] **remote-proxy-arp**

Context **[Tree]** (config>service>ies>if remote-proxy-arp)
[Tree] (config>service>ies>sub-if>grp-if remote-proxy-arp)
[Tree] (config>service>vprn>if remote-proxy-arp)
[Tree] (config>service>vprn>nw-if remote-proxy-arp)
[Tree] (config>service>vprn>sub-if>grp-if remote-proxy-arp)

Full Context configure service ies interface remote-proxy-arp
configure service ies subscriber-interface group-interface remote-proxy-arp
configure service vprn interface remote-proxy-arp
configure service vprn nw-if remote-proxy-arp
configure service vprn subscriber-interface group-interface remote-proxy-arp

Description This command enables remote proxy ARP on the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Remote proxy ARP is similar to proxy ARP. It allows the router to answer an ARP request on an interface for a subnet that is not provisioned on that interface. This allows the router to forward to the other subnet on behalf of the requester. To distinguish remote proxy ARP from local proxy ARP, local proxy ARP performs a similar function but only when the requested IP is on the receiving interface.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface remote-proxy-arp
- configure service ies subscriber-interface group-interface remote-proxy-arp

All

- configure service vprn interface remote-proxy-arp
- configure service ies interface remote-proxy-arp

remote-proxy-arp

Syntax [**no**] **remote-proxy-arp**

Context **[Tree]** (config>subscr-mgmt>git>ipv4 remote-proxy-arp)

Full Context configure subscriber-mgmt group-interface-template ipv4 remote-proxy-arp

Description This command enables remote proxy ARP on the interface.

Remote proxy ARP is similar to proxy ARP. It allows the router to answer an ARP request on an interface for a subnet that is not provisioned on that interface. This allows the router to forward to the other subnet on behalf of the requester. To distinguish remote proxy ARP from local proxy ARP, local proxy ARP performs a similar function but only when the requested IP address is on the receiving interface.

The **no** form of this command disables remote proxy ARP on the interface.

Default no remote-proxy-arp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

remote-proxy-arp

Syntax [**no**] **remote-proxy-arp**

Context **[Tree]** (config>router>if remote-proxy-arp)

Full Context configure router interface remote-proxy-arp

Description This command enables remote proxy ARP on the interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no remote-proxy-arp

Platforms All

22.143 remote-servers

remote-servers

Syntax **remote-servers**

Context **[Tree]** (config>service>vprn>aaa remote-servers)

Full Context configure service vprn aaa remote-servers

Description Commands in this context configure AAA remote servers on the VPRN.

Platforms All

22.144 remote-source

remote-source

Syntax [**no**] **remote-source**

Context **[Tree]** (config>mirror>mirror-dest remote-source)

Full Context configure mirror mirror-dest remote-source

Description This command is used on a destination router in a remote mirroring solution. The mirroring (packet copy) is performed on the source router and sent via an SDP to the destination router. Remote mirroring requires remote source configuration on the destination router.

Remote mirroring allows a destination router to terminate SDPs from multiple remote source routers. This allows consolidation of packet sniffers or analyzers at a single or small set of points in a network (for example, a sniffer or analyze farm, or lawful interception gateway).

A **remote-source** entry must be configured on the destination router for each source router from which mirrored traffic is being sent via SDPs.

A mirror destination service that is configured for a destination router must not be configured as for a source router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The emote source configuration is not applicable when routable LI encapsulation is being used on the mirror source router. The remote source configuration is only used when a source router is sending mirrored traffic to a destination router via SDPs.

Two types of remote-source entries can be configured:

- far end
- spoke SDP

Certain remote source types are applicable with certain SDP types. For descriptions of the command usage in the **mirror-dest** context, see the **far-end** and **spoke-sdp** commands.

The **no** form of this command removes all remote-source entries.

Platforms All

22.145 remote-v6-ip

remote-v6-ip

Syntax **remote-v6-ip any**
remote-v6-ip *ipv6-prefix/prefix-length*
no remote-v6-ip

Context **[Tree]** (config>router>ipsec>sec-plcy>entry remote-v6-ip)
[Tree] (config>service>vprn>ipsec>sec-plcy>entry remote-v6-ip)

Full Context configure router ipsec security-policy entry remote-v6-ip
configure service vprn ipsec security-policy entry remote-v6-ip

Description This command specifies the remote v6 prefix for the security-policy entry.

Parameters *ipv6-prefix/prefix-length* — Specifies the local v6 prefix and length.

Values

ipv6-address/prefix: ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D
	host bits must be 0
	:: not allowed
	prefix-length [1 to 28]

any — A keyword to specify that any address can be used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec security-policy entry remote-v6-ip

VSR

- configure router ipsec security-policy entry remote-v6-ip

22.146 remote-ve-name

remote-ve-name

Syntax [**no**] **remote-ve-name** *name*

Context **[Tree]** (config>service>epipe>bgp-vpws remote-ve-name)

Full Context configure service epipe bgp-vpws remote-ve-name

Description This command creates or edits a remote-ve-name. A single remote-ve-name can be created per BGP VPWS instance if the service is single-homed or uses a single pseudowire to connect to a pair of dual-homed systems. When the service requires active/standby pseudowires to be created to remote dual-homed systems then two remote-ve-names must be configured.

This context defines the remote PE to which a pseudowire will be signaled.

remote-ve-name commands can be added even if bgp-vpws is not shutdown.

The **no** form of this command removes the configured remote-ve-name from the bgp vpws node. It can be used when the BGP VPWS status is either shutdown or “no shutdown”.

Parameters *name* — Specifies a site name up to 32 characters in length.

Platforms All

22.147 remove-oldest

remove-oldest

Syntax [**no**] **remove-oldest**

Context **[Tree]** (config>subscr-mgmt>sla-profile>host-limits remove-oldest)

Full Context configure subscriber-mgmt sla-profile host-limits remove-oldest

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command removes the oldest subscriber host when the host limit is reached.

The **no** form of this command maintains the oldest subscriber host when the host limit is reached.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.148 remove-private

remove-private

Syntax [**no**] **remove-private**

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy remove-private)

Full Context configure subscriber-mgmt bgp-peering-policy remove-private

Description This command allows private AS numbers to be removed from the AS path before advertising them to BGP peers.

The OS software recognizes the set of AS numbers that are defined by IANA as private. These are AS numbers in the range 64512 through 65535, inclusive.

The **no** form of this command used at the global level reverts to default value.

Private AS numbers are included in the AS path attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

remove-private

Syntax **remove-private** [**limited**] [**skip-peer-as**] [**replace**]
no remove-private

Context **[Tree]** (config>service>vprn>bgp remove-private)
[Tree] (config>service>vprn>bgp>group remove-private)
[Tree] (config>service>vprn>bgp>group>neighbor remove-private)

Full Context configure service vprn bgp group neighbor remove-private
configure service vprn bgp group remove-private
configure service vprn bgp remove-private

Description When this command is configured private AS numbers are removed or replaced when they are found inside the AS path of BGP routes advertised to peers within the scope of the command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The set of AS numbers that are defined by IANA as private are in the range of 64512 to 65534, and 4200000000 to 4294967294, inclusive. In SR OS, this command also removes ASN 65535 and ASN 4294967295, which are reserved values.

The **no** form of this command (at the BGP instance level) implements the default behavior, private AS numbers are allowed without restriction or modification in routes advertised to peers.

Default no remove-private

Parameters **limited** — This keyword instructs BGP to process private ASNs only up to the first public ASN encountered. Private ASNs beyond that first public AS will not be stripped or replaced.

skip-peer-as — This keyword instructs BGP to not strip or replace a private ASN from the AS-Path if that ASN is the same as the BGP peer AS number.

replace — When this keyword is configured, private ASNs are not stripped. Each occurrence is replaced by the ASN of the advertising BGP router (the ASN the router advertised to its peer in its OPEN message). When the **replace** keyword is not configured, private ASNs are stripped, subject to influence by the other keyword options. This generally results in a shortening of AS_PATH length.

Platforms All

remove-private

Syntax **remove-private** [**limited**] [**skip-peer-as**] [**replace**]
no remove-private

Context **[Tree]** (config>router>bgp remove-private)
[Tree] (config>router>bgp>group remove-private)
[Tree] (config>router>bgp>group>neighbor remove-private)

Full Context configure router bgp group neighbor remove-private
configure router bgp group remove-private
configure router bgp remove-private

Description When this command is configured private AS numbers are removed or replaced when they are found inside the AS path of BGP routes advertised to peers within the scope of the command.

The set of AS numbers that are defined by IANA as private are in the range of 64512 to 65534, and 4200000000 to 4294967294, inclusive. In SR OS, this command also removes ASN 65535 and ASN 4294967295, which are reserved values.

The **no** form of this command (at the BGP instance level) implements the default behavior, private AS numbers are allowed without restriction or modification in routes advertised to peers.

Default no remove-private

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **limited** — This keyword instructs BGP to process private ASNs only up to the first public ASN encountered. Private ASNs beyond that first public AS will not be stripped or replaced.

skip-peer-as — This keyword instructs BGP to not strip or replace a private ASN from the AS-Path if that ASN is the same as the BGP peer AS number.

replace — When this keyword is configured, private ASNs are not stripped. Each occurrence is replaced by the ASN of the advertising BGP router (the ASN the router advertised to its peer in its OPEN message). When the **replace** keyword is not configured, private ASNs are stripped, subject to influence by the other keyword options. This generally results in a shortening of AS_PATH length.

Platforms All

22.149 renew

renew

Syntax **renew est-profile** *name* **cert** *cert-filename* **key** *key-filename* [**hash-alg** *hash-algorithm*] **output** *output-cert-filename* [**validate-cert-chain**] [**force**]

Context **[Tree]** (admin>certificate>est renew)

Full Context admin certificate est renew

Description This command renews an imported certificate (specified by the **cert** *cert-filename*) with a Certificate Authority (CA) using the EST protocol specified by the **est-profile** name, with an imported private key specified the key parameter. The key can be either the key of the certificate to be renewed or a new key.

The authentication between system and EST server is specified by the est-profile.

The **hash-alg** *hash-alorithm* parameter is used to generate the CSR (Certificate Signing Request) in the EST request message.

Parameters *name* — Specifies EST profile name, up to 32 characters

cert-filename — Specifies the certificate file name, up to 95 characters

key-filename — Specifies the file name of a key, up to 95 characters

hash-algorithm — Specifies the hash algorithm to be used in a certificate request.

Values sha1, sha224, sha256, sha384, sha512

output-cert-filename — Specifies the output cert file name, up to 200 characters

validate-cert-chain — Specifies that the the system validates the certificate chain of the result certificate before importing it

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

force — Specifies the system to overwrite the existing file with same **output** *output-cert-filename*

Platforms All

22.150 renew-timer

renew-timer

Syntax **renew-timer** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no renew-timer

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ipv6-lease-times renew-timer)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ipv6-lease-times renew-timer)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy-server renew-timer)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy renew-timer)
[Tree] (config>router>dhcp6>server>pool>prefix renew-timer)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix renew-timer)

Full Context configure router dhcp6 local-dhcp-server pool prefix renew-timer
configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server renew-timer
configure service vprn dhcp6 local-dhcp-server pool prefix renew-timer
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server renew-timer
configure subscriber-mgmt local-user-db ipoe host ipv6-lease-times renew-timer
configure subscriber-mgmt local-user-db ppp host ipv6-lease-times renew-timer

Description This command configures the lease renew time (T1) via LUDB.

The T1 is the time at which the client contacts the addressing authority to extend the lifetimes of the DHCPv6 leases (addresses or prefixes). T1 is a time duration relative to the current time expressed in units of seconds.

The IP addressing authority controls the time at which the client contacts the addressing authority to extend the lifetimes on assigned addresses through the T1 and T2 parameters assigned to an IA. At time T1 for an IA, the client initiates a Renew/Reply message exchange to extend the lifetimes on any addresses in the IA. The client includes an IA option with all addresses currently assigned to the IA in its Renew message. Recommended values for T1 and T2 are .5 and .8 times the shortest preferred lifetime of the addresses in the IA that the addressing authority is willing to extend, respectively.

The configured renew timer should always be smaller than or equal to the rebind timer.

The T1 and T2 are carried in the IPv6 address option that is within the IA.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default renew-timer min 30

Parameters *renew-timer* — Specifies the preferred lifetime.

Values

days *days*	0 to 7
hrs *hours*	0 to 23
min *minutes*	0 to 59
sec *seconds*	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

renew-timer

Syntax **renew-timer** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no renew-timer

Context **[Tree]** (config>router>dhcp6>server>defaults renew-timer)

Full Context configure router dhcp6 local-dhcp-server defaults renew-timer

Description This command configures the default renew timer.

The **no** form of this command reverts to the default.

Default renew-timer min 30

Parameters *renew-timer* — Specifies the timer after which the lease is renewed.

Values

days:	0 to 7
hours:	0 to 23
minutes:	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.151 renotify

renotify

Syntax **renotify** *value*
no renotify

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>mac-notification renotify)

Full Context configure service vpls mac-notification renotify

Description This command controls the periodic interval at which sets of MAC notification messages are sent. At each expiration of the renotify timer, a new burst of notification messages is sent, specifically <count> frames at <interval> deci-seconds.

Default no renotify

Parameters *value* — Specifies the time interval between re-notification, in seconds

Values 240 to 840

Platforms All

22.152 renum

renum

Syntax **renum** *src-entry-id* **to** *dst-entry-id*

Context [Tree] (config>service>mrp>mrp-policy renum)

Full Context configure service mrp mrp-policy renum

Description This command renumbers existing MRP policy entries to properly sequence policy entries. This may be required in some cases since the implementation exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *src-entry-id* — Specifies the entry number of an existing entry.

Values 1 to 65535

new-entry-id — Specifies the new entry number to be assigned to the old entry. If the new entry exists, an error message is generated.

Values 1 to 65535

Platforms All

renum

Syntax **renum** *old-entry-id new-entry-id*

Context [Tree] (config>qos>sap-ingress>ip-criteria renum)
[Tree] (config>qos>sap-egress>ip-criteria renum)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>qos>sap-ingress>ipv6-criteria renum)
[Tree] (config>qos>sap-egress>ipv6-criteria renum)
[Tree] (config>qos>sap-ingress>mac-criteria renum)

Full Context
configure qos sap-egress ip-criteria renum
configure qos sap-egress ipv6-criteria renum
configure qos sap-ingress ip-criteria renum
configure qos sap-ingress ipv6-criteria renum
configure qos sap-ingress mac-criteria renum

Description This command renumbers existing QoS policy criteria entries to properly sequence policy entries.

This can be required in some cases since the router exits when the first match is found and executes the actions in accordance with the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *old-entry-id* — Enter the entry number of an existing entry.

Values 1 to 65535

new-entry-id — Enter the new entry number to be assigned to the old entry.

Values 1 to 65535

Platforms All

renum

Syntax **renum** *old-entry-number new-entry-number*

Context
[Tree] (config>qos>network>ingress>ip-criteria renum)
[Tree] (config>qos>network>ingress>ipv6-criteria renum)
[Tree] (config>qos>network>egress>ip-criteria renum)
[Tree] (config>qos>network>egress>ipv6-criteria renum)

Full Context
configure qos network egress ip-criteria renum
configure qos network egress ipv6-criteria renum
configure qos network ingress ip-criteria renum
configure qos network ingress ipv6-criteria renum

Description This command renumbers existing QoS policy criteria entries to properly sequence policy entries.

This can be required in some cases since the router exits when the first match is found and executes the actions in accordance with the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *old-entry-number* — Enter the entry number of an existing entry.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

new-entry-number — Enter the new entry number to be assigned to the old entry.

Values 1 to 65535

Platforms All

renum

Syntax **renum** *old-entry-id new-entry-id*

Context **[Tree]** (config>filter>ip-exception renum)
[Tree] (config>filter>ip-filter renum)
[Tree] (config>filter>ipv6-exception renum)
[Tree] (config>filter>ipv6-filter renum)
[Tree] (config>filter>mac-filter renum)

Full Context configure filter ip-exception renum
configure filter ip-filter renum
configure filter ipv6-exception renum
configure filter ipv6-filter renum
configure filter mac-filter renum

Description This command renumbers existing MAC, IPv4/IPv6, IP exception filter, or IPv6 exception filter entries to properly sequence filter entries.

This may be required in some cases since the OS exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *old-entry-id* — Specifies the entry number of an existing entry, as a decimal integer.

Values 1 to 2097151

new-entry-id — Specifies the new entry-number to be assigned to the old entry, as a decimal integer.

Values 1 to 2097151

Platforms All

- configure filter ip-filter renum
- configure filter ipv6-filter renum
- configure filter mac-filter renum

VSR

- configure filter ip-exception renum
- configure filter ipv6-exception renum

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

renum

Syntax **renum** *old-entry-number new-entry-number*

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter renum)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter renum)
[Tree] (config>system>security>mgmt-access-filter>mac-filter renum)

Full Context configure system security management-access-filter ip-filter renum
configure system security management-access-filter ipv6-filter renum
configure system security management-access-filter mac-filter renum

Description This command renumbers existing management access filter entries for an IP(v4), IPv6, or MAC filter to re-sequence filter entries.

The exits on the first match found and executes the actions in accordance with the accompanying **action** command. This may require some entries to be re-numbered differently from most to least explicit.

Parameters *old-entry-number* — Specifies the entry number of the existing entry.

Values 1 to 9999

new-entry-number — Specifies the new entry number that will replace the old entry number.

Values 1 to 9999

Platforms All

renum

Syntax **renum** *old-entry-id new-entry-id*

Context **[Tree]** (config>sys>sec>cpm>ip-filter renum)
[Tree] (config>sys>sec>cpm>ipv6-filter renum)
[Tree] (config>sys>sec>cpm>mac-filter renum)

Full Context configure system security cpm-filter ip-filter renum
configure system security cpm-filter ipv6-filter renum
configure system security cpm-filter mac-filter renum

Description This command renumbers existing IP(IPv4), IPv6, or MAC filter entries to re-sequence filter entries.

This may be required in some cases since the OS exits when the first match is found and execute the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters *old-entry-id* — Specifies the entry number of an existing entry.

Values 1 to 6144 for ip-filter and ipv6-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

1 to 2048 for mac-filter

new-entry-id — Specifies the new entry number to be assigned to the old entry.

Values 1 to 6144 for ip-filter and ipv6-filter
1 to 2048 for mac-filter

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

renum

Syntax **renum** *old-entry-number new-entry-number*

Context **[Tree]** (config>system>security>profile renum)

Full Context configure system security profile renum

Description This command renumbers profile entries to re-sequence the entries.

Since the OS exits when the first match is found and executes the actions according to accompanying action command, re-numbering is useful to rearrange the entries from most explicit to least explicit.

Parameters *old-entry-number* — Enter the entry number of an existing entry.

Values 1 **to** 9999

new-entry-number — Enter the new entry number.

Values 1 **to** 9999

Platforms All

22.153 renumber

renumber

Syntax **renumber from** *entry-id* **to** *entry-id*

Context **[Tree]** (config>router>policy-options>policy-statement renumber)

Full Context configure router policy-options policy-statement renumber

Description This command allows the operator to renumber the existing entry ID to a new entry ID. When performing the renumbering action, the two entry IDs must be different. The existing (**from**) *entry-id* must exist. The new (**to**) *entry-id* must not exist.

Renumbering is not saved in the configuration because it is a performing action.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **from** *entry-id* — Specifies the existing entry ID to be renumbered.

Values 1 to 4294967295

to *entry-id* — Specifies the new entry ID to be assigned.

Values 1 to 4294967295

Platforms All

22.154 reorder-audio

reorder-audio

Syntax **reorder-audio** *time*
no reorder-audio

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video reorder-audio)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video reorder-audio)

Full Context configure mcast-management multicast-info-policy bundle channel video reorder-audio
configure mcast-management multicast-info-policy bundle video reorder-audio

Description This command configures the time, in milliseconds, by which the audio packets are reordered in the ad stream.

Configuring this parameter depends on what is configured on the A Server and the GOP sizes of the network stream. Typically, this configuration should match the A Server configuration.

The **no** form of the command removes the time value from the configuration.

Default no reorder-audio

Parameters *time* — Specifies the audio reorder time, in milliseconds.

Values 100 to 1000

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.155 repair

repair

Syntax **repair** [*cflash-id*]

Context **[Tree]** (file repair)

Full Context file repair

Description This command checks a compact flash device for errors and repairs any errors found.

Parameters *cflash-id* — Specifies the compact flash slot ID to be shut down or enabled. When a specific *cflash-id* is specified, then that drive is shut down. If no *flash-id* is specified, the drive referred to by the current working directory is assumed. If a slot number is not specified, then the active CSM is assumed.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Default the current compact flash device.

Platforms All

22.156 repeated-characters

repeated-characters

Syntax **repeated-characters** *count*
no repeated-characters

Context **[Tree]** (config>system>security>password>complexity-rules repeated-characters)

Full Context configure system security password complexity-rules repeated-characters

Description The number of times a characters can be repeated consecutively.

The **no** form of this command resets to default.

Default no repeated-characters

Parameters *count* — Specifies the minimum count of consecutively repeated characters.

Values 2 to 8

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.157 replace

replace

Syntax **replace** [*line*]

Context **[Tree]** (candidate replace)

Full Context candidate replace

Description This command displays the specified line (a single line only) and allows it to be changed.

Parameters *line* — Indicates which line to replace starting at the point indicated by the following options.

Values

line, offset, **first**, **edit-point**, **last**

line	absolute line number
offset	relative line number to current edit point. Prefixed with '+' or '-'
first	keyword - first line
edit-point	keyword - current edit point
last	keyword - last line that is not 'exit'

22.158 replace-result-code

replace-result-code

Syntax **replace-result-code** *code* [*code*]
no replace-result-code

Context **[Tree]** (config>router>l2tp replace-result-code)
[Tree] (config>service>vprn>l2tp replace-result-code)

Full Context configure router l2tp replace-result-code
configure service vprn l2tp replace-result-code

Description This command replaces CDN Result-Code 4, 5 and 6 on LNS with the Result Code 2. This is needed for interoperability with some implementation of LAC which only takes action based on CDN Result-Code 2 while ignoring CDN Result-Code 4, 5 and 6.

Default no replace-result-code

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *code* — Specifies the L2TP Result codes that need to be replaced. Up to three codes can be specified.

Values cdn-tmp-no-facilities — CDN Result-Code 4 on LNS are replaced with the result code 2 before it is sent to LAC.

cdn-prem-no-facilities — CDN Result-Code 5 on LNS are replaced with the result code 2 before it is sent to LAC.

cdn-inv-dest — CDN Result-Code 6 on LNS are replaced with the result code 2 before it is sent to LAC.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.159 replay-protection

replay-protection

Syntax [**no**] **replay-protection**

Context **[Tree]** (config>macsec>connectivity-association replay-protection)

Full Context configure macsec connectivity-association replay-protection

Description Specifies the size of the replay protection window.

This command must be configured to force packet discard when it has detected a packet that is not within the replay-window-size.

When replay protection is enabled, the sequence of the ID number of the received packets are checked. If the packet arrives out of sequence and the difference between the packet numbers exceeds the replay window size, the packet is counted by the receiving port and then discarded. For example, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is counted and discarded because it falls outside the parameters of the replay window size.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

Default no replay-protection

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.160 replay-window

replay-window

Syntax **replay-window** *replay-window-size*
no replay-window

Context **[Tree]** (config>ipsec>tnl-temp replay-window)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel replay-window)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel replay-window)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel replay-window)
[Tree] (config>ipsec>trans-mode-prof replay-window)

Full Context configure ipsec tunnel-template replay-window
configure ipsec ipsec-transport-mode-profile replay-window
configure service ies interface ipsec ipsec-tunnel replay-window
configure service vprn interface ipsec ipsec-tunnel replay-window
configure service vprn interface sap ipsec-tunnel replay-window

Description This command specifies the size of the anti-replay window. The anti-replay window protocol further secures IPsec against an entity that can inject a recorded message in a message stream from a source to a destination computer on the Internet.

Default no replay-window

Parameters *replay-window-size* — Specifies the size of the SA anti-replay window.

Values 32, 64, 128, 256, 512

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel replay-window
- configure ipsec ipsec-transport-mode-profile replay-window
- configure ipsec tunnel-template replay-window

VSR

- configure service vprn interface ipsec ipsec-tunnel replay-window
- configure service ies interface ipsec ipsec-tunnel replay-window

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.161 replay-window-size

replay-window-size

Syntax **replay-window-size** *number-of-packet*s
no replay-window-size

Context **[Tree]** (config>macsec>connectivity-association replay-window-size)

Full Context configure macsec connectivity-association replay-window-size

Description This command specifies the size of the replay protection window.

This command must be configured to enable replay protection. When replay protection is enabled, the sequence of the ID number of received packets are checked. If the packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving port. For example, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

When the *number-of-packets* variable is set to 0, all packets that arrive out-of-order are dropped.

The **no** form of this command reverts to the default value.

Default replay-window-size 0

Parameters *number-of-packets* — Specifies the window for which the packets can arrive out of order.

Values 0 to 4294967294

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.162 replication-segment

replication-segment

Syntax [**no**] **replication-segment** *policy-name*

Context **[Tree]** (config>router>p2mp-sr-tree replication-segment)

Full Context configure router p2mp-sr-tree replication-segment

Description This command creates a P2MP SR tree replication segment entry for the P2MP LSP.

The **no** form of this command deletes the replication segment entry.

Parameters *policy-name* — Specifies the P2MP policy name, up to 32 characters, associated with the forwarding instructions contained in the replication segment.

Platforms All

22.163 replication-sid

replication-sid

Syntax **replication-sid** *label* [*label*]
no replication-sid

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment>next-hop-id replication-sid)

Full Context configure router p2mp-sr-tree replication-segment next-hop-id replication-sid

Description This command configures the replication SID or a SID list for the next hop of the P2MP SR tree replication segment.

When a SID list is configured, the replication SID is at the bottom of the stack and the unicast node or the adjacency SID is at the top of the stack. The SID at the top of the stack must be configured first in the list and the replication SID at the bottom of the list must be configured last in the list.

The **no** form of this command removes the replication SID.

Parameters *label* — Specifies the label of the replication SID; up to a maximum of 11 labels.

Values 3, 16 to 1048576, 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.164 replication-threshold

replication-threshold

Syntax **replication-threshold** *seconds*
no replication-threshold

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy replication-threshold)

Full Context configure isa nat-group inter-chassis-redundancy replication-threshold

Description This command configures the minimum duration of the flow that needs to be met before it is synchronized to the standby node. This way, flow synchronization and statefulness in a multi-chassis environment are limited only to long-lived flows.

The **no** form of this command reverts to the default values.

Default replication-threshold 20

Parameters *seconds* — Specifies the minimum flow existence time before it is synchronized.

Values 0 to 300

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.165 reply-on-padt

reply-on-padt

Syntax [**no**] **reply-on-padt**

Context **[Tree]** (config>subscr-mgmt>ppp-policy reply-on-padt)

Full Context configure subscriber-mgmt ppp-policy reply-on-padt

Description This command enables replying to PPPoE Active Discovery Terminate (PADT) packets. Some of the PPPoE clients expect reply on PADT message before the context of the session is cleared up. To support such client, a command enabling reply to PADT is provided.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.166 report-alarm

report-alarm

Syntax [**no**] **report-alarm** [**ais**] [**los**] [**oof**] [**rai**] [**looped**]

Context [Tree] (config>port>tdm>ds3 report-alarm)
[Tree] (config>port>tdm>e3 report-alarm)

Full Context configure port tdm ds3 report-alarm
configure port tdm e3 report-alarm

Description This command enables logging of DS-3 and E-3 alarms for a DS-3/E-3 port or channel.

The **no** form of this command disables logging of the specified alarms.

Parameters **ais** — Reports alarm indication signal errors. When configured, **ais** alarms are not raised and cleared.

Default **ais** alarms are issued

los — Reports loss of signal errors. When configured, **los** traps are not raised and cleared.

Default **los** traps are issued

oof — Reports out-of-frame errors. When configured, **oof** alarms are not raised and cleared.

Default **oof** alarms are not issued

rai — Reports resource availability indicator events. When configured, **rai** events are not raised and cleared.

Default **rai** alarms are not issued

looped — Reports looped packets errors.

Default **looped** alarms are not issued

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

report-alarm

Syntax [**no**] **report-alarm** [**signal-fail**] [**remote**] [**local**] [**no-frame-lock**] [**high-ber**] [**no-block-lock**] [**no-am-lock**] [**duplicate-lane**]

Context [Tree] (config>port>ethernet report-alarm)

Full Context configure port ethernet report-alarm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies when and if to generate alarms and alarm clear notifications for this port.

Parameters **signal-fail** — Reports an Ethernet signal lost alarm.

remote — Reports remote faults.

local — Reports local faults.

no-frame-lock — Reports a 'not locked on the Ethernet framing sequence' alarm.

high-ber — Reports High Bit Error Rate.

no-block-lock — Reports 40G/100G PCS Lanes Not Block Locked.

no-am-lock — Reports 40G/100G PCS Alignment Marker Loss of Lock.

duplicate-lane — Reports 40G/100G PCS Duplicate Lane Marker.

Platforms All

report-alarm

Syntax [**no**] **report-alarm** [**loc**] [**lais**] [**lrdi**] [**ss1f**] [**lb2er-sd**] [**lb2er-sf**] [**slof**] [**slos**] [**lrei**]

Context **[Tree]** (config>port>sonet-sdh report-alarm)

Full Context configure port sonet-sdh report-alarm

Description This command enables logging of SONET (SDH) line and section alarms for a SONET-SDH port. Only line and section alarms can be configured in the SONET/SDH context, for path alarms see the **sonet-sdh**>**path** context.

The **no** form of this command disables logging of the specified alarms.

This command is supported on TDM satellites.

Parameters **loc** — Reports a loss of clock which causes the operational state of the port to be shut down.

Default **loc** alarms are issued

lais — Reports line alarm indication signal errors. When configured, **lais** alarms are raised and cleared.

Default **lais** alarms are not issued

lrdi — Reports line remote defect indication errors. LRDI's are caused by remote LOF, LOC, LOS. When configured, **lrdi** alarms are raised and cleared.

Default **lrdi** alarms are issued

ss1f — Reports section synchronization failure which is detected when the S1 byte is not consistent for 8 consecutive frames. When configured, **ss1f** alarms are raised and cleared.

Default **ss1f** alarms are not issued

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

lb2er-sd — Reports line signal degradation BER (bit interleaved parity) errors. Use the threshold command to set the error rate(s) that when crossed determine signal degradation and signal failure. When configured, **lb2er-sd** alarms are raised and cleared.

Default **lb2er-sd** alarms are not issued

lb2er-sf — Reports line signal failure BER errors. Use the threshold command to set the error rate(s) that when crossed determine signal degradation and signal failure. When configured, **lb2er-sf** alarms are raised and cleared.

Default **lb2er-sf** alarms are issued

slof — Reports section loss of frame errors. When configured, **slof** alarms are raised and cleared.

Default **slof** alarms are issued

slos — Reports a section loss of signal error on the transmit side. When configured, **slos** alarms are raised and cleared.

Default **slos** alarms are issued

lrei — Reports a line error condition raised by the remote as a result of b1 errors received from this node. When configured, **lrei** traps are raised but not cleared.

Default **lrei** traps are not issued

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

report-alarm

Syntax [**no**] **report-alarm** {**pais** | **plop** | **prdi** | **pplm** | **prei**}

Context **[Tree]** (config>port>sonet-sdh>path report-alarm)

Full Context configure port sonet-sdh path report-alarm

Description This command enables logging of SONET (SDH) path alarms for a SONET-SDH port. Only path alarms can be configured in the channel context.

The **no** form of this command disables logging of the specified alarms.

Parameters **pais** — Reports path alarm indication signal errors. When configured, **pais** alarms are raised and cleared.

Default pais alarms are not issued

plop — Reports path loss of pointer (per tributary) errors. When configured, **plop** traps are raised but not cleared.

Default plop traps are issued

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prdi — Reports path remote defect indication errors. When configured, **prdi** alarms are raised and cleared.

Default prdi alarms are not issued

pplm — Reports a path payload mismatch, as a result the channel will be brought down. When configured, **pplm** traps are raised but not cleared.

Default pplm traps are issued

prei — Reports a path error condition raised by the remote as a result of b3 errors received from this node. When configured, **prei** traps are raised but not cleared.

Default prei traps are not issued

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

report-alarm

Syntax [**no**] **report-alarm** [**ais**] [**los**] [**oof**] [**rai**] [**looped**] [**ber-sd**] [**ber-sf**]

Context **[Tree]** (config>port>tdm>ds1 report-alarm)
[Tree] (config>port>tdm>e1 report-alarm)

Full Context configure port tdm ds1 report-alarm
configure port tdm e1 report-alarm

Description This command enables logging of DS-1/DS-3 or E-1/E-3 alarms for DS-1/DS-3 or E-1/E-3 ports or channels.

The **no** form of this command disables logging of the specified alarms.

Parameters **ais** — Reports alarm indication signal errors. When configured, **ais** alarms are not raised and cleared.

Default **ais** alarms are issued

los — Reports loss of signal errors. When configured, **los** traps are not raised and cleared.

Default **los** traps are issued.

oof — Reports out-of-frame errors. When configured, **oof** alarms are not raised and cleared.

Default **oof** alarms are not issued.

rai — Reports resource availability indicator events. When configured, **rai** events are not raised and cleared.

Default **rai** alarms are not issued

looped — Reports looped packets errors.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

looped alarms are not issuedlof — Reports loss of frame errors. When configured, **lof** traps are not raised and cleared.

Default **lof** traps are issued

ber-sd — Specifies the BER that specifies signal degradation.

ber-sf — Specifies the BER that specifies signal failure.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

report-alarm

Syntax [**no**] **report-alarm** [**stray**] [**malformed**] [**pktloss**] [**overrun**] [**underrun**] [**rpktloss**] [**rfault**] [**rrdi**]

Context **[Tree]** (config>service>cpipe>sap>cem report-alarm)
[Tree] (config>service>epipe>sap>cem report-alarm)

Full Context configure service cpipe sap cem report-alarm
configure service epipe sap cem report-alarm

Description This command indicates the type of CEM SAP alarm.

The **no** form of this command removes the parameter from the configuration.

Default On: stray, malformed, pktloss and overrun

Off: rpktloss, rfault, rrdi

Parameters **stray** — Reports the reception of packets not destined for this CES circuit.

malformed — Reports the reception of packet not properly formatted as CES packets.

pktloss — Reports the lack of reception of CES packets.

overrun — Reports the reception of too many CES packets resulting in a overrun of the receive jitter buffer.

underrun — Reports the reception of too few CES packets resulting in a overrun of the receive jitter buffer.

rpktloss — Reports that the remote peer is currently in packet loss status.

rfault — Reports that the remote TDM interface is currently not in service.

rrdi — Reports that the remote TDM interface is currently in RDI status.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap cem report-alarm

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure service epipe sap cem report-alarm

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

report-alarm

Syntax **report-alarm severity** {**tnc** | **qos** | **poa**}
no report-alarm

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms report-alarm)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms report-alarm)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms report-alarm)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms report-alarm
configure mcast-management multicast-info-policy bundle channel video analyzer alarms report-alarm
configure mcast-management multicast-info-policy bundle video analyzer alarms report-alarm

Description This command configures the type of alarm to monitor and raise through SNMP. The severity of alarms increases from TNC, to QoS, and then to POA. For example, if QoS alarms are configured, the analyzer only raises alarms and events related to QoS. The analyzer may raise alarms for POA events if they occur, but alarms for TNC are not sent.

Default no report-alarm

Parameters **severity** — Keyword to configure the type of alarm.

tnc — Specifies to monitor and raise alarms for TNC events.

qos — Specifies to monitor and raise alarms for QoS events.

poa — Specifies to monitor and raise alarms for POA events.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.167 report-alarms

report-alarms

Syntax [**no**] **report-alarms** [**modflt**] [**mod**] [**netrx**] [**nettx**] [**hosttx**]

Context **[Tree]** (config>port>dwdm>coherent report-alarms)

Full Context configure port dwdm coherent report-alarms

Description This command configures the alarms that will be reported for the coherent module.

Default modflt mod netrx nettx hosttx

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **modflt** — Reports module fault alarm.

mod — Reports module alarm.

netrx — Reports network (optical side) receive alarm.

nettx — Reports network (optical side) transmit alarm.

hosttx — Reports host (electrical side) transmit alarm.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

report-alarms

Syntax [**no**] **report-alarms** [**loc**] [**los**] [**lof**] [**lom**] [**otu-ais**] [**otu-ber-sf**] [**otu-ber-sd**] [**otu-bdi**] [**otu-tim**] [**otu-iae**] [**otu-biae**] [**fec-sf**] [**fec-sd**] [**fec-fail**] [**fec-uncorr**] [**odu-ais**] [**odu-oci**] [**odu-lck**] [**odu-bdi**] [**odu-tim**] [**opu-plm**]

Context **[Tree]** (config>port>otu report-alarms)

Full Context configure port otu report-alarms

Description This command enables OTU alarms. Specify specific alarms to add to the list of reported alarms.

The **no** form of this command disables OTU alarm reporting.

Default loc, los, lof, lom, otu-ber-sf, otu-bdi, fec-sf

Parameters **alarms** — Refer to Table 119 for alarm descriptions.

Table 119 **Alarm Descriptions**

Alarm	Description
loc	Loss of clock.
lof	Loss of OTU framing.
lom	Loss of Multi-frame.
los	Loss of signal transitions on the data.
otu-ais	OTU Alarm Indication Signal (all 1s, overwrites all OTU overhead, even framing bytes).
otu-ber-sf	SM Signal Fail (based on BPI8).
otu-ber-sd	SM Signal Degrade (based on BPI8).
otu-bdi	SM Backward defect indication.
otu-tim	SM Trace Id Mismatch.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 119 **Alarm Descriptions**

Alarm	Description
otu-iae	SM Incoming Alignment Error.
otu-biae	SM Backward Incoming Alignment Error.
fec-sf	Signal Fail (based on FEC corrected bits).
fec-sd	Signal Degrade (based on FEC corrected bits).
fec-fail	FEC Mode mismatch (EFEC-GFEC) or High Uncorrectable rate (>10E-2).
fec-uncorr	One or More Uncorrectable FEC errors.
odu-ais	ODU Alarm Indication Signal.
odu-oci	ODU Open connection Indication.
odu-lck	ODU Locked.
odu-bdi	PM Backward Defect indication.
odu-tim	PM Trace Id Mismatch.
opu-plm	OPU PSI Payload Type Mismatch.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.168 report-ip-address-event

report-ip-address-event

Syntax [**no**] **report-ip-address-event**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx report-ip-address-event)

Full Context configure subscriber-mgmt diameter-application-policy gx report-ip-address-event

Description This command enables triggered CCR-u messages based on IP address allocation or de-allocation for the subscriber host.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the requests for both IP address families (IPv4 and IPv6) arrive at approximately the same time, a single CCR-i is sent containing the IP addresses from both address families, IPv4 and IPv6 (NA, PD, or SLAAC). When the requests for IP addresses are not nearly simultaneous, the CCR-i contains only the IP address that was allocated first (the one that triggered the session creation). The request for the second IP address family, depending on configuration, triggers an additional CCR-u that will carry the IP address allocation update to the PCRF along with the UE_IP_ADDRESS_ALLOCATE (18) event. The CCR-u content mirrors the content of the CCR-i with the exception of already allocated IP address(es).

When this command is disabled, IP address-triggered CCR-u messages are not sent.

The **no** form of this command disables the command.

Default report-ip-address-event

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.169 report-local-routes

report-local-routes

Syntax [**no**] **report-local-routes**

Context **[Tree]** (config>bmp>station report-local-routes)

Full Context configure bmp station report-local-routes

Description This command enables local route reporting to the BMP monitoring station.

The **no** form of this command disables the local route reporting.

Platforms All

22.170 report-path-constraints

report-path-constraints

Syntax **report-path-constraints**
no report-path-constraints

Context **[Tree]** (config>router>pcep>pcc report-path-constraints)

Full Context configure router pcep pcc report-path-constraints

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the inclusion of LSP path constraints in the PCE report messages sent from the PCC to a PCE.

In order for the PCE to know about the original constraints for an LSP which is delegated, but for which there is no prior state in its LSP database, such as if no PCReq message was sent for the same PLSP-ID, the following proprietary behavior is observed:

- PCC appends a duplicate of each of the LSPA, METRIC, and BANDWIDTH objects in the PCRpt message. The only difference between two objects of the same type is that the P-flag is set in the common header of the duplicate object to indicate that it is a mandatory object for processing by PCE.
- The value of the metric or bandwidth in the duplicate object contains the original constraint value, while the first object contains the operational value. This is applicable to hop metrics in the METRIC and BANDWIDTH objects only. The SR OS PCC does not support configuring a boundary on the path computation IGP or TE metrics.
- The path computation on the PCE must use the first set of objects when updating a path if the PCRpt contained a single set. If the PCRpt contained a duplicate set, PCE path computation must use the constraints in the duplicate set.

The **no** form of the command disables the above behavior in case of interoperability issues with third-party PCE implementations.

Default report-path-constraints

Platforms All

22.171 report-rate

report-rate

Syntax **report-rate agg-rate-limit**
report-rate scheduler *scheduler-name*
report-rate pppoe-actual-rate
report-rate policer *policer-id*
report-rate rfc5515-actual-rate
no report-rate

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress report-rate)
[Tree] (config>subscr-mgmt>sla-prof>egress report-rate)

Full Context configure subscriber-mgmt sla-profile egress report-rate
configure subscriber-mgmt sla-profile ingress report-rate

Description This command configures the source for Tx and Rx connect speeds in AVP 38 (Rx Connect Speed) and AVP 24 (Tx Connect Speed) of an L2TP session established on a LAC.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters **agg-rate-limit** — Specifies that the rate (egress only) is taken from:

1. the agg-rate RADIUS override (RADIUS VSA “Alc-Subscriber-QoS-Override” in a RADIUS Access-Accept message) if present
2. the configured agg-rate-limit in the **config>subscr-mgmt>sub-prof>egr** context
3. fall back to the default (no report-rate)

scheduler-name — Specifies the rate taken from the **scheduler** *scheduler-name* up to 32 characters. If the **scheduler** *scheduler-name* is not present in the scheduler-policy configured in the **config>subscr-mgmt>sub-prof>egr** context, fall back to the default (no report-rate).

pppoe-actual-rate — Specifies rates taken from the DSL Line characteristics PPPoE tags (Actual Data Rate Upstream/Downstream) if present; otherwise fall back to the default (no report-rate).

policer-id — Specifies the rate taken from the policer with the specified ID.

Values 1 to 63

rfc5515-actual-rate — Puts the same value as the transmitted Actual-Data-Rate-Upstream AVP in the Rx-Connect-Speed AVP, and the same value as the transmitted Actual-Data-Rate-Downstream AVP in the Tx-Connect-Speed AVP

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.172 report-src-ip

report-src-ip

Syntax **report-src-ip** *ip-address*
no report-src-ip

Context **[Tree]** (config>service>vpls>igmp-snooping report-src-ip)

Full Context configure service vpls igmp-snooping report-src-ip

Description This command configures the source IPv4 address used when generating IGMP reports. According the IGMPv3 standard, a zero source address is allowed in sending IGMP reports. However, for interoperability with some multicast routers, the source IP address of IGMP group reports can be configured using this command.

Default report-src-ip 0.0.0.0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the source IPv4 address in transmitted IGMP reports.

Values a.b.c.d

Platforms All

report-src-ip

Syntax **report-src-ip** *ipv6-address*
no report-src-ip

Context **[Tree]** (config>service>vpls>mld-snooping report-src-ip)

Full Context configure service vpls mld-snooping report-src-ip

Description This command configures the source IPv6 address used when generating MLD reports. A zero source address is allowed in sending MLD reports. However, for interoperability with some multicast routers, the source IP address of MLD reports can be configured using this command.

Default report-src-ip 0:0:0:0:0:0:0:0

Parameters *ipv6-address* — Specifies the source IPv6 address in transmitted MLD reports.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

Platforms All

22.173 report-wlan-location

report-wlan-location

Syntax [**no**] **report-wlan-location**

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile report-wlan-location)

Full Context configure subscriber-mgmt gtp peer-profile report-wlan-location

Description This command enables reporting the WLAN location or cellular location of the UE in the signaling interface (S2a or Gn) between the WLAN GW and the mobile gateway (PGW or GGSN).

The **no** form of this command disables location reporting.

Default no report-wlan-location

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.174 reporting

reporting

Syntax [**no**] **reporting**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>efh>interim-c reporting)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling interim-credit reporting

Description This command enables reporting of the used interim credit for each rating group when a new Diameter Gy session is successfully established with the Online Charging Server (OCS). When enabled, the used interim credit report includes:

- the unreported used credit assigned via the initial Diameter Gy session when Extended Failure Handling (EFH) became active
- the used interim credits during EFH
- the used credits assigned via the new established Diameter Gy session

The **no** form of this command disables interim credit reporting. Only credit assigned via the new established Diameter Gy session is reported.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.175 request

request

Syntax **request** *seconds*

Context **[Tree]** (config>li>x-interfaces>x2>timeouts request)
[Tree] (config>li>x-interfaces>x3>timeouts request)

Full Context configure li x-interfaces x2 timeouts request
configure li x-interfaces x3 timeouts request

Description This command configures the X2 and X3 keep-alive timeout.

Parameters *seconds* — Specifies the maximum time to wait for a LIC reply to a request. The system retries up to three more times, and if no reply is received, the system initiates a connection release and logs the failure event.

Values 5 to 30

Default 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.176 request-format

request-format

Syntax **request-format**

Context **[Tree]** (config>system>security>tacplus request-format)

Full Context configure system security tacplus request-format

Description Commands in this context configure access operations that are sent to the TACACS+ server during authorization.

Platforms All

22.177 request-script-policy

request-script-policy

Syntax **request-script-policy** *script-policy*
no request-script-policy

Context **[Tree]** (config>aaa>l2tp-accounting-policy request-script-policy)
[Tree] (config>aaa>radius-srv-plcy request-script-policy)

Full Context configure aaa l2tp-accounting-policy request-script-policy
configure aaa radius-server-policy request-script-policy

Description This command configures a RADIUS script policy to modify Access-Request.

The **no** form of this command removes the policy-name from the configuration.

Parameters *script-policy* — Specifies the name of the Python script used to modify Access-Request messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

request-script-policy

Syntax **request-script-policy** *policy-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no request-script-policy

Context [Tree] (config>subscr-mgmt>auth-plcy request-script-policy)

Full Context configure subscriber-mgmt authentication-policy request-script-policy

Description This command configures the RADIUS script policy used to change the RADIUS attributes of the outgoing Access-Request messages.

The **no** form of this command removes the policy name from the configuration.

Parameters *policy-name* — Specifies the name of the Python script to modify Access-Request messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.178 request-timer

request-timer

Syntax **request-timer** *timer1* **retry-timer** *timer2* **timeout-multiplier** *multiplier*
no request-timer

Context [Tree] (config>service>apipe>spoke-sdp>control-channel-status request-timer)
[Tree] (config>service>cpipe>spoke-sdp>control-channel-status request-timer)
[Tree] (config>service>epipe>spoke-sdp>control-channel-status request-timer)
[Tree] (config>service>vpls>spoke-sdp>control-channel-status request-timer)

Full Context configure service apipe spoke-sdp control-channel-status request-timer
configure service cpipe spoke-sdp control-channel-status request-timer
configure service epipe spoke-sdp control-channel-status request-timer
configure service vpls spoke-sdp control-channel-status request-timer

Description This command configures the control channel status request mechanism. When it is configured, control channel status request procedures are used. These augment the procedures for control channel status messaging from RFC 6478. This command cannot be used with a non-zero refresh-timer value.

Parameters *timer1* — Specifies the interval, in seconds, at which pseudowire status messages, including a reliable delivery TLV with the “request” bit set, are sent.

Values 10 to 65535

timer2 — specifies the timeout interval, in seconds, if no response to a pseudowire status request is received. This parameter must be configured. A value of zero (0) disables retries.

Values 0, 3 to 60

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multiplier — If a requesting node does not receive a valid response to a pseudowire status request within a number of seconds equal to the retry timer multiplied by this multiplier, then it will assume the pseudowire is down. This parameter is optional.

Values 3 to 20

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp control-channel-status request-timer

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp control-channel-status request-timer

All

- configure service epipe spoke-sdp control-channel-status request-timer
- configure service vpls spoke-sdp control-channel-status request-timer

request-timer

Syntax **request-timer** *request-timer-secs* **retry-timer** *retry-timer-secs* **timeout-multiplier** *multiplier*
no request-timer

Context **[Tree]** (config>service>vpls>spoke-sdp>control-channel-status request-timer)

Full Context configure service vpls spoke-sdp control-channel-status request-timer

Description This command configures the control channel status request mechanism. When it is configured, control channel status request procedures are used. These augment the procedures for control channel status messaging from RFC 6478, *Pseudowire Status for Static Pseudowires*. This command cannot be used with a non-zero refresh-timer value.

Parameters *request-timer-secs* — Specifies the interval, in seconds, at which pseudowire status messages, including a reliable delivery TLV with the “request” bit set, are sent.

Values 10 to 65535

retry-timer-secs — specifies the timeout interval, in seconds, if no response to a pseudowire status request is received. This parameter must be configured. A value of zero (0) disables retries.

Values 0, 3 to 60

multiplier — If a requesting node does not receive a valid response to a pseudowire status request within a number of seconds equal to the retry timer multiplied by this multiplier, then it will assume the pseudowire is down. This parameter is optional.

Values 3 to 20

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

request-timer

Syntax **request-timer** *timer1* **retry-timer** *timer2* **timeout-multiplier** *multiplier*
no request-timer

Context **[Tree]** (config>service>ies>if>spoke-sdp>control-channel-status request-timer)

Full Context configure service ies interface spoke-sdp control-channel-status request-timer

Description This command configures the control channel status request mechanism. When it is configured, control channel status request procedures are used. These augment the procedures for control channel status messaging from RFC 6478. This command is mutually exclusive with a non-zero refresh-timer value.

Parameters *timer1* — Specifies the interval at which pseudowire status messages, including a reliable delivery TLV, with the “request” bit set, are sent.

Values 10 to 65535 seconds

retry-timer *timer2* — Specifies the timeout interval if no response to a pseudowire status request is received. This parameter must be configured. A value of zero (0) disables retries.

Values 0, 3 to 60 seconds

timeout-multiplier *multiplier* — If a requesting node does not receive a valid response to a pseudowire status request within this multiplier times the retry timer, then it will assume the pseudowire is down. This parameter is optional.

Values 3 to 20 seconds

Platforms All

request-timer

Syntax **request-timer** *request-timer-secs* **retry-timer** *retry-timer-secs* **timeout-multiplier** *multiplier*
no request-timer

Context **[Tree]** (config>service>vprn>if>spoke-sdp>control-channel-status request-timer)
[Tree] (config>service>vprn>red-if>spoke-sdp>control-channel-status request-timer)

Full Context configure service vprn interface spoke-sdp control-channel-status request-timer
configure service vprn redundant-interface spoke-sdp control-channel-status request-timer

Description This command configures the control channel status request mechanism. When it is configured, control channel status request procedures are used. These augment the procedures for control channel status messaging from RFC 6478. This command is mutually exclusive with a non-zero refresh-timer value.

Parameters *request-timer-secs* — Specifies the interval, in seconds, at which pseudowire status messages, including a reliable delivery TLV, with the “request” bit set, are sent.

Values 10 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

retry-timer *retry-timer-secs* — Specifies the timeout interval, in seconds, if no response to a pseudowire status request is received. This parameter must be configured. A value of zero (0) disables retries.

Values 0, 3 to 60

timeout-multiplier *multiplier* — Specifies the multiplier, in seconds. If a requesting node does not receive a valid response to a pseudowire status request within this multiplier times the retry timer, then it assume the pseudowire is down. This parameter is optional.

Values 3 to 15

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp control-channel-status request-timer

All

- configure service vprn interface spoke-sdp control-channel-status request-timer

request-timer

Syntax **request-timer** *request-timer-secs* **retry-timer** *retry-timer-secs* **timeout-multiplier** *multiplier*
no request-timer

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp>control-channel-status request-timer)
[Tree] (config>mirror>mirror-dest>spoke-sdp>control-channel-status request-timer)

Full Context configure mirror mirror-dest remote-source spoke-sdp control-channel-status request-timer
configure mirror mirror-dest spoke-sdp control-channel-status request-timer

Description This command configures the control channel status request mechanism. When it is configured, control channel status request procedures are used. These augment the procedures for control channel status messaging from RFC 6478. This command is mutually exclusive with a non-zero refresh-timer value.

Parameters *request-timer-secs* — Specifies the interval, in seconds, at which pseudowire status messages, including a reliable delivery TLV, with the “request” bit set, are sent.

Values 10 to 65535

retry-timer-secs — Specifies the timeout interval, in seconds, if no response to a pseudowire status request is received. This parameter must be configured. A value of zero (0) disables retries.

Values 3 to 60

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

multiplier — Specifies the multiplier, in seconds, that if a requesting node does not receive a valid response to a pseudowire status request within this multiplier times the retry timer, then it will assume the pseudowire is down. This parameter is optional.

Values 3 to 15

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.179 requests

requests

Syntax [**no**] **requests** [**neighbor** *ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>rip requests)

Full Context debug router rip requests

Description This command enables debugging for RIP requests.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP requests sent on the neighbor IP address or interface.

Platforms All

requests

Syntax [**no**] **requests** [**neighbor** *ip-int-name* | *ipv6-address*]

Context **[Tree]** (debug>router>ripng requests)

Full Context debug router ripng requests

Description This command enables debugging for RIP requests.

Parameters *ip-int-name* | *ipv6-address* — Debugs the RIP requests sent on the neighbor IP address or interface.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.180 required

required

Syntax **required** [**lowercase** *count*] [**uppercase** *count*] [**numeric** *count*] [**special-character** *count*]
no required

Context **[Tree]** (config>system>security>password>complexity-rules required)

Full Context configure system security password complexity-rules required

Description Force the minimum number of different character classes required.

The **no** form of this command resets to default.

Default required lowercase 0 uppercase 0 numeric 0 special-character 0

Parameters *count* — Specifies the minimum count of characters classes.

Values 0 to 10

Platforms All

22.181 rescue-location

rescue-location

Syntax **rescue-location** *file-url*
no rescue-location

Context **[Tree]** (config>system>rollback rescue-location)

Full Context configure system rollback rescue-location

Description The location and filename of the rescue configuration is configurable to be local (on compact flash) or remote. The suffix .rc will be automatically appended to the filename when a rescue configuration file is saved. Trivial FTP (TFTP) is not supported for remote locations.

Default no rescue location

Parameters *file-url* — Specifies the URL or filename.

Values

local-url | *remote-url*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length of up to 99 characters each
remote-url	[{ftp://}*login*:*pswd*@ *remote-locn*/][*file-path*] up to 255 characters, directory length of up to 99 characters each
remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
	x:x:x:x:x:x:d.d.d.d[-*interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface - 32 chars max, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:
rescue filename	suffixed with .rc during the rescue file creation

Platforms All

22.182 reserved

reserved

Syntax **reserved** *num-sessions*
no reserved

Context **[Tree]** (config>isa>nat-group>session-limits reserved)

Full Context configure isa nat-group session-limits reserved

Description This command configures the number of sessions per block that are reserved for prioritized sessions.

Default no reserved

Parameters *num-sessions* — Specifies the number of sessions reserved for prioritized sessions.

Values 0 to 6291456

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

reserved

Syntax **reserved** *num-sessions*
no reserved

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>nat>firewall-policy>session-limits reserved)
[Tree] (config>service>nat>nat-policy>session-limits reserved)
[Tree] (config>service>nat>up-nat-policy>session-limits reserved)

Full Context configure service nat firewall-policy session-limits reserved
configure service nat nat-policy session-limits reserved
configure service nat up-nat-policy session-limits reserved

Description This command configures the number of sessions per block that will be reserved for prioritized sessions.

Default no reserved

Parameters *num-sessions* — Specifies the number of sessions reserved for prioritized sessions.

Values 0 to 65534

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy session-limits reserved
- configure service nat up-nat-policy session-limits reserved

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy session-limits reserved

reserved

Syntax **reserved** *num-ports*
no reserved

Context [Tree] (config>service>nat>nat-policy>port-limits reserved)
[Tree] (config>service>nat>up-nat-policy>port-limits reserved)

Full Context configure service nat nat-policy port-limits reserved
configure service nat up-nat-policy port-limits reserved

Description This command configures the number of ports per block that will be reserved for prioritized sessions.

Default no reserved

Parameters *num-ports* — Specifies the number of ports to reserve for prioritized sessions.

Values 1 to 65534

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.183 reserved-label-block

reserved-label-block

Syntax [**no**] **reserved-label-block** *name*

Context **[Tree]** (config>router>mpls-labels reserved-label-block)

Full Context configure router mpls-labels reserved-label-block

Description Commands in this context configure a block of labels from the dynamic range to be locally assigned for specific applications, such as Segment Routing adjacency SIDs. The reserved label block is not advertised by the IGP.

The **no** form of this command removes a reserved label block.

Parameters *name* — Specifies the name of the reserved label block, up to 64 characters

Platforms All

reserved-label-block

Syntax **reserved-label-block** *name*
no reserved-label-block

Context **[Tree]** (config>router>rib-api>mpls reserved-label-block)

Full Context configure router rib-api mpls reserved-label-block

Description This command specifies the reserved label block for use in all label-FIB entries programmed using the RIB-API gRPC service. The named reserved label block must already have been configured under **config**>**router**>**mpls**>**mpls-labels**.

The **no** form of this command removes the assignment of the reserved label block, causing all existing label-FIB entry programming, using the RIB-API gRPC service, to become invalid and unusable.

Default no reserved-label-block

Parameters *name* — Specifies the name of the reserved label block up to 64 characters in length.

Platforms All

reserved-label-block

Syntax **reserved-label-block** *name*
no reserved-label-block

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>mpls>fwd-policies reserved-label-block)

Full Context configure router mpls forwarding-policies reserved-label-block

Description This command specifies the reserved label block to use for all MPLS forwarding policies. The named reserved label block must already have been configured under **config>router>mpls-labels**.

The **no** form of the command removes the assignment of the reserved label block.

Parameters *name* — Specifies the name of the reserved label block, up to 64 characters.

Platforms All

reserved-label-block

Syntax **reserved-label-block** *name*
no reserved-label-block

Context [Tree] (config>router>segment-routing>sr-policies reserved-label-block)

Full Context configure router segment-routing sr-policies reserved-label-block

Description This command associates a reserved label block with segment routing policies. The *name* must already exist. Reserved label blocks are configured under the **config>router>mpls-labels** hierarchy.

A locally-targeted segment routing policy (statically configured or BGP signaled) cannot be activated if its binding SID (BSID) is not an available label between the start-label and end-label of the referenced reserved label block.

The **no** form of this command removes any association of segment routing policies with a reserved label block.

Default no reserved-label-block

Parameters *name* — Specifies the name of a **reserved-label-block** that has already been configured, up to 64 characters.

Platforms All

22.184 reserved-lbl-block

reserved-lbl-block

Syntax **reserved-lbl-block** *reserved-lbl-block*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no reserved-lbl-block

Context [Tree] (config>router>p2mp-sr-tree reserved-lbl-block)

Full Context configure router p2mp-sr-tree reserved-lbl-block

Description This command configures the reserved label block name for the P2MP SR tree. Before configuring for the P2MP SR tree, the reserved label block name must be configured on the root node of the P2MP policy in the **config**>**router**>**mpls-labels** context.

The **no** form of this command removes the reserved label block name for the P2MP SR tree.

Default no reserved-lbl-block

Parameters *reserved-lbl-block* — Specifies the value of the reserved label block name, up to 64 characters.

Platforms All

22.185 reset-on-recoverable-error

reset-on-recoverable-error

Syntax [**no**] **reset-on-recoverable-error**

Context [Tree] (config>card reset-on-recoverable-error)

Full Context configure card reset-on-recoverable-error

Description This command configures the behavior of the card when a fatal memory parity error is detected on a Q-chip of the card. If **reset-on-recoverable-error** is enabled, the card is reset, regardless of the setting of the **fail-on-error** parameter.

The **no** form of this command specifies that the recovery action is taken instead of resetting the card.

Default no reset-on-recoverable-error

Platforms 7450 ESS, 7750 SR-7/12/12e

reset-on-recoverable-error

Syntax [**no**] **reset-on-recoverable-error**

Context [Tree] (config>card>mda reset-on-recoverable-error)

Full Context configure card mda reset-on-recoverable-error

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the behavior of the MDA when a fatal memory parity error is detected on a Q-chip of the MDA. If **reset-on-recoverable-error** is enabled, the MDA is reset, regardless of the setting of the **fail-on-error** parameter.

The **no** form of this command specifies that the recovery action is taken instead of resetting the MDA.

Default no reset-on-recoverable-error

Platforms 7750 SR-s, 7950 XRS

reset-on-recoverable-error

Syntax [**no**] **reset-on-recoverable-error**

Context **[Tree]** (config>card>xiom reset-on-recoverable-error)

Full Context configure card xiom reset-on-recoverable-error

Description This command configures the behavior of the XIOM when a fatal memory parity error is detected on a Q-chip of the XIOM. If **reset-on-recoverable-error** is enabled, the XIOM is reset, regardless of the setting of the **fail-on-error** parameter.

The **no** form of this command specifies that the recovery action is taken instead of resetting the XIOM.

Default no reset-on-recoverable-error

Platforms 7750 SR-s

22.186 reset-policy-exclusive

reset-policy-exclusive

Syntax **reset-policy-exclusive**

Context **[Tree]** (admin reset-policy-exclusive)

Full Context admin reset-policy-exclusive

Description This command allows an authorized administrator to reset the exclusive policy editing lock. This will reset the lock flag and end the policy editing session in progress, discarding any policy edits.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.187 reset-query

reset-query

Syntax [**no**] **reset-query**

Context **[Tree]** (debug>router>rpki-session>packet reset-query)

Full Context debug router rpki-session packet reset-query

Description This command enables debugging for reset query RPKI packets.

The **no** form of this command disables debugging for reset query RPKI packets.

Platforms All

22.188 reset-unknown-tcp

reset-unknown-tcp

Syntax [**no**] **reset-unknown-tcp**

Context **[Tree]** (config>service>nat>nat-policy reset-unknown-tcp)
[Tree] (config>service>nat>up-nat-policy reset-unknown-tcp)

Full Context configure service nat nat-policy reset-unknown-tcp
configure service nat up-nat-policy reset-unknown-tcp

Description This command enables the system to drop a TCP packet and generate a TCP reset, when a TCP packet without the SYN flag set is received by the NAT inside for an unknown flow.

The **no** form of this command disables sending the reset, but the packet is still dropped.

Default no reset-unknown-tcp

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.189 resignal-on-igp-event

resignal-on-igp-event

Syntax [**no**] **resignal-on-igp-event**

Context **[Tree]** (config>router>mpls>sr-te-resignal resignal-on-igp-event)

Full Context configure router mpls sr-te-resignal resignal-on-igp-event

Description This command introduces the ad-hoc resignaling of all SR-TE LSPs at the receipt of one or more IGP link down events in TE-DB. Once the re-optimization is triggered, the behavior is exactly the same as the timer based resignal or the **delay** option of the manual based resignal. MPLS forces the expiry of the resignal timer and asks TE-DB to re-evaluate the active paths of all SR-TE LSPs. The re-evaluation consists of updating the total IGP or TE metric of the current path, checking the validity of the hops and labels, and computing a new CSPF for each SR-TE LSP. MPLS programs the new path only if the total metric of the new computed path is different than the updated metric of the current path, or if one or more hops or labels of the current path are invalid. Otherwise, the current path is considered to be one of the most optimal ECMP paths and is not updated in data path.

Platforms All

22.190 resignal-on-igp-overload

resignal-on-igp-overload

Syntax [**no**] **resignal-on-igp-overload**

Context **[Tree]** (config>router>mpls resignal-on-igp-overload)

Full Context configure router mpls resignal-on-igp-overload

Description This command enables the resignaling of all RSVP-TE LSPs at the receipt of the IS-IS overload bit in the TE-DB.

Once the re-optimization is triggered, the behavior is the same as the timer-based resignal or the **delay** option of the manual-based resignal. MPLS forces the expiry of the resignal timer and requests the TE-DB to compute a new CSPF for each RSVP-TE LSP active path.

This re-optimization effectively causes the immediate move of transit RSVP-TE LSP paths away from the IS-IS node in overload.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, MPLS re-optimizes, using the MBB procedure, the transit paths away from the node in an IS-IS overload state only at the time a manual or timer-based resignal is performed for the LSP paths. MPLS does not act immediately on the receipt of the IS-IS overload bit.

Note: This command and the **retry-on-overload** command are mutually exclusive.

The **no** form of this command results in the MPLS not acting immediately to the request of the IS-IS overload bit.

Default no resignal-on-overload

Platforms All

22.191 resignal-timer

resignal-timer

Syntax **resignal-timer** *minutes*
no resignal-timer

Context **[Tree]** (config>router>mpls resignal-timer)

Full Context configure router mpls resignal-timer

Description This command specifies the value for the LSP resignal timer. The resignal timer is the time, in minutes, the software waits before attempting to resignal the LSPs.

When the resignal timer expires, if the new computed path for an LSP has a better metric than the current recorded hop list, an attempt is made to resignal that LSP using the make-before-break mechanism. If the attempt to resignal an LSP fails, the LSP continues to use the existing path and a resignal will be attempted the next time the timer expires.

The **no** form of this command disables timer-based LSP resignaling.

Default no resignal-timer

Parameters *minutes* — Specifies the time the software waits before attempting to resignal the LSPs.

Values 30 to 10080

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

resignal-timer

Syntax **resignal-timer** *minutes*
no resignal-timer

Context **[Tree]** (config>router>mpls>sr-te-resignal resignal-timer)

Full Context configure router mpls sr-te-resignal resignal-timer

Description This command specifies the value for the SR-TE LSP resignal timer when the path computation method is set to the local CSPF or the PCE.

The resignal timer is the time, in minutes, MPLS waits before attempting to re-optimize all paths of all SR-TE LSPs. The re-optimization is performed by the local CSPF or the PCE, depending on the value of the parameter **path-computation-method**.

When local CSPF is used and the resignal timer expires, MPLS provides the current path of the SR-TE LSP and TE-DB updates the total IGP or TE metric of the current path and checks the validity of the hops and labels. CSPF then computes a new path for each SR-TE LSP. MPLS programs the new path only if the total metric of the new computed path is different than the updated metric of the current path, or if one or more hops or labels of the current path are invalid. Otherwise, the current path is considered to be one of the most optimal ECMP paths and is not updated in data path.

The **no** form of this command disables timer-based LSP resignaling.

Default no resignal-timer

Parameters *minutes* — Specifies the time, in minutes, the software waits before attempting to resignal the SR-TE TSPs.

Values 30 to 10080

Platforms All

22.192 resolution

resolution

Syntax **resolution** {**disabled** | **any** | **filter**}

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel resolution)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel resolution)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel resolution)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel resolution)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn bgp-evpn mpls auto-bind-tunnel resolution
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution

Description This command configures the resolution mode in the automatic binding of a BGP-EVPN or BGP-IPVPN MPLS service to tunnels to MP-BGP peers.

Default resolution disabled

Parameters **any** — Enables the binding to any supported tunnel type in a BGP-EVPN or BGP-IPVPN MPLS context following TTM preference.

disabled — Disables the automatic binding of a BGP-EVPN or BGP-IPVPN MPLS service to tunnels to MP-BGP peers.

filter — Enables the binding to the subset of tunnel types configured the **resolution-filter** context.

Platforms All

resolution

Syntax **resolution** {**any** | **disabled** | **filter**}

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop resolution)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution

Description This command determines the resolution mode for the associated static route to a tunnel next hop.

Default resolution any

Parameters **any** — Allows the associated static route to be resolved to any active entry in the TTM, following the TTM preference order.

disabled — Disables the resolution of the associated static route to any active entry in the TTM. As a result, the static route can only be resolved via IP RTM resolution of the static route's next hop.

filter — Allows the associated static route to be resolved to active tunnels in the TTM using the resolution-filter restrictions.

Platforms All

resolution

Syntax **resolution** {**any** | **filter** | **disabled**}

Context **[Tree]** (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family resolution)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution

Description This command configures the resolution mode in the resolution of BGP label routes using tunnels to BGP peers.

Parameters **any** — Enables the binding to any supported tunnel type in the BGP label route context following TTM preference.

filter — Enables the binding to the subset of tunnel types configured under **resolution-filter**.

disabled — Disables the resolution of BGP label routes using tunnels to BGP peers.

Platforms All

resolution

Syntax **resolution** {**any** | **filter** | **disabled**}

Context **[Tree]** (config>router>bgp>next-hop-res>shortcut-tunn>family resolution)

Full Context configure router bgp next-hop-resolution shortcut-tunnel family resolution

Description This command configures the resolution mode in the resolution of BGP prefixes using tunnels to BGP peers.

Parameters **any** — Enables the binding to any supported tunnel type in BGP shortcut context following TTM preference.

filter — Enables the binding to the subset of tunnel types configured under **resolution-filter**.

disabled — Disables the resolution of BGP prefixes using tunnels to BGP peers.

Platforms All

resolution

Syntax **resolution** {**any** | **disabled** | **filter** | **match-family-ip**}

Context **[Tree]** (config>router>isis>igp-shortcut>tunnel-next-hop>family resolution)

Full Context configure router isis igp-shortcut tunnel-next-hop family resolution

Description This command configures resolution mode in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

Parameters **any** — Enables the binding to any supported tunnel type following TTM preference.

disabled — Disables the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

filter — Enables the binding to the subset of tunnel types configured under **resolution-filter**.

match-family-ip — Enables the resolution of the SR tunnel family to match that of the corresponding IP prefix family.

Platforms All

resolution

Syntax **resolution** {**any** | **disabled** | **filter** | **match-family-ip**}

Context **[Tree]** (config>router>ospf>igp-shortcut>tunnel-next-hop>family resolution)

Full Context configure router ospf igp-shortcut tunnel-next-hop family resolution

Description This command configures resolution mode in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

Parameters **any** — Enables the binding to any supported tunnel type following TTM preference.

disabled — Disables the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

filter — Enables the binding to the subset of tunnel types configured under **resolution-filter**.

match-family-ip — Enables the resolution of the SR tunnel family to match that of the corresponding IP prefix family.

Platforms All

resolution

Syntax **resolution** {**any** | **disabled** | **filter**}

Context **[Tree]** (config>router>ospf3>igp-shortcut>tunnel-next-hop>family resolution)

Full Context configure router ospf3 igp-shortcut tunnel-next-hop family resolution

Description This command configures resolution mode in the resolution of the IPv6 prefix using IGP shortcuts.

Parameters **any** — Enables the binding to any supported tunnel type following TTM preference.

disabled — Disables the resolution of the IPv6 prefix using IGP shortcuts.

filter — Enables the binding to the subset of tunnel types configured under **resolution-filter**.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

resolution

Syntax **resolution** {**any** | **disabled** | **filter**}

Context **[Tree]** (config>service>vprn>auto-bind-tunnel resolution)

Full Context configure service vprn auto-bind-tunnel resolution

Description This command configures the resolution method for tunnel selection.

Default resolution any

Parameters **any** — Allows the associated static route to be resolved to any active entry in the TTM, following the TTM preference order.

disabled — Disables the associated static route to be resolved to any active entry in the TTM. As a result, the static route can only be resolved via IP RTM resolution of the static route's nexthop.

filter — Allows the associated static route to be resolved to active tunnels in the TTM using the resolution-filter restrictions.

22.193 resolution-filter

resolution-filter

Syntax **resolution-filter**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel resolution-filter)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel resolution-filter)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel resolution-filter)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel resolution-filter)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter

Description Commands in this context configure the subset of tunnel types that can be used in the resolution of BGP-EVPN or BGP-IPVPN routes within the automatic binding of BGP-EVPN or BGP-IPVPN MPLS service to tunnels to MP-BGP peers.

The following tunnel types are supported in a BGP-EVPN or BGP-IPVPN MPLS context: BGP, LDP, RIB-API, RSVP, SR-ISIS, SR-OSPF, SR-policy, SR-TE, UDP, and MPLS forwarding policy.

The user must set **resolution** to **filter** to activate the list of tunnel-types configured under **resolution-filter**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: UDP tunnels are created through import policies with action **create-udp-tunnel**.

Platforms All

resolution-filter

Syntax **resolution-filter**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop resolution-filter)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter

Description This command creates the context to configure the tunnel next-hop resolution options.

If one or more tunnel filter criteria are specified, the static route nexthop is resolved to an available tunnel from one of those LSP types. The tunnel type is selected based on the TTM preference.

Platforms All

resolution-filter

Syntax **resolution-filter**

Context **[Tree]** (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family resolution-filter)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter

Description Commands in this context set resolution filter types.

Platforms All

resolution-filter

Syntax **resolution-filter** [**bgp**] [**ldp**] [**rsvp**] [**sr-isis**] [**sr-ospf**] [**sr-policy**] [**sr-te**]

Context **[Tree]** (config>router>bgp>next-hop-res>shortcut-tunn>family resolution-filter)

Full Context configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter

Description This command configures the subset of tunnel types that can be used to resolve BGP unlabeled routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **bgp** — Selects the BGP label route tunnel type.

ldp — Selects the LDP tunnel type.

rsvp — Selects the RSVP-TE tunnel type.

sr-isis — Selects the SR tunnel type programmed by an IS-IS instance in TTM.

sr-ospf — Selects the SR tunnel type programmed by an OSPF instance in TTM.

sr-policy — Selects the SR tunnel type programmed by an SR policy instance in TTM.

sr-te — Selects the SR tunnel type programmed by a TE instance in TTM.

Platforms All

resolution-filter

Syntax **resolution-filter**

Context **[Tree]** (config>router>isis>igp-shortcut>tunnel-next-hop>family resolution-filter)

Full Context configure router isis igp-shortcut tunnel-next-hop family resolution-filter

Description Commands in this context configure the subset of tunnel types which can be used in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

Parameters **rsvp** — Selects the RSVP-TE tunnel type.

sr-te — Selects the SR-TE tunnel type.

Platforms All

resolution-filter

Syntax **resolution-filter**

Context **[Tree]** (config>router>ospf>igp-shortcut>tunnel-next-hop>family resolution-filter)
[Tree] (config>router>ospf3>igp-shortcut>tunnel-next-hop>family resolution-filter)

Full Context configure router ospf igp-shortcut tunnel-next-hop family resolution-filter
configure router ospf3 igp-shortcut tunnel-next-hop family resolution-filter

Description Commands in this context configure the subset of tunnel types that can be used in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.194 resolve

resolve

Syntax **resolve** *minutes*

Context **[Tree]** (config>service>vpls>proxy-arp>dynamic resolve)
[Tree] (config>service>vpls>proxy-nd>dynamic resolve)

Full Context configure service vpls proxy-arp dynamic resolve
configure service vpls proxy-nd dynamic resolve

Description This command configures the frequency at which a resolve message is sent. The resolve message is an ARP-request or NS message flooded to all the non-EVPN endpoints in the service irrespective of the current status of the **unknown-arp-request-flood-evpn** or **unknown-ns-flood-evpn** commands.

Default resolve 5

Parameters *minutes* — Specifies the frequency in minutes at which the **resolve** message is issued.

Values 1 to 60

Default 5

Platforms All

22.195 resolve-root-using

resolve-root-using

Syntax **resolve-root-using** {**ucast-rtm** | **mcast-rtm**}

Context **[Tree]** (config>router>ldp resolve-root-using)

Full Context configure router ldp resolve-root-using

Description By default, MLDP resolves the FEC using the unicast RTM. When this command is set to **mcast-rtm**, MLDP will resolve the FEC using the multicast route table. The multicast route table does not include any IGP shortcuts, unlike the unicast RTM. MLDP cannot resolve a FEC using an IGP shortcut, so if IGP shortcuts are used for unicast, enable multicast MLDP lookups.

If this command is set to **mcast-rtm**:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- For FEC resolution using IGP, static or local, the ROOT in this FEC is resolved using the multicast RTM.
- A FEC being resolved using BGP is recursive, so the FEC next-hop (ASBR/ABR) is resolved using the multicast RTM first and, if this fails, it is resolved using the unicast RTM. This next-hop needs to be recursively resolved again using IGP/Static-Route or Local, this second resolution (recursive resolution) uses the multicast RTM only.
- In all cases, MLDP uses the unicast RTM to resolve the FEC and will not resolve the FEC if its next hop is resolved using an IGP shortcut.

Default resolve-root-using ucast-rtm

Platforms All

22.196 resolve-static

resolve-static

Syntax [**no**] **resolve-static**

Context **[Tree]** (config>router>policy-options>policy-statement>default-action resolve-static)
[Tree] (config>router>policy-options>policy-statement>entry>action resolve-static)

Full Context configure router policy-options policy-statement default-action resolve-static
configure router policy-options policy-statement entry action resolve-static

Description This command has an affect only in BGP route-table-import policies and applies only to BGP IPv4 and IPv6 routes created by importing static routes with indirect next-hops. When such a route matches a policy entry with this action, the BGP next-hop is the resolved next-hop of the static route.

The **no** form of this command reverts to the default behavior, which copies the indirect next-hop of the static route into the BGP next-hop without resolving it further.

Default no resolve-static

Platforms All

22.197 responder-url

responder-url

Syntax **responder-url** *url-string*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no responder-url

Context [Tree] (config>system>security>pki>ca-profile>ocsp responder-url)

Full Context configure system security pki ca-profile ocsp responder-url

Description This command specifies HTTP URL of the OCSP responder for the CA, this URL will only be used if there is no OCSP responder defined in the AIA extension of the certificate to be verified.

Default no responder-url

Parameters *url-string* — Specifies the HTTP URL of the OCSP responder

Platforms All

22.198 response-signing-cert

response-signing-cert

Syntax **response-signing-cert** *filename*
no response-signing-cert

Context [Tree] (config>system>security>pki>ca-profile>cmpv2 response-signing-cert)

Full Context configure system security pki ca-profile cmpv2 response-signing-cert

Description This command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA's certificate will be used.

Default no response-signing-cert

Parameters *filename* — Specifies the filename of the imported certificate.

Platforms All

response-signing-cert

Syntax **response-signing-cert** *filename*
no response-signing-cert

Context [Tree] (config>system>security>pki>ca-profile>cmp2 response-signing-cert)

Full Context configure system security pki ca-profile cmp2 response-signing-cert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA's certificate will be used.

Default no response-signing-cert

Parameters *filename* — Specifies the filename of the imported certificate.

22.199 restart-backoff

restart-backoff

Syntax **restart-backoff initial-time** *seconds* **max-time** *seconds*
no restart-backoff

Context **[Tree]** (config>subscr-mgmt>pppoe-client-policy restart-backoff)

Full Context configure subscriber-mgmt pppoe-client-policy restart-backoff

Description This command configures backoff timer parameters that determine how often and how long the system will attempt to restart a PPPoE client after a failure. When a client first fails, the system immediately tries to re-establish connectivity. If this attempt is also unsuccessful, the system initiates a backoff timer and waits until it expires before attempting to restart the client again, to avoid flooding the BNG. The initial duration of the backoff timer is configured with the **initial-time** parameter. With each subsequent failure, the backoff timer is doubled until the configured **max-time** is reached.

The **no** form of this command reverts to the default.

Default restart-backoff initial-time 30 max-time 600

Parameters **initial-time** *seconds* — Specifies the initial backoff time to wait before attempting a client restart.

Values 10 to 3600

max-time *seconds* — Specifies the maximum time to attempt client restarts.

Values 10 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.200 restart-time

restart-time

Syntax **restart-time** *seconds*
no restart-time

Context **[Tree]** (config>service>vprn>bgp>graceful-restart restart-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart restart-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart restart-time)

Full Context configure service vprn bgp graceful-restart restart-time
configure service vprn bgp group graceful-restart restart-time
configure service vprn bgp group neighbor graceful-restart restart-time

Description This command sets the value of the restart-time that is advertised in the router's graceful-restart capability. If this command is not configured, the default is 300.

Default no restart-time

Parameters *seconds* — Specifies the restart-time that is advertised in the router's graceful-restart capability.

Values 0 to 4095 seconds

Default 300

Platforms All

restart-time

Syntax **restart-time** *seconds*
no restart-time

Context **[Tree]** (config>router>bgp>graceful-restart restart-time)
[Tree] (config>router>bgp>group>graceful-restart restart-time)
[Tree] (config>router>bgp>group>neighbor>graceful-restart restart-time)

Full Context configure router bgp graceful-restart restart-time
configure router bgp group graceful-restart restart-time
configure router bgp group neighbor graceful-restart restart-time

Description This command sets the value of the restart-time that is advertised in the router's graceful-restart capability. If this command is not configured, the default is 300.

Default no restart time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the restart-time that is advertised in the router's graceful-restart capability.

Values 0 to 4095 seconds

Default config>router>bgp>graceful-restart: 120 seconds
config>router>bgp>group>graceful-restart: 300 seconds
config>router>bgp>group>neighbor>graceful-restart: 300 seconds

Platforms All

22.201 restore-disconnected

restore-disconnected

Syntax [**no**] **restore-disconnected**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wpp restore-disconnected)
[Tree] (config>service>vprn>sub-if>grp-if>wpp restore-disconnected)

Full Context configure service ies subscriber-interface group-interface wpp restore-disconnected
configure service vprn subscriber-interface group-interface wpp restore-disconnected

Description This command specifies that the initial profiles must be restored after a DHCP host has disconnected. The behavior that system will restore the **initial-sla-profile**, **initial-sub-profile**, or **initial-app-profile** when hosts disconnects instead of removing them.

The **no** form of this command specifies that the initial profiles will not be restored after a DHCP host has disconnected.

Default restore-disconnected

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

restore-disconnected

Syntax **restore-disconnected** {**restore** | **no-restore**}
no restore-disconnected

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>wpp restore-disconnected)

Full Context configure subscriber-mgmt local-user-db ipoe host wpp restore-disconnected

Description This command specifies the behavior that system will restore the **initial-sla-profile**, **initial-sub-profile**, or **initial-app-profile** when hosts disconnects instead of removing them.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **restore** — Specifies that the initial profiles must be restored after a DHCP host has disconnected.

no-restore — Specifies that the initial profiles will not be restored after a DHCP host has disconnected.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.202 restrict-protected-src

restrict-protected-src

Syntax **restrict-protected-src discard-frame**
restrict-protected-src [**alarm-only**]
no restrict-protected-src

Context **[Tree]** (config>service>vpls>sap restrict-protected-src)
[Tree] (config>service>vpls>spoke-sdp restrict-protected-src)
[Tree] (config>service>vpls>mesh-sdp restrict-protected-src)
[Tree] (config>service>vpls>split-horizon-group restrict-protected-src)
[Tree] (config>service>vpls>endpoint restrict-protected-src)
[Tree] (config>service>pw-template restrict-protected-src)
[Tree] (config>service>pw-template>split-horizon-group restrict-protected-src)

Full Context configure service pw-template restrict-protected-src
configure service pw-template split-horizon-group restrict-protected-src
configure service vpls endpoint restrict-protected-src
configure service vpls mesh-sdp restrict-protected-src
configure service vpls sap restrict-protected-src
configure service vpls split-horizon-group restrict-protected-src
configure service vpls spoke-sdp restrict-protected-src

Description This command indicates how the agent will handle relearn requests for protected MAC addresses, either manually added using the mac-protect command or automatically added using the **auto-learn-mac-protect** command. While enabled all packets entering the configured SAP, spoke SDP, mesh SDP, or any SAP that is part of the configured split horizon group (SHG) is verified not to contain a protected source MAC address. If the packet is found to contain such an address, the action taken depends on the parameter specified on the **restrict-protected-src** command, namely:

- No parameter — The packet is discarded, an alarm is generated and the SAP, spoke SDP or mesh SDP is set operationally down. The SAP, spoke SDP or mesh SDP must be shut down and enabled (**no shutdown**) for this state to be cleared.
- **alarm-only** — The packet is forwarded, an alarm is generated but the source MAC is not learned on the SAP, spoke SDP or mesh SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **discard-frame** — The packet is discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per MAC address per FP per 10 minutes in a given VPLS service. This parameter is only applicable to automatically protected MAC addresses.

When the **restrict-protected-src** is enabled on an SHG the action only applies to the associated SAPs (no action is taken by default for spoke SDPs in the SHG) and is displayed in the SAP show output as the oper state unless it is overridden by the configuration of **restrict-protected-src** on the SAP itself. To enable this function for spoke SDPs within a SHG, the **restrict-protected-src** must be enabled explicitly under the spoke SDP. If required, **restrict-protected-src** can also be enabled explicitly under specific SAPs within the SHG.

When this command is applied or removed, with either the **alarm-only** or **discard-frame** parameters, the MAC addresses are cleared from the related object.

The use of **restrict-protected-src discard-frame** is mutually exclusive with the configuration of manually protected MAC addresses within a given VPLS.

The **alarm-only** parameter is not supported on the 7750 SR-a, 7750 SR-1e/2e/3e, 7950 XRS, 7750 SR-1,or 7750 SR-1s/2s/7s/14s platforms.

The **no** form of the command reverts to the default.

Default no restrict-protected-src

Parameters **alarm-only** — Specifies that the packet is forwarded, an alarm is generated but the source MAC is not learned on the SAP, spoke SDP, or mesh SDP.

Default no alarm-only

discard-frame — Specifies that the packet is discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per MAC address per FP per 10 minutes within a given VPLS service.

Default no discard-frame

Platforms All

restrict-protected-src

Syntax **restrict-protected-src discard-frame**
no restrict-protected-src

Context **[Tree]** (config>service>vpls>pbb>backbone-vpls restrict-protected-src)

Full Context configure service vpls pbb backbone-vpls restrict-protected-src

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command indicates how the agent handles relearn requests for protected MAC addresses, either manually added using the **mac-protect** command or automatically added using the **auto-learn-mac-protect** command. While enabled, all packets entering the configured SAP, spoke SDP, mesh SDP, or any SAP that is part of the configured split horizon group (SHG) is verified not to contain a protected source MAC address. If the packet is found to contain such an address, the action taken depends on the parameter specified on the **restrict-protected-src** command, namely:

- No parameter — The packet is discarded, an alarm is generated and the SAP, spoke SDP or mesh SDP will be set as operationally down. The SAP, spoke SDP or mesh SDP must be shutdown and enabled (no shutdown) for this state to be cleared.
- **discard-frame** — The packet is discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per MAC address per FP per 10 minutes in a specified VPLS service. This parameter is only applicable to automatically protected MAC addresses.

When the **restrict-protected-src** is enabled on an SHG, the action only applies to the associated SAPs (no action is taken by default for spoke-SDPs in the SHG) and is displayed in the SAP show output as the oper state unless it is overridden by the configuration of **restrict-protected-src** on the SAP itself. To enable this function for spoke SDPs within a SHG, the **restrict-protected-src** must be enabled explicitly under the spoke SDP. If required, **restrict-protected-src** can also be enabled explicitly under specific SAPs within the SHG.

When this command is applied or removed, with the **discard-frame** parameter, the MAC addresses are cleared from the related object.

The use of **restrict-protected-src discard-frame** is mutually exclusive with the configuration of manually protected MAC addresses within a specified VPLS.

Default no restrict-protected-src

Parameters **discard-frame** — Specifies that the packet is discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per MAC address per FP per 10 minutes within a specified VPLS service

Platforms All

restrict-protected-src

Syntax **restrict-protected-src discard-frame**
no restrict-protected-src

Context **[Tree]** (config>service>vpls>vxlan restrict-protected-src)

Full Context configure service vpls vxlan restrict-protected-src

Description This command enables protected SRS MAC restrictions.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.203 restrict-unprotected-dst

restrict-unprotected-dst

Syntax **restrict-unprotected-dst**
no restrict-unprotected-dst

Context **[Tree]** (config>service>vpls restrict-unprotected-dst)
[Tree] (config>service>vpls>sap restrict-unprotected-dst)
[Tree] (config>service>pw-template>split-horizon-group restrict-unprotected-dst)
[Tree] (config>service>vpls>split-horizon-group restrict-unprotected-dst)

Full Context configure service pw-template split-horizon-group restrict-unprotected-dst
configure service vpls restrict-unprotected-dst
configure service vpls sap restrict-unprotected-dst
configure service vpls split-horizon-group restrict-unprotected-dst

Description This command indicates how the system will forward packets destined for an unprotected MAC address, either manually added using the **mac-protect** command or automatically added using the **auto-learn-mac-protect** command. While enabled all packets entering the configured SAP or SAPs within a split horizon group (but not spoke or mesh-SDPs) will be verified to contain a protected destination MAC address. If the packet is found to contain a non-protected destination MAC, it will be discarded. Detecting a non-protected destination MAC on the SAP will not cause the SAP to be placed in the operationally down state. No alarms are generated.

If the destination MAC address is unknown, even if the packet is entering a restricted SAP, with **restrict-unprotected-dst** enabled, it will be flooded.

Default no restrict-unprotected-dst

Platforms All

22.204 restricted-to-home

restricted-to-home

Syntax [**no**] **restricted-to-home**

Context **[Tree]** (config>system>security>user restricted-to-home)
[Tree] (config>system>security>user-template restricted-to-home)

Full Context configure system security user restricted-to-home
configure system security user-template restricted-to-home

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command prevents users from navigating above their home directories for file access (either by means of CLI sessions with the file command, '>' redirection, or by means of FTP). A user is not allowed to navigate to a directory higher in the directory tree on the home directory device. The user is allowed to create and access subdirectories below their home directory.

When enabled, this command prevents a user from being able to execute an **admin save** command for the configuration if they do not have access to the directory where the configuration file is saved. The same behavior applies for the **bof save** command and the **li save** command.

If a home-directory is not configured or the home directory is not available, then the user has no file access.

The **no** form of this command allows the user access to navigate to directories above their home directory.

Default no restricted-to-home

Platforms All

22.205 results

results

Syntax **results** *file-url*
no results

Context **[Tree]** (config>system>script-control>script-policy results)

Full Context configure system script-control script-policy results

Description This command is used to specify the location where the system writes the output of an event script's execution.

The **no** form of the command removes the file location from the configuration. Scripts will not execute if there is no result location defined.

Default no results

Parameters *file-url* — Specifies the location to send CLI output from script runs. The *file-url* is a location, directory, and filename prefix to which a data and timestamp suffix is added when the results files are created during a script run, as follows:

*file-url*_YYYYMMDD-hhmmss.uuuuuu.out

where:

YYYYMMDD — date

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hhmmss — hours, minutes, and seconds

uuuuuu — microseconds (padded to 6 characters with leading zeros)

Values *local-url* | *remote-url*

local-url — [*cflash-id/*] [*file-path*] 167 chars max, including *cflash-idfile-path* 166 chars max

remote url — [{ftp:// | tftp://}*login*:*password*@*remote-location*/][*file-path*] 255 characters max directory length 99 characters max each

remote-location — [*hostname* | *ipv4-address* | *ipv6-address*]

ipv4-address — *a.b.c.d*

ipv6-address — x:x:x:x:x:x:x:x[-*interface*] x:x:x:x:x:x:d.d.d.d[-*interface*] x — [0 to FFFF]H d — [0 to 255]D interface — 32 characters max, for link local addresses

cflash-id — cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

22.206 resv

resv

Syntax [**no**] **resv**

Context **[Tree]** (debug>router>gmpls>event resv)

Full Context debug router gmpls event resv

Description This command enables and disables debugging for GMPLS Resv events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

resv

Syntax **resv** [**detail**]
no resv

Context **[Tree]** (debug>router>gmpls>packet resv)

Full Context debug router gmpls packet resv

Description This command enables debugging for GMPLS Resv packets.

The **no** form of the command disables debugging for GMPLS Resv packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

resv

Syntax **resv** [**detail**]
no resv

Context **[Tree]** (debug>router>rsvp>event resv)

Full Context debug router rsvp event resv

Description This command debugs RSVP reservation events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about RSVP reservation events.

Platforms All

resv

Syntax **resv** [**detail**]
no resv

Context **[Tree]** (debug>router>rsvp>packet resv)

Full Context debug router rsvp packet resv

Description This command enables debugging for RSVP resv packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about RSVP Resv events.

Platforms All

22.207 resv-cbs

resv-cbs

Syntax **resv-cbs** *percent-or-default* **amber-alarm-action step** *percent* **max** *percent*
resv-cbs *percent-or-default*
no resv-cbs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>access>egress>channel>pool resv-cbs)
[Tree] (config>port>access>egress>pool resv-cbs)
[Tree] (config>port>access>ingress>pool resv-cbs)
[Tree] (config>port>network>egress>pool resv-cbs)

Full Context configure port access egress channel pool resv-cbs
configure port access egress pool resv-cbs
configure port access ingress pool resv-cbs
configure port network egress pool resv-cbs

Description This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command:

- A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated.
- The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting.

It is important to note that this command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueuing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The resv-cbs parameter can be changed at any time.

If the total pool size is 10 Mb and the resv-cbs set to 5, the ‘reserved size’ is 500 kb.

The **no** form of this command clears all the adaptive configurations. There cannot be any adaptive sizing enabled for default **resv-cbs**.

Default resv-cbs 30

Parameters *percent-or-default* — Specifies the pool buffer size percentage.

Values 0 to 100, **default**

amber-alarm-action step *percent* — Specifies the percentage step-size for the reserved CBS size of the pool. When using the default value, the adaptive CBS sizing is disabled. To enable adaptive CBS sizing, **step** *percent* must be set to non-default value along with the **max** parameter. When reserved CBS is default adaptive CBS sizing cannot be enabled. The reserved CBS (Committed Burst Size) defines the amount of buffer space within the pool that is not considered shared.

Values 1 to 100

Default 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max *percent* — Specifies the maximum percentage for the reserved CBS size of the pool. When using the default value, the adaptive CBS sizing is disabled. To enable adaptive CBS sizing, **max** value must be set to non-default value along with the **step** *percent*. When reserved CBS is default adaptive CBS sizing cannot be enabled. The reserved CBS (Committed Burst Size) defines the amount of buffer space within the pool that is not considered shared. Max reserved CBS must not be more than the reserved CBS.

Values 1 to 100

Default 0

Platforms All

resv-cbs

Syntax **resv-cbs min** *percentage* **max** *percentage*
no resv-cbs

Context **[Tree]** (config>card>fp>egress>wred-queue-control resv-cbs)

Full Context configure card fp egress wred-queue-control resv-cbs

Description This command defines the amount of buffers within the WRED mega-pool that will be set aside for WRED queues operating within their configured CBS thresholds. **Note** that the **min** *percentage* and **max** *percentage* parameters must be set to the same value. The forwarding plane protects against WRED queue buffer starvation by setting aside a portion of the buffers within the WRED mega-pool. The WRED queue CBS threshold defines when a WRED queue requests buffers from reserved portion of the WRED mega-pool and when it starts requesting buffers from the shared portion of the mega-pool. With proper oversubscription provisioning, this prevents a seldom active queue from being denied a buffer from the mega-pool when the shared portion of the mega-pool is congested.

The WRED mega-slope reserve CBS size is controlled in the same manner as the overall sizing of the WRED mega-pool. A min and max parameter is provided to scope the range that the reserved portion based on percentages of the WRED mega-pool current size.

The **no** form of this command immediately restores the default min and max percentage values for sizing the WRED mega-pool CBS reserve.

Default resv-cbs min 25.00 max 25.00

Parameters **min** *percentage* — Specifies that the required keyword defines the minimum percentage of the WRED mega-pool buffers that will be applied to the CBS reserve. The value given for *percentage* must be less than or equal to the value given for the **max** *percentage*. Percentages are defined with an accuracy of hundredths of a percent in the nn.nn format (15.65 = 15.65%).

Values 0.00 to 99.99

Default 25.00

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

max *percentage* — Specifies that the required keyword defines the maximum percentage of the IOM3-XP WRED mega-pool buffers that may be applied to the CBS reserve. The value given for *percentage* must be greater than or equal to the value given for the **min** *percentage*. Percentages are defined with an accuracy of hundredths of a percent in the nn.nn format (15.65 = 15.65%).

Values 0.01 to 99.99

Default 25.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

resv-cbs

Syntax **resv-cbs** *percent-or-default*
resv-cbs *percent-or-default* **amber-alarm-action step** *percent* **max** *percent*
no resv-cbs

Context **[Tree]** (config>card>fp>ingress>network>pool resv-cbs)

Full Context configure card fp ingress network pool resv-cbs

Description This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command:

- A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated.
- The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting.

It is important to note that this command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueuing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The **resv-cbs** parameter can be changed at any time.

If the total pool size is 10 Mb and the **resv-cbs** set to 5, the ‘reserved size’ is 500 kb.

The **no** form of this command clears all the adaptive configurations. There cannot be any adaptive sizing enabled for default **resv-cbs**.

Default resv-cbs 30

Parameters *percent-or-default* — Specifies the pool buffer size percentage.

Values 0 to 100, **default**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

amber-alarm-action step *percent* — Specifies the percentage step-size for the reserved CBS size of the pool. When using the default value, the adaptive CBS sizing is disabled. To enable adaptive CBS sizing, step percent must be set to non-default value along with the max parameter. When reserved CBS is default adaptive CBS sizing cannot be enabled. The reserved CBS defines the amount of buffer space within the pool that is not considered shared.

Values 1 to 100

Default 0

max *percent* — Specifies the maximum percentage for the reserved CBS size of the pool. When using the default value, the adaptive CBS sizing is disabled. To enable adaptive CBS sizing, **max** value must be set to non-default value along with the **step** *percent*. When reserved CBS is default adaptive CBS sizing cannot be enabled. The reserved CBS defines the amount of buffer space within the pool that is not considered shared. Max reserved CBS must not be more than the reserved CBS.

Values 1 to 100

Default 0

Platforms All

resv-cbs

Syntax **resv-cbs** *percent-or-default*
no resv-cbs

Context **[Tree]** (config>isa>aa-grp>qos>egress>from-subscriber>pool resv-cbs)
[Tree] (config>isa>aa-grp>qos>egress>to-subscriber>pool resv-cbs)

Full Context configure isa application-assurance-group qos egress from-subscriber pool resv-cbs
configure isa application-assurance-group qos egress to-subscriber pool resv-cbs

Description This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command.

- A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated.
- The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueuing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The resv-cbs parameter can be changed at any time.

If the total pool size is 10 MB and the **resv-cbs** set to 5, the 'reserved size' is 500 KB.

The **no** form of this command restores the default value of 30.

Default resv-cbs default

Parameters *percent-or-default* — Specifies the pool buffer size percentage.

Values 0 to 100, default

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.208 resv-ret

resv-ret

Syntax **resv-ret** *resv-ret*

Context **[Tree]** (config>isa>video-group resv-ret)

Full Context configure isa video-group resv-ret

Description This command provides a mechanism to reserve an explicit amount of egress bandwidth, in Mb/s, for RET for all the ISAs within a video group. If the amount of egress bandwidth is less than the reserved amount, FCC requests are discarded and only RET requests processed. The bandwidth is dynamically adjusted per ISA within the video group if an ISA becomes operational/non-operational within the group.

Default resv-ret 0

Parameters *resv-ret* — Specifies the egress bandwidth in Mb/s.

Values 0 to 10500

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.209 resverr

resverr

Syntax **resverr** [**detail**]
no resverr

Context **[Tree]** (debug>router>gmpls>packet resverr)

Full Context debug router gmpls packet resverr

Description This command enables debugging for GMPLS ResvErr packets.

The **no** form of the command disables debugging for GMPLS ResvErr packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

resverr

Syntax **resverr** [**detail**]
no resverr

Context **[Tree]** (debug>router>rsvp>packet resverr)

Full Context debug router rsvp packet resverr

Description This command debugs ResvErr packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about ResvErr packets.

Platforms All

22.210 resvtear

resvtear

Syntax **resvtear** [**detail**]
no resvtear

Context **[Tree]** (debug>router>gmpls>packet resvtear)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router gmpls packet resvtear

Description This command enables debugging for GMPLS ResvTear packets.

The **no** form of the command disables debugging for GMPLS ResvTear packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

resvtear

Syntax **resvtear** [**detail**]
no resvtear

Context **[Tree]** (debug>router>rsvp>packet resvtear)

Full Context debug router rsvp packet resvtear

Description This command debugs ResvTear packets.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about ResvTear packets.

Platforms All

22.211 ret

ret

Syntax **ret** *percent*

Context **[Tree]** (config>isa>video-group>watermark>bandwidth ret)
[Tree] (config>isa>video-group>watermark>session ret)

Full Context configure isa video-group watermark bandwidth ret
configure isa video-group watermark session ret

Description This command sets the watermark to trigger the SNMP trap if the RET bandwidth or session exceeds the configured percentage. The bandwidth is the available egress bandwidth of the ISA. The SNMP trap is cleared when the consumption is lowered by 10%. For example, if the system resource of the bandwidth available is 10 Gb/s and the watermark is configured to be 90%, the SNMP trap is raised as the bandwidth exceeds 9 Gb/s (90% of 10 Gb/s). The SNMP trap is cleared when the bandwidth drops below 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s). The default value of the watermark is set at 90% of the system resources for both bandwidth and session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default ret 90

Parameters *percent* — Specifies the percentage of the system resources per ISA.

Values 1 to 99

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.212 ret-session-timeout

ret-session-timeout

Syntax **ret-session-timeout** *seconds*
no ret-session-timeout

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if ret-session-timeout)

Full Context configure mcast-management multicast-info-policy video-policy video-interface ret-session-timeout

Description By default, the video ISA will wait for 5 minutes before closing the RTCP session from the subscriber. The RTCP session can be adjusted from 5 second to 5 minutes. The timeout is applicable to both RET and FCC RTCP sessions.

The **no** form of the command reverts to the default.

Default ret-session-timeout 300

Parameters *seconds* — Specifies the RET session timeout, in seconds.

Values 5 to 300

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.213 retail-service-id

retail-service-id

Syntax **retail-service-id** *service-id*
no retail-service-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host retail-service-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host retail-service-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt local-user-db ipoe host retail-service-id
configure subscriber-mgmt local-user-db ppp host retail-service-id

Description This command indicates the service ID of the retailer VPRN service to which this session belongs. If the value of this object is non-zero, the session belongs to a retailer VPRN.

The **no** form of this command removes the service ID from the configuration.

Parameters *service-id* — Specifies the retailer service ID or name.

Values
service-id: 1 to 2147483647
service-name: up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.214 retail-svc-id

retail-svc-id

Syntax **retail-svc-id** *service-id*
retail-svc-id

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host retail-svc-id)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host retail-svc-id)

Full Context configure service ies subscriber-interface group-interface sap static-host retail-svc-id
configure service vprn subscriber-interface group-interface sap static-host retail-svc-id

Description This command specifies the service id of the retailer IES/VPRN service to which the static IPv6 host belongs. A corresponding retailer subscriber interface must exist in the specified service.

The **no** form of this command reverts to the default.

Parameters *service-id* — Specifies the retailer service ID or retailer service name.

Values *service-id*: 1 to 2148007978
svc-name: A string up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retail-svc-id

Syntax **retail-svc-id** *service-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no retail-svc-id

Context [Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range retail-svc-id)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range retail-svc-id)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range retail-svc-id
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range retail-svc-id

Description This command configures the retailer service.

Parameters *service-id* — Specifies the identifier of the retail service.

Values 1 to 2147483650
svc-name: up to 64 characters

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.215 retransmission-interval

retransmission-interval

Syntax **retransmission-interval** *milliseconds*

Context [Tree] (config>router>lmp>peer retransmission-interval)

Full Context configure router lmp peer retransmission-interval

Description This command specifies the interval between resubmitted LMP messages.

Default retransmission-interval 500

Parameters *milliseconds* — Specifies the retransmission interval, in ms.

Values 10 to 60000

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.216 retransmit-interval

retransmit-interval

Syntax **retransmit-interval** *seconds*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no retransmit-interval

Context [Tree] (config>service>vpls>sap>spb retransmit-interval)
[Tree] (config>service>vpls>spoke-sdp>spb retransmit-interval)

Full Context configure service vpls sap spb retransmit-interval
configure service vpls spoke-sdp spb retransmit-interval

Description This command configures the minimum time between LSP PDU retransmissions on a point-to-point interface. This command is valid only for interfaces on control B-VPLS.

The no form of this command reverts to the default value.

Default retransmit-interval 5

Parameters *seconds* — The interval in seconds that SPB IS-IS LSPs can be sent on the interface.

Values 1 to 65535

Platforms All

retransmit-interval

Syntax **retransmit-interval** *seconds*
no retransmit-interval

Context [Tree] (config>service>vpls>sap>spb retransmit-interval)
[Tree] (config>service>vpls>spoke-sdp>spb retransmit-interval)

Full Context configure service vpls sap spb retransmit-interval
configure service vpls spoke-sdp spb retransmit-interval

Description This command configures the minimum time between LSP PDU retransmissions on a point-to-point interface.

The **no** form of this command reverts to the default value.

Default retransmit-interval 100

Parameters *seconds* — Specifies the interval in seconds that IS-IS LSPs can be sent on the interface

Values 1 to 65535

Platforms All

retransmit-interval

Syntax **retransmit-interval** *seconds*
no retransmit-interval

Context [Tree] (config>service>vprn>isis>if retransmit-interval)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn isis interface retransmit-interval

Description This command configures the minimum time between LSP PDU retransmissions on a point-to-point interface.

The **no** form of this command reverts to the default value.

Default retransmit-interval 5

Parameters *seconds* — Specifies the interval in seconds that IS-IS LSPs can be sent on the interface
1 to 65535.

Platforms All

retransmit-interval

Syntax **retransmit-interval** *seconds*
no retransmit-interval

Context **[Tree]** (config>service>vprn>ospf>area>if retransmit-interval)
[Tree] (config>service>vprn>ospf>area>virtual-link retransmit-interval)
[Tree] (config>service>vprn>ospf3>area>if retransmit-interval)
[Tree] (config>service>vprn>ospf3>area>virtual-link retransmit-interval)
[Tree] (config>service>vprn>ospf>area>sham-link retransmit-interval)

Full Context configure service vprn ospf area interface retransmit-interval
configure service vprn ospf area sham-link retransmit-interval
configure service vprn ospf area virtual-link retransmit-interval
configure service vprn ospf3 area interface retransmit-interval
configure service vprn ospf3 area virtual-link retransmit-interval

Description This command specifies the length of time, in seconds, that OSPF will wait before retransmitting an unacknowledged link state advertisement (LSA) to an OSPF neighbor.

The value should be longer than the expected round trip delay between any two routers on the attached network. Once the retransmit interval expires and no acknowledgment is received, the LSA is retransmitted.

The **no** form of this command reverts to the default interval.

Default retransmit-interval 5

Parameters *seconds* — The retransmit interval in seconds expressed as a decimal integer.

Values 1 to 3600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

retransmit-interval

Syntax **retransmit-interval** *seconds*
no retransmit-interval

Context **[Tree]** (config>router>isis>interface retransmit-interval)

Full Context configure router isis interface retransmit-interval

Description This command configures the minimum time between LSP PDU retransmissions on a point-to-point interface.

The **no** form of this command reverts to the default value.

Default retransmit-interval 5

Parameters *seconds* — Specifies the interval, in seconds, that IS-IS LSPs can be sent on the interface.

Values 1 to 65535

Platforms All

retransmit-interval

Syntax **retransmit-interval** *seconds*
no retransmit-interval

Context **[Tree]** (config>router>ospf>area>interface retransmit-interval)
[Tree] (config>router>ospf>area>virtual-link retransmit-interval)
[Tree] (config>router>ospf3>area>interface retransmit-interval)
[Tree] (config>router>ospf3>area>virtual-link retransmit-interval)

Full Context configure router ospf area interface retransmit-interval
configure router ospf area virtual-link retransmit-interval
configure router ospf3 area interface retransmit-interval
configure router ospf3 area virtual-link retransmit-interval

Description This command specifies the length of time, in seconds, that OSPF will wait before retransmitting an unacknowledged link state advertisement (LSA) to an OSPF neighbor.

The value should be longer than the expected round trip delay between any two routers on the attached network. After the retransmit-interval expires and no acknowledgment has been received, the LSA will be retransmitted.

The **no** form of this command reverts to the default interval.

Default retransmit-interval 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the retransmit interval in seconds expressed as a decimal integer.

Values 1 to 1800

Platforms All

22.217 retransmit-time

retransmit-time

Syntax **retransmit-time** *milli-seconds*
no retransmit-time

Context **[Tree]** (config>router>router-advert>if retransmit-time)
[Tree] (config>service>ies>sub-if>ipv6>rtr-adv retransmit-time)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv retransmit-time)
[Tree] (config>service>vprn>router-advert>if retransmit-time)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv retransmit-time)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv retransmit-time)
[Tree] (config>subscr-mgmt>rtr-adv-plcy retransmit-time)

Full Context configure router router-advertisement interface retransmit-time
configure service ies subscriber-interface group-interface ipv6 router-advertisements retransmit-time
configure service ies subscriber-interface ipv6 router-advertisements retransmit-time
configure service vprn router-advertisement interface retransmit-time
configure service vprn subscriber-interface group-interface ipv6 router-advertisements retransmit-time
configure service vprn subscriber-interface ipv6 router-advertisements retransmit-time
configure subscriber-mgmt router-advertisement-policy retransmit-time

Description This command configures the value to be placed in the retransmit timer field in router advertisements sent from this interface.

The **no** form of this command reverts to the default.

Default retransmit-time 0

Parameters *milli-seconds* — Specifies the retransmit time, in milli-seconds, for advertisement from this group-interface.

Values 0 to 1800000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt router-advertisement-policy retransmit-time
- configure service vprn subscriber-interface group-interface ipv6 router-advertisements retransmit-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies subscriber-interface group-interface ipv6 router-advertisements retransmit-time
- configure service ies subscriber-interface ipv6 router-advertisements retransmit-time
- configure service vprn subscriber-interface ipv6 router-advertisements retransmit-time

All

- configure router router-advertisement interface retransmit-time
- configure service vprn router-advertisement interface retransmit-time

22.218 retries

retries

Syntax **retries** *number*
no retries

Context **[Tree]** (config>subscr-mgmt>pfcp-association>heartbeat retries)

Full Context configure subscriber-mgmt pfcp-association heartbeat retries

Description This command configures the number of times the same Heartbeat Request message is sent before the PFCP path to the peer is considered down.

The **no** form of this command reverts to the default value.

Default retries 4

Parameters *number* — Specifies the number of times the same Heartbeat Request message is sent. This value should be identical on both the BNG UPF and CPF. For information about the BNG CUPS CPF configuration, refer to the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide*.

Values 1 to 15

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retries

Syntax **retries** *number*
no retries

Context **[Tree]** (config>subscr-mgmt>pfcp-association>tx retries)

Full Context configure subscriber-mgmt pfcp-association tx retries

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the number of times a message is retried before the message is considered lost. This retry number is also known as N1.

The **no** form of this command reverts to the default value.

Default retries 3

Parameters *number* — Specifies the number of times a message is retried.

This value should be identical on both the BNG UPF and CPF. For information about the BNG CUPS CPF configuration, refer to the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide*.

Values 1 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retries

Syntax **retries** *count*
no retries

Context **[Tree]** (config>system>grpc>tcp-keepalive retries)

Full Context configure system grpc tcp-keepalive retries

Description This command configures the number of TCP keepalive probes sent by the router that must be unacknowledged before the connection is closed.

The **no** form of this command reverts to the default value.

Default retries 4

Parameters *count* — Specifies the number of missed keep-alives before the TCP connection is declared down.

Values 3 to 100

Default 4

Platforms All

retries

Syntax **retries** *count*
no retries

Context **[Tree]** (config>system>grpc-tunnel>destination-group>tcp-keepalive retries)
[Tree] (config>system>telemetry>destination-group>tcp-keepalive retries)

Full Context configure system grpc-tunnel destination-group tcp-keepalive retries

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure system telemetry destination-group tcp-keepalive retries

Description This command configures the number of missed TCP keepalive probes before the TCP connection is closed and attempts are made to reach other destinations within the same destination group.

The **no** form of this command reverts to the default value.

Default retries 4

Parameters *count* — Specifies the number of missed keep-alives before the TCP connection is declared down.

Values 3 to 100

Default 4

Platforms All

22.219 retry

retry

Syntax **retry** *count*

Context **[Tree]** (config>aaa>l2tp-acct-plcy>radius-acct-server retry)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server retry

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication.

Note: The retry count includes the first attempt.

The **no** form of this command reverts to the default value.

Default retry 3 (the initial attempt as well as two retried attempts)

Parameters *count* — Specifies the retry count.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

retry

Syntax **retry** *count*

Context **[Tree]** (config>app-assure>rad-acct-plcy>server retry)

Full Context configure application-assurance radius-accounting-policy radius-accounting-server retry

Description This command configures the number of times the router attempts to contact the RADIUS accounting server if a response to the initial message is not received.

The **no** form of this command reverts to the default value.

Default retry 3

Parameters *count* — Specifies the retry count.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

retry

Syntax **retry** *count*
no retry

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server retry)
[Tree] (config>subscr-mgmt>acct-plcy>server retry)

Full Context configure subscriber-mgmt radius-accounting-policy radius-accounting-server retry
configure subscriber-mgmt authentication-policy radius-authentication-server retry

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication or accounting, if not successful the first time.

The **no** form of this command reverts to the default value.

Default retry 3

Parameters *count* — Specifies the retry count.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retry

Syntax **retry** *count*
no retry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>aaa>radius-srv-plcy>servers retry)

Full Context configure aaa radius-server-policy servers retry

Description This command configures the number of times the router attempts to contact the RADIUS server, if not successful the first time.

The **no** form of this command reverts to the default.

Default retry 3

Parameters *count* — Specifies the number of times a signaling request message is transmitted towards the same peer.

Values 1 to 256

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retry

Syntax **retry** *minutes*
no retry

Context [Tree] (config>service>vpls>bgp-evpn>mac-duplication retry)

Full Context configure service vpls bgp-evpn mac-duplication retry

Description Specifies the timer after which the MAC in hold-down state is automatically flushed and the mac-duplication process starts again. This value is expected to be equal to two times or more than that of window.

If **no** retry is configured, this implies that, when mac-duplication is detected, MAC updates for that MAC will be held down till the user intervenes or a network event (that flushes the MAC) occurs.

Default retry 9

Parameters *minutes* — Specifies the BGP EVPN MAC duplication retry in minutes.

Values 2 to 60

Platforms All

retry

Syntax **retry** *count*
no retry

Context [Tree] (config>service>vprn>aaa>remote-servers>radius retry)

Full Context configure service vprn aaa remote-servers radius retry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

The **no** form of this command reverts to the default value.

Default retry 3

Parameters *count* — Specifies the retry count.

Values 1 to 10

Platforms All

retry

Syntax **retry** *count*
no retry

Context **[Tree]** (config>system>file-trans-prof retry)

Full Context configure system file-transmission-profile retry

Description This command specifies the number of retries on transport protocol level.

When the virtual router does not receive any data from a server (e.g., FTP or HTTP server) after the configured **timeout** *seconds*, the router may repeat the request to the server. The number of retries specifies the maximum number of repeated requests.

The **no** form of this command disables the retry.

Default no retry

Parameters *count* — Specifies the number of retries.

Values 1 to 256

Platforms All

retry

Syntax **retry** *count*

Context **[Tree]** (config>aaa>isa-radius-plcy>servers retry)

Full Context configure aaa isa-radius-policy servers retry

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.

The **no** form of the command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default retry 3

Parameters *count* — Specifies the retry count.

Values 1 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

retry

Syntax **retry** *count*
no retry

Context **[Tree]** (config>system>security>radius retry)
[Tree] (config>system>security>dot1x>radius-plcy retry)

Full Context configure system security dot1x radius-plcy retry
configure system security radius retry

Description This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.

The **no** form of this command reverts to the default value.

Default retry 3

Parameters *count* — Specifies the retry count.

Values 1 to 10

Platforms All

retry

Syntax **retry** *count*
no retry

Context **[Tree]** (config>system>security>ldap retry)

Full Context configure system security ldap retry

Description This command configures the number of retries for the SR OS in its attempt to reach the current LDAP server before attempting the next server.

The **no** form of this command reverts to the default value.

Default retry 3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the number of retransmissions.

Values 1 to 10

Default 3

Platforms All

22.220 retry-count

retry-count

Syntax **retry-count** [*count*]
no retry-count

Context **[Tree]** (config>subscr-mgmt>shcv-policy>periodic retry-count)

Full Context configure subscriber-mgmt shcv-policy periodic retry-count

Description This command configures the number of retransmissions.

The **no** form of this command reverts to the default.

Default retry-count 1 — For trigger-type ip-conflict, host-limit-exceeded and mobility

retry-count 10 — For trigger-type inactivity and MAC learning

Parameters *count* — Specifies the number of retransmissions in periodic connectivity verification.

Values 2 to 29

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retry-count

Syntax **retry-count** [*count*]
no retry-count

Context **[Tree]** (config>subscr-mgmt>shcv-policy>trigger retry-count)

Full Context configure subscriber-mgmt shcv-policy trigger retry-count

Description This command configures the number of retransmissions in periodic connectivity verification.

The **no** form of this command reverts to the default.

Default retry-count 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *count* — Specifies the number of retransmissions in periodic connectivity verification.

Values 1 to 29

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retry-count

Syntax **retry-count** *retry-count*
no retry-count

Context **[Tree]** (config>service>epipe>spoke-sdp-fec retry-count)

Full Context configure service epipe spoke-sdp-fec retry-count

Description This optional command specifies the number of attempts software should make to reestablish the spoke SDP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the spoke-sdp is put into the shutdown state.

Use the no shutdown command to bring up the path after the retry limit is exceeded.

The **no** form of this command reverts the parameter to the default value.

Default retry-count 30

Parameters *retry-count* — The maximum number of retries before putting the spoke-sdp into the shutdown state.

Values 10 to 10000

Platforms All

retry-count

Syntax **retry-count** *retry-count*
no retry-count

Context **[Tree]** (config>test-oam>ldp-treetrace>path-discovery retry-count)
[Tree] (config>test-oam>ldp-treetrace>path-probing retry-count)

Full Context configure test-oam ldp-treetrace path-discovery retry-count
configure test-oam ldp-treetrace path-probing retry-count

Description In the path discovery phase of the LDP tree trace feature, this command configures the number of retransmissions of an LSP trace message to discover the path of an LDP FEC when no response is received within the **timeout** parameter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In the path-probing phase of the LDP tree trace, this command configures the number of retransmissions of an LSP ping message to probe the path of an LDP FEC when no response is received within the **timeout** parameter.

The **no** form of this command resets the retry count to its default value.

Default no retry-count

Parameters *retry-count* — Specifies the maximum number of consecutive time outs allowed before failing a path probe (ping).

Platforms All

retry-count

Syntax **retry-count** [*count*]
no retry-count

Context **[Tree]** (config>service>pw-routing retry-count)

Full Context configure service pw-routing retry-count

Description This optional command specifies the number of attempts software should make to re-establish the spoke SDP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the spoke SDP is put into the shutdown state.

Use the **no shutdown** command to bring up the path after the retry limit is exceeded.

The **no** form of this command reverts the parameter to the default value.

Default no retry-count

Parameters *count* — Specifies the maximum number of retries before putting the spoke SDP into the shutdown state.

Values 10 to 10000

Platforms All

22.221 retry-down

retry-down

Syntax **retry-down** *retries*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no retry-down

Context **[Tree]** (config>system>atm>oam retry-down)

Full Context configure system atm oam retry-down

Description This command specifies the number of OAM loopback attempts that must fail after the periodic attempt before the endpoint will transition to AIS-LOC state.

The retry values are configured on a system wide basis and are affective on the next period cycle of any ATM VC SAP using **periodic-loopback**, if changed. The timeout for receiving a loopback response from the remote peer and declaring the loopback failed is 1 second and is not configurable.

Default no retry-down

Parameters *retries* — Specifies the number of failed loopback attempts before an ATM VC goes down.

Values 0 to 10 (A zero value means that the endpoint will transition to AIS-LOC state immediately if the periodic loopback attempt fails.)

Default 4

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

22.222 retry-interval

retry-interval

Syntax **retry-interval min** *minimum* **max** *maximum*
no retry-interval

Context **[Tree]** (config>aaa>route-downloader retry-interval)

Full Context configure aaa route-downloader retry-interval

Description This command sets the duration, in minutes, of the retry interval. The retry interval is the interval meant for the system to retry sending an Access Request message after the previous one was unanswered (not with an access reject but rather just a RADIUS failure or ICMP port unreachable). This timer is actually an exponential backoff timer that starts at **min** and is capped at **max** minutes.

The **no** form of this command reverts to the default values.

Default retry-interval min 10 max 20

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **min** *minimum* — Specifies the duration, in minutes, of the retry interval. This duration grows exponentially after each sequential failure.

Values 1 to 1440

max *maximum* — Specifies the maximum duration, in minutes, of the retry interval.

Values 1 to 1440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retry-interval

Syntax **retry-interval** *milliseconds*
no retry-interval

Context **[Tree]** (config>router>wpp>portals>portal retry-interval)
[Tree] (config>service>vprn>wpp>portals>portal retry-interval)

Full Context configure router wpp portals portal retry-interval
configure service vprn wpp portals portal retry-interval

Description This command configures the time interval between two consecutive retransmissions

The **no** form of this command reverts to the default.

Default retry-interval 2000

Parameters *milliseconds* — Specifies the time interval between two consecutive retransmissions.

Values 10 to 2000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

retry-interval

Syntax **retry-interval** *seconds*
no retry-interval

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update retry-interval)

Full Context configure system security pki ca-profile auto-crl-update retry-interval

Description This command specifies the interval, in seconds, that the system waits before retrying the configured **url-entry** list when **schedule-type** is **next-update-based** and none of the URLs return a qualified CRL.

The **no** form of this command causes the system to retry immediately without waiting.

Default retry-interval 3600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies an interval, in seconds, before retrying to update the CRL.

Values 1 to 31622400

Platforms All

22.223 retry-limit

retry-limit

Syntax **retry-limit** *count*
no retry-limit

Context **[Tree]** (config>port>ml-bundle>mlfr retry-limit)

Full Context configure port multilink-bundle mlfr retry-limit

Description This command specifies the value of the MLFR bundle N_RETRY counter.

The counter specifies the number of times a retransmission onto a bundle link will be attempted before an error is declared and the appropriate action taken.

Default retry-limit 2

Parameters *count* — Specifies the number of retransmission attempts.

Values 1 to 5

Platforms 7450 ESS, 7750 SR-7/12/12e

retry-limit

Syntax **retry-limit** *limit*
no retry-limit

Context **[Tree]** (config>router>lmp>peer retry-limit)

Full Context configure router lmp peer retry-limit

Description This command specifies how many times LMP resends a message before restarting the process.

Default no retry-limit

Parameters *limit* — Specifies the number of reattempts.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

retry-limit

Syntax **retry-limit** *retry-limit*
no retry-limit

Context **[Tree]** (config>router>gmpls>lsp retry-limit)

Full Context configure router gmpls lsp retry-limit

Description This optional command specifies the number of attempts software should make to re-establish the GMPLS LSP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the GMPLS LSP path is put into the **shutdown** state.

Use the **config router gmpls lsp** *lsp-name* **no shutdown** command to bring up the path after the retry limit is exceeded.

Default retry-limit 0 (no limit, retries forever)

Parameters *retry-limit* — Specifies the number of retries.

Values 0 to 10000

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

retry-limit

Syntax **retry-limit** *number*
no retry-limit

Context **[Tree]** (config>router>mpls>lsp retry-limit)
[Tree] (config>router>mpls>lsp-template retry-limit)

Full Context configure router mpls lsp retry-limit
configure router mpls lsp-template retry-limit

Description This optional command specifies the number of attempts software should make to re-establish the LSP after it has failed LSP. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the LSP path is put into the **shutdown** state.

Use the config router **mpls lsp** *lsp-name* **no shutdown** command to bring up the path after the retry-limit is exceeded.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For P2MP LSP that are created based on the LSP template, all S2Ls must attempt to retry-limit before the client application is informed of failure.

The **no** form of this command reverts to the default value.

Default retry-limit 0 (no limit, retries forever)

Parameters *number* — Specifies the number of times software will attempt to re-establish the LSP after it has failed. Allowed values are integers in the range of 0 to 10000.

Values 0 to 10000

Platforms All

22.224 retry-on-igp-overload

retry-on-igp-overload

Syntax [**no**] **retry-on-igp-overload**

Context **[Tree]** (config>router>mpls retry-on-igp-overload)

Full Context configure router mpls retry-on-igp-overload

Description This command allows for the global configuration of the handling in the ingress LER of the LSP paths which transit an LSR that advertised the IS-IS overload bit.

By default, MPLS re-optimizes using make-before-break (MBB) the transit paths away from the node in an IS-IS overload state only at the time a manual or timer-based re-signal is performed for the LSP paths. MPLS will not act immediately on the receipt of the IS-IS overload bit.

When this command is enabled, MPLS in the ingress LER immediately tears down and re-signals all LSP paths away from a transit LSR node which advertised the IS-IS overload bit.

LSP paths that terminate on the node that advertised the IS-IS overload bit are not acted on whether this command is enabled or disabled.

The **no** form of this command returns to the default behavior.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.225 retry-timeout

retry-timeout

Syntax **retry-timeout** *timer*
no retry-timeout

Context **[Tree]** (config>port>ethernet>dwl retry-timeout)

Full Context configure port ethernet down-when-looped retry-timeout

Description This command configures the minimum wait time before re-enabling port after loop detection.

Default no retry-timeout

Parameters *timer* — Specifies the minimum wait time before re-enabling port after loop detection.

Values 0, 10 to 160

Platforms All

retry-timeout

Syntax **retry-timeout** *timeout*
no retry-timeout

Context **[Tree]** (config>service>vpls>mac-move retry-timeout)
[Tree] (config>service>template>vpls-template>mac-move retry-timeout)

Full Context configure service template vpls-template mac-move retry-timeout
configure service vpls mac-move retry-timeout

Description This indicates the time in seconds to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled.

It is recommended that the retry-timeout value is larger or equal to 5s * cumulative factor of the highest priority port so that the sequential order of port blocking will not be disturbed by re-initializing lower priority ports.

A zero value indicates that the SAP will not be automatically re-enabled after being disabled. If, after the SAP is re-enabled it is disabled again, the retry timeout is increased with the provisioned retry timeout in order to avoid thrashing. For example, when retry-timeout is set to 15, it increments (15,30,45,60...).

The **no** form of this command reverts to the default value.

Default retry-timeout 10 (when mac-move is enabled)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *timeout* — Specifies the time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled.

Values 0 to 120

Platforms All

22.226 retry-timer

retry-timer

Syntax **retry-timer** *retry-timer*
no retry-timer

Context **[Tree]** (config>service>epipe>spoke-sdp-fec retry-timer)

Full Context configure service epipe spoke-sdp-fec retry-timer

Description This command specifies a retry-timer for the spoke SDP. This is a configurable exponential back-off timer that determines the interval between retries to reestablish a spoke SDP if it fails and a label withdraw message is received with the status code “AII unreachable”.

The **no** form of this command reverts the timer to its default value.

Default retry-timer 30

Parameters *retry-timer* — The initial retry-timer value in seconds.

Values 10 to 480

Platforms All

retry-timer

Syntax **retry-timer** *seconds*
no retry-timer

Context **[Tree]** (config>router>gmpls>lsp retry-timer)

Full Context configure router gmpls lsp retry-timer

Description This command configures the time (in s), for LSP re-establishment attempts after it has failed. The retry time is jittered to +/- 25% of its nominal value.

The **no** form of this command resets the parameter to the default value.

Default retry-timer 30

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the amount of time (in s), between attempts to re-establish the LSP after it has failed.

Values 1 to 600 s

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

retry-timer

Syntax **retry-timer** *seconds*
no retry-timer

Context **[Tree]** (config>router>mpls>lsp retry-timer)
[Tree] (config>router>mpls>lsp-template retry-timer)

Full Context configure router mpls lsp retry-timer
configure router mpls lsp-template retry-timer

Description This command configures the time (in s), for LSP re-establishment attempts after it has failed. The retry time is jittered to +/- 25% of its nominal value.

For P2MP LSP created based on LSP template, all S2Ls must attempt to retry-limit before client application is informed of failure.

The **no** form of this command reverts to the default value.

Default retry-timer 30

Parameters *seconds* — Specifies the amount of time (in s), between attempts to re-establish the LSP after it has failed. Allowed values are integers in the range of 1 to 600.

Values 1 to 600

Platforms All

retry-timer

Syntax **retry-timer** *secs*
no retry-timer

Context **[Tree]** (config>service>pw-routing retry-timer)

Full Context configure service pw-routing retry-timer

Description This command configures a retry-timer for the spoke-SDP. This is a configurable exponential back-off timer that determines the interval between retries to re-establish a spoke-SDP if it fails and a label withdraw message is received with the status code “AII unreachable”.

The **no** form of this command reverts the timer to its default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no retry-timer

Parameters *secs* — Specifies initial retry-timer value in seconds.

Values 10 to 480

Platforms All

22.227 retry-up

retry-up

Syntax **retry-up** *retries*
no retry-up

Context **[Tree]** (config>system>atm>oam retry-up)

Full Context configure system atm oam retry-up

Description This command specifies the number of consecutive OAM loopback attempts that must succeed after the periodic attempt before the endpoint will transition the state to up.

Default no retry-up

Parameters *retries* — Specifies the number of successful loopback replies before an ATM VC goes up.

Values 0 to 10 (A zero value means that the endpoint will transition to the up state immediately if the periodic loopback attempt succeeds.)

Default 2

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

22.228 return-path-label

return-path-label

Syntax **return-path-label** *label-value*
no return-path-label

Context **[Tree]** (config>router>mpls>lsp>bfd return-path-label)
[Tree] (config>router>mpls>lsp>primary>bfd return-path-label)
[Tree] (config>router>mpls>lsp>sec>bfd return-path-label)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>mpls>lsp-template>bfd return-path-label)

Full Context configure router mpls lsp bfd return-path-label
configure router mpls lsp primary bfd return-path-label
configure router mpls lsp secondary bfd return-path-label
configure router mpls lsp-template bfd return-path-label

Description This command configures the Seamless Bidirectional Forwarding Detection (S-BFD) session to echo mode and adds an additional MPLS label, referring to an MPLS-labeled reply path for the S-BFD packet, to the bottom of the label stack for the S-BFD packet.

The command applies to the initiator of the S-BFD sessions. The return path label may be a binding SID for an SR policy or other MPLS path configured on the reflector router. Instead of being routed through the IGP path, the S-BFD packet returns to the initiator through this MPLS return path.

The **no** form of this command disables the controlled return path label and echo mode for S-BFD. S-BFD returns to asynchronous mode and the initiator node does not push a return path label. Any S-BFD packets for this LSP or path that the reflector receives are sent back using a routed return path.

Default no return-path-label

Parameters *label-value* — Specifies the label value.

Values 32 to 1048512

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.229 reuse

reuse

Syntax **reuse** *integer*
no reuse

Context **[Tree]** (config>router>policy-options>damping reuse)

Full Context configure router policy-options damping reuse

Description This command configures the reuse parameter for the route damping profile.

When the Figure of Merit (FoM) value falls below the **reuse** threshold, the route is once again considered valid and can be reused or included in route advertisements.

The **no** form of this command removes the reuse parameter from the damping profile.

Default no reuse

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *integer* — Specifies the reuse value expressed as a decimal integer.

Values 1 to 20000

Platforms All

22.230 reuse-ext-ip

reuse-ext-ip

Syntax [**no**] **reuse-ext-ip**

Context **[Tree]** (config>service>nat>pcp-server-policy reuse-ext-ip)

Full Context configure service nat pcp-server-policy reuse-ext-ip

Description This command enables the system to reuse the external IP address assigned to a subscriber when the requested well-known port or external IP mapping is not available.

The **no** form of this command causes a request for a well-known port to be allocated exactly as requested but on a different external IP address from the one that the subscriber is already using. This occurs if the requested well-known port is already allocated to another subscriber which is sharing the same external IP address. The existing external IP address is initially allocated to the subscriber by the virtue of initial traffic flow.

Default no reuse-ext-ip

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.231 reverse-path

reverse-path

Syntax [**no**] **reverse-path**

Context **[Tree]** (config>router>mpls>mpls-tp>transit-path reverse-path)

Full Context configure router mpls mpls-tp transit-path reverse-path

Description This command enables the reverse path of an MPLS-TP reverse path to be created or edited.

The reverse path must be created after the forward path.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the reverse path. The reverse path must be removed before the forward path.

Default no reverse-path

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.232 revert

revert

Syntax **revert** {**latest-rb**| *checkpoint-id* | **rescue**} [**now**]

Context **[Tree]** (admin>rollback revert)

Full Context admin rollback revert

Description This command initiates a configuration rollback revert operation that will return the configuration state of the node to a previously saved checkpoint. The rollback revert minimizes impacts to running services. There are no impacts in areas of configuration that did not change since the checkpoint. Configuration parameters that changed (or items on which changed configuration have dependencies) are first removed (revert to default) and the previous values are then restored (can be briefly service impacting in changed areas).

Parameters **latest-rb** — Specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file).

checkpoint-id — Specifies the configuration to return to (which rollback checkpoint file to use). Checkpoint-id of 1 corresponds to the file-url.rb.1 rollback checkpoint file. The higher the id, the older the checkpoint. Max is the highest rollback checkpoint supported or configured.

Values 1 to 9

rescue — Specifies to revert to the rescue checkpoint.

now — Forces a rollback revert without any interactive confirmations (assumes 'y' for any confirmations that would have occurred).

Platforms All

revert

Syntax [**no**] **revert**

Context **[Tree]** (config>system>sync-if-timing revert)

Full Context configure system sync-if-timing revert

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the clock to revert to a higher priority reference if the current reference goes offline or becomes unstable. When the failed reference becomes operational, it is eligible for selection. When the mode is non-revertive, a failed clock source is not selected again.

Default no revert

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.233 revert-members

revert-members

Syntax **revert-members** [*1..8*]
no revert-members

Context **[Tree]** (config>service>vprn>isis>link-group>level revert-members)

Full Context configure service vprn isis link-group level revert-members

Description This command sets the threshold for the minimum number of operational links to return the associated link group to its normal operating state and remove the associated offsets to the IS-IS metrics. If the number of operational links is equal to or greater than the configured **revert-members** threshold, the configured offsets are removed.

The **no** form of this command reverts the threshold back to the default, which is equal to the **oper-members** threshold value.

Default no revert-members oper-members

Parameters *1..8* — Specifies the number of revert members.

Values 1 to 8

Platforms All

revert-members

Syntax **revert-members** [*1..8*]
no revert-members

Context **[Tree]** (config>router>isis>link-group>level revert-members)

Full Context configure router isis link-group level revert-members

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the threshold for the minimum number of operational links to return the associated link group to its normal operating state and remove the associated offsets to the IS-IS metrics. If the number of operational links is equal to or greater than the configured revert-member threshold then the configured offsets are removed.

The **no** form of this command reverts the threshold back to the default which is equal to the oper-member threshold value.

Default no revert-members oper-members

Parameters *1..8* — Specifies the threshold for revertive members.

Values 1 to 8

Platforms All

22.234 revert-time

revert-time

Syntax **revert-time** *minutes*
no revert-time

Context **[Tree]** (config>port>aps revert-time)

Full Context configure port aps revert-time

Description This command configures the revert-time timer to determine how long to wait before switching back to the working circuit after that circuit has been restored into service.

A change in the *minutes* value takes effect upon the next initiation of the wait to restore (WTR) timer. It does not modify the length of a WTR timer that has already been started. The WTR timer of a non-revertive switch can be assumed to be infinite.

The **no** form of this command restores the default (non-revertive mode).

Default The default is to not revert back unless the protect circuit fails or there is an operator intervention.

Parameters *minutes* — Specifies the time, in minutes, to wait before reverting back to the original working circuit after it has been restored into service.

Values 0 to 60 minutes

Default 5

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

revert-time

Syntax **revert-time** *time*
no revert-time

Context **[Tree]** (config>eth-tunnel revert-time)

Full Context configure eth-tunnel revert-time

Description This command configure how long to wait before switching back to the primary path after it has been restored to Ethernet tunnel.

The **no** form of this command disables the revert behavior, effectively setting the revert time to zero.

Default no revert-time

Parameters *time* — Specifies the re-activation delay, in seconds, for the primary path.

Values 1 to 720

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

revert-time

Syntax **revert-time** [*revert-time* | **infinite**]
no revert-time

Context **[Tree]** (config>service>apipe>endpoint revert-time)
[Tree] (config>service>cpipe>endpoint revert-time)
[Tree] (config>service>epipe>endpoint revert-time)
[Tree] (config>service>fpipe>endpoint revert-time)
[Tree] (config>service>ipipe>endpoint revert-time)

Full Context configure service apipe endpoint revert-time
configure service cpipe endpoint revert-time
configure service epipe endpoint revert-time
configure service fpipe endpoint revert-time
configure service ipipe endpoint revert-time

Description This command configures the time to wait before reverting back to the primary spoke SDP defined on this service endpoint, after having failed over to a backup spoke SDP.

Parameters *revert-time* — Specifies the time, in seconds, to wait before reverting to the primary SDP.

Values 0 to 600

Default 0

infinite — Causes the endpoint to be non-revertive.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service cpipe endpoint revert-time
- configure service fpipe endpoint revert-time

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe endpoint revert-time

All

- configure service ipipe endpoint revert-time
- configure service epipe endpoint revert-time

revert-time

Syntax **revert-time** *revert-time* | **infinite**
no revert-time

Context **[Tree]** (config>service>vpls>endpoint revert-time)

Full Context configure service vpls endpoint revert-time

Description This command configures the time to wait before reverting to primary spoke-SDP.

In a regular endpoint the revert-time setting affects just the pseudowire defined as primary (precedence 0). For a failure of the primary pseudowire followed by restoration the revert-timer is started. After it expires the primary pseudowire takes the active role in the endpoint. This behavior does not apply for the case when both pseudowires are defined as secondary. For example, if the active secondary pseudowire fails and is restored it will stay in standby until a configuration change or a force command occurs.

Parameters *revert-time* — Specifies the time to wait, in seconds, before reverting back to the primary spoke-SDP defined on this service endpoint, after having failed over to a backup spoke-SDP

Values 0 to 600

infinite — Specifying this keyword makes endpoint non-revertive

Platforms All

revert-time

Syntax **revert-time** {*revert-time* | **infinite**}
no revert-time

Context **[Tree]** (config>mirror>mirror-dest>endpoint revert-time)

Full Context configure mirror mirror-dest endpoint revert-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the time to wait before reverting to the primary spoke SDP. This command has an effect only when used in conjunction with an endpoint which contains a SDP of type 'primary'. It is ignored and has no effect in all other cases. The revert-timer is the delay in seconds the system waits before it switches the path of the mirror service from an active secondary SDP in the endpoint into the endpoint primary SDP after the latter comes back up.

The **no** form of this command resets the timer to the default value of 0. This means that the mirror-service path is switched back to the endpoint primary sdp immediately after it comes back up.

Parameters *revert-time* — Specifies a delay, in seconds, the system waits before it switches the path of the mirror service from an active secondary SDP in the endpoint into the endpoint primary SDP after the latter comes back up.

Values 0 to 600

infinite — Forces the mirror or LI service path to never revert to the primary SDP as long as the currently active secondary SDP is UP.

Platforms All

revert-time

Syntax **revert-time** {*revert-time* | **infinite**}
no revert-time

Context **[Tree]** (config>service>sdp>mixed-lsp-mode revert-time)

Full Context configure service sdp mixed-lsp-mode revert-time

Description This command configures the delay period the SDP must wait before it reverts to a higher priority LSP type when one becomes available.

The **no** form of the command resets the timer to the default value of 0. This means the SDP reverts immediately to a higher priority LSP type when one becomes available.

Default no revert-time

Parameters *revert-time* — Specifies the delay period, in seconds, that the SDP must wait before it reverts to a higher priority LSP type when one becomes available. A value of zero means the SDP reverts immediately to a higher priority LSP type when one becomes available.

Values 0 to 600

infinite — This keyword forces the SDP to never revert to another higher priority LSP type unless the currently active LSP type is down.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

revert-time

Syntax **revert-time** *time*
no revert-time

Context **[Tree]** (config>eth-ring revert-time)

Full Context configure eth-ring revert-time

Description This command configures the revert time for an Eth-Ring. It ranges from 60 seconds to 720 second by 1 second intervals.

The **no** form of this command means non-revertive mode and revert time is essentially 0, and the revert timers are not set.

Default revert-time 300

Parameters *time* — Specifies the guard-time, in seconds.

Values 60 to 720

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.235 revert-timer

revert-timer

Syntax **revert-timer** *seconds*
no revert-timer

Context **[Tree]** (config>router>gmpls>lsp revert-timer)

Full Context configure router gmpls lsp revert-timer

Description This command configures the time (in s), for LSP reversion attempts after it has failed.

The **no** form of the command resets the timer to the default value.

Default revert-timer 0

Parameters *seconds* — Specifies the time (in s), for the LSP to attempt reversion after failure.

Values 0 to 1800

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

revert-timer

Syntax **revert-timer** *timer-value*
no revert-timer

Context **[Tree]** (config>router>mpls>lsp revert-timer)

Full Context configure router mpls lsp revert-timer

Description This command configures a revert timer on an LSP. The timer starts when the LSP primary path recovers from a failure. The LSP reverts from a secondary path to the primary path when the timer expires, or when the secondary path fails.

The **no** form of this command cancels any currently outstanding revert timer. If the LSP is up when a no revert-timer is issued, the LSP will revert to the primary path. Otherwise the LSP reverts when the primary path is restored.

Default no revert-timer

Parameters *timer-value* — Specifies the amount of time, in one minute increments, between attempts to re-establish the LSP after it has failed. Allowed values are integers in the range of 0 to 4320.

Values 0 to 4320

Platforms All

revert-timer

Syntax **revert-timer** *seconds*
no revert-timer

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy revert-timer)

Full Context configure router mpls forwarding-policies forwarding-policy revert-timer

Description This command configures the revert timer in an MPLS forwarding policy.

When the primary direct or indirect next hop is restored and is added back into the routing table, CPM waits for an amount of time equal to the user-programmed revert timer before activating it and updating the data path. However, if the backup direct or indirect next hop fails while the timer is running, CPM activates it and updates the data path immediately.

A value of 0 disables the revert timer; meaning the policy reverts immediately.

The **no** form of this command removes the revert timer from the MPLS forwarding policy.

Default revert-timer 0

Parameters *seconds* — Specifies the revert-timer value, in number of seconds.

Values 0 to 600

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

revert-timer

Syntax **revert-timer** *revert-timer*
no revert-timer

Context **[Tree]** (config>router>segment-routing>maintenance-policy revert-timer)

Full Context configure router segment-routing maintenance-policy revert-timer

Description This command configures the revert timer for SR Policy candidate paths.

The revert timer is started when the primary path (for example, the best preference programmed candidate path) recovers (for example, after the number of S-BFD sessions that are up is ≥ **threshold** and the **hold-down-timer** has expired) and switches back when the timer expires.

The **no** form of this command removes the revert timer from the SR policy.

Default no revert-timer

Parameters *revert-timer* — Specifies the revert timer, in minutes.

Values 1 to 4320

Platforms All

22.236 revertive

revertive

Syntax [**no**] **revertive**

Context **[Tree]** (config>router>mpls>mpls-tp>protection-template revertive)

Full Context configure router mpls mpls-tp protection-template revertive

Description This command configured revertive behavior for MPLS-TP linear protection. The protect-tp-path MEP must be in the shutdown state for of the MPLS-TP LSPs referencing this protection template in order to change the revertive parameter.

Default revertive

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.237 revertive-timer

revertive-timer

Syntax **revertive-timer** *sec*
no revertive-timer

Context [Tree] (config>service>vprn>mvpn>pt>inclusive>umh-rm revertive-timer)
[Tree] (config>service>vprn>mvpn>pt>selective>umh-rm>group>source revertive-timer)

Full Context configure service vprn mvpn provider-tunnel inclusive umh-rate-monitoring revertive-timer
configure service vprn mvpn provider-tunnel selective umh-rate-monitoring group source revertive-timer

Description This command configures the timer value (in seconds) after which to revert to the primary UMH after traffic is restored. This value must account for the traffic flapping from the primary UMH. If there is traffic flapping, the timer resets and starts over.

The **no** form of the command means that there is no revertive behavior.

Default no revertive-timer

Parameters *sec* — Specifies the timer value (in seconds).

Values 1 to 3600

Platforms All

22.238 revocation-check

revocation-check

Syntax **revocation-check** {**crl** | **crl-optional**}

Context [Tree] (config>system>security>pki>ca-profile revocation-check)

Full Context configure system security pki ca-profile revocation-check

Description This command specifies the revocation method system used to check the revocation status of certificate issued by the CA, the default value is **crl**, which will use CRL. But if it is **crl-optional**, then it means when the user disables the ca-profile, then the system will try to load the configured CRL (specified by the **crl-file** command). However, if the system fails to load it for following reasons, then the system still brings the ca-profile oper-up, but leaves the CRL as **non-exist**.

- CRL file does not exist

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- CRL is not properly encoded - maybe due to interrupted file transfer
- CRL does not match cert
- Wrong CRL version
- CRL expired

If the system needs to use the CRL of a specific ca-profile to check the revocation status of an end-entity cert, and the CRL is non-existent due to the above reasons, then the system will treat it as being unable to get an answer from CRL and fall back to the next status-verify method or default-result.

If the system needs to check the revocation of a CA cert in cert chain, and if the CRL is non-existent due to the above reasons, then the system will skip checking the revocation status of the CA cert. For example, if CA1 is issued by CA2, if CA2's revocation-check is **crl-optional** and the CA2's CRL is non-existent, then the system will not check CA1 cert's revocation status and consider it as "good".

Note: Users must shutdown the ca-profile to change the revocation-check configuration.

Default revocation-check crl

Parameters **crl** — Specifies to use the configured CRL.

crl-optional — Specifies that the CRL is optional.

Platforms All

22.239 rib-api

rib-api

Syntax [**no**] **rib-api**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter rib-api)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter rib-api)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter rib-api)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter rib-api)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter rib-api
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter rib-api
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter rib-api
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter rib-api

Description This command selects the RIB-API tunnel type.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This command enables tunnels programmed using the RibApi gRPC service to be used in resolving the next hops of routes imported into the EVPN service.

The **no** form of this command disables tunnels programmed using the RibApi gRPC service from being used in resolving the next hops.

Default no rib-api

Platforms All

rib-api

Syntax **rib-api**

Context **[Tree]** (config>router rib-api)

Full Context configure router rib-api

Description Commands in this context configure parameters related to the RIB-API gRPC service.

Platforms All

rib-api

Syntax [**no**] **rib-api**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter rib-api)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter rib-api

Description This command enables tunnels programmed using the RibApi gRPC service for use in resolving the indirect next hops of statically-configured IPv4 and IPv6 routes.

Platforms All

rib-api

Syntax [**no**] **rib-api**

Context **[Tree]** (debug>router rib-api)

Full Context debug router rib-api

Description This command enables debugging for RIB-API protocol entities.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rib-api

Syntax **rib-api**

Context **[Tree]** (config>system>grpc rib-api)

Full Context configure system grpc rib-api

Description Commands in this context control the RibAPI gRPC service.

Platforms All

rib-api

Syntax [**no**] **rib-api**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter rib-api)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter rib-api)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter rib-api
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter rib-api

Description This command enables tunnels programmed using the RibApi gRPC service for use in resolving the next hops of label-IPv4 or label-IPv6 routes.

Platforms All

22.240 rib-api-getversion

rib-api-getversion

Syntax **rib-api-getversion** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization rib-api-getversion)

Full Context configure system security profile grpc rpc-authorization rib-api-getversion

Description This command permits the use of GetVersion RPC provided by the RibApi service.

The **no** form of this command reverts to the default value.

Default rib-api-getversion permit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **permit** — Specifies that the use of the GetVersion RPC is permitted.

deny — Specifies that the use of the GetVersion RPC is denied.

Platforms All

22.241 rib-api-modify

rib-api-modify

Syntax **rib-api-modify** {**permit** | **deny**}

Context **[Tree]** (config>system>security>profile>grpc>rpc-authorization rib-api-modify)

Full Context configure system security profile grpc rpc-authorization rib-api-modify

Description This command permits the use of Modify RPC provided by the RibApi service.

The **no** form of this command reverts to the default value.

Default rib-api-modify permit

Parameters **permit** — Specifies that the use of the Modify RPC is permitted.

deny — Specifies that the use of the Modify RPC is denied.

Platforms All

22.242 rib-management

rib-management

Syntax **rib-management**

Context **[Tree]** (config>service>vprn>bgp rib-management)

Full Context configure service vprn bgp rib-management

Description Commands in this context configure RIB management parameters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rib-management

Syntax **rib-management**

Context **[Tree]** (config>router>bgp rib-management)

Full Context configure router bgp rib-management

Description Commands in this context configure RIB management parameters.

Platforms All

22.243 rib-priority

rib-priority

Syntax **rib-priority high** {*prefix-list-name* | **tag** *tag*}
no rib-priority

Context **[Tree]** (config>service>vprn>isis rib-priority)

Full Context configure service vprn isis rib-priority

Description This command enabled RIB prioritization for the IS-IS protocol and specifies the prefix list or IS-IS tag value that will be used to select the specific routes that should be processed through the IS-IS route calculation process at a higher priority.

The **no** form of this command disables RIB prioritization.

Default no rib-priority

Parameters *prefix-list-name* — Specifies the prefix list which is used to select the routes that are processed at a higher priority through the route calculation process.

tag tag-value — Specifies the tag value that is used to match IS-IS routes that are to be processed at a higher priority through the route calculation process.

Values 1 to 4294967295

Platforms All

rib-priority

Syntax [**no**] **rib-priority**

Context **[Tree]** (config>service>vprn>ospf>area>if rib-priority)
[Tree] (config>service>vprn>ospf3>area>if rib-priority)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ospf area interface rib-priority
configure service vprn ospf3 area interface rib-priority

Description This command enables RIB prioritization for the OSPF/OSPFv3 protocol. When enabled at the OSPF interface level, all routes learned through the associated OSPF interface will be processed through the OSPF route calculation process at a higher priority.

The **no** form of **rib-priority** command disables RIB prioritization at the associated level.

Default no rib-priority

Platforms All

rib-priority

Syntax **rib-priority** {**high**} *prefix-list-name*
no rib-priority

Context **[Tree]** (config>service>vprn>ospf rib-priority)
[Tree] (config>service>vprn>ospf3 rib-priority)

Full Context configure service vprn ospf rib-priority
configure service vprn ospf3 rib-priority

Description This command enabled RIB prioritization for the OSPF protocol and specifies the prefix list that will be used to select the specific routes that should be processed through the OSPF route calculation process at a higher priority.

The **no** form of **rib-priority** command disables RIB prioritization at the associated level.

Default no rib-priority

Parameters *prefix-list-name* — Specifies the prefix list which is used to select the routes that are processed at a higher priority through the route calculation process.

Platforms All

rib-priority

Syntax **rib-priority high** {*prefix-list-name* | **tag** *tag-value*}
no rib-priority

Context **[Tree]** (config>router>isis rib-priority)

Full Context configure router isis rib-priority

Description This command enabled RIB prioritization for the IS-IS protocol and specifies the prefix list or IS-IS tag value that will be used to select the specific routes that should be processed through the IS-IS route calculation process at a higher priority.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The no rib-priority form of command disables RIB prioritization.

Default no rib-priority high

Parameters *prefix-list-name* — Specifies the prefix list which is used to select the routes that are processed at a higher priority through the route calculation process.

tag tag-value — Specifies the tag value that is used to match IS-IS routes that are to be processed at a higher priority through the route calculation process.

Values 1 to 4294967295

Platforms All

rib-priority

Syntax **rib-priority** {**high**} *prefix-list-name*
no rib-priority {**high**}

Context **[Tree]** (config>router>ospf rib-priority)
[Tree] (config>router>ospf3 rib-priority)

Full Context configure router ospf rib-priority
configure router ospf3 rib-priority

Description This command enabled RIB prioritization for the OSPF protocol and specifies the prefix list that will be used to select the specific routes that should be processed through the OSPF route calculation process at a higher priority.

The **no** form of this command disables RIB prioritization at the associated level.

Default no rib-priority high

Parameters *prefix-list-name* — Specifies the prefix list, up to 32 characters, which is used to select the routes that are processed at a higher priority through the route calculation process.

Platforms All

rib-priority

Syntax **rib-priority** {**high**}
no rib-priority

Context **[Tree]** (config>router>ospf>area>interface rib-priority)
[Tree] (config>router>ospf3>area>interface rib-priority)

Full Context configure router ospf area interface rib-priority
configure router ospf3 area interface rib-priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables RIB prioritization for the OSPF/OSPFv3 protocol. When enabled at the OSPF interface level, all routes learned through the associated OSPF interface will be processed through the OSPF route calculation process at a higher priority.

The **no** form of **rib-priority** command disables RIB prioritization at the associated level.

Default no rib-priority

Parameters **high** — Specifies that the name of the prefix list which contains prefixes get high priority for RIB-download. The high priority prefixes are downloaded first to the RIB. In doing so, the convergence time for these prefixes is better.

Platforms All

22.244 ring

ring

Syntax **ring** *sync-tag* [**create**]
no ring *sync-tag*

Context **[Tree]** (config>redundancy>mc>peer>mcr ring)

Full Context configure redundancy multi-chassis peer mc-ring ring

Description This command configures a multi-chassis ring.

The **no** form of this command removes the sync-tag from the configuration.

Parameters *sync-tag* — Specifies a synchronization tag, up to 32 characters, to be used while synchronizing this port with the multi-chassis peer.

create — Creates he multi-chassis peer ring instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

22.245 ring-node

ring-node

Syntax **ring-node** *ring-node-name* [**create**]
no ring-node *ring-node-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>redundancy>mc>peer>mcr>ring ring-node)

Full Context configure redundancy multi-chassis peer mc-ring ring ring-node

Description This command specifies the unique name of a multi-chassis ring access node.

Parameters *ring-node-name* — Specifies the unique name of a multi-chassis ring access node. The name can be up to 32 characters.

create — Keyword used to create the ring node instance. The **create** keyword requirement can be enabled or disabled in the **environment**>**create** context.

Platforms All

ring-node

Syntax **ring-node** *ring-node-name*
no ring-node

Context [Tree] (config>service>epipe>sap ring-node)

Full Context configure service epipe sap ring-node

Description This command configures a multi-chassis ring-node for this SAP.

The **no** form of this command removes the name from the configuration.

Platforms All

22.246 rip

rip

Syntax [**no**] **rip**

Context [Tree] (config>service>vprn rip)
[Tree] (config>service>ies rip)

Full Context configure service ies rip
configure service vprn rip

Description This command enables the RIP protocol on the given VPRN IP interface.

The **no** form of this command disables the RIP protocol from the given VPRN IP interface.

Default no rip

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rip

Syntax [**no**] **rip**

Context **[Tree]** (config>router rip)

Full Context configure router rip

Description This command creates the context to configure the RIP protocol instance.

When a RIP instance is created, the protocol is enabled by default. To start or suspend execution of the RIP protocol without affecting the configuration, use the [**no**] **shutdown** command.

The **no** form of the command deletes the RIP protocol instance removing all associated configuration parameters.

Default no rip

Platforms All

22.247 rip-policy

rip-policy

Syntax **rip-policy** *policy-name*
no rip-policy

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host rip-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host rip-policy)

Full Context configure subscriber-mgmt local-user-db ipoe host rip-policy
configure subscriber-mgmt local-user-db ppp host rip-policy

Description This command configures the RIP policy name. This policy is applied to a subscriber IPv4 host to enable the BNG to learn RIP routes from the host. RIP routes are never sent to the hosts.

The **no** form of this command removes the RIP policy name from the configuration.

Parameters *policy-name* — Specifies the RIP policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rip-policy

Syntax **rip-policy** *policy-name* [**create**]
no rip-policy *policy-name*

Context **[Tree]** (config>subscr-mgmt rip-policy)

Full Context configure subscriber-mgmt rip-policy

Description This command creates a RIP policy. This policy is applied to a subscriber IPv4 host to enable the BNG to learn RIP routes from the host. RIP routes are never sent to the hosts.

Parameters *policy-name* — Specifies the RIP policy name up to 32 characters.

create — Keyword required to create the configuration context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

rip-policy

Syntax **rip-policy** *rip-policy-name*
no rip-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host rip-policy)

Full Context configure service ies subscriber-interface group-interface sap static-host rip-policy

Description This command specifies the name of the RIP policy up to 32 characters.

The **no** form of this command removes the policy name from the static-host configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.248 ripng

ripng

Syntax [**no**] **ripng**

Context **[Tree]** (config>router ripng)

Full Context configure router ripng

Description This command creates the context to configure the RIPng protocol instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a RIPng instance is created, the protocol is enabled by default. To start or suspend execution of the RIP protocol without affecting the configuration, use the [**no**] **shutdown** command.

The **no** form of this command deletes the RIP protocol instance removing all associated configuration parameters.

Default no ripng

Platforms All

22.249 rmon

rmon

Syntax **rmon**

Context **[Tree]** (config>system>thresholds rmon)

Full Context configure system thresholds rmon

Description This command creates the context to configure generic RMON alarms and events.

Generic RMON alarms can be created on any SNMP object-ID that is valid for RMON monitoring (for example, an integer-based datatype).

The configuration of an event controls the generation and notification of threshold crossing events configured with the alarm command.

Platforms All

22.250 roaming

roaming

Syntax **roaming** *bit* [*bit*]
no roaming

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile>charging roaming)

Full Context configure subscriber-mgmt gtp peer-profile charging-characteristics roaming

Description This command configures the charging characteristics for roaming UE.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the *bit* value from the configuration.

Default no roaming

Parameters *bit* — Specifies up to 16 bits to set in the Charging Characteristics Information Element (IE) for roaming UE, if not known by other means such as RADIUS.

Values bit0, bit1, bit2, bit3, bit4, bit5, bit6, bit7, bit8, bit9, bit10, bit11, bit12, bit13, bit14, bit15

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.251 robust-count

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context **[Tree]** (config>service>vpls>igmp-snooping robust-count)
[Tree] (config>service>vpls>sap>igmp-snooping robust-count)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping robust-count)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping robust-count)
[Tree] (config>service>vpls>sap>mld-snooping robust-count)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping robust-count)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping robust-count)

Full Context configure service vpls igmp-snooping robust-count
configure service vpls mesh-sdp igmp-snooping robust-count
configure service vpls mesh-sdp mld-snooping robust-count
configure service vpls sap igmp-snooping robust-count
configure service vpls sap mld-snooping robust-count
configure service vpls spoke-sdp igmp-snooping robust-count
configure service vpls spoke-sdp mld-snooping robust-count

Description If the **send-queries** command is enabled, this parameter allows tuning for the expected packet loss on a SAP or SDP. The robust-count variable allows tuning for the expected packet loss on a subnet and is comparable to a retry count. If this SAP or SDP is expected to be 'lossy', this parameter may be increased. IGMP snooping on this SAP or SDP is robust to (robust-count-1) packet losses.

If **send-queries** is not enabled, this parameter will be ignored.

Default robust-count 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *robust-count* — Specifies the robust count for the SAP or SDP

Values 2 to 7 (for **config>service>vpls>sap>igmp-snooping**) 1 to 255 (for **config>service>vpls>igmp-snooping**)

Platforms All

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp robust-count)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping robust-count

Description This command configures the IGMP robustness variable. If the **send-queries** command is enabled, this parameter allows tuning for the expected packet loss on a SAP or SDP. The robust-count variable allows tuning for the expected packet loss on a subnet and is comparable to a retry count. If an MSAP or SDP is expected to be “lossy”, this parameter may be increased. IGMP snooping on an MSAP or SDP is robust to (robust-count-1) packet losses.

If send-queries is not enabled, this parameter is ignored.

The **no** form of this command reverts to the default.

Default robust-count 2

Parameters *robust-count* — Specifies the robust count for the SAP or SDP.

Values 2 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context **[Tree]** (config>service>vprn>igmp robust-count)
[Tree] (config>service>vprn>mld robust-count)

Full Context configure service vprn igmp robust-count
configure service vprn mld robust-count

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default robust-count 2

Parameters *robust-count* — Specifies the robust count value.

Values 2 to 10

Platforms All

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context **[Tree]** (config>router>igmp robust-count)

Full Context configure router igmp robust-count

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default robust-count 2

Parameters *robust-count* — Specify the robust count value.

Values 2 to 10

Platforms All

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context **[Tree]** (config>router>mld robust-count)

Full Context configure router mld robust-count

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default robust-count 2

Parameters *robust-count* — Specify the robust count value.

Values 2 to 10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context **[Tree]** (config>service>pw-template>igmp-snooping robust-count)

Full Context configure service pw-template igmp-snooping robust-count

Description If the **send-queries** command is enabled, this parameter allows tuning for the expected packet loss. The robust-count variable allows tuning for the expected packet loss on a subnet and is comparable to a retry count.

If send-queries is not enabled, this parameter will be ignored.

Default robust-count 2

Parameters *robust-count* — Specifies the robust count for the SAP or SDP.

Values 2 to 7

Platforms All

22.252 role

role

Syntax **role** *role-type*

Context **[Tree]** (config>system>satellite>port-template>port role)

Full Context configure system satellite port-template port role

Description This command configures the role that the associated port is to take on.

Parameters **none** — Clears the role association for the associated port.

uplink — Specifies that the associated satellite port is assigned the role of an uplink port.

client — Specifies that the associated satellite port is assigned the role of a satellite client port.

system-default — Specifies that the associated satellite port is returned to the system default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.253 rollback

rollback

Syntax **rollback**

Context **[Tree]** (config>system rollback)

Full Context configure system rollback

Description Configure parameters of the classic CLI configuration rollback functionality. Configuration rollback provides the ability to undo configuration and revert back to previous router configuration states.

Platforms All

rollback

Syntax **rollback**

Context **[Tree]** (admin rollback)

Full Context admin rollback

Description Commands in this context configure rollback operations.

Platforms All

22.254 rollback-location

rollback-location

Syntax **rollback-location** *file-url* /*rollback filename*
no rollback-location

Context **[Tree]** (config>system>rollback rollback-location)

Full Context configure system rollback rollback-location

Description The location and name of the rollback checkpoint files is configurable to be local (on compact flash) or remote. The *file-url* must not contain a suffix (just a path/directory + filename). The suffixes for rollback checkpoint files are “.rb”, ".rb.1", ..., ".rb.9" and are automatically appended to rollback checkpoint files.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no rollback-location

Parameters *file-url* — Specifies the URL or rollback filename.

Values

local-url | *remote-url*	
local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length of up to 99 characters each
remote-url	[{ftp://}*login*:*pswd*@ *remote-locn*/][*file-path*] up to 255 characters, directory length of up to 99 characters each
remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
	x:x:x:x:x:x:d.d.d.d[-*interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface - up to 32 characters each, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

rollback-filename — Specifies the rollback file name.

Values suffixed with .rb, .rb.1 up to .9 during rollback checkpoint creation

Platforms All

22.255 rollback-sync

rollback-sync

Syntax **rollback-sync**

Context **[Tree]** (admin>redundancy rollback-sync)

Full Context admin redundancy rollback-sync

Description This command copies the entire set of rollback checkpoint files from the active CPM CF to the standby CPM CF.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rollback-sync

Syntax [**no**] **rollback-sync**

Context **[Tree]** (config>redundancy rollback-sync)

Full Context configure redundancy rollback-sync

Description The operator can enable automatic synchronization of rollback checkpoint files between the active CPM and standby CPM. When this automatic synchronization is enabled, a rollback save will cause the new checkpoint file to be saved on both the active and standby CPMs. The suffixes of the old checkpoint files on both active and standby CPMs are incremented. Note that automatic sync only causes the one new checkpoint file to be copied to both CFs (the other 9 checkpoints are not automatically copied from active to standby but that can be done manually with **admin red rollback-sync**).

Automatic synchronization of rollback checkpoint files across CPMs is only performed if the rollback-location is configured as a local file-url (for example, "cf3:/rollback-files/rollback). Synchronization is not done if the rollback-location is remote.

The **config red sync {boot-env | config}** and **admin red sync {boot-env | config}** do not apply to rollback checkpoint files. These commands do not manually or automatically sync rollback checkpoint files. The dedicated **rollback-sync** commands must be used to sync rollback checkpoint files.

Default no rollback-sync

Platforms All

22.256 rollover

rollover

Syntax **rollover** *minutes* [**retention** *hours*]
no rollover

Context **[Tree]** (config>log>file-id rollover)

Full Context configure log file-id rollover

Description This command configures how often an event or accounting log is rolled over or partitioned into a new file.

An event or accounting log is actually composed of multiple, individual files. The system creates a new file for the log based on the **rollover** time, expressed in minutes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The *retention* option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file.

If logs are needed to be retained for more than 16 days, use a CRON job to move the logs to a different location, either on a local drive or a remote server. For more information, contact Nokia support.

When multiple **rollover** commands for a *file-id* are entered, the last command overwrites the previous command.

The **no** form of this command reverts to the default values.

Default rollover 1440 retention 12

Parameters *minutes* — Specifies the rollover time, in minutes.

Values 5 to 10080

retention hours — Specifies the retention period in hours, expressed as a decimal integer. The retention time is based on the time creation time of the file. The file becomes a candidate for removal once the creation datestamp + rollover time + retention time is less than the current timestamp.

Default 12

Values 1 to 500

Platforms All

22.257 root

root

Syntax **root**

Context **[Tree]** (config>qos>policer-control-policy root)

Full Context configure qos policer-control-policy root

Description The **root** node contains the policer control policies configuration parameters for the root arbiter. Within the node, the parent policer's maximum rate limit can be set, the strict priority level, and fair threshold portions may be defined per priority level.

The root node always exists and does not need to be created.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.258 root-address

root-address

Syntax **root-address** *ip-address*
no root-address

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy root-address)

Full Context configure router p2mp-sr-tree p2mp-policy root-address

Description This command configures the IP address of the P2MP SR tree root node of the P2MP policy. The root tree ID and the root address uniquely identify the P2MP policy on the root node.

The **no** form of this command removes the root address entry.

Parameters *ip-address* — Specifies the IPv4 address of the root node.

Values a.b.c.d

Platforms All

root-address

Syntax **root-address** *ip-address*
no root address

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment root-address)

Full Context configure router p2mp-sr-tree replication-segment root-address

Description This command configures the replication segment with the IP address of the root node of the P2MP SR tree replication segment.

The **no** form of this command removes the root node address.

Parameters *ip-address* — Specifies the IPv4 address.

Values a.b.c.d

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.259 root-and-leaf

root-and-leaf

Syntax [**no**] **root-and-leaf**

Context **[Tree]** (config>service>vpls>provider-tunnel>inclusive root-and-leaf)

Full Context configure service vpls provider-tunnel inclusive root-and-leaf

Description This command configures the node to operate as both root and leaf of the I-PMSI in a specified VPLS/B-VPLS instance.

By default, a node will behave as a leaf-only node. When the node is leaf only for the I-PMSI of type P2MP RSVP LSP, no PMSI Tunnel Attribute is included in BGP-AD route update messages and therefore no RSVP P2MP LSP is signaled but the node can join RSVP P2MP LSP rooted at other PE nodes participating in this VPLS/B-VPLS service. The user must still configure a LSP template even if the node is a leaf only.

For the I-PMSI of type mLDP, the leaf-only node will join I-PMSI rooted at other nodes it discovered but will not include a PMSI Tunnel Attribute in BGP-AD route update messages. This way a leaf-only node will forward packets to other nodes in the VPLS/B-VPLS using the point-to-point spoke-SDPs.

The **no** version of this command re-instates the default value.

Platforms All

22.260 root-guard

root-guard

Syntax [**no**] **root-guard**

Context **[Tree]** (config>service>vpls>sap>stp root-guard)
[Tree] (config>service>template>vpls-sap-template>stp root-guard)
[Tree] (config>service>vpls>spoke-sdp>stp root-guard)

Full Context configure service template vpls-sap-template stp root-guard
configure service vpls sap stp root-guard
configure service vpls spoke-sdp stp root-guard

Description This command specifies whether this port is allowed to become an STP root port. It corresponds to the restrictedRole parameter in 802.1Q. If set, it can cause lack of spanning tree connectivity.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no root-guard

Platforms All

root-guard

Syntax [**no**] **root-guard**

Context **[Tree]** (config>service>pw-template>stp root-guard)

Full Context configure service pw-template stp root-guard

Description This command specifies whether this port is allowed to become an STP root port. It corresponds to the restrictedRole parameter in 802.1Q. If set, it can cause lack of spanning tree connectivity.

Default no root-guard

Platforms All

22.261 root-pool

root-pool

Syntax [**no**] **root-pool** *root-pool-id*

Context **[Tree]** (config>qos>hs-pool-policy>root-tier root-pool)

Full Context configure qos hs-pool-policy root-tier root-pool

Description Commands in this context configure root tier parameters. Within the **root-tier** context, root pools can be sized using the **allocation-weight** command or a slope policy can be associated with a root pool.

The **no** form of the command restores the default **allocation-weight** value and default slope policy to the specified root pool. Root pool 1 has a different default weight than root pools 2 through 16. The **no root-pool** command fails for root pools 2 through 16 if the root pool is currently the parent of a mid-tier pool.

Parameters *root-pool-id* — Specifies the root pool ID. This is a required parameter when executing the **root-pool** command and specifies which root pool context is being entered.

Values 1 to 16

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.262 root-tier

root-tier

Syntax **root-tier**

Context **[Tree]** (config>qos>hs-pool-policy root-tier)

Full Context configure qos hs-pool-policy root-tier

Description Commands in this context configure root pool parameters. Within the **root-tier** context, root pools can be sized using the **allocation-weight** command or a slope policy can be associated with a root pool.

Platforms 7750 SR-7/12/12e

22.263 root-tree-id

root-tree-id

Syntax **root-tree-id** *tree-id*
no root-tree-id

Context **[Tree]** (config>router>p2mp-sr-tree>p2mp-policy root-tree-id)

Full Context configure router p2mp-sr-tree p2mp-policy root-tree-id

Description This command configures the P2MP SR tree ID on the root node of the P2MP policy. The root tree ID and the root address uniquely identify the P2MP policy on the root node.

The **no** form of this command removes the root tree ID entry.

Parameters *tree-id* — Specifies the ID of the tree.

Values 8193 to 16286

Platforms All

root-tree-id

Syntax **root-tree-id** *tree-id*
no root-tree-id

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment root-tree-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router p2mp-sr-tree replication-segment root-tree-id

Description This command configures the root-tree ID for the replication segment of the P2MP SR tree.

The **no** form of this command removes the root-tree ID.

Parameters *tree-id* — Specifies the root-tree ID.

Values 8193 to 16286

Platforms All

22.264 round-robin-inactive-records

round-robin-inactive-records

Syntax [**no**] **round-robin-inactive-records**

Context **[Tree]** (config>mcast-mgmt>chassis-level round-robin-inactive-records)

Full Context configure mcast-management chassis-level round-robin-inactive-records

Description This command specifies whether initially inactive multicast records use the IOM default secondary multicast path or not. When enabled, the system redistributes newly populated inactive records among all available IOM multicast paths and multicast switch fabric planes. When disabled, the system continues to set all initially inactive multicast records to use the IOM default secondary multicast path.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

22.265 route index

route index

Syntax **route index** *index* [**realm** *realm-string*] [**application** *application*] [**create**]
no route index *index*

Context **[Tree]** (config>aaa>diam>node>peer route index)

Full Context configure aaa diameter node peer route index

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the index of the static route within the Diameter peer used to reach remote realms that are not directly connected to the origin realm, or to override the route preference (peer preference) of the directly-connected realms.

The **no** form of this command removes the route index information from the configuration.

Parameters *index* — Specifies the index of the static route within the Diameter peer.

Values 1 to 15

realm-string — Specifies the destination realm reachable through this static route, up to 80 characters.

application — Specifies the ID of the Diameter application of the static route.

Values nasreq, gy, gx

create — Keyword used to create the route index. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

22.266 route-admin-tag-policy

route-admin-tag-policy

Syntax [**no**] **route-admin-tag-policy** *policy-name*

Context **[Tree]** (config>router>admin-tags route-admin-tag-policy)

Full Context configure router admin-tags route-admin-tag-policy

Description This command configures a route admin tag policy.

Up to 2,000 policies can be configured per system.

The **no** form of this command removes the route admin tag policy.

Parameters *policy-name* — The name of the route admin tag policy, up to 32 characters.

Platforms All

22.267 route-advertisement

route-advertisement

Syntax **[no] route-advertisement**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp>group>srv6 route-advertisement)
[Tree] (config>router>bgp>group>neighbor>srv6 route-advertisement)

Full Context configure router bgp group neighbor segment-routing-v6 route-advertisement
configure router bgp group segment-routing-v6 route-advertisement

Description Commands in this context configure the route advertisement options.

The **no** form of this command deletes the context.

Default no route-advertisement

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

22.268 route-distinguisher

route-distinguisher

Syntax **route-distinguisher auto-rd**
route-distinguisher *rd*
no route-distinguisher

Context [Tree] (config>subscr-mgmt>isa-svc-chain>evpn>bgp route-distinguisher)

Full Context configure subscriber-mgmt isa-service-chaining evpn bgp route-distinguisher

Description This command configures the Route Distinguisher (RD) field that is signaled in NLRI in EVPN routes.

The **no** form of this command reverts to the default.

Parameters **auto-rd** — Specifies that the system automatically generates an RD.

rd — Specifies the RD.

Values rd: *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*
ip-addr: a.b.c.d
comm-val: [0 to 65535]
2byte-asnumber: [1 to 65535]
ext-comm-val: [0 to 4294967295]
4byte-asnumber: [1 to 4294967295]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

route-distinguisher

Syntax **route-distinguisher auto-rd**
no route-distinguisher
route-distinguisher *rd*

Context **[Tree]** (config>service>epipe>bgp route-distinguisher)
[Tree] (config>service>vpls>bgp route-distinguisher)

Full Context configure service epipe bgp route-distinguisher
configure service vpls bgp route-distinguisher

Description This command configures the Route Distinguisher (RD) component that will be signaled in the MP-BGP NLRI for L2VPN and EVPN families. This value will be used for BGP-AD, BGP VPLS and BGP multi-homing NLRI if these features are configured.

If this command is not configured, the RD is automatically built using the BGP-AD VPLS ID. The following rules apply:

- if BGP AD VPLS-id is configured and no RD is configured under BGP node - RD=VPLS-ID
- if BGP AD VPLS-id is not configured then an RD value must be configured under BGP node (this is the case when only BGP VPLS is configured)
- if BGP AD VPLS-id is configured and an RD value is also configured under BGP node, the configured RD value prevails

Values and format (6 bytes, other 2 bytes of type will be automatically generated)

Alternatively, the **auto-rd** option allows the system to automatically generate an RD based on the **bgp-auto-rd-range** command configured at the service level. For **BGP-EVPN** enabled VPLS and Epipe services, the **route-distinguisher** value can also be auto-derived from the **evi** value (**config>service>vpls>bgp-evpn>evi** or **config>service>epipe>bgp-evpn>evi**) if this command is not configured. See the **config>service>system>bgp-evpn>eth-seg>service-carving>manual evi** command description for more information.

Parameters *ip-addr:comm-val* — Specifies the IP address.

Values *ip-addr*: a.b.c.d
comm-val: 0 to 65535

as-number:ext-comm-val — Specifies the AS number.

Values *as-number*: 1 to 65535
ext-comm-val: 0 to 4294967295

auto-rd — The system will generate an RD for the service according to the IP address and range configured in the **bgp-auto-rd-range** command.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

route-distinguisher

Syntax **route-distinguisher** [*ip-addr:comm-val* | *as-number:ext-comm-val*]
no route-distinguisher

Context **[Tree]** (config>service>system>bgp-evpn route-distinguisher)

Full Context configure service system bgp-evpn route-distinguisher

Description This command configures the Route Distinguisher (RD) component that will be signaled in the MP-BGP NLRI for EVPN corresponding to the base EVPN instance (Ethernet Segment routes). If the route-distinguisher component is not configured, the system will use system:ip-address as the default route-distinguisher

Default no route-distinguisher

Parameters *ip-addr:comm-val* — Specifies the IP address.

Values *ip-addr*: a.b.c.d
comm-val: 0 to 65535

as-number:ext-comm-val — Specifies the AS number.

Values *as-number*: 1 to 65535
ext-comm-val: 0 to 4294967295

Platforms All

route-distinguisher

Syntax **route-distinguisher** *rd*
route-distinguisher auto-rd
no route-distinguisher

Context **[Tree]** (config>service>vprn>bgp-evpn>mpls route-distinguisher)
[Tree] (config>service>vprn>bgp-ipvpn>mpls route-distinguisher)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 route-distinguisher)

Full Context configure service vprn bgp-evpn mpls route-distinguisher
configure service vprn bgp-ipvpn mpls route-distinguisher
configure service vprn bgp-ipvpn segment-routing-v6 route-distinguisher

Description This command specifies an identifier attached to a route, which enables the user to identify the VPN to which the route belongs. Each routing instance must have a unique (within the carrier's domain) route distinguisher (RD) associated with it.

Alternatively, the **auto-rd** option allows the system to automatically generate an RD based on the **bgp-auto-rd-range** command configured at the service level.

The **no** form of this command removes the RD configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no route-distinguisher

Parameters **auto-rd** — Keyword that allows the system to generate an RD for the service according to the IP address and range configured in the **bgp-auto-rd-range** command.

rd — Specifies the route distinguisher.

Values rd: *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

ip-addr: a.b.c.d

comm-val: [0 to 65535]

2byte-asnumber: [1 to 65535]

ext-comm-val: [0 to 4294967295]

4byte-asnumber: [1 to 4294967295]

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service vprn bgp-ipvpn segment-routing-v6 route-distinguisher

All

- configure service vprn bgp-evpn mpls route-distinguisher
- configure service vprn bgp-ipvpn mpls route-distinguisher

22.269 route-downloader

route-downloader

Syntax **route-downloader** *name* [**create**]
no route-downloader *name*

Context **[Tree]** (config>aaa route-downloader)

Full Context configure aaa route-downloader

Description Commands in this context configure a route-downloader instance. The route-downloader is a process that uses radius access-request messages to a particular server. The server returns either an access-accept or access-deny message. Access-accept messages also contain the prefixes (in the form of static blackhole routes in various formats). Only a single route-downloader object can be created.

The **no** form of this command removes the name from the configuration. The object must be shutdown prior to deletion. No prefix is needed to delete an existing route-download object.

Parameters *name* — Specifies the name of this RADIUS route downloader.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — This keyword is mandatory while creating an instance of the route-download object.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.270 route-entry

route-entry

Syntax [**no**] **route-entry** {*ip-prefix/length* | *ip-prefix netmask*}
[**no**] **route-entry** {*ipv6-prefix/prefix-length* [**metric** *metric-value*]

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host>managed-routes route-entry)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host>managed-routes route-entry)

Full Context configure service ies subscriber-interface group-interface sap static-host managed-routes route-entry
configure service vprn subscriber-interface group-interface sap static-host managed-routes route-entry

Description This command assigns managed-route to a given subscriber-host. As a consequence, a static route pointing subscriber-host ip address as a next hop will be installed in FIB. Up to 16 managed routes per subscriber-host can be configured.

The **no** form of this command removes the respective route. Per default, there are no managed-routes configured.

Parameters *ip-prefix/length* — Specifies the IP prefix and length.

Syntax:

ip-prefix/length:	ip-prefix	a.b.c.d
	ip-prefix-length	0 to 32

netmask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (0.0.0.0 not allowed)

ipv6-prefix/prefix-length — The IP prefix in dotted decimal notation.

Values

ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-length	0 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

metric-value — Specifies the metric value.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.271 route-exists

route-exists

Syntax **route-exists** *expression*
no route-exists

Context **[Tree]** (config>router>policy-options>policy-statement>entry>cond-expr route-exists)

Full Context configure router policy-options policy-statement entry conditional-expression route-exists

Description This command is used to specify a route existence expression to control evaluation of the policy entry. If the route existence expression evaluates to 'true' the matching and action commands of the policy entry are applied as normal. If the route existence expression evaluates to 'false' the entire policy entry is skipped and processing continues with the next entry; however, conditional expressions are only parsed when the route policy is used as a BGP export policy or VRF export policy.

Default no route-exists

Parameters *expression* — "["<prefix-list-name>"]" [all | none]

If neither the all nor the none keyword are used the match logic is 'any' – that is, the route expression evaluates as 'true' if any exact match entry in the referenced prefix-list has an active route in the route table associated with the policy.

all – the route expression evaluates as 'true' only if all the exact match entries in the referenced prefix-list have an active route in the route table associated with the policy.

none – the route expression evaluates as 'true' only if none of the exact match entries in the referenced prefix-list have an active route in the route table associated with the policy.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.272 route-limit

route-limit

Syntax **route-limit** [*limit*]

Context **[Tree]** (config>router>nat>outside>dnat-only route-limit)
[Tree] (config>service>vprn>nat>outside>dnat-only route-limit)

Full Context configure router nat outside dnat-only route-limit
configure service vprn nat outside dnat-only route-limit

Description This command limits the number of source routes (inside routes) that are installed on the outside in **dnat-only** case. In case that the number of actual routes is larger than the number of configured routes, the excess of the routes will not be installed in the routing table and a log will be raised.

The source IP addresses on the inside must be known in advance in a **dnat-only** instance. This is required so that the corresponding routes can be installed in the routing table and thus the downstream traffic is properly routed towards the MS-ISAs where the original translation was performed (and state is kept).

In the dnat-only case, it is mandatory that the inside (private side) and the outside (public side) are in separated VPRNs.

Default route-limit 32768

Parameters [1..131072] — Specifies the maximum number of source routes installed on the outside the **dnat-only** scenario.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.273 route-monitoring

route-monitoring

Syntax **route-monitoring pre-policy** [**post-policy**]
route-monitoring post-policy
no route-monitoring

Context **[Tree]** (config>router>bgp>monitor route-monitoring)
[Tree] (config>router>bgp>group>monitor route-monitoring)
[Tree] (config>router>bgp>group>neighbor>monitor route-monitoring)
[Tree] (config>service>vprn>bgp>monitor route-monitoring)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>bgp>group>monitor route-monitoring)

Full Context configure router bgp group monitor route-monitoring
configure router bgp group neighbor monitor route-monitoring
configure router bgp monitor route-monitoring
configure service vprn bgp group monitor route-monitoring
configure service vprn bgp monitor route-monitoring

Description This command specifies if BMP sends pre-policy route monitoring messages, post-policy route monitoring messages, both types of messages, or none.

The **no** form of this command disables sending of route-monitoring messages.

Parameters **pre-policy** — Enables sending pre-policy route monitoring messages using the pre-policy path attribute values, if available.

post-policy — Enables sending post-policy route monitoring messages using the post-policy path attribute values, if available.

Platforms All

22.274 route-next-hop

route-next-hop

Syntax **route-next-hop** {**system-ipv4** | **system-ipv6** | *ip-address*}

Context [Tree] (config>service>epipe>bgp-evpn>mpls route-next-hop)
[Tree] (config>service>epipe>bgp-evpn>srv6 route-next-hop)
[Tree] (config>service>vpls>bgp-evpn>mpls route-next-hop)

Full Context configure service epipe bgp-evpn mpls route-next-hop
configure service epipe bgp-evpn segment-routing-v6 route-next-hop
configure service vpls bgp-evpn mpls route-next-hop

Description This command configures the next hop of the EVPN routes.

Default route-next-hop system-ipv4

Parameters **system-ipv4** — Specifies the system IPv4 address as the next hop for the service EVPN routes.

system-ipv6 — Specifies the system IPv6 address as the next hop for the service EVPN routes.

ip-address — Specifies the IPv4 address value as the next hop for the service EVPN.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe bgp-evpn segment-routing-v6 route-next-hop

All

- configure service epipe bgp-evpn mpls route-next-hop
- configure service vpls bgp-evpn mpls route-next-hop

route-next-hop

Syntax **route-next-hop** {*ip-address* | *ipv6-address*}
no route-next-hop

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg route-next-hop)

Full Context configure service system bgp-evpn ethernet-segment route-next-hop

Description This command modifies the next hop to the configured IP address value, for the following routes:

- ES
- AD per-ES (irrespective of the **evi-rt-set** or **evi-rt configuration mode**)

The **no** form of the command changes the originating IP address back to the system-ip.

Default no route-next-hop

Parameters *ip-address* — Specifies an IPv4 or IPv6 address.

Values *ip-address* | *ipv6-address*

Platforms All

22.275 route-next-hop-policy

route-next-hop-policy

Syntax **route-next-hop-policy**

Context **[Tree]** (config>router route-next-hop-policy)

Full Context configure router route-next-hop-policy

Description This command creates the context to configure route next-hop policies.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.276 route-preference

route-preference

Syntax **route-preference primary** {**inband** | **outband**} **secondary** {**inband** | **outband** | **none**}
no route-preference

Context **[Tree]** (config>log route-preference)

Full Context configure log route-preference

Description This command specifies the primary and secondary routing preference for traffic generated for SNMP notifications and syslog messages. If the remote destination is not reachable through the routing context specified by primary route preference then the secondary routing preference will be attempted.

The **no** form of this command reverts to the default values.

Default no route-preference

Parameters **primary** — Specifies the primary routing preference for traffic generated for SNMP notifications and syslog messages.

Default outband

secondary — Specifies the secondary routing preference for traffic generated for SNMP notifications and syslog messages. The routing context specified by the secondary route preference will be attempted if the remote destination was not reachable by the primary routing preference, specified by primary route preference. The value specified for the secondary routing preference must be distinct from the value for primary route preference.

Default inband

inband — Specifies that the logging utility will attempt to use the base routing context to send SNMP notifications and syslog messages to remote destinations.

outband — Specifies that the logging utility will attempt to use the management routing context to send SNMP notifications and syslog messages to remote destinations.

none — Specifies that no attempt will be made to send SNMP notifications and syslog messages to remote destinations.

Platforms All

route-preference

Syntax **route-preference** {**both** | **inband** | **outband**}
no route-preference

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>security>ldap route-preference)
[Tree] (config>system>security>radius route-preference)
[Tree] (config>system>security>tacplus route-preference)

Full Context configure system security ldap route-preference
configure system security radius route-preference
configure system security tacplus route-preference

Description This command specifies the routing preference to reach the AAA server. If the configured option is to use both in-band and out-of-band routes, the out-of-band routes in the management routing instance are used to reach the server before the in-band routes in the Base routing instance.

The **no** form of this command reverts to the default value.

Default route-preference both

Parameters **both** — Specifies the use of out-of-band routes before in-band routes.

inband — Specifies the use of in-band routes only.

outband — Specifies the use of out-of-band routes only.

Platforms All

route-preference

Syntax **route-preference** {**both** | **inband** | **outband**}
no route-preference

Context [Tree] (config>router>pcep>pcc>peer route-preference)

Full Context configure router pcep pcc peer route-preference

Description This command specifies the routing preference to reach the PCE server. If the configured option is to use both in-band and out-of-band routes, the out-of-band routes in the management routing instance are used to reach the server before the in-band routes in the Base routing instance.

The **no** form of this command reverts to the default value.

Default route-preference both

Parameters **both** — Specifies the use of out-of-band routes before in-band routes.

inband — Specifies the use of in-band routes only.

outband — Specifies the use of out-of-band routes only.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.277 route-recovery-wait

route-recovery-wait

Syntax **route-recovery-wait** *seconds*
no route-recovery-wait

Context **[Tree]** (config>log>app-route-notifications route-recovery-wait)

Full Context configure log app-route-notifications route-recovery-wait

Description The time delay that must pass before notifying specific CPM applications after the recovery or change of a route during normal operation.

The **no** form of this command disables the time-delay configuration.

Default no route-recovery-wait

Parameters *seconds* — Time delay in seconds.

Values 1 to 100

Platforms All

22.278 route-refresh

route-refresh

Syntax **route-refresh** [**neighbor** *ip-address* | **group** *name*]
no route-refresh

Context **[Tree]** (debug>router>bgp route-refresh)

Full Context debug router bgp route-refresh

Description This command enables debugging for BGP route-refresh.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

22.279 route-table

route-table

Syntax **route-table** [*ip-prefix*/*prefix-length*]
route-table *ip-prefix*/*prefix-length* **longer**
no route-table

Context **[Tree]** (debug>router>ip route-table)

Full Context debug router ip route-table

Description This command configures route table debugging.

Parameters *ip-prefix/prefix-length* — The IP prefix for prefix list entry in dotted decimal notation.

Values The following values apply to the 7750 SR and 7950 XRS:

ipv4-prefix	a.b.c.d (host bits must be 0)	
ipv4-prefix-length	0 to 32	
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D
ipv6-prefix-length	0 to 128	

Values The following values apply to the 7450 ESS:

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32

longer — Specifies the prefix list entry matches any route that matches the specified *ip-prefix* and prefix *mask* length values greater than the specified *mask*.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.280 route-table-import

route-table-import

Syntax **route-table-import** *policy-name*
no route-table-import

Context **[Tree]** (config>service>vprn>bgp>rib-management>ipv4 route-table-import)
[Tree] (config>service>vprn>bgp>rib-management>label-ipv4 route-table-import)
[Tree] (config>service>vprn>bgp>rib-management>ipv6 route-table-import)

Full Context configure service vprn bgp rib-management ipv4 route-table-import
configure service vprn bgp rib-management ipv6 route-table-import
configure service vprn bgp rib-management label-ipv4 route-table-import

Description This command specifies the name of a route policy to control the importation of active routes from the IP route table into one of the BGP RIBs.

If the **route-table-import** command is not configured, or if the command refers to an empty policy, all non-BGP routes from the IP route table are imported into the applicable RIB.

If the **route-table-import** command is configured, then routes dropped or rejected by the configured policy are not installed in the associated RIB. Rejected routes cannot be advertised to BGP peers associated with the RIB, but they can still be used to resolve BGP next-hops of routes in that RIB. If the active route for a prefix is rejected by the **route-table-import** policy, then the best BGP route for that prefix in the BGP RIB can be advertised to peers as though it is used.

Aggregate routes are always imported into each RIB, independent of the **route-table-import** policy.

Route modifications specified in the actions of a **route-table-import** policy are ignored and have no effect on the imported routes.

Default no route-table-import

Parameters *policy-name* — Specifies the name of a policy-statement (up to 64 characters).

Platforms All

route-table-import

Syntax **route-table-import** *policy-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no route-table-import

Context [Tree] (config>router>bgp>rib-management>ipv4 route-table-import)
[Tree] (config>router>bgp>rib-management>label-ipv4 route-table-import)
[Tree] (config>router>bgp>rib-management>ipv6 route-table-import)
[Tree] (config>router>bgp>rib-management>label-ipv6 route-table-import)

Full Context configure router bgp rib-management ipv4 route-table-import
configure router bgp rib-management ipv6 route-table-import
configure router bgp rib-management label-ipv4 route-table-import
configure router bgp rib-management label-ipv6 route-table-import

Description This command specifies the name of a policy to control the importation of active routes from the IP route table into one of the BGP RIBs.

If the **route-table-import** command is not configured, or if the command refers to an empty policy, all non-BGP routes from the IP route table are imported into the applicable RIB.

If the **route-table-import** command is configured, then routes dropped or rejected by the configured policy are not installed in the associated RIB. Rejected routes cannot be advertised to BGP peers associated with the RIB, but they can still be used to resolve BGP next-hops of routes in that RIB. If the active route for a prefix is rejected by the **route-table-import** policy, then the best BGP route for that prefix in the BGP RIB can be advertised to peers as though it is used.

Aggregate routes are always imported into each RIB, independent of the **route-table-import** policy.

Route modifications specified in the actions of a **route-table-import** policy are ignored and have no effect on the imported routes.

Default no route-table-import

Parameters *policy-name* — Specifies the name of a policy-statement (up to 64 characters).

Platforms All

22.281 route-target

route-target

Syntax **route-target export** *ext-community* **import** *ext-community*
no route-target

Context [Tree] (config>subscr-mgmt>isa-svc-chain>evpn>bgp route-target)

Full Context configure subscriber-mgmt isa-service-chaining evpn bgp route-target

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures route target attributes to be signaled in EVPN routes used for service chaining.

The **no** form of this command removes the parameters from the configuration.

Parameters **export** — Specifies the route target to be used by BGP in this EVPN service when exporting EVPN routes.

import — Specifies the route target to be used by BGP in this EVPN service when importing EVPN routes.

ext-community — Specifies the extended community.

Values rd: *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

ip-addr: a.b.c.d

comm-val: [0 to 65535]

2byte-asnumber: [1 to 65535]

ext-comm-val: [0 to 4294967295]

4byte-asnumber: [1 to 4294967295]

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

route-target

Syntax **route-target {***ext-community* **| {[export** *ext-community***][import** *ext-community***]}}**
no route-target

Context **[Tree]** (config>service>epipe>bgp route-target)
[Tree] (config>service>vpls>bgp route-target)
[Tree] (config>service>vpls>bgp-ad route-target)

Full Context configure service epipe bgp route-target
configure service vpls bgp route-target
configure service vpls bgp-ad route-target

Description This command configures the route target (RT) component that will be signaled in the related MP- BGP attribute to be used for BGP auto-discovery, BGP VPLS, BGP multi-homing and EVPN if these features are configured in this VPLS service, or for BGP multi-homing, BGP-VPWS and EVPN in case of Epipe services.

If this command is not used in VPLS services, the RT is built automatically using the VPLS ID. The extended community can have the same two formats as the VPLS ID, a two-octet AS-specific extended community, IPv4 specific extended community. For BGP EVPN enabled VPLS and Epipe services, the route target can also be auto-derived from the **evi** value (**config>service>vpls>bgp-evpn>evi** or **config>service>epipe>bgp-evpn>evi**) if this command is not configured.

Parameters **export** *ext-community* — Specifies communities allowed to be sent to remote PE neighbors.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

import *ext-community* — Specifies communities allowed to be accepted from remote PE neighbors.

Platforms All

22.282 route-target-list

route-target-list

Syntax **route-target-list** *comm-id* [*comm-id*]]
no route-target-list [*comm-id*]

Context **[Tree]** (config>router>bgp route-target-list)

Full Context configure router bgp route-target-list

Description This command specifies the route target(s) to be accepted from or advertised to peers. If the **route-target-list** is a non-null list, only routes with one or more of the given route targets are accepted from or advertised to peers.

The **route-target-list** is assigned at the global level and applies to all peers connected to the system.

This command is only applicable if the router is a route-reflector server.

The **no** form of this command with a specified route target community removes the specified community from the **route-target-list**. The **no** form of this command entered without a route target community removes all communities from the list.

Default no route-target-list

Parameters *comm-id* — Specifies up to 15 route target communities.

Values [**target:** {*ip-address*:*comm-val* | *2byte-asnumber*:*ext-comm-val* | *4byte-asnumber*:*comm-val*}

where:

- *ip-address* — a.b.c.d
- *comm-val* — 0 to 65535
- *2byte-asnumber* — 0 to 65535
- *ext-comm-val* — 0 to 4294967295
- *4byte-asnumber* — 0 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.283 route-unknown

route-unknown

Syntax [**no**] **route-unknown** [{*ip-prefix/mask* | *ipv6-address/prefix-length*}]

Context **[Tree]** (config>vrrp>policy>priority-event route-unknown)

Full Context configure vrrp policy priority-event route-unknown

Description This command creates a context to configure a route unknown priority control event that monitors the existence of a specific active IP route prefix within the routing table.

The **route-unknown** command configures a priority control event that defines a link between the VRRP priority control policy and the Route Table Manager (RTM). The RTM registers the specified route prefix as monitored by the policy. If any change (add, delete, new next hop) occurs relative to the prefix, the policy is notified and takes correct action according to the priority event definition. If the route prefix exists and is active in the routing table according to the conditions defined, the event is in the cleared state. If the route prefix is removed, becomes inactive or fails to meet the event criteria, the event is in the set state.

The command creates a **route-unknown** node identified by *prefix/mask-length* and containing event control commands.

Multiple unique (different *prefix/mask-length*) **route-unknown** event nodes can be configured within the **priority-event** node up to the maximum limit of 32 events.

The **route-unknown** command can reference any valid IP address mask-length pair. The IP address and associated mask length define a unique IP router prefix. The dynamic monitoring of the route prefix results in one of the event operational states listed in Table 120.

Table 120 **Route-unknown Operational States**

route-unknown Operational State	Description
Set – non-existent	The route does not exist in the route table
Set – inactive	The route exists in the route table but is not being used
Set – wrong next hop	The route exists in the route table but does not meet the **next-hop** requirements
Set – wrong protocol	The route exists in the route table but does not meet the **protocol** requirements
Set – less specific found	The route exists in the route table but does is not an exact match and does not meet any **less-specific** requirements

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 120 **Route-unknown Operational States**

route-unknown Operational State	Description
Set – default best match	The route exists in the route table as the default route but the default route is not allowed for route matching
Cleared – less specific found	A less specific route exists in the route table and meets all criteria including the **less-specific** requirements
Cleared – found	The route exists in the route table manager and meets all criteria

An existing route prefix in the RTM must be active (used by the IP forwarding engine) to clear the event operational state. It may be less specific (the defined prefix may be contained in a larger prefix according to Classless Inter-Domain Routing (CIDR) techniques) if the event has the **less-specific** statement defined. The less specific route that incorporates the router prefix may be the default route (0.0.0.0) if the **less-specific allow-default** statement is defined. The matching prefix may be required to have a specific next hop IP address if defined by the event **next-hop** command. Finally, the source of the RTM prefix may be required to be one of the dynamic routing protocols or be statically defined if defined by the event **protocol** command. If an RTM prefix is not found that matches all the above criteria (if defined in the event control commands), the event is considered to be set. If a matching prefix is found in the RTM, the event is considered to be cleared.

When an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instances in-use priority value. As the event transitions from clear to set, a hold-set timer is loaded with the value configured by the events **hold-set** command. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the **hold-set** value, extending the time before another clear can take effect.

The **no** form of the command is used to remove the specific *prefix/mask-length* monitoring event. The event can be removed at anytime. When the event is removed, the in-use priority of all associated virtual router instances must be reevaluated. The events **hold-set** timer has no effect on the removal procedure.

Default no route-unknown — No route unknown priority control events are defined for the priority control event policy.

Parameters *ip-prefix/mask* — The IP prefix address in dotted decimal notation and the subnet mask length expressed as a decimal integer associated with the IP *prefix* defining the route prefix to be monitored by the route unknown priority control event.

Values The following values apply to the 7750 SR, 7950 XRS, and 7450 ESS:

ip-prefix/mask:	ip-prefix	a.b.c.d (host bits must be 0)
	mask	0 to 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-address/prefix-length — The IPv6 address of the host for which the specific event will monitor connectivity. The *ipv6-address* can only be monitored by a single event in this policy. The IPv6 address can be monitored by multiple VRRP priority control policies. The IPv6 address can be used in one or multiple **ping** requests. Each VRRP priority control **host-unreachable** and **ping** destined to the same *ipv6-address* is uniquely identified on a per message basis. Each session originates a unique identifier value for the ICMP echo request messages it generates. This allows received ICMP echo reply messages to be directed to the appropriate sending application.

Values The following values apply to the 7750 SR and 7950 XRS:

ipv6-address/ *prefix-length*:	ipv6-address	x:x:x:x:x:x:x:x	(eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d	
		x:	[0..FFFF]H
	prefix-length	0 to 128	

Platforms All

22.284 router

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context **[Tree]** (config>aaa>l2tp-acct-plcy>radius-acct-server router)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server router

Description This command specifies the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.

The **no** form of this command reverts to the default value.

Parameters *router-instance* — Specifies the router instance.

Values

router-name | *vprn-svc-id*

router-name	Base, management
	Default - Base
vprn-svc-id	1 to 2147483647

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

service-name — Specifies the service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context **[Tree]** (config>app-assure>rad-acct-plcy>server router)

Full Context configure application-assurance radius-accounting-policy radius-accounting-server router

Description This command specifies the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.

The **no** form of this command reverts to the default value.

Default no router

Parameters *router-instance* — Specifies the router name or service ID used to specify the router instance.

service-name — Specifies the service name to identify the service, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server router)
[Tree] (config>subscr-mgmt>acct-plcy>server router)

Full Context configure subscriber-mgmt radius-accounting-policy radius-accounting-server router
configure subscriber-mgmt authentication-policy radius-authentication-server router

Description This command specifies the virtual router instance applicable for the set of configured RADIUS servers. This value cannot be changed once a RADIUS server is configured for this policy. When the value is zero, both base and management router instances are matched.

The **no** form of this command reverts to the default.

Parameters *router-instance* — Specifies the virtual router instance

Values
router-name: Base, management

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

service-id: 1 to 2147483647

service-name — Specifies the service name, up to 64 characters..

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance* **address** *ip-address*
no router

Context **[Tree]** (config>aaa>diam-peer-plcy>proxy router)

Full Context configure aaa diameter-peer-policy proxy router

Description This command configures the IPv4or IPv6 address and routing context on which the Diameter proxy is listening for the client connections and is applicable to Diameter proxy only.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Parameters *router-instance* — Specifies the routing context in which Diameter proxy is configured.

ip-address — Specifies the IPv4 or IPv6 address to which the Diameter proxy is listening.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
router service *service-name*
no router

Context **[Tree]** (config>aaa>diam-peer-plcy router)
[Tree] (config>aaa>diam>node router)

Full Context configure aaa diameter node router
configure aaa diameter-peer-policy router

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command references the routing-instance from which diameter peering connection is initiated.

The **no** form of this command reverts to the default.

Default router “Base”

Parameters *router-instance* — Specifies the router instance.

Values *router-name* | *vprn-svc-id*
router-name: Base, management Default - Base
vprn-svc-id: 1 to 2147483647

service-name — Specifies the service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
no router

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query router)

Full Context configure subscriber-mgmt wlan-gw tunnel-query router

Description This command enables matching only on tunnels that are terminated in the specified routing instance.

The **no** form of this command disables matching on a routing instance.

Default no router

Parameters *router-instance* — Specifies the routing instance in the form of *router-name* or *vprn-svc-id*.

Values *router-name* — Base
vprn-svc-id — 1 to 2147483647

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context **[Tree]** (config>aaa>radius-srv-plcy>servers router)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa radius-server-policy servers router

Description This command specifies the virtual router instance applicable for the set of configured RADIUS servers. This value cannot be changed once a RADIUS server is configured for this policy.

The **no** form of this command reverts to the default.

Parameters *router-instance* — Specifies the router instance.

Values

service-name	Service name, up to 64 characters.	
	router-instance:	router-name, service-id
	router-name:	Base, management
	service-id:	1 to 2147483647

service-name — Specifies the router name service-id up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
no router

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw router)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw router)

Full Context configure service ies subscriber-interface group-interface wlan-gw router
configure service vprn subscriber-interface group-interface wlan-gw router

Description This command specifies the routing instance that wlan-gw gateway endpoint resides in.

The **no** form of this command removes the value from the wlan-gw configuration.

Default router

Parameters *router-instance* — Specifies the identifier of the virtual router instance where the tunneled UE traffic is routed.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** [*router-instance*] [**create**]
no router [*router-instance*]

Context **[Tree]** (config router)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router

Description Commands in this context configure router parameters including interfaces, route policies and protocols. This command is also used to create CPM router instances.

For CPM router instances, this command enters or creates a user-created CPM router instance. A CPM router instance is a not a VPRN router instance. VPRN router instances are configured under **configure service vprn**. CPM router instances are the only type of non-VPRN router instances that can be created by a user, and they have a user-defined name. CPM router instances only use CPM/CCM ethernet ports as interfaces.

Parameters *router-instance* — Specifies the router name or CPM router instance.

Values

router-instance : *router name*

router-name	Base | management | *cpm-vr-name*
cpm-vr-name	[32 characters maximum]

Default Base

create — Mandatory keyword when creating a router instance. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

router

Syntax **router** *router-instance* **group** *tunnel-group-name*
router group *tunnel-group-name* **service-name** *service-name*
no router

Context **[Tree]** (config>service>epipe>sap>l2tpv3-session router)
[Tree] (config>service>vpls>sap>l2tpv3-session router)

Full Context configure service epipe sap l2tpv3-session router
configure service vpls sap l2tpv3-session router

Description This command configures the service and L2TPv3 group to which this L2TPv3 session should be associated. The associated services are used to provide transport for the L2TPv3 tunnel. The service can be specified with either the service-name or router ID. The group name specifies the L2TPv3 group parameters that should be associated with the session.

The **no** form of this command deletes the router configuration.

Parameters *router-instance* — Specifies the router name or service ID used to identify the router instance.

Values

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-instance: *router-name* or *vprn-svc-id*

router-name	"Base"
vprn-svc-id	1 to 2147483647

Default Base

tunnel-group-name — Specifies the tunnel group name, up to 32 characters.

service-name — Specifies the service name, up to 64 characters.

Platforms All

router

Syntax **router** [*router-instance*]
router service-name *service-name*

Context **[Tree]** (debug router)

Full Context debug router

Description Commands in this context enable debugging of various protocols and areas of a *router-instance*.

Parameters *router-instance* — Specifies the router name, CPM router instance, or service ID.

Values *router-name* or *service-id*

router-instance : *router-name*

router-name	Base | management | *cpm-vr-name*
cpm-vr-name	[32 characters maximum]

service-id: 1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

Platforms All

router

Syntax **router** *router-instance*
router service *vprn-service-name*

Context **[Tree]** (config>system>file-trans-prof router)

Full Context configure system file-transmission-profile router

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the routing instance that the transport protocol uses.

Default router Base

Parameters *router-instance* — Specifies the router instance on which the file transmission connection will be established.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **router service** *vprn-service-name* variant can be used in all configuration modes.

Values {router-name | *vprn-svc-id*}

router-name: Base, management
router-name is an alias for input only. The *router-name* gets replaced with an id automatically by SR OS in the configuration).

vprn-svc-id: 1 to 2147483647

Default Base

service *vprn-service-name* — Identifies the service, up to 64 characters.

Platforms All

router

Syntax **router** *router-instance*
router service *vprn-service-instance*
no router

Context **[Tree]** (config>system>management-interface>remote-management router)

Full Context configure system management-interface remote-management router

Description This command defines the router instance in which all remote managers are reachable.

If this command is also configured for a specific manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command configures management as the router (default).

Default router management

Parameters *router-instance* — Specifies a router instance on which the remote management connection is established, up to 32 characters.

service *vprn-service-instance* — Specifies a VPRN service instance, up to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

router

Syntax **router** *router-instance*
router service *vprn-service-instance*
no router

Context **[Tree]** (config>system>management-interface>remote-management>manager router)

Full Context configure system management-interface remote-management manager router

Description This command defines the router instance in which this manager is reachable.

This command takes precedence over the same command configured in the global context (**config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command causes the router to be inherited from the global context (**config**>**system**>**management-interface**>**remote-management**).

Default management

Parameters *router-instance* — Specifies the router instance on which the remote management connection is established for this manager, up to 32 characters.

service *vprn-service-instance* — Specifies a VPRN service instance, up to 64 characters.

Platforms All

router

Syntax **router** *router-instance*
no router

Context **[Tree]** (config>isa>nat-group>inter-chassis-redundancy router)

Full Context configure isa nat-group inter-chassis-redundancy router

Description This command configures routing instance through which ISAs communicate between redundant nodes and synchronize their flow state.

The **no** form of this command removes the router instance from the configuration.

Default no router

Parameters *router-instance* — Specifies the router name or service ID for the router instance.

Values *<router-name>*| *<vprn-svc-id>*
router-name: "Base"

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vprn-svc-id: 1 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context **[Tree]** (config>aaa>isa-radius-plcy>servers router)

Full Context configure aaa isa-radius-policy servers router

Description This command specifies the number of times the router attempts to contact the RADIUS server for authentication, if not successful the first time.

The **no** form of the command reverts to the default value.

Default no router

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

router

Syntax **router** *router-instance*
router service-name *service-name*
no router

Context **[Tree]** (config>mirror>mirror-dest>encap>layer-3-encap router)

Full Context configure mirror mirror-dest encap layer-3-encap router

Description This command specifies the routing instance into which to inject the mirrored packets. The packets are forwarded in the routing instance based on the configurable destination IP address in the inserted IP header. If a mirror-dest is configured to inject into a VPRN service, then that VPRN service cannot be deleted. A mirror-dest with layer-3-encap is set to operationally down if the configured destination IP address is not reachable via an interface in the routing instance or service configured for the mirror-dest. No changes are allowed to the router configuration once a gateway is configured. A service must already exist before it is specified as a router-instance. VPRN and IES services share the same number space for the service-id, but IES services cannot be specified as the router-instance for routable LI encap.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Forwarding of routable encapsulated LI packets out an R-VPLS interface is not supported. A mirror-dest configured with routable encapsulation can be bound to a routing instance that also has an R-VPLS bound to it but the operator must ensure that the destination of the LI packets is not reachable via any R-VPLS interfaces. Any routable encapsulated LI packets that arrive at the egress of an R-VPLS interface are discarded. Parallel use of routable LI encapsulation and R-VPLS in the same routing instance is supported as long as the mirrored packets do not egress out the R-VPLS interface.

Default router Base

Parameters *router-instance* — Specifies the router instance.

Values <*router-name*> | <*service-id*>

router-name	"Base", *name*
service-id	1 to 2147483647

service-name — Specifies the service name, up to 64 characters.

Platforms All

router

Syntax **router** *router-instance*
no router

Context **[Tree]** (config>li>mirror-dest-template>layer-3-encap router)

Full Context configure li mirror-dest-template layer-3-encap router

Description This command specifies the routing instance into which to inject the mirrored packets. The packets will be forwarded in the routing instance based on the configurable destination IP address in the inserted IP header. This parameter can be overridden by RADIUS.

If a mirror destination is configured to inject into a VPRN service, that VPRN service cannot be deleted. A mirror destination with Layer 3 encapsulation will be set to operationally down if the configured destination IP address is not reachable via an interface in the routing instance or service configured for the mirror destination. A service must exist before it is specified as a router instance. VPRN and IES services share the same number space for the service ID; however, IES services cannot be specified as the router instance for routable LI encapsulation.

Default router "Base"

Parameters *router-instance* — Specifies the router instance using the router name or service ID.

Values		
router-instance	*router-name* | *vprn-svc-id*	
	router-name	"Base"

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vprn-svc-id	1 to 2147483647

Platforms All

router

Syntax **router** *router-name*
no router

Context **[Tree]** (config>li>x-interfaces>lics>lic router)

Full Context configure li x-interfaces lics lic router

Description This command configures the router instance that the X-interfaces must use for communication.

The **no** form of this command reverts to the default.

Parameters *router-name* — Specifies the router name or VPRN service ID.

Values <*router-name*>, <*vprn-svc-id*>

router-name	Base
vprn-svc-id	1 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

router

Syntax **router** *router-or-service*
router service-name *service-name*
no router

Context **[Tree]** (config>oam-pm>session>ip router)

Full Context configure oam-pm session ip router

Description This command numerically references the source context from which the TWAMP Light packet is launched. The **router-instance** *router-instance* configuration, under the same context as the **router** command, is the preferred method for referencing. This method references the launch context by name, and not number, or alias that converts **service-name** to a number.

The **no** form of this command restores the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *router-or-service* — Specifies the numerical reference to the router instance or service. Well known router-name "Base" is allowed for convenience, but mapped numerically.

Values {*router-name* | *vprn-svc-id*}

router-name: Base
vprn-svc-id: 1 to 2147483647

The parameter *router-instance* is preferred for specifying the router or service.

service-name — Specifies the alias function that allows the service-name to be used converted and stored as service ID, up to 64 characters. The parameter *router-instance* is preferred for specifying the router or service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

router

Syntax [**no**] **router** *router-instance* **interface** *interface-name*

Context **[Tree]** (config>cflowd>collector>exp-filter>if-list router)

Full Context configure cflowd collector export-filter interface-list router

Description This command identifies an interface for which ingress sampled data flows should be sent to the associated collector.

The **no** form of this command removes the specified interface from the **interface-list** filter.

Parameters *router-instance* — Specifies the router instance ID associated with the interface name

Values *router-name* | *vprn-svc-id*
router-name: Base, management Default - Base
vprn-svc-id: 1 to 2147483647

interface-name — Specifies the interface name, up to 32 characters and must start with a letter, for the desired router to the service interface or SAP

Platforms All

router

Syntax [**no**] **router** *router-instance*

Context **[Tree]** (config>cflowd>collector>export-filter router)

Full Context configure cflowd collector export-filter router

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the flow data from only specific router instances to be sent to the associated collector.

Multiple router instances can be configured by issuing the command multiple times with the different router-instances.

The **no** form of this command removes the specified router-instance restriction, which means flows from that router-instance will no longer be exported. If all router-instances are removed, then flows from all router instances are sent to the associated collector.

Default no router

Parameters *router-instances* — Specifies the router name or router instance VPRN service ID. Only "Base" is supported.

Values router-name: Base, management Default - management
vprn-svc-id: 1 to 2147483647

Platforms All

router

Syntax **router** {*router-name* | *vprn-svc-id*}

Context **[Tree]** (config>cflowd>collector router)

Full Context configure cflowd collector router

Description This command configures the flow data sent to the associated collector to be sent within the specified router context. If this parameter is not specified, flow data is exported using the management routing context.

Default router management

Parameters *router-name* — Specifies the router name.

Values Base, management

Default management

vprn-svc-id — Specifies the router instance VPRN service ID.

Values 1 to 2147483647

Platforms All

router

Syntax **router** *router-instance*
router service-name *service-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no router

Context [Tree] (config>filter>redirect-policy router)

Full Context configure filter redirect-policy router

Description This command enhances VRF support in redirect policies. When a router instance is specified, the configured destination tests are run in the specified router instance, and the PBR action is executed in the specified router instance. If no destination is active or if the hardware does not support PBR action “next-hop router”, action forward will be executed (i.e. routing will be performed in the context of the incoming interface routing instance).

The **no** form of the command preserves backward-compatibility. Tests always run in the “Base” routing instance context, and the PBR action executes in the routing context of the ingress interface that the filter using this redirect policy is deployed on.

Default no router

Parameters *router-instance* — Specifies a router instance in the form of **router-name** or **service-id**.

Values **router-name** — Base

service-id — Specifies an existing Layer 3 service [1 to 2147483647]

service-name — Specifies the name of a configured Layer 3 service.

Platforms All

router

Syntax **router** {**eq** | **neq**} *router-instance* [**regexp**]
no router

Context [Tree] (config>log>filter>entry>match router)

Full Context configure log filter entry match router

Description This command specifies the log event matches for the router.

The **no** form of this command removes the log event matches.

Parameters **eq** — Determines if the matching criteria should be equal to the specified value.

neq — Determines if the matching criteria should not be equal to the specified value.

router-instance — Specifies a router name, up to 32 characters, to be used in the match criteria.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** keyword is specified, the string in the **router** command is a regular expression string that will be matched against the subject string in the log event being filtered.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

router

Syntax **router service-name** *service-name*
router *router-instance*
no router

Context [Tree] (config>system>security>mgmt-access-filter>ip-filter>entry router)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry router)

Full Context configure system security management-access-filter ip-filter entry router
configure system security management-access-filter ipv6-filter entry router

Description This command configures a router name or service ID to be used as a management access filter match criterion.

The **no** form the command removes the router name or service ID from the match criteria.

Parameters *router-instance* — Specifies one of the following parameters for the router instance:

router-name — Specifies a router name or CPM router instance, up to 32 characters to be used in the match criteria.

Values "Base" | "management" | "vpls-management"
Default Base

vprn-svc-id — Specifies a CPM router instance to be used in the match criteria.

Values 1 to 2147483647

service name — Specifies an existing service name, up to 64 characters.

Platforms All

router

Syntax **router service-name** *service-name*
router *router-instance*
no router

Context [Tree] (cfg>sys>sec>cpm>ip-filter>entry>match router)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match router)

Full Context configure system security cpm-filter ip-filter entry match router
configure system security cpm-filter ipv6-filter entry match router

Description This command specifies a router name or a service-id to be used in the match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no router

Parameters *router-instance* — Specifies one of the following parameters for the router instance:

router-name — Specifies a router name up to 32 characters to be used in the match criteria.

service-id — Specifies an existing service ID to be used in the match criteria.

Values 1 to 2147483647

service-name — Specifies an existing service name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

router

Syntax **router service-name** *service-name*
router *router-instance*
no router

Context **[Tree]** (config>bmp>station>connection router)

Full Context configure bmp station connection router

Description This command configures the router instance to be used to connect to the associate BMP monitoring station.

The **no** form of this command removes the parameters from the configuration.

Parameters *service-name* — Specifies the name associated with the VPRN service through which the BMP monitoring station connection should traverse.

router-instance — Specifies the routing instance where the lead pool resides.

Values *router-name* | *vprn-service-id*
router-name: "Base" Default - Base
vprn-svc-id: 1 to 2147483647
service-name: The service name up to 64 characters in length.

Platforms All

22.285 router-advertisement

router-advertisement

Syntax [**no**] **router-advertisement**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn router-advertisement)

Full Context configure service vprn router-advertisement

Description This command configures router advertisement properties. By default, it is disabled for all IPv6 enabled interfaces.

The **no** form of this command disables all IPv6 interface. However, the **no interface** *interface-name* command disables a specific interface.

Default no router-advertisement

Platforms All

router-advertisement

Syntax [**no**] **router-advertisement**

Context [Tree] (config>router router-advertisement)

Full Context configure router router-advertisement

Description This command configures router advertisement properties. By default, it is disabled for all IPv6 enabled interfaces.

The **no** form of this command disables all IPv6 interface. However, the **no interface** *interface-name* command disables a specific interface.

Default disabled

Platforms All

22.286 router-advertisement-policy

router-advertisement-policy

Syntax **router-advertisement-policy** *policy*
no router-advertisement-policy

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host router-advertisement-policy)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host router-advertisement-policy)

Full Context configure subscriber-mgmt local-user-db ipoe host router-advertisement-policy
configure subscriber-mgmt local-user-db ppp host router-advertisement-policy

Description This command applies an RA policy to the host.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the policy from the configuration.

Parameters *policy* — Specifies the policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router-advertisement-policy

Syntax **router-advertisement-policy** *name* [**create**]
no router-advertisement-policy *name*

Context **[Tree]** (config>subscr-mgmt router-advertisement-policy)

Full Context configure subscriber-mgmt router-advertisement-policy

Description This command creates a router advertisement policy or enters the context to configure a router advertisement policy. The keyword **create** is mandatory when creating a router advertisement policy the first time.

The **no** form of this command deletes the specified router advertisement policy.

Parameters *name* — Specifies the router advertisement policy name up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — Specifies the keyword used to create the router advertisement policy. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.287 router-advertisements

router-advertisements

Syntax [**no**] **router-advertisements**

Context **[Tree]** (config>service>ies>sub-if>ipv6 router-advertisements)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 router-advertisements)
[Tree] (config>service>vprn>sub-if>ipv6 router-advertisements)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 router-advertisements)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements
configure service ies subscriber-interface ipv6 router-advertisements
configure service vprn subscriber-interface group-interface ipv6 router-advertisements

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface ipv6 router-advertisements

Description This command enables IPv6 router advertisements for this interface.

The **no** form of this command disables the router advertisements.

Default router-advertisements

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.288 router-id

router-id

Syntax **router-id** *ip-address*
no router-id

Context **[Tree]** (config>service>vprn router-id)
[Tree] (config>service>vprn>ospf router-id)
[Tree] (config>service>vprn>bgp router-id)

Full Context configure service vprn bgp router-id
configure service vprn ospf router-id
configure service vprn router-id

Description This command sets the router ID for a specific VPRN context.

When configuring the router ID in the base instance of OSPF it overrides the router ID configured in the **config>router** context. The default value for the base instance is inherited from the configuration in the **config>router** context. If the router ID in the **config>router** context is not configured, the following applies:

- The system uses the system interface address (which is also the loopback address).
- If a system interface address is not configured, use the last 32 bits of the chassis MAC address.

If neither the router ID nor system interface are defined, the router ID from the base router context is inherited.

This is a **required** command when configuring multiple instances and the instance being configured is not the base instance.

When configuring a new router ID, the instance is not automatically restarted with the new router ID. The next time the instance is initialized, the new router ID is used.

To force the new router ID to be used, issue the **shutdown** and **no shutdown** commands for the instance, or reboot the entire router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

It is possible to configure an SR OS to operate with an IPv6 only BOF and no IPv4 system interface address. When configured in this manner, the operator must explicitly define IPv4 router IDs for protocols such as OSPF and BGP as there is no mechanism to derive the router ID from an IPv6 system interface address.

The **no** form of this command removes the router ID definition from the given VPRN context.

Default no router-id

Parameters *ip-address* — The IP address must be given in dotted decimal notation.

Platforms All

router-id

Syntax **router-id** *ip-address*
no router-id

Context **[Tree]** (config>service>vprn>isis router-id)

Full Context configure service vprn isis router-id

Description This command sets the router ID for a specific VPRN context.

If neither the router ID nor system interface are defined, the router ID from the base router context is inherited.

The **no** form of this command removes the router ID definition from the given VPRN context.

Default no router-id

Parameters *ip-address* — The IP address must be given in dotted decimal notation.

Platforms All

router-id

Syntax [**no**] **router-id** *ip*

Context **[Tree]** (config>router>mpls>srlg-database router-id)

Full Context configure router mpls srlg-database router-id

Description Commands in this context configure the link members of SRLG groups for a specific router in the network. The user must also use this command to enter the local interface SRLG membership into the user SRLG database. Use by CSPF of all interface SRLG membership information of a specific router ID may be temporarily disabled by shutting down the node. If this occurs, CSPF assumes these interfaces have no SRLG membership association.

The **no** form of this command will delete all interface entries under the router ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the router ID for this system. This must be the router ID configured under the base router instance, the base OSPF instance or the base IS-IS instance.

Platforms All

router-id

Syntax **router-id** *ip-address*
no router-id

Context **[Tree]** (config>router router-id)

Full Context configure router router-id

Description This command configures the router ID for the router instance.

The router ID is used by both OSPF and BGP routing protocols in this instance of the routing table manager. IS-IS uses the router ID value as its system ID.

When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is initialized, the new router ID is used. This can result in an interim period of time when different protocols use different router IDs.

It is possible to configure SR OS to operate with an IPv6 only BOF and no IPv4 system interface address. When configured in this manner, the operator must explicitly define IPv4 router IDs for protocols such as OSPF and BGP as there is no mechanism to derive the router ID from an IPv6 system interface address.

To force the new router ID to be used, issue the **shutdown** and **no shutdown** commands for each protocol that uses the router ID, or restart the entire router.

The system uses the system interface address which is also the loopback address. If a system interface address is not configured, use the last 32 bits of the chassis MAC address.

The **no** form of this command removes the configured value and the last 32 bits of the chassis MAC address are used.

Default no router-id

Parameters *ip-address* — Specifies the 32 bit router ID expressed in dotted decimal notation or as a decimal value.

Platforms All

router-id

Syntax **router-id** *ip-address*
no router-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp router-id)

Full Context configure router bgp router-id

Description This command specifies the router ID to be used with this BGP instance.

Changing the BGP router ID on an active BGP instance causes the BGP instance to restart with the new router ID.

It is possible to configure an SR OS to operate with an IPv6 only BOF and no IPv4 system interface address. When configured in this manner, the operator must explicitly define IPv4 router IDs for protocols such as OSPF and BGP as there is no mechanism to derive the router ID from an IPv6 system interface address.

When no **router-id** is configured for BGP, the system interface IP address is used.

Default no router-id

Parameters *ip-address* — Specifies the router ID, expressed as any non-zero value in the range 0.0.0.1 to 255.255.255.255 (or when converted to decimal it can have any value in the range 1-4294967295). It is recommended to use the system IPv4 address.

Platforms All

router-id

Syntax **router-id** *router-id*
no router-id

Context [Tree] (config>router>isis router-id)

Full Context configure router isis router-id

Description This command configures the router ID.

The **no** form of this command deletes the router ID.

Parameters *router-id* — The IP address of the router.

Platforms All

router-id

Syntax **router-id** *ip-address*
no router-id

Context [Tree] (config>router>ospf router-id)
[Tree] (config>router>ospf3 router-id)

Full Context configure router ospf router-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ospf3 router-id

Description This command configures the router ID for the OSPF instance. This command configures the router ID for the OSPF instance.

When configuring the router ID in the base instance of OSPF it overrides the router ID configured in the **config**>**router** context.

The default value for the base instance is inherited from the configuration in the **config**>**router** context. If the router ID in the **config**>**router** context is not configured, the following applies:

- the system uses the system interface address (which is also the loopback address)
- if a system interface address is not configured, it uses the last 32 bits of the chassis MAC address

This is a **required** command when configuring multiple instances and the instance being configured is not the base instance.

When configuring a new router ID, the instance is not automatically restarted with the new router ID. The next time the instance is initialized, the new router ID is used.

To force the new router ID to be used, issue the **shutdown** and **no shutdown** commands for the instance, or reboot the entire router.

It is possible to configure an SR OS to operate with an IPv6 only BOF and no IPv4 system interface address. When configured in this manner, the operator must explicitly define IPv4 router IDs for protocols such as OSPF and BGP as there is no mechanism to derive the router ID from an IPv6 system interface address.

The **no** form of this command to reverts to the default value.

Platforms All

22.289 router-instance

router-instance

Syntax **router-instance** *router-instance*
no router-instance

Context **[Tree]** (config>oam-pm>session>ip router-instance)

Full Context configure oam-pm session ip router-instance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command references the source context from which the TWAMP Light packet is launched by name. The **router-instance** *router-instance* configuration is the preferred method for referencing and references the launch context by name, not number or alias that converts **service-name** to a number.

The **no** form of this command restores the default value.

Parameters *router-instance* — Specifies the preferred method for entering a service name. Stored as the service name. Only the service linking function is allowed for both mixed-mode and model-driven configuration modes, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

router-instance

Syntax **router-instance** *router-instance*
router-instance service *vprn-service-instance*
no router-instance

Context **[Tree]** (config>system>grpc-tunnel>destination-group>destination router-instance)
[Tree] (config>system>telemetry>destination-group>destination router-instance)

Full Context configure system grpc-tunnel destination-group destination router-instance
configure system telemetry destination-group destination router-instance

Description This command configures the router instance for the destination group.

The **no** form of this command reverts to the default value.

Default router-instance management

Parameters *router-instance* — Specifies the router instance type, up to 32 characters.

Values management, base

vprn-service-instance — Specifies the VPRN service instance, up to 64 characters.

Platforms All

22.290 router-lifetime

router-lifetime

Syntax **router-lifetime** *seconds*
router-lifetime no-default-router
no router-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>rtr-adv-plcy router-lifetime)

Full Context configure subscriber-mgmt router-advertisement-policy router-lifetime

Description This command specifies the router lifetime.

The **no** form of this command returns the command to the default setting.

Default router-lifetime 4500

Parameters *seconds* — Specifies the time, in seconds, for the prefix to remain preferred.

Values 2700 to 9000

no-default-router — Specifies that the router is not to be used as a default router.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

router-lifetime

Syntax **router-lifetime** *seconds*
router-lifetime no-default-router
no router-lifetime

Context [Tree] (config>service>ies>sub-if>ipv6>rtr-adv router-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv router-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv router-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv router-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements router-lifetime
configure service ies subscriber-interface ipv6 router-advertisements router-lifetime
configure service vprn subscriber-interface group-interface ipv6 router-advertisements router-lifetime
configure service vprn subscriber-interface ipv6 router-advertisements router-lifetime

Description This command configures the value to be placed in the router lifetime field of router advertisements sent from this interface. A value of zero indicates this router should not be used by hosts as a default router.

The **no** form of this command reverts to the default.

Default router-lifetime 4500

Parameters *seconds* — Specifies the router lifetime in seconds for this group-interface.

Values 2700 to 9000

no-default-router — Specifies that the router is not to be used as a default router.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-lifetime

Syntax **router-lifetime** *seconds*
no router-lifetime

Context **[Tree]** (config>router>router-advert>if router-lifetime)
[Tree] (config>service>vprn>router-advert>if router-lifetime)

Full Context configure router router-advertisement interface router-lifetime
configure service vprn router-advertisement interface router-lifetime

Description This command sets the router lifetime.

Default router life-time 1800

Parameters *seconds* — The length of time, in seconds, (relative to the time the packet is sent) that the prefix is valid for route determination.

Values 0, 4 to 9000 seconds. 0 means that the router is not a default router on this link.

Platforms All

22.291 router-solicit

router-solicit

Syntax **router-solicit**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6 router-solicit)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6 router-solicit)
[Tree] (config>service>vprn>sub-if>ipv6 router-solicit)
[Tree] (config>service>ies>sub-if>ipv6 router-solicit)

Full Context configure service ies subscriber-interface group-interface ipv6 router-solicit
configure service ies subscriber-interface ipv6 router-solicit
configure service vprn subscriber-interface group-interface ipv6 router-solicit
configure service vprn subscriber-interface ipv6 router-solicit

Description Commands in this context configure parameters used for router-solicit based authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.292 router-solicitation

router-solicitation

Syntax [**no**] **router-solicitation**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6>auto-reply router-solicitation)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>auto-reply router-solicitation)

Full Context configure service ies subscriber-interface group-interface ipv6 auto-reply router-solicitation
configure service vprn subscriber-interface group-interface ipv6 auto-reply router-solicitation

Description This command enables auto-reply router solicitation.

The **no** form of this command disables auto-reply router solicitation.

Default router-solicitation

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.293 router-target-as-number

router-target-as-number

Syntax **router-target-as-number** *as-number*
no router-target-as-number

Context **[Tree]** (config>subscr-mgmt>vrgw>lanext router-target-as-number)

Full Context configure subscriber-mgmt vrgw lanext router-target-as-number

Description This command specifies the AS number for the HLE service. It is used to derive the route target (RT) and route distinguisher (RD) for the HLE EVPN service only when the RADIUS server does not return a specific route target or route distinguisher.

The derived RT is in the “target:<configured-router-target-as-number>:<returned Alc-Bridge-Id>” format.

The derived RD is in the “<configured-router-target-as-number>:<returned Alc-Bridge-Id>” format.

The **no** form of this command removes the AS number from the configuration.

Parameters *as-number* — Specifies the AS number of the HLE service.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.294 router-unsolicited-na-flood-evpn

router-unsolicited-na-flood-evpn

Syntax [**no**] **router-unsolicited-na-flood-evpn**

Context **[Tree]** (config>service>vpls>proxy-nd router-unsolicited-na-flood-evpn)

Full Context configure service vpls proxy-nd router-unsolicited-na-flood-evpn

Description This command controls whether the system floods router unsolicited Neighbor Advertisements to EVPN. The NA messages impacted by this command are NA messages with the following flags: S=0 and R=1.

The **no** form of the command will only flood to local SAPs/binds but not to EVPN destinations. This is only recommended in networks where CEs are routers directly connected to the PEs. Networks using aggregation switches between the host/routers and the PEs should flood unsolicited NA messages in EVPN to ensure that the remote caches are updated and BGP does not miss the advertisement of these entries.

Default router-unsolicited-na-flood-evpn

Platforms All

22.295 routing-type0

routing-type0

Syntax **routing-type0** {**true** | **false**}
no routing-type0

Context **[Tree]** (config>filter>ipv6-filter>entry>match routing-type0)

Full Context configure filter ipv6-filter entry match routing-type0

Description This command enables match on existence of Routing Type Extension Header type 0 in the IPv6 filter policy.

The **no** form of this command ignores Routing Type Extension Header type 0 presence/absence in a packet when evaluating match criteria of a given filter policy entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no routing-type0

Parameters **true** — Specifies whether a packet contains Routing Type Extension Header type 0.

false — Specifies whether a packet does not contain Routing Type Extension Header type 0.

Platforms All

22.296 rp

rp

Syntax **rp**

Context **[Tree]** (config>service>vprn>pim rp)

Full Context configure service vprn pim rp

Description This command enables access to the context to configure the rendezvous point (RP) of a PIM protocol instance.

A Nokia PIM router acting as an RP must respond to a PIM register message specifying an SSM multicast group address by sending stop register message(s) to the first hop router. It does not build an (S, G) shortest path tree toward the first hop router. An SSM multicast group address can be either from the SSM default range of 232/8 or from a multicast group address range that was explicitly configured for SSM.

Default rp enabled when PIM is enabled.

Platforms All

rp

Syntax **rp**

Context **[Tree]** (config>router>pim rp)

Full Context configure router pim rp

Description Commands in this context configure rendezvous point (RP) parameters. The address of the root of the group's shared multicast distribution tree is known as its RP. Packets received from a source upstream and join messages from downstream routers rendezvous at this router.

If this command is not enabled, then the router can never become the RP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.297 rp-candidate

rp-candidate

Syntax **rp-candidate**

Context **[Tree]** (config>service>vprn>pim>rp rp-candidate)
[Tree] (config>service>vprn>pim>rp>ipv6 rp-candidate)

Full Context configure service vprn pim rp ipv6 rp-candidate
configure service vprn pim rp rp-candidate

Description Commands in this context configure the candidate rendezvous point (RP) parameters.

Default enabled when PIM is enabled

Platforms All

rp-candidate

Syntax **rp-candidate**

Context **[Tree]** (config>router>pim>rp rp-candidate)
[Tree] (config>router>pim>rp>ipv6 rp-candidate)

Full Context configure router pim rp ipv6 rp-candidate
configure router pim rp rp-candidate

Description Commands in this context configure the Candidate RP parameters.

Routers use a set of available rendezvous points distributed in Bootstrap messages to get the proper group-to-RP mapping. A set of routers within a domain are also configured as candidate RPs (C-RPs); typically, these will be the same routers that are configured as candidate BSRs.

Every multicast group has a shared tree through which receivers learn about new multicast sources and new receivers learn about all multicast sources. The rendezvous point (RP) is the root of this shared tree.

Default rp-candidate shutdown

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.298 rp-set-peer

rp-set-peer

Syntax [**no**] **rp-set-peer** *ip-address*

Context **[Tree]** (config>service>vprn>pim>rp>anycast rp-set-peer)

Full Context configure service vprn pim rp anycast rp-set-peer

Description This command configures a peer in the anycast RP-set. The address identifies the address used by the other node as the RP candidate address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this RP-set.

Although there is no set maximum of addresses that can be configured in an RP-set, up to 15 multicast addresses is recommended.

The **no** form of this command removes an entry from the list.

Parameters *ip-address* — Specifies the address used by the other node as the RP candidate address for the same multicast group address range as configured on this node.

Platforms All

rp-set-peer

Syntax [**no**] **rp-set-peer** *ipv6-address*

Context **[Tree]** (config>service>vprn>pim>rp>ipv6>anycast rp-set-peer)

Full Context configure service vprn pim rp ipv6 anycast rp-set-peer

Description This command configures an IPv6 peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP- set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum of addresses that can be configured in an rp-set, up to 15 multicast addresses is recommended.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes an entry from the list.

Parameters *ipv6-address* — Specifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

Values

ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D

Platforms All

rp-set-peer

Syntax [**no**] **rp-set-peer** *ip-address*

Context **[Tree]** (config>router>pim>rp>anycast rp-set-peer)

Full Context configure router pim rp anycast rp-set-peer

Description This command configures an IP peer in the anycast RP-set. The address identifies the address used by the other node as the RP candidate address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this RP-set.

Although there is no set maximum number of addresses that can be configured in an RP-set, up to 15 IP addresses is recommended.

The **no** form of this command removes an entry from the list.

Parameters *ip-address* — Specifies an IP peer in the anycast RP-set.

Platforms All

rp-set-peer

Syntax [**no**] **rp-set-peer** *ipv6-address*

Context **[Tree]** (config>router>pim>rp>ipv6>anycast rp-set-peer)

Full Context configure router pim rp ipv6 anycast rp-set-peer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a peer in the anycast RP-set. The address identifies the address used by the other node as the RP candidate address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this RP-set.

Although there is no set maximum number of addresses that can be configured in an RP-set, up to 15 IP addresses is recommended.

The **no** form of this command removes the IPv6 address from the anycast RP set.

Parameters *ipv6-address* — Specifies an IPv6 peer in the anycast RP-set.

Platforms All

22.299 rpc-authorization

rpc-authorization

Syntax **rpc-authorization**

Context **[Tree]** (config>system>security>profile>grpc rpc-authorization)

Full Context configure system security profile grpc rpc-authorization

Description This command opens a configuration context for configuring user privileges related to RPCs.

Platforms All

22.300 rpf-select

rpf-select

Syntax **rpf-select**

Context **[Tree]** (config>service>vprn>mvpn rpf-select)

Full Context configure service vprn mvpn rpf-select

Description This command enables context for VRF extranet mapping for C-instance receivers in this receiver MVPN instance to multicast streams in P-instance core MVPN instances.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.301 rpf-table

rpf-table

Syntax **rpf-table** {**rtable-m** | **rtable-u** | **both**}
no rpf-table

Context **[Tree]** (config>service>vprn>msdp rpf-table)

Full Context configure service vprn msdp rpf-table

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/rendezvous point. However, the operator can specify the following:

- use the unicast route table only
- use the multicast route table only or
- use both the route tables

The **no** form of this command reverts to the default.

Default rpf-table rtable-u

Parameters **rtable-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table will contain routes submitted by static routes, ISIS and OSPF.

rtable-u — Specifies only that the unicast route table will be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Will always look up first in the multicast route table and, if there is a route, it will use it. If PIM does not find a route in the first lookup, it will try to find it in the unicast route table. Rtable-m is checked before rtable-u.

Platforms All

rpf-table

Syntax **rpf-table** {**rtable-m** | **rtable-u** | **both**}
no rpf-table

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>pim rpf-table)
[Tree] (config>router>msdp rpf-table)

Full Context configure router msdp rpf-table
configure service vprn pim rpf-table

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/rendezvous point. However, the operator can specify the following:

- use the unicast route table only
- use the multicast route table only
- use both the route tables

Default rpf-table rtable-u

Parameters **rtable-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table will contain routes submitted by static routes, IS-IS and OSPF.

rtable-u — Specifies only that the unicast route table will be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Specifies that the multicast route table will be used first by the multicast protocol (PIM) for checks, and then the unicast route table will be used if the multicast route table lookup fails. rtable-m is checked before rtable-u.

Platforms All

rpf-table

Syntax **rpf-table** {**rtable-m** | **rtable-u** | **both**}
no rpf-table

Context [Tree] (config>router>pim rpf-table)

Full Context configure router pim rpf-table

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source or rendezvous point. However, the operator can specify one of the following:

- use the unicast route table only
- use the multicast route table only
- use both the route tables

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default rpf-table rtable-u

Parameters **rtable-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table will contain routes submitted by static routes, ISIS and OSPF.

rtable-u — Specifies only that the unicast route table will be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Specifies to always lookup first in the multicast route table and if there is a route, it will use it. If PIM does not find a route in the first lookup, it will try to find it in the unicast route table. Rtable-m is checked before rtable-u.

Platforms All

22.302 rpf6-table

rpf6-table

Syntax **rpf6-table** {**rtable6-m** | **rtable6-u** | **both**}
no rpf6-table

Context **[Tree]** (config>service>vprn>pim rpf6-table)

Full Context configure service vprn pim rpf6-table

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a specific multicast route.

By default, only the unicast route table is looked up to calculate the RPF interface toward the source/rendezvous point. However, the operator can specify to use the following:

- unicast route table only
- multicast route table only
- both route tables

Default rpf6-table rtable6-u

Parameters **rtable6-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by static routes, ISIS and OSPF.

rtable6-u — Specifies that only the unicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by all unicast routing protocols.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

both — Specifies that the multicast route table will be used first by the multicast protocol (PIM) for IPv6 RPF checks, then the unicast route table will be used if the multicast route table lookup fails.

Platforms All

rpf6-table

Syntax **rpf6-table** {**rtable6-m** | **rtable6-u** | **both**}
no rpf6-table

Context **[Tree]** (config>router>pim rpf6-table)

Full Context configure router pim rpf6-table

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/rendezvous point. However, the operator can specify the following:

- use unicast route table only
- use multicast route table only or
- use both the route tables

The **no** form of this command reverts to the default value.

Default rpf6-table rtable6-u

Parameters **rtable6-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by static routes, ISIS and OSPF.

rtable6-u — Specifies that only the unicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Specifies that the multicast route table will be used first by the multicast protocol (PIM) for IPv6 RPF checks, and then the unicast route table will be used if the multicast route table lookup fails.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.303 rpfv

rpfv

Syntax **rpfv** [**detail**]
no rpfv

Context **[Tree]** (debug>router>pim rpfv)

Full Context debug router pim rpfv

Description This command enables debugging for PIM RPF vector.

The **no** form of this command disables debugging for PIM RPF vector.

Parameters **detail** — Debugs detailed RPF vector information.

Platforms All

rpfv

Syntax **rpfv core**
rpfv mvpn
rpfv core mvpn
no rpfv [**core**] [**mvpn**]

Context **[Tree]** (config>router>pim rpfv)

Full Context configure router pim rpfv

Description This command enables RPF Vector processing for Inter-AS Rosen MVPN Option-B and Option-C. The **rpfv** must be enabled on every node for Inter-AS Option B/C MVPN support.

If **rpfv** is configured, MLDP inter-AS resolution cannot be used. These two features are mutually exclusive.

The **no** form of this command reverts to the default.

Default no rpfv

Parameters **mvpn** — Enables MVPN RPF vector processing for Inter-AS Option B/C MVPN based on RFC 5496 and RFC 6513. If a core RPF vector is received, it will be dropped before a message is processed.

core — Enables core RPF vector (no RD) processing for Inter-AS Option B/C MVPN, which allows SR OS interoperability as P-router with third-party vendors that do not encode RD in the RPF vector for Inter-AS MVPN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

core mvpn — Enables core RPF vector (no RD) processing for Inter-AS Option B/C MVPN, which allows SR OS interoperability as P-router with third-party vendors that do not encode RD in the RPF vector for Inter-AS MVPN.

The **no** version of this command disables RPF Vector processing. If RPF vector is received in a PIM join message, the vector will be removed before local processing of PIM message starts.

Platforms All

22.304 rpki-session

rpki-session

Syntax [**no**] **rpki-session** *ip-address*

Context **[Tree]** (config>router>origin-validation rpki-session)

Full Context configure router origin-validation rpki-session

Description This command configures a session with an RPKI local cache server by using the RPKI-Router protocol. It is over these sessions that the router learns dynamic VRP entries expressing valid origin AS and prefix associations. SR OS supports the RPKI-Router protocol over TCP/IPv4 or TCP/IPv6 transport. The router can set up an RPKI-Router session using the base routing table (in-band) or the management router (out-of-band). Configure the command in the **config**>**router management** instance to configure a session using the management port.

Default no rpki-session

Parameters *ip-address* — Specifies the IPv4 address or an IPv6 address. If the IPv6 address is link-local then the interface name must be appended to the IPv6 address after a hyphen (-).

Platforms All

rpki-session

Syntax [**no**] **rpki-session** *ip-address*

Context **[Tree]** (debug>router rpki-session)

Full Context debug router rpki-session

Description This command enables and configures debugging for RPKI session.

The **no** form of this command disables debugging for RPKI session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Debugs the RPKI session associated with the specified IP address.

Values		
ipv4-address:	a.b.c.d	
ipv6-address	x:x:x:x:x:x:x:x	[-interface]
	x:x:x:x:x:x:d.d.d.d	[-interface]
	x:	[0 to FFFF]H
	d:	[0 to 255]D
	interface	up to 32 characters, mandatory for link local addresses

Platforms All

22.305 rpl-end

rpl-end

Syntax [**no**] **rpl-end**

Context **[Tree]** (config>eth-ring>path rpl-end)

Full Context configure eth-ring path rpl-end

Description This command configures the G.8032 path as a ring protection link end. The ring should be declared as either a RPL owner or RPL neighbor for this command to be allowed. Only path a or path b can be declared an RPL-end.

The **no** form of this command sets the rpl-end to default no rpl-end.

Default no rpl-end

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.306 rpl-node

rpl-node

Syntax **rpl-node** [**owner** | **nbr**]
no rpl-node

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>eth-ring rpl-node)

Full Context configure eth-ring rpl-node

Description This command configures the G.8032 ring protection link type as owner or neighbor. The **no** form of the command means this node is not connected to an RPL link. When RPL owner or neighbor is specified either the a or b path must be configured with the **rpl-end** command. An owner is responsible for operation of the rpl link. Configuring the RPL as neighbor is optional (can be left as no rpl-node) but if the command is used the nbr is mandatory.

On a sub-ring without virtual channel it is mandatory to configure sub-ring non-virtual-link on all nodes on the sub-ring to propagate the R-APS messages around the sub-ring.

The **no** form of this command removes the RPL link.

Default no rpl-node

Parameters **owner** — Specifies the owner link type.

nbr — Specifies the neighbor link type.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.307 rr

rr

Syntax [**no**] **rr**

Context [Tree] (debug>router>gmpls>event rr)

Full Context debug router gmpls event rr

Description This command enables and disables debugging for GMPLS Refresh Reduction events.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rr

Syntax [**no**] **rr**

Context [Tree] (debug>router>rsvp>event rr)

Full Context debug router rsvp event rr

Description This command debugs refresh reduction events.

The **no** form of the command disables the debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.308 rr-use-route-table

rr-use-route-table

Syntax **rr-use-route-table**
no rr-use-route-table

Context **[Tree]** (config>router>bgp>next-hop-res>labeled-routes rr-use-route-table)

Full Context configure router bgp next-hop-resolution labeled-routes rr-use-route-table

Description This command enables BGP to perform a lookup of IGP routes in the route table to resolve the BGP next-hop of label-IPv4 and label-IPv6 routes. This is useful for a Route Reflector (RR) that does not participate in tunnel signaling protocols such as LDP and RSVP and therefore, does not have tunnels to resolve the BGP next-hops of label-unicast routes.

Configure the **disable-route-table-install** command before you configure the **rr-use-route-table** command because forwarding would otherwise be incorrect for cases where label routes are resolved this way.

Default no rr-use-route-table

Platforms All

22.309 rs-fec-mode

rs-fec-mode

Syntax **rs-fec-mode** *rs-fec-mode*
no rs-fec-mode

Context **[Tree]** (config>port>connector rs-fec-mode)

Full Context configure port connector rs-fec-mode

Description This command is used for breakout connectors when all connector ports must use the same **rs-fec-mode** setting.

In all other cases, the **rs-fec-mode** is set using the **configure port ethernet rs-fec-mode** command for each individual connector port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

See "Forward Error Correction" in the *Interface Configuration Guide* for more information about **rs-fec-mode** settings.

Default no rs-fec-mode

Parameters *rs-fec-mode* — Specifies the RS-FEC mode to support.

Values cl91-514-528, cl91-514-544

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rs-fec-mode

Syntax **rs-fec-mode** *rs-fec-mode*
no rs-fec-mode

Context **[Tree]** (config>port>ethernet rs-fec-mode)

Full Context configure port ethernet rs-fec-mode

Description This command enables RS-FEC on the Ethernet port. RS-FEC Clause 91 is required for QSFP28, CFP4, 100GBase-SR4, 100GBase-ER4 lite, and CWDM4 for the QSFP28 package optics for short-reach optics.

See "Forward Error Correction" in the *Interface Configuration Guide* for more information about **rs-fec-mode** settings.

Default no rs-fec-mode

Parameters *rs-fec-mode* — Specifies the RS-FEC mode to support.

Values cl91-514-528, cl74, cl108

Platforms All

22.310 rsa

rsa

Syntax **rsa**

Context **[Tree]** (config>system>security>user>public-keys rsa)

Full Context configure system security user public-keys rsa

Description This command allows the user to enter the context to configure RSA public keys.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.311 rsa-key

rsa-key

Syntax **rsa-key** *key-id* [**create**]
no rsa-key *key-id*

Context **[Tree]** (config>system>security>user>public-keys>rsa rsa-key)

Full Context configure system security user public-keys rsa rsa-key

Description This command creates an RSA public key and associates it with the username. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.

Parameters **create** — Keyword used to create the RSA key. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

key-id — Specifies the key identifier.

Values 1 to 32

Platforms All

22.312 rsa-signature

rsa-signature

Syntax **rsa-signature** {**pkcs1** | **pss**}

Context **[Tree]** (config>ipsec>cert-profile>entry rsa-signature)

Full Context configure ipsec cert-profile entry rsa-signature

Description This command specifies the signature scheme for RSA key.

Default rsa-signature pkcs1

Parameters **pkcs1** — Specifies the RSA pkcs#1 v1.5 signature scheme.

pss — Specifies the RSA probabilistic signature scheme.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.313 rsvp

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>res-filter rsvp)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>res-filter rsvp)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>res-filter rsvp)
[Tree] (config>service>vprn>auto-bind-tunnel>res-filter rsvp)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter rsvp
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter rsvp
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter rsvp
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter rsvp

Description This command selects the RSVP-TE tunnel type.

The **rsvp** value instructs BGP to search for the best metric RSVP LSP to the address of the BGP next hop. This address can correspond to the system interface or to another loopback interface used by the BGP instance on the remote node. The LSP metric is provided by MPLS in the tunnel table. In the case of multiple RSVP LSPs with the same lowest metric, BGP selects the LSP with the lowest **tunnel-id**.

The **no** form of this command removes the RSVP-TE tunnel type.

Default no rsvp

Platforms All

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (config>service>vpls>provider-tunnel>inclusive rsvp)

Full Context configure service vpls provider-tunnel inclusive rsvp

Description This command creates the context to configure the parameters of an RSVP P2MP LSP used for forwarding Broadcast, Unicast unknown and Multicast (BUM) packets of a VPLS or B-VPLS instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rsvp

Syntax **rsvp**
no rsvp

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive rsvp)
[Tree] (config>service>vprn>mvpn>pt>selective rsvp)

Full Context configure service vprn mvpn provider-tunnel inclusive rsvp
configure service vprn mvpn provider-tunnel selective rsvp

Description Commands in this context configure the RSVP P2MP LSP for the provider tunnel.

The **no** form of this command removes the rsvp context including all the statements in the context.

Default no rsvp

Platforms All

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (config>router rsvp)

Full Context configure router rsvp

Description Commands in this context configure RSVP protocol parameters. RSVP is not enabled by default and must be explicitly enabled (**no shutdown**).

RSVP is used to set up LSPs. RSVP should be enabled on all router interfaces that participate in signaled LSPs.

The **no** form of this command deletes this RSVP protocol instance and removes all configuration parameters for this RSVP instance. To suspend the execution and maintain the existing configuration, use the **shutdown** command. RSVP must be shutdown before the RSVP instance can be deleted. If RSVP is not shutdown, the **no rsvp** command does nothing except issue a warning message on the console indicating that RSVP is still administratively enabled.

Default no shutdown

Platforms All

rsvp

Syntax **rsvp** [**lsp** *lsp-name*] [**sender** *source-address*] [**endpoint** *endpoint-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**interface** *ip-int-name*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no rsvp

Context **[Tree]** (debug>router rsvp)

Full Context debug router rsvp

Description This command enables and configures debugging for RSVP.

Parameters **lsp** *lsp-name* — Specifies the LSP name up to 64 characters in length.

sender *source-address* — Specifies the IP address of the sender.

endpoint *endpoint-address* — Specifies the far-end IP address.

tunnel-id *tunnel-id* — Specifies the RSVP tunnel ID.

Values 0 to 4294967295

lsp-id *lsp-id* — Specifies the LSP ID.

Values 1 to 65535

interface *ip-int-name* — Specifies the interface name. The interface name can be up to 32 characters long and must be unique. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (config>router>gtm>pt>inclusive rsvp)
[Tree] (config>router>gtm>pt>selective rsvp)

Full Context configure router gtm provider-tunnel inclusive rsvp
configure router gtm provider-tunnel selective rsvp

Description This command enables the use of P2MP RSVP as the inclusive or selective provider tunnel.

The **no** form of this command removes the RSVP context including all the statements in the context.

Default no rsvp

Platforms All

rsvp

Syntax **rsvp**

Context **[Tree]** (config>oam-pm>session>mpls>lsp rsvp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure oam-pm session mpls lsp rsvp

Description Commands in this context configure an RSVP LSP and its attributes to be tested.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (config>router>bgp>next-hop-res>lbl-routes>transport-tunn>family>res-filter rsvp)
[Tree] (config>router>bgp>next-hop-res>shortcut-tunn>family>res-filter rsvp)

Full Context configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter rsvp
configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter rsvp

Description This command selects RSVP tunneling for next-hop resolution and specifies RSVP tunnels in a tunnel table to IPv4 destinations. This option allows BGP to use the best metric RSVP LSP to the address of the BGP next-hop. This address can correspond to the system interface or to another loopback interface of the remote BGP router. In the case of multiple RSVP LSPs with the same lowest metric, BGP selects the LSP with the lowest tunnel ID.

Platforms All

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (conf>router>isis>igp-sc>tunn-nh>family>res-filter rsvp)

Full Context configure router isis igp-shortcut tunnel-next-hop family resolution-filter rsvp

Description This command selects the RSVP-TE tunnel type in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

Platforms All

rsvp

Syntax [**no**] **rsvp**

Context **[Tree]** (config>router>ospf>igp-sc>tunnel-nh>family>res-filter rsvp)
[Tree] (config>router>ospf3>igp-sc>tunnel-nh>family>res-filter rsvp)

Full Context configure router ospf igp-shortcut tunnel-next-hop family resolution-filter rsvp
configure router ospf3 igp-shortcut tunnel-next-hop family resolution-filter rsvp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command selects the RSVP-TE tunnel type in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

Platforms All

22.314 rsvp-auto

rsvp-auto

Syntax **rsvp-auto**

Context **[Tree]** (config>oam-pm>session>mpls>lsp rsvp-auto)

Full Context configure oam-pm session mpls lsp rsvp-auto

Description Commands in this context configure the RSVP auto LSP and its attributes for testing.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.315 rsvp-resv-style

rsvp-resv-style

Syntax **rsvp-resv-style** [**se** | **ff**]

Context **[Tree]** (config>router>mpls>lsp rsvp-resv-style)

Full Context configure router mpls lsp rsvp-resv-style

Description This command specifies the RSVP reservation style, shared explicit (se) or fixed filter (ff). A reservation style is a set of control options that specify a number of supported parameters. The style information is part of the LSP configuration.

Default rsvp-resv-style se

Parameters **ff** — Fixed filter is single reservation with an explicit scope. This reservation style specifies an explicit list of senders and a distinct reservation for each of them. A specific reservation request is created for data packets from a particular sender. The reservation scope is determined by an explicit list of senders.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

se — Shared explicit is shared reservation with a limited scope. This reservation style specifies a shared reservation environment with an explicit reservation scope. This reservation style creates a single reservation over a link that is shared by an explicit list of senders. Because each sender is explicitly listed in the RESV message, different labels can be assigned to different sender-receiver pairs, thereby creating separate LSPs.

Platforms All

22.316 rsvp-shortcut

rsvp-shortcut

Syntax **rsvp-shortcut** [*ip-address*]
no rsvp-shortcut

Context **[Tree]** (debug>router>ospf rsvp-shortcut)

Full Context debug router ospf rsvp-shortcut

Description This command debugs the OSPFv2 RSVP shortcut.

Parameters *ip-address* — Specifies the IP address to debug.

Platforms All

22.317 rsvp-te

rsvp-te

Syntax **rsvp-te** *rsvp-te*
no rsvp-te

Context **[Tree]** (config>router>mpls>lsp-self-ping rsvp-te)

Full Context configure router mpls lsp-self-ping rsvp-te

Description This command enables LSP Self Ping on all RSVP-TE LSPs, unless an individual LSP is explicitly disabled under the **lsp**>**lsp-self-ping** command or in the LSP template.

The **no** form of this command reverts to the default value.

Default rsvp-te disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *rsvp-te* — Specifies whether LSP Self Ping is enabled on RSVP-TE LSPs.

Values enable, disable

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rsvp-te

Syntax **rsvp-te** *value*
no rsvp-te

Context **[Tree]** (config>router>mpls>tunnel-table-pref rsvp-te)

Full Context configure router mpls tunnel-table-pref rsvp-te

Description This command configures the tunnel table preference for RSVP-TE LSP tunnel type away from its default value.

The tunnel table preference applies to the next-hop resolution of BGP routes of the following families: EVPN, IPv4, IPv6, VPN-IPv4, VPN-IPv6, label-IPv4, and label-IPv6 in the tunnel table.

This feature does not apply to a VPRN, VPLS, or VLL service with explicit binding to an SDP that enabled the **mixed-lsp-mode** option. The tunnel preference in such an SDP is fixed and is controlled by the service manager. The configuration of the tunnel table preference parameter does not modify the behavior of such an SDP and the services that bind to it.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

The **no** form of this command reverts to the default.

Default rsvp-te 7

Parameters *value* — Specifies the tunnel table preference value for RSVP-TE LSP.

Values 1 to 255

Default 7

Platforms All

rsvp-te

Syntax [**no**] **rsvp-te**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter rsvp-te)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter rsvp-te

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the use of RSVP-TE sourced tunnel entries in the TTM to resolve the associated static route next-hop.

The rsvp-te value instructs the code to search for the set of lowest metric RSVP-TE LSPs to the address of the indirect next-hop. The LSP metric is provided by MPLS in the tunnel table. The static route treats a set of RSVP-TE LSPs with the same lowest metric as an ECMP set. The user has the option of configuring a list of RSVP-TE LSP names to be used exclusively instead of searching in the tunnel table. In that case, all LSPs must have the same LSP metric in order for the static route to use them as an ECMP set. Otherwise, only the LSPs with the lowest common metric value will be selected.

A P2P auto-lsp that is instantiated via an LSP template can be selected in TTM when resolution is set to any. However, Nokia does not recommend configuring an auto-lsp name explicitly under the rsvp-te node as the auto-generated name can change if the node reboots, which will blackhole the traffic of the static route.

Default no rsvp-te

Platforms All

22.318 rt-buffer-size

rt-buffer-size

Syntax **rt-buffer-size** *rt-buffer-size*
no rt-buffer-size

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video rt-buffer-size)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video rt-buffer-size)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video rt-buffer-size
configure mcast-management multicast-info-policy bundle channel video rt-buffer-size

Description This command configures the retransmission buffer for channels within the bundle or channel range.

The **no** form of the command returns the parameter to the default value.

Default 300

Parameters *rt-buffer-size* — Specifies the buffer size, in milliseconds, to store channel packets.

Values 300 to 8000

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.319 rt-client

rt-client

Syntax **rt-client** [**group** *group-addr*]
no rt-client

Context **[Tree]** (debug>service>id>video-interface rt-client)

Full Context debug service id video-interface rt-client

Description This command enables debugging the RET client.

Parameters **group** *group-addr* — Specifies the multicast group address.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.320 rt-client-src-address

rt-client-src-address

Syntax **rt-client-src-address** *ip-address*
no rt-client-src-address

Context **[Tree]** (config>service>ies>video-interface rt-client-src-address)
[Tree] (config>service>vpls>video-interface rt-client-src-address)
[Tree] (config>service>vprn>video-interface rt-client-src-address)

Full Context configure service ies video-interface rt-client-src-address
configure service vpls video-interface rt-client-src-address
configure service vprn video-interface rt-client-src-address

Description This command assigns the IP address for the retransmission client on the video interface within the service. The RET client IP address is the originating address used for communication with upstream RET servers. If no RET client address is assigned, the RT client is operationally down as the RET client configuration is incomplete.

For a VPLS service, the RET client address cannot be the same as an existing address for the video interface, but it must be an address within a video interface subnet. For IES and VPRN, the RET client address can be the same as an existing address for the video interface or an address within a video interface subnet.

The **no** form of the command deletes the RT client address from the video interface.

Default none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the IP address for the retransmission client on the video interface within the service.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.321 rt-payload-type

rt-payload-type

Syntax **rt-payload-type** *payload-type*
no rt-payload-type

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if rt-payload-type)

Full Context configure mcast-management multicast-info-policy video-policy video-interface rt-payload-type

Description This command describes the format to be used by Retransmission (RT) server to send retransmission packets. The RET server interface allows the payload type within the retransmission packets to be configured.

Default rt-payload-type 99 — Indicates that the frames will be sent in the RFC 4588, *RTP Retransmission Payload Format*, format.

Parameters *payload-type* — Indicates the format expected for received retransmission packets. The value 33 indicates that the frames will be received as originally sent. A value between 96 and 127 indicates the dynamic payload type value (per RFC 3551) to be used for RFC 4588 formatted retransmission packets.

Values 33, 96 to 127

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.322 rt-rate

rt-rate

Syntax **rt-rate** *rt-burst-percentage*
no rt-rate

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd rt-rate)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip rt-rate)
[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if rt-rate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd rt-rate)

Full Context configure mcast-management multicast-info-policy video-policy video-interface hd rt-rate
configure mcast-management multicast-info-policy video-policy video-interface pip rt-rate
configure mcast-management multicast-info-policy video-policy video-interface rt-rate
configure mcast-management multicast-info-policy video-policy video-interface sd rt-rate

Description This command sets the rate of nominal bandwidth at which retransmission packets are sent to the retransmission client for requests directed to the IP address.

The **no** form of the command returns the parameter to the default value.

Default rt-rate 5

Parameters *rt-burst-percentage* — Specifies the percentage of nominal bandwidth to send retransmission packets.

Values 1 to 100

Default 5

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.323 rt-server

rt-server

Syntax **rt-server disable**
rt-server *ip-address* **port** *port-num*
no rt-server

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video rt-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video rt-server)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video rt-server)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video rt-server
configure mcast-management multicast-info-policy bundle channel video rt-server
configure mcast-management multicast-info-policy bundle video rt-server

Description This command enables and configures the upstream retransmission server configuration parameters.

The **no** form of the command removes the upstream retransmission server configuration and implies the configuration is inherited from a higher context or from the default policy.

Default no rt-server – The upstream retransmission server settings are inherited.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **disable** — This keyword explicitly disables the upstream retransmission server within the policy. For the default bundle within the default Multicast Information Policy, the **no** form of the command and the disable keyword have the same meaning and imply the server is disabled.

ip-address — The IP address of the upstream retransmission server.

port *num* — The UDP port to use to send RET requests to the upstream RET server.

Values 1024 to 5999, 6251 to 65535

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

rt-server

Syntax **rt-server** [**client** *client-ip* [**source-port** *src-port*]]
no rt-server

Context **[Tree]** (debug>service>id>video-interface rt-server)

Full Context debug service id video-interface rt-server

Description This command enables debugging for the RET server.

Parameters **client** *client-ip* — Specifies the client IP address.

source *src-port* — Specifies the source port.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

22.324 rtm

rtm

Syntax **rtm** [*rp-address*]
no rtm

Context **[Tree]** (debug>router>msdp rtm)

Full Context debug router msdp rtm

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) route table manager (RTM).

The **no** form of the command disables MSDP RTM debugging.

Parameters *rp-address* — Debugs the IP multicast address for which this entry contains information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

rtm

Syntax **rtm** [**detail**]
no rtm

Context **[Tree]** (debug>router>pim rtm)

Full Context debug router pim rtm

Description This command enables debugging for PIM RTM.

The **no** form of this command disables debugging for PIM RTM.

Parameters **detail** — Displays detailed RTM information.

Platforms All

rtm

Syntax **rtm** [**neighbor** *ip-address* | **group** *name*]
no rtm

Context **[Tree]** (debug>router>bgp rtm)

Full Context debug router bgp rtm

Description This command logs RTM changes in the debug log.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rtm

Syntax **rtm** [*ip-address*]
no rtm

Context **[Tree]** (debug>router>isis rtm)

Full Context debug router isis rtm

Description This command enables debugging for IS-IS route table manager (RTM).

The **no** form of the command disables debugging.

Parameters *ip-address* — The specified IP address.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

rtm

Syntax **rtm** [*ip-address*]
no rtm

Context **[Tree]** (debug>router>ospf rtm)
[Tree] (debug>router>ospf3 rtm)

Full Context debug router ospf rtm
debug router ospf3 rtm

Description This command enables debugging for OSPF RTM.

Parameters *ip-address* — Specifies the IP address to debug.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

22.325 rtm-debounce-time

rtm-debounce-time

Syntax **rtm-debounce-time** *debounce-time*
no rtm-debounce-time

Context [Tree] (config>router>l2tp rtm-debounce-time)
[Tree] (config>service>vprn>l2tp rtm-debounce-time)

Full Context configure router l2tp rtm-debounce-time
configure service vprn l2tp rtm-debounce-time

Description This command configures the amount of time, in milliseconds, that the system waits before declaring an L2TP tunnel down when the remote endpoint IP address cannot be resolved to an active IP route in the local routing table.

The default behavior is for the L2TP tunnel to not be declared down based on the remote endpoint IP address reachability.

The **no** form of this command returns the **rtm-debounce-time** to a value of 0.

Default no rtm-debounce-time

Parameters *debounce-time* — Specifies the amount of time, in milliseconds, that the system waits before declaring the associated L2TP tunnel as down.

Values 0 to 5000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.326 rtp-header

rtp-header

Syntax [**no**] **rtp-header**

Context [Tree] (config>service>cpipe>sap>cem rtp-header)
[Tree] (config>service>epipe>sap>cem rtp-header)

Full Context configure service cpipe sap cem rtp-header
configure service epipe sap cem rtp-header

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies whether an RTP header is used when packets are transmitted to the packet service network (PSN) by the CEM SAP. This mode must be enabled for differential-timed DS1/E1s. It can optionally be enabled for other DS1/E1s for interoperability purposes.

Default no rtp-header

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

rtp-header

Syntax [**no**] **rtp-header**

Context **[Tree]** (config>mirror>mirror-dest>sap>cem rtp-header)

Full Context configure mirror mirror-dest sap cem rtp-header

Description This command specifies whether an RTP header is used when packets are transmitted to the packet service network (PSN) by the CEM SAP.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

22.327 rtp-performance

rtp-performance

Syntax **rtp-performance**

Context **[Tree]** (config>app-assure>group>cflowd rtp-performance)

Full Context configure application-assurance group cflowd rtp-performance

Description This command configures the cflowd RTP performance export.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.328 rtr-adv-lsa-limit

rtr-adv-lsa-limit

Syntax **rtr-adv-lsa-limit** [*1..4294967295*] [**log-only**] [**threshold** *percent*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rtr-adv-lsa-limit [*1..4294967295*] [**log-only**] [**threshold** *percent*] **overload-timeout forever**
rtr-adv-lsa-limit [*1..4294967295*] [**log-only**] [**threshold** *percent*] **overload-timeout** *seconds*
no rtr-adv-lsa-limit

Context **[Tree]** (config>service>vprn>ospf rtr-adv-lsa-limit)

Full Context configure service vprn ospf rtr-adv-lsa-limit

Description This command configures the maximum number of LSAs OSPF can learn from another router, in order to protect the system from a router that accidentally advertises a large number of LSAs. When the number of advertised LSAs reaches the configured percentage of this limit, an SNMP trap is sent. If the limit is exceeded, OSPF goes into overload.

The **overload-timeout** option allows the administrator to control how long OSPF is in overload as a result of the advertised LSA limit being reached. At the end of this duration of time the system automatically attempts to restart OSPF. One possible value for the **overload-timeout** is **forever**, which means OSPF is never restarted automatically and this corresponds to the default behavior when the **overload-timeout** option is not configured.

The **no** form of this command removes the **rtr-adv-lsa-limit**.

Default rtr-adv-lsa-limit forever

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, overload is not set.

percent — The threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

seconds — Specifies duration in seconds before restarting OSPF.

Values 1 to 1800

Platforms All

rtr-adv-lsa-limit

Syntax **rtr-adv-lsa-limit** *limit* [**log-only**] [**threshold** *percent*]
rtr-adv-lsa-limit *limit* [**log-only**] [**threshold** *percent*] [**overload-timeout** {*seconds* | **forever**}]
no rtr-adv-lsa-limit

Context **[Tree]** (config>router>ospf rtr-adv-lsa-limit)
[Tree] (config>router>ospf3 rtr-adv-lsa-limit)

Full Context configure router ospf rtr-adv-lsa-limit
configure router ospf3 rtr-adv-lsa-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum number of LSAs OSPF can learn from another router, in order to protect the system from a router that accidentally advertises a large number of LSAs. When the number of advertised LSAs reaches the configured percentage of this limit, an SNMP trap is sent. If the limit is exceeded, OSPF goes into overload.

The overload-timeout option allows the administrator to control how long OSPF is in overload as a result of the advertised LSA limit being reached. At the end of this duration of time, the system automatically exits overload. One possible value for the overload-timeout is forever, which means OSPF is never exiting overload.

The **no** form of this command removes the **rtr-adv-lsa-limit**.

Default no rtr-adv-lsa-limit

Parameters **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, overload is not set.

percent — Specifies the threshold value (as a percentage) that triggers a warning message to be sent.

Values 0 to 100

limit — Specifies the number of LSAs that can be learned expressed as a decimal integer.

Values 1 to 4294967295

second — Specifies duration in minutes before restarting OSPF.

Values Values 1 to 1800

forever — Specifies that OSPF is restarted only after the **clear router ospf | ospf3 overload rtr-adv-lsa-limit** command is executed.

Platforms All

22.329 rtr-solicit-user-db

rtr-solicit-user-db

Syntax **rtr-solicit-user-db** *local-user-db*
no rtr-solicit-user-db

Context **[Tree]** (config>service>vpls>sap rtr-solicit-user-db)

Full Context configure service vpls sap rtr-solicit-user-db

Description This command enabled access to LUDB for SLAAC hosts under the capture SAP. The name of this ludb must match the name of ludb configured under the **configure>service>vprn/ies>sub-if>group-if>ipv6>router-solicit** hierarchy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *local-user-db* — Specifies the name of the local-user-database up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

22.330 rtsp

rtsp

Syntax [**no**] **rtsp**

Context **[Tree]** (config>service>nat>firewall-policy>alg rtsp)
[Tree] (config>service>nat>nat-policy>alg rtsp)
[Tree] (config>service>nat>up-nat-policy>alg rtsp)

Full Context configure service nat firewall-policy alg rtsp
configure service nat nat-policy alg rtsp
configure service nat up-nat-policy alg rtsp

Description This command enables RTSP ALG.

The **no** form of the command disables RTSP ALG.

Default no rtsp

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy alg rtsp
- configure service nat nat-policy alg rtsp

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy alg rtsp

22.331 rtt-threshold

rtt-threshold

Syntax **rtt-threshold** *threshold*
no rtt-threshold

Context **[Tree]** (config>app-assure>group>anl>source rtt-threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>app-assure>group>aa-sub-cong rtt-threshold)

Full Context configure application-assurance group aa-sub-congestion-detection rtt-threshold
configure application-assurance group access-network-location source rtt-threshold

Description This command configures the roundtrip delay threshold used by the DEM gateway algorithm to determine ANL congestion or subscriber congestion for NLB-DEM.

Default rtt-threshold 173

Parameters *threshold* — Specifies the maximum acceptable round trip time (RTT), in milliseconds, for TCP connections with no congestion. Any measured RTT above the threshold is considered an indication of possible congestion.

Values 0 to 500

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.332 rtt-threshold-rat

rtt-threshold-rat

Syntax **rtt-threshold-rat rat-type** *rat-type* **rtt-threshold** *rtt-threshold*
no rtt-threshold-rat rat-type *rat-type*

Context [Tree] (config>app-assure>group>aa-sub-cong rtt-threshold-rat)
[Tree] (config>app-assure>group>anl>source rtt-threshold-rat)

Full Context configure application-assurance group aa-sub-congestion-detection rtt-threshold-rat
configure application-assurance group access-network-location source rtt-threshold-rat

Description This command configures the roundtrip delay threshold for each RAT type to be used for a congestion detection algorithm (if applicable).

The **no** form of this command reverts to the default value.

Default rtt-threshold-rat 173

Parameters *rat-type* — Specifies the 3GPP RAT type.

Values utran, geran, wlan, gan, hspa-evol, eutran, virtual, eutran-nb, ehrpd, hrpd, cdma-1x, umb, wifi, nr, lte-m

rtt-threshold — Specifies the parameter used by the DEM-GW algorithm that determines ANL congestion or subscriber congestion in the case of NLB-DEM. It specifies the maximum acceptable round trip time (RTT), under no congestion, in milliseconds. Any measured RTT above the threshold is considered an indication of possible congestion.

Values 0 to 500

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.333 rtt-threshold-tolerance

rtt-threshold-tolerance

Syntax **rtt-threshold-tolerance** *tolerance*
no rtt-threshold-tolerance

Context **[Tree]** (config>app-assure>group>anl>source rtt-threshold-tolerance)
[Tree] (config>app-assure>group>aa-sub-cong rtt-threshold-tolerance)

Full Context configure application-assurance group aa-sub-congestion-detection rtt-threshold-tolerance
configure application-assurance group access-network-location source rtt-threshold-tolerance

Description This command configures the ANL roundtrip delay threshold tolerance used by the DEM gateway algorithm to determine ANL-level or subscriber-level congestion.

Default rtt-threshold-tolerance 50

Parameters *tolerance* — Specifies the ratio, in percentage, of RTTs above the configured threshold (**rtt-threshold**) over the total RTT measurements.

The ratio is calculated as follows, measured across a one-minute period:

rtt-threshold-tolerance = #(RTTs > **rtt-threshold**)/ (Total #RTTs)

If the **rtt-threshold-tolerance** ratio is exceeded, the ANL is declared congested.

Values 0 to 100

Default 50

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

22.334 rule-prefix

rule-prefix

Syntax **rule-prefix** *rule-prefix*
no rule-prefix

Context **[Tree]** (config>service>nat>map-domain>mapping-rule rule-prefix)

Full Context configure service nat map-domain mapping-rule rule-prefix

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a MAP rule prefix.

Parameters *rule-prefix* — Specifies the IPv6 MAP rule prefix.

Values <*ipv6-prefix/prefix-length*> :
ipv6-prefix —— *x:x:x:x:x:x:x:x* (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x—[0 to FFFF]H
d—[0 to 255]D
prefix-length—[0 to 64]

Platforms VSR

22.335 rx-discard-on-ndf

rx-discard-on-ndf

Syntax **rx-discard-on-ndf** {**bm** | **bum** | **none**}

Context **[Tree]** (config>service>vpls>vxlan rx-discard-on-ndf)

Full Context configure service vpls vxlan rx-discard-on-ndf

Description This command, supported by static and BGP-EVPN VXLAN binds, determines the type of traffic that the Non Designated Forwarder (NDF) PE discards in an EVPN multi-homed Ethernet Segment. It is only relevant when the VXLAN instance is associated to a network-interconnect-vxlan ES. The option BM is the default option and discards BM on reception (unicast, known and known is allowed). The option BUM discards any BUM frame on reception. Option none allows any BUM traffic on reception.

Default rx-discard-on-ndf bm

Parameters **bm** — Discards Broadcast and Multicast on the EVPN Non Designated Forwarder (NDF) router, but not Unknown Unicast.

bum — Discards Broadcast, Multicast and Unknown Unicast traffic on the NDF.

none — Allows Broadcast, Multicast or Unknown Unicast traffic on the NDF.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

22.336 rx-eth-ed

rx-eth-ed

Syntax [**no**] **rx-eth-ed**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>lag>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>port>ethernet>eth-cfm>mep>grace>eth-ed rx-eth-ed)

Full Context configure eth-ring path eth-cfm mep grace eth-ed rx-eth-ed
configure eth-tunnel path eth-cfm mep grace eth-ed rx-eth-ed
configure lag eth-cfm mep grace eth-ed rx-eth-ed
configure port ethernet eth-cfm mep grace eth-ed rx-eth-ed

Description This command enables the reception and processing of the ITU-T Y.1731 ETH-ED PDU on the MEP.

The **no** form of this command disables the reception of the ITU-T Y.1731 ETH-ED PDU on the MEP.

Default rx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rx-eth-ed

Syntax [**no**] **rx-eth-ed**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)

Full Context configure service epipe sap eth-cfm mep grace eth-ed rx-eth-ed
configure service epipe spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed
configure service ipipe sap eth-cfm mep grace eth-ed rx-eth-ed

Description This command enables the reception and processing of the ITU-T Y.1731 ETH-ED PDU on the MEP.

The **no** form of this command disables the reception of the ITU-T Y.1731 ETH-ED PDU on the MEP.

Default rx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

rx-eth-ed

Syntax [**no**] **rx-eth-ed**

Context **[Tree]** (config>service>vpls>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)

Full Context configure service vpls eth-cfm mep grace eth-ed rx-eth-ed
configure service vpls mesh-sdp eth-cfm mep grace eth-ed rx-eth-ed
configure service vpls sap eth-cfm mep grace eth-ed rx-eth-ed
configure service vpls spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed

Description This command enables the reception and processing of the ITU-T Y.1731 ETH-ED PDU on the MEP.

The **no** form of this command disables the reception of the ITU-T Y.1731 ETH-ED PDU on the MEP.

Default rx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rx-eth-ed

Syntax [**no**] **rx-eth-ed**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)

Full Context configure service ies interface sap eth-cfm mep grace eth-ed rx-eth-ed
configure service ies interface spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed rx-eth-ed

Description This command enables the reception and processing of the ITU-T Y.1731 ETH-ED PDU on the MEP.

The **no** form of this command disables the reception of the ITU-T Y.1731 ETH-ED PDU on the MEP.

Default rx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed rx-eth-ed

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies interface spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed
- configure service ies interface sap eth-cfm mep grace eth-ed rx-eth-ed

rx-eth-ed

Syntax [**no**] **rx-eth-ed**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace>eth-ed rx-eth-ed)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed rx-eth-ed)

Full Context configure service vprn interface sap eth-cfm mep grace eth-ed rx-eth-ed
configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed rx-eth-ed

Description This command enables the reception and processing of the ITU-T Y.1731 ETH-ED PDU on the MEP.

The **no** form of this command disables the reception of the ITU-T Y.1731 ETH-ED PDU on the MEP.

Default rx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed rx-eth-ed

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed rx-eth-ed
- configure service vprn interface sap eth-cfm mep grace eth-ed rx-eth-ed

rx-eth-ed

Syntax [**no**] **rx-eth-ed**

Context **[Tree]** (config>router>if>eth-cfm>mep>grace>eth-ed rx-eth-ed)

Full Context configure router interface eth-cfm mep grace eth-ed rx-eth-ed

Description This command enables the reception and processing of the ITU-T Y.1731 ETH-ED PDU on the MEP.

The **no** form of this command disables the reception of the ITU-T Y.1731 ETH-ED PDU on the MEP.

Default rx-eth-ed

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.337 rx-eth-vsm-grace

rx-eth-vsm-grace

Syntax [**no**] **rx-eth-vsm-grace**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>lag>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>port>ethernet>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)

Full Context configure eth-ring path eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure eth-tunnel path eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure lag eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure port ethernet eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

Description This command enables the reception and processing of the Nokia ETH-CFM Grace PDU on the MEP.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **no** form of this command disables the reception of the Nokia ETH-CFM Grace PDU on the MEP.

Default rx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rx-eth-vsm-grace

Syntax [**no**] **rx-eth-vsm-grace**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)

Full Context configure service epipe sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service epipe spoke-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service ipipe sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

Description This command enables the reception and processing of the Nokia ETH-CFM Grace PDU on the MEP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **no** form of this command disables the reception of the Nokia ETH-CFM Grace PDU on the MEP.

Default rx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rx-eth-vsm-grace

Syntax [**no**] **rx-eth-vsm-grace**

Context **[Tree]** (config>service>vpls>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)

Full Context configure service vpls eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service vpls mesh-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service vpls sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service vpls spoke-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

Description This command enables the reception and processing of the Nokia ETH-CFM Grace PDU on the MEP.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **no** form of this command disables the reception of the Nokia ETH-CFM Grace PDU on the MEP.

Default rx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

rx-eth-vsm-grace

Syntax [**no**] **rx-eth-vsm-grace**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service ies interface spoke-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

Description This command enables the reception and processing of the Nokia ETH-CFM Grace PDU on the MEP.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **no** form of this command disables the reception of the Nokia ETH-CFM Grace PDU on the MEP.

Default rx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
- configure service ies interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

rx-eth-vsm-grace

Syntax [**no**] **rx-eth-vsm-grace**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)

Full Context configure service vprn interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service vprn interface spoke-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

Description This command enables the reception and processing of the Nokia ETH-CFM Grace PDU on the MEP.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the reception of the Nokia ETH-CFM Grace PDU on the MEP.

Default rx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace
- configure service vprn interface sap eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

rx-eth-vsm-grace

Syntax [**no**] **rx-eth-vsm-grace**

Context **[Tree]** (config>router>if>eth-cfm>mep>grace>eth-vsm-grace rx-eth-vsm-grace)

Full Context configure router interface eth-cfm mep grace eth-vsm-grace rx-eth-vsm-grace

Description This command enables the reception and processing of the Nokia ETH-CFM Grace PDU on the MEP.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **no** form of this command disables the reception of the Nokia ETH-CFM Grace PDU on the MEP.

Default rx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.338 rx-los-reaction

rx-los-reaction

Syntax **rx-los-reaction** {**squelch**}
no rx-los-reaction

Context **[Tree]** (config>port>dwdm>coherent rx-los-reaction)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port dwdm coherent rx-los-reaction

Description This command configures the reaction to an RX LOS.

Parameters **squelch** — Specifies to squelch (turn off) the transmit signal on RX LOS.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.339 rx-los-thresh

rx-los-thresh

Syntax **rx-los-thresh** *threshold*

Context **[Tree]** (config>port>dwdm>coherent rx-los-thresh)

Full Context configure port dwdm coherent rx-los-thresh

Description This command configures the average input power LOS threshold.

Default -23.00

Parameters *threshold* — Specifies the RX LOS threshold.

Values -30.00 to -13.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

22.340 rx-must-be-encrypted

rx-must-be-encrypted

Syntax [**no**] **rx-must-be-encrypted**

Context **[Tree]** (config>port>ethernet>dot1x>macsec rx-must-be-encrypted)

Full Context configure port ethernet dot1x macsec rx-must-be-encrypted

Description When the **rx-must-be-encrypted** option is enabled, all traffic that is not MACsec-secured that is received on the port is dropped.

When the **rx-must-be-encrypted** option is disabled, all arriving traffic, whether MACsec secured or not, will be accepted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: This command is only available on the NULL port level and does not have per-VLAN granularity.

The **no** form of this command disables the **rx-must-be encrypted** option.

Default rx-must-be-encrypted

Platforms All

22.341 rx-update-pacing

rx-update-pacing

Syntax **rx-update-pacing** *seconds*

Context **[Tree]** (config>port>ethernet>eth-cfm>mep>eth-bn rx-update-pacing)

Full Context configure port ethernet eth-cfm mep eth-bn rx-update-pacing

Description This command sets the pace for update messages to and from the **eth-cfm** subsystem to the QoS subsystem. The most recent update messages are held by the ETH-CFM subsystem, but the most recent update is held until the expiration of the pacing timer.

Parameters *seconds* — The time to wait before sending subsequent updates (in seconds).

Values 1 to 600

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23 s Commands

23.1 s-pmsi

s-pmsi

Syntax **s-pmsi** [{*vpnSrcAddr* [*vpnGrpAddr*]} [*mdSrcAddr*]]
no s-pmsi

Context **[Tree]** (debug>router>pim s-pmsi)

Full Context debug router pim s-pmsi

Description This command enables debugging for PIM selective provider multicast service interface.

The **no** form of this command disables the debugging.

Parameters *vpnSrcAddr* — Specifies the VPN source address.

vpnGrpAddr — Specifies the VPN group address.

mdSrcAddr — Specifies the source address of the multicast domain.

Platforms All

23.2 s-tag

s-tag

Syntax **s-tag** *qtag1* **c-tag-range** *qtag2* [**to** *qtag2*]
no s-tag *qtag1* **c-tag-range** *qtag2*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>qinq s-tag)

Full Context configure service system bgp-evpn ethernet-segment qinq s-tag

Description This command determines the inner VIDs (for a specified outer VID) associated with the virtual Ethernet Segment on a specific qinq port or LAG based on the following:

- Values *, null, 0 to 4094 are allowed.
- Any SAP for which the outer and inner service-delimiting qtags match the range is associated with the virtual ES, and only those, for example, SAP 1/1/1:10.* will not match port 1/1/1, s-tag 10 c-tag-range 10 to 100.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- A maximum of 8 ranges (including the s-tag ranges) are allowed in the qinq context.
- A c-tag range can be comprised of a single qtag.
- Shutting down the ES is not required prior to making changes.
- A qtag included in the **s-tag-range** command cannot be included in the s-tag qtag of this command.

Note: Not all qtag1 and qtag2 combinations are valid for values 0, *, and null. The following combinations are allowed:

- s-tag 0 c-tag-range *
- s-tag * c-tag-range *
- s-tag * c-tag-range null
- s-tag null c-tag-range null
- s-tag X c-tag-range 0 (where: X=1 to 4094)
- s-tag X c-tag-range * (where: X=1 to 4094)

The **no** form of the command removes the configured range. Only the first qtag1 value is required to remove the range.

Parameters *qtag1* — Specifies the outer VID for the c-tag range.

Values *, null, 0 to 4094

qtag2 — Specifies the inner VID for the c-tag range. When configuring a range of qtags (and not a single value), the second qtag1 value must be greater than the value of the first qtag1.

Values *, null, 0 to 4094

Platforms All

23.3 s-tag-range

s-tag-range

Syntax **s-tag-range** *qtag1* [**to** *qtag1*]
no s-tag-range *qtag1*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>qinq s-tag-range)

Full Context configure service system bgp-evpn ethernet-segment qinq s-tag-range

Description This command determines the VIDs associated with the virtual Ethernet Segment on a specific qinq port or LAG based on the following considerations:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Values *, 0 to 4094 are allowed.
- Any SAP for which the service-delimiting qtag matches the range is associated with the virtual ES, and only those, for example, SAP 1/1/1:0.* will not match port 1/1/1, s-tag-range 100.
- Maximum 8 ranges are allowed in the qinq context.
- A range can be comprised of a single qtag.
- Shutting down the ES is not required prior to making changes in the q-tag-range.

The **no** form of the command removes the configured range. Only the first qtag1 value is required to remove the range.

Parameters *qtag1* — Specifies the outer VID. When configuring a range of qtags (and not a single value), the second qtag1 value must be greater than the first qtag1.

Values *, 0 to 4094

Platforms All

23.4 s11

s11

Syntax **s11**

Context **[Tree]** (config>router>gtp s11)
[Tree] (config>service>vprn>gtp s11)

Full Context configure router gtp s11
configure service vprn gtp s11

Description This command enables GTP configuration related to S11 termination in this VRF.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.5 s2l-path

s2l-path

Syntax [**no**] **s2l-path** *path-name* **to** *ip-address*

Context **[Tree]** (config>router>mpls>lsp>primary-p2mp-instance s2l-path)

Full Context configure router mpls lsp primary-p2mp-instance s2l-path

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a root-to-leaf (S2L) sub-LSP path for the primary instance of a P2MP LSP. The primary instance of a P2MP LSP is modeled as a set of root-to-leaf (S2L) sub-LSPs. The root, for example, head-end node, triggers signaling using one path message per S2L path. The leaf sub-LSP paths are merged at branching points.

Each S2L sub-LSP is signaled in a separate path message. Each leaf node will respond with its own RESV message. A branch LSR node will forward the path message of each S2L sub-LSP to the downstream LSR without replicating it. It will also forward the RESV message of each S2L sub-LSP to the upstream LSR without merging it with the RESV messages of other S2L sub-LSPs of the same P2MP LSP. The same is done for subsequent refreshes of the path and RESV states.

The S2L paths can be empty paths or can specify a list of explicit hops. The path name must exist and must have been defined using the **config>router>mpls>path** command. The same path name can be re-used by more than one S2L of the primary P2MP instance. However, the **to** keyword must have a unique argument per S2L as it corresponds to the address of the egress LER node.

This command is not supported on the 7450 ESS.

Parameters *path-name* — Specifies the name of the path which consists of up to 32 alphanumeric characters.

to *ip-address* — Specifies the IP address of the egress router.

Platforms All

23.6 sa-db

sa-db

Syntax **sa-db** [**group** *grpAddr*] [**source** *srcAddr*] [**rp** *rpAddr*]
no sadb

Context **[Tree]** (debug>router>msdp sa-db)

Full Context debug router msdp sa-db

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) source-active requests.

The **no** form of the command disables the MSDP source-active database debugging.

Parameters *grpAddr* — Debugs the IP address of the group.

srcAddr — Debugs the source IP address.

rpAddr — Debugs the specified rendezvous point RP address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.7 sa-mac

sa-mac

Syntax **sa-mac** *ieee-address* **da-mac** *ieee-address*
no sa-mac

Context **[Tree]** (config>mirror>mirror-dest>sap>egress>ip-mirror sa-mac)

Full Context configure mirror mirror-dest sap egress ip-mirror sa-mac

Description This command configures the source and destination MAC addresses for IP mirroring.

The **no** form of this command reverts to the default.

Parameters **sa-mac** *ieee-address* — Specifies the source MAC address. Multicast, Broadcast and zeros are not allowed.

da-mac *ieee-address* — Specifies the destination MAC address. Zeros are not allowed.

Platforms All

23.8 sa-timeout

sa-timeout

Syntax **sa-timeout** *seconds*
no sa-timeout

Context **[Tree]** (config>service>vprn>msdp sa-timeout)

Full Context configure service vprn msdp sa-timeout

Description This command configures the value for the SA entries in the cache. If these entries are not refreshed within the timeout value, they are removed from the cache. Normally, the entries are refreshed at least once a minute. But under high load with many of MSDP peers, the refresh cycle could be incomplete. A higher timeout value (more then 90) could be useful to prevent instabilities in the MSDP cache.

Default 90

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the time, in seconds, to wait for a response from the peer before declaring the peer unavailable.

Values 90 to 600

Platforms All

sa-timeout

Syntax **sa-timeout** *seconds*
no sa-timeout

Context **[Tree]** (config>router>msdp sa-timeout)

Full Context configure router msdp sa-timeout

Description This command configures the value for the SA entries in the cache. If these entries are not refreshed within the timeout value, they are removed from the cache. Normally, the entries are refreshed at least once a minute. But under high load with many of MSDP peers, the refresh cycle could be incomplete. A higher timeout value (more than 90) could be useful to prevent instabilities in the MSDP cache.

Default sa-timeout 90

Parameters *seconds* — Specifies the time, in seconds, to wait for a response from the peer before declaring the peer unavailable.

Values 90 to 600

Platforms All

23.9 saa

saa

Syntax **saa**

Context **[Tree]** (config saa)

Full Context configure saa

Description Commands in this context configure the Service Assurance Agent (SAA) tests.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

saa

Syntax **saa** *test-name* [**owner** *test-owner*] {**start** | **stop**} [**no-accounting**]

Context **[Tree]** (oam saa)

Full Context oam saa

Description This command starts or stops an SAA test that is not configured as continuous.

Parameters *test-name* — Specifies the name of the SAA test, up to 32 characters. The test name must already be configured in the **config>saa>test** context.

test-owner — Specifies the owner of an SAA operation, up to 32 characters. If a *test-owner* value is not specified, the default owner is used.

Default "TiMOS CLI"

start — Starts the test. A test cannot be started if the same test is still running.

A test cannot be started if it is in a shut-down state. An error message and log event is generated to indicate a failed attempt to start an SAA test run. A test cannot be started if it is in a continuous state.

stop — Stops a test in progress. A test cannot be stopped if it is not in progress. A log message is generated to indicate that an SAA test run has been aborted. A test cannot be stopped if it is in a continuous state.

no-accounting — Disables the recording results in the accounting policy. When specifying **no-accounting** the MIB record produced at the end of the test is not added to the accounting file. It uses one of the three MIB rows available for the accounting module for collection.

Platforms All

23.10 saii-type2

saii-type2

Syntax **saii-type2** *global-id:node-id:ac-id*
no saii-type2

Context **[Tree]** (config>service>epipe>spoke-sdp>pw-path-id saii-type2)
[Tree] (config>service>cpipe>spoke-sdp>pw-path-id saii-type2)
[Tree] (config>service>apipe>spoke-sdp>pw-path-id saii-type2)
[Tree] (config>service>vpls>spoke-sdp>pw-path-id saii-type2)

Full Context configure service apipe spoke-sdp pw-path-id saii-type2
configure service cpipe spoke-sdp pw-path-id saii-type2
configure service epipe spoke-sdp pw-path-id saii-type2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls spoke-sdp pw-path-id saii-type2

Description This command configures the Source Individual Attachment Identifier (SAII) for an MPLS-TP spoke-sdp. If this is configured on a spoke-sdp for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the taii-type2 of the mate spoke-sdp.

Parameters *global-id* — Specifies the global ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values 0 to 4294967295

node-id — Specifies the node ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values a.b.c.d or 0 to 4294967295

ac-id — Specifies the attachment circuit ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls spoke-sdp pw-path-id saii-type2
- configure service cpipe spoke-sdp pw-path-id saii-type2
- configure service epipe spoke-sdp pw-path-id saii-type2

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp pw-path-id saii-type2

saii-type2

Syntax **saii-type2** *global-id:prefix:ac-id*
no saii-type2

Context **[Tree]** (config>service>epipe>spoke-sdp-fec saii-type2)

Full Context configure service epipe spoke-sdp-fec saii-type2

Description This command configures the source attachment individual identifier for the spoke-sdp. This is only applicable to FEC129 AII type 2.

Parameters *global-id* — A Global ID of this router T-PE. This value must correspond to one of the global_id values configured for a local-prefix under **config>service>pw-routing>local-prefix** context.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix — The prefix on this router T-PE that the spoke-sdp SDP is associated with. This value must correspond to one of the prefixes configured under **config>service>pw-routing>local-prefix** context.

Values an IPv4-formatted address a.b.c.d or 1 to 4294967295

ac-id — An unsigned integer representing a locally unique identifier for the spoke SDP.

Values 1 to 4294967295

Platforms All

saii-type2

Syntax **saii-type2** *global-id:node-id:ac-id*
no saii-type2

Context **[Tree]** (config>service>vprn>if>spoke-sdp>pw-path-id saii-type2)
[Tree] (config>service>vprn>red-if>spoke-sdp>pw-path-id saii-type2)

Full Context configure service vprn interface spoke-sdp pw-path-id saii-type2
configure service vprn redundant-interface spoke-sdp pw-path-id saii-type2

Description This command configures the source individual attachment identifier (SAII) for an MPLS-TP spoke SDP. If this is configured on a spoke SDP for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the taii-type2 of the mate spoke SDP.

Parameters *global-id* — Specifies the global ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values 0 to 4294967295

node-id — Specifies the node ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values a.b.c.d or 1 to 4294967295

ac-id — Specifies the attachment circuit ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn redundant-interface spoke-sdp pw-path-id saii-type2

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface spoke-sdp pw-path-id saii-type2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

saii-type2

Syntax **saii-type2** *global-id:node-id:ac-id*
no saii-type2

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp>pw-path-id saii-type2)
[Tree] (config>mirror>mirror-dest>spoke-sdp>pw-path-id saii-type2)

Full Context configure mirror mirror-dest remote-source spoke-sdp pw-path-id saii-type2
configure mirror mirror-dest spoke-sdp pw-path-id saii-type2

Description This command configures the source individual attachment identifier (SAII) for an MPLS-TP spoke SDP. If this is configured on a spoke SDP for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the taii-type2 of the mate spoke SDP.

Parameters *global-id* — Specifies the global ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values 0 to 4294967295

node-id — Specifies the node ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values a.b.c.d or 1 to 4294967295

ac-id — Specifies the attachment circuit ID at the source PE or T-PE for the MPLS-TP PW for a spoke SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.11 same-recipnonce-for-pollreq

same-recipnonce-for-pollreq

Syntax [**no**] **same-recipnonce-for-pollreq**

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 same-recipnonce-for-pollreq)

Full Context configure system security pki ca-profile cmpv2 same-recipnonce-for-pollreq

Description This command enables the system to use same recipNonce as the last CMPv2 response for poll request.

Default no same-recipnonce-for-pollreq

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

same-recipnonce-for-pollreq

Syntax [**no**] **same-recipnonce-for-pollreq**

Context **[Tree]** (config>system>security>pki>ca-profile>cmp2 same-recipnonce-for-pollreq)

Full Context configure system security pki ca-profile cmp2 same-recipnonce-for-pollreq

Description This command enables the system to use same recipNonce as the last CMPv2 response for poll request.

The **no** form of this command disables system to use same recipNonce as the last CMPv2 response for poll request.

Default no same-recipnonce-for-pollreq

23.12 sample-interval

sample-interval

Syntax **sample-interval** *interval*

Context **[Tree]** (config>router>rsvp>dbw-accounting sample-interval)

Full Context configure router rsvp dbw-accounting sample-interval

Description This command sets the dark bandwidth sample interval to the specified value. Changing this parameter in the course of dark bandwidth accounting restarts the accounting cycle. The user is encouraged to specify values as multiples of 10. Selecting other values may lead to inconsistent estimation of Dark Bandwidth.

Default sample-interval 30

Parameters *interval* — Specifies the sample interval, expressed in seconds.

Values 10 to 600

sample-interval

Syntax **sample-interval** *sample-period*
no sample-interval

Context **[Tree]** (config>qos>adv-config-policy>child-control>offered-measurement sample-interval)

Full Context configure qos adv-config-policy child-control offered-measurement sample-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to define the number of intervening sample periods before a new offered rate is measured and is only applicable when the policy is applied to a policer. By decreasing the sampling interval, the system will measure a child's new offered rate more frequently. Inversely, increasing the sampling interval causes the child's offered rate to be measured less frequently.

The overall number of offered rate measurements the system attempts within a given timeframe is not affected by the sample-interval command. If the system is asked to perform offered rate measurements more often on some policers, it will take longer to get to all children.

When this command is not specified or removed, the system evaluates the offered rate of each child after 1 sampling period.

The **no** form of this command is used to restore the sampling interval default of 1 sample period.

Parameters *sample-period* — The sample-periods parameter is specified as a whole number between 1 and 8. The value '1' represents the fastest sampling rate available and the value '8' represents the slowest sampling period available.

Default 1

Values 1 to 8

Platforms All

sample-interval

Syntax **sample-interval** *interval*

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription sample-interval)

Full Context configure system telemetry persistent-subscriptions subscription sample-interval

Description This command configures the sample interval for persistent subscription.

This sampling interval only applies when the **mode** command is set to either **target-defined** or **sample**.

Default sample-interval 10000

Parameters *interval* — Specifies the sample interval, in milliseconds.

Values 1000 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.13 sample-multiplier

sample-multiplier

Syntax **sample-multiplier** *multiplier*

Context **[Tree]** (config>router>rsvp>dbw-accounting sample-multiplier)

Full Context configure router rsvp dbw-accounting sample-multiplier

Description This command sets the dark bandwidth sample interval multiplier to the specified value. Changing this parameter in the course of dark bandwidth accounting restarts the accounting cycle.

Default sample-multiplier 3

Parameters *multiplier* — Specifies the sample interval multiplier, expressed as an integer.

Values 1 to 10

23.14 sample-profile

sample-profile

Syntax **sample-profile** *profile-id* [**create**]
no sample-profile *profile-id*

Context **[Tree]** (config>cflowd sample-profile)

Full Context configure cflowd sample-profile

Description Commands in this context create and define sampling parameters.

The **no** form of this command removes the associated sample-profile. **sample-profile** 1 cannot be deleted.

Parameters *profile-id* — Specifies the rate profile.

Values 1 to 5

create — Mandatory keyword when creating a sample profile. The create keyword requirement can be enabled or disabled in the **environment**>**create** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sample-profile

Syntax **sample-profile** *sample-profile-id*
no sample-profile

Context **[Tree]** (config>filter>ip-filter>entry sample-profile)
[Tree] (config>filter>ipv6-filter>entry sample-profile)

Full Context configure filter ip-filter entry sample-profile
configure filter ipv6-filter entry sample-profile

Description This command allows traffic matching of an IPv4 or IPv6 filter to be sampled for cflowd processing using a specific sample profile.

This command is only compatible if the associated interface is configured for interface-based sampling and is only supported for ingress sampling.

An IP filter can only specify a single alternate sample profile for cflowd sampling, but that sample profile can be used in multiple entries.

The **no** form of this command removes the specified sampling profile from the configuration. Cflowd continues to process traffic based on the default or configured interface cflowd sampling profile.

Default no sample-profile

Parameters *sample-profile-id* — Specifies the cflowd sample profile to be used for packets matching this filter entry.

Values 1 to 5

Platforms All

23.15 sample-rate

sample-rate

Syntax **sample-rate** [*rate*]

Context **[Tree]** (config>cflowd>sample-profile sample-rate)

Full Context configure cflowd sample-profile sample-rate

Description This command defines the cflowd sampling rate for the sample profile ID.

The sample rate indicates that the associated interface samples 1 in N packets for cflowd analysis. Only one rate profile below 1:256 with a specific IOM, IMM, or XMA can be associated.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default sample-rate 1000

Parameters *rate* — Specifies the rate at which traffic is sampled and forwarded for cflowd analysis.

Values 1 to 60000

Platforms All

23.16 sample-window

sample-window

Syntax **sample-window** *seconds*
no sample-window

Context **[Tree]** (config>oam-pm>streaming>delay-template sample-window)

Full Context configure oam-pm streaming delay-template sample-window

Description This command specifies the sample window duration in seconds for the template. This configuration option represents time over which the average will be calculated and subsequently streamed.

The **no** form of this command reverts to the default.

Default sample-window 60

Parameters *seconds* — Specifies the sample window duration.

Values 10 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

sample-window

Syntax **sample-window**

Context **[Tree]** (config>test-oam>link-meas>template sample-window)

Full Context configure test-oam link-measurement measurement-template sample-window

Description Commands in this context configure sample window parameters to be used when the **measurement-template** is assigned to an IP interface. The sample window is the collection of individual probe results, over a defined period.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.17 sampling

sampling

Syntax **sampling** {**unicast** | **multicast**} **type** {**acl** | **interface**} [**direction** {**ingress-only** | **egress-only** | **both**}] [**sample-profile** [*profile-id*]]
no sampling {**unicast** | **multicast**}

Context **[Tree]** (config>service>ies>if>cflowd-parameters sampling)
[Tree] (config>service>ies>sub-if>grp-if>cflowd-parameters sampling)
[Tree] (config>service>vprn>if>cflowd-parameters sampling)
[Tree] (config>service>vprn>nw-if>cflowd-parameters sampling)
[Tree] (config>service>vprn>sub-if>grp-if>cflowd-parameters sampling)

Full Context configure service ies interface cflowd-parameters sampling
configure service ies subscriber-interface group-interface cflowd-parameters sampling
configure service vprn interface cflowd-parameters sampling
configure service vprn network-interface cflowd-parameters sampling
configure service vprn subscriber-interface group-interface cflowd-parameters sampling

Description This command enables and configures the cflowd sampling behavior to collect traffic flow samples through a router for analysis.

This command can be used to configure the sampling parameters for unicast and multicast traffic separately. If sampling is not configured for either **unicast** or **multicast** traffic, then that type of traffic will not be sampled.

If cflowd is enabled without either **egress-only** or **both** keywords specified or with the **ingress-only** keyword specified, then only ingress sampling is enabled on the associated IP interface.

The **no** form of this command disables the associated type of traffic sampling.

Parameters **unicast | multicast** — Specifies unicast or multicast sampling.

type — Specifies the cflowd sampling type on the given virtual router interface.

Values acl — Specifies ACL cflowd analysis be applied to the given virtual router interface.

interface — Specifies interface cflowd analysis be applied to the given virtual router interface

direction — Specifies the direction of the cflowd analysis that is applied to the given virtual router interface.

Values ingress-only — Specifies an ingress only direction of the cflowd analysis be applied to the given virtual router interface.

egress-only — Specifies an egress only direction of the cflowd analysis be applied to the given virtual router interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

both — Specifies both ingress and egress direction of the cflowd analysis be applied to the given virtual router interface.

profile-id — Defines the sampling rate profile to be associated with this interface.

Values 1 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface cflowd-parameters sampling
- configure service ies subscriber-interface group-interface cflowd-parameters sampling

All

- configure service vprn network-interface cflowd-parameters sampling
- configure service vprn interface cflowd-parameters sampling
- configure service ies interface cflowd-parameters sampling

sampling

Syntax **sampling** {**unicast** | **multicast**} **type** {**acl** | **interface**} [**direction** {**ingress-only** | **egress-only** | **both**}] [**sample-profile** *profile*]
no sampling {**unicast** | **multicast**}

Context **[Tree]** (config>router>if>cflowd-parameters sampling)

Full Context configure router interface cflowd-parameters sampling

Description This command enables and configures the cflowd sampling behavior to collect traffic flow samples through a router for analysis.

This command can be used to configure the sampling parameters for unicast and multicast traffic separately. If sampling is not configured for either unicast or multicast traffic, then that type of traffic will not be sampled.

If cflowd is enabled without either **egress-only** or **both** specified or with the **ingress-only** keyword specified, then only ingress sampling will be enabled on the associated IP interface.

The **no** form of this command disables the associated type of traffic sampling on the associated interface.

Default no sampling

Parameters **unicast** — Specifies that the sampling command will control the sampling of unicast traffic on the associated interface/SAP.

multicast — Specifies that the sampling command will control the sampling of multicast traffic on the associated interface/SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type — Specifies whether the traffic sampling is based on an **acl** match, or all traffic entering or exiting the associated interface.

Values **acl** — Specifies that the sampled traffic is controlled via an IP traffic filter entry with the action “filter-sample” configured.

interface — Specifies that all traffic entering or exiting the interface is subject to sampling.

direction — Specifies the direction to collect traffic flow samples.

Values **ingress-only** — Enables ingress sampling only on the associated interface.

egress-only — Enables egress sampling only on the associated interface.

both — Enables both ingress and egress cflowd sampling.

profile — Specifies the sampling profile to be associated with this interface.

Values 1 to 5

Platforms All

23.18 sampling-rate

sampling-rate

Syntax **sampling-rate** *sampling-rate*
no sampling-rate

Context **[Tree]** (config>mirror>mirror-dest sampling-rate)

Full Context configure mirror mirror-dest sampling-rate

Description This command configures the packet sampling rate for mirrored traffic and is supported with **config** and **debug** mirror sources. The sampling rate is common to all endpoints on a specified line card FP per mirror destination service.

The **no** form of this command disables the packet sampling rate for mirrored traffic.

Default no sampling-rate

Parameters *sampling-rate* — Specifies the sampling rate.

Values 256 to 100000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.19 sap

sap

Syntax **sap** *sap-id* [**split-horizon-group** *group-name*] [**create**] [**capture-sap**] [**eth-ring** *ring-index*]
sap *sap-id* [**split-horizon-group** *group-name*] [**create**] [**capture-sap**] [**eth-ring** *ring-index*] **leaf-ac**
sap *sap-id* [**split-horizon-group** *group-name*] [**create**] [**capture-sap**] [**eth-ring** *ring-index*] **root-leaf-tag leaf-tag** *leaf-tag*
no sap *sap-id*

Context **[Tree]** (config>service>vpls sap)

Full Context configure service vpls sap

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the 7450 ESS or 7750 SR. Each SAP must be unique. All SAPs must be explicitly created within a service or on an IP interface.

Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command. Channelized TDM ports are always access ports (TDM applies to the 7750 SR only).

If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down although all traffic traversing the service is discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP are also deleted. For Internet Ethernet Service (IES), the IP interface must be shut down before the SAP on that interface may be removed.

Special Cases **VPLS SAP —** A VPLS SAP can be defined with Ethernet ports, SONET/SDH or TDM channels (TDM is supported on the 7750 SR only).

A default SAP has the following format: port-id:*. This type of SAP is supported only on Ethernet MDAs and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS). This type of SAP is mutually exclusive with a SAP defined by explicit null encapsulation (for example, 1/1/1:0).

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

port-id — Specifies the physical port ID in the *slot/mda/port* format.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number [.channel] format. For example 6/2/3 specifies port 3 on MDA 2 in slot 6.

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels, the port ID must include the channel ID. A period "." separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

group-name — Specifies the name of the split horizon group to which the SAP belongs. This parameter applies to the 7450 ESS or 7750 SR only.

capture-sap — Specifies a capturing SAP in which triggering packets are sent to the CPM. Non-triggering packets captured by the capture SAP are dropped. This parameter applies to the 7450 ESS or 7750 SR only.

create — Keyword used to create a SAP instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

root-leaf-tag — Specifies a SAP as a root leaf tag SAP. Only SAPs of the form dot1q (for example, 1/1/1:X) or qinq (for example, 1/1/1:X.Y, 1/1/1:X.*) are supported. The default E-Tree SAP type is a root AC, if *root-leaf-tag* **(**or *leaf-ac***)** is not specified at SAP creation. This option is only available when the VPLS is designated as an E-Tree VPLS.

leaf-tag-vid — Specifies to replace the outer SAP-ID for leaf traffic. The leaf tag VID is only significant between peering VPLS but the values must be consistent on each end.

leaf-ac — Specifies a SAP as a leaf access (AC) SAP. The default E-Tree SAP type is root AC if **leaf-ac** (or **root-leaf-tag**) is not specified at SAP creation. This option is only available when the VPLS is designated as an E-Tree VPLS.

Platforms All

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (config>service>vpls>pbb>backbone-vpls sap)

Full Context configure service vpls pbb backbone-vpls sap

Description This command configures attributes of a SAP on the B-VPLS service.

Platforms All

sap

Syntax **sap** *sap-id* [**create**] [**no-endpoint**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap *sap-id* [**create**] **endpoint** *endpoint-name*
no sap *sap-id*

Context
[Tree] (config>service>apipe sap)
[Tree] (config>service>cpipe sap)
[Tree] (config>service>epipe sap)
[Tree] (config>service>fpipe sap)
[Tree] (config>service>ipipe sap)

Full Context
configure service apipe sap
configure service cpipe sap
configure service epipe sap
configure service fpipe sap
configure service ipipe sap

Description
This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the device. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port. Channelized TDM ports are always access ports.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded.

The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The following are supported on the 7750 SR only:

- ATM VPI/VCI on an ATM port for vc-type atm-vcc and atm-sdu
- ATM VPI on an ATM port for vc-type atm-vpc
- ATM virtual trunk - a range of VPIs on an ATM port for vc-type atm-cell
- ATM port for vc-type atm-cell
- ATM connection profile for vc-type atm-cell
- Frame Relay DLCI on a port for vc-type atm-sdu
- ATM SAP carries the IPv4 packet using RFC 2684, VC-Mux or LLC/SNAP routed PDU encapsulation for an Ipipe service
- Frame Relay SAP RFC 2427, routed PDU encapsulation for an Ipipe service
- Ethernet SAP RFC 1332, PPP IPCP encapsulation of an IPv4 packet for an Ipipe service
- Ethernet SAP HDLC SAP uses the routed IPv4 encapsulation for an Ipipe service
- ATM - Frame Relay, PPP/IPCP - PPP/IPCP

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Frame Relay-Frame Relay, ATM - ATM
- Ethernet-Ethernet
- cHDLC-cHDLC
- An ATM SAP can be part of an IMA bundle.
- A PPP SAP can be part of an MLPPP bundle.
- A FR SAP can be part of a MLFR bundle.

Ethernet SAPs support null, dot1q, and qinq is supported for all routers.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed.

By default, no SAPs are defined.

Special Cases **Special Cases —** A SAP can be defined with Ethernet ports, SONET/SDH or TDM channels. At most, only one sdp-id can be bound to an VLL service. Since a VLL is a point-to-point service, it can have, at most, two end points. The two end points can be one SAP and one SDP or two SAPs. Up to 49 SDPs can be associated with a service in a single router. Each SDP must have a unique router destination, or an error will be generated.

A default SAP has the following format: port-id:*. This type of SAP is supported only on Ethernet MDAs and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS). This type of SAP is mutually exclusive with a SAP defined by explicit null encapsulation (for example, 1/1/1:0).

Two Frame Relay SAPs cannot be configured on an Apipe service on the 7750 SR. The limitation is for an Apipe service in local mode, which has two SAPs associated with the service, as opposed to a configuration with a SAP and a SDP in remote case, the only combination of the type of SAPs allowed is either two ATM SAPs or an ATM SAP and a Frame Relay SAP. The CLI prevents adding two Frame Relay SAPs under an Apipe service.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP.

port-id — Specifies the physical port ID.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 6/2/3 specifies port 3 on MDA 2 in slot 6.

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels, the port ID must include the channel ID. A period "." separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pxc-id	pxc-*id*.*sub-port*	
	pxc	keyword
	id	1 to 64
	sub-port	a, b

endpoint — Adds a SAP endpoint association.

no endpoint — Removes the association of a SAP or a spoke SDP with an explicit endpoint name.

create — Keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Output The following is an example of VLL SAP information.

Sample Output

```
*A:bksim2801>config>service>apipe>sap$
===============================================================
ATM PVCs, Port 1/1/1
===============================================================
VPI/VCI     Owner     Type     Ing.TD   Egr.TD  Adm  OAM     Opr
---------------------------------------------------------------
2/102       SAP       PVC      1        1       up   ETE-AIS dn
10/100      SAP       PVC      1        1       up   ETE-AIS dn
===============================================================
*A:bksim2801#

*A:test>config>service>epipe 200 name "200" customer 1 info detail
===============================================================
            sap 1/1/c5/1:200.200 create
                no shutdown
            exit
            sap pw-21:200.200 create
                no shutdown
            exit
            no shutdown
        exit
    exit
===============================================================
```

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap
- configure service fpipe sap

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe sap
- configure service ipipe sap

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context **[Tree]** (config>service>ies sap)
[Tree] (config>service>ies>if sap)
[Tree] (config>service>ies>sub-if>grp-if sap)
[Tree] (config>service>vprn sap)
[Tree] (config>service>vprn>if sap)
[Tree] (config>service>vprn>sub-if>grp-if sap)

Full Context configure service ies interface sap
configure service ies sap
configure service ies subscriber-interface group-interface sap
configure service vprn interface sap
configure service vprn sap
configure service vprn subscriber-interface group-interface sap

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command. For the 7750 SR, channelized TDM ports are always access ports.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

Note: Configure an IES interface as a loopback interface by issuing the **loopback** command instead of the **sap** *sap-id* command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP are also deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed. The no form of this command causes the ptp-hw-assist to be disabled.

Default No SAPs are defined.

Special Cases **IES —** For the 7750 SR, an IES SAP can be defined with Ethernet ports, SONET/SDH or TDM channels. For the 7450 ESS, IES SAP can be defined with Ethernet or SONET/SDH ports. A SAP is defined within the context of an IP routed interface. Each IP interface is limited to a single SAP definition. For the 7750 SR, group interfaces allow more than one SAP. Attempts to create a second SAP on an IP interface fails and generate an error; the original SAP will not be affected.

Command syntax for the 7750 SR: **sap ipsec**-*id*.**private** | **public**:*tag* associates an IPsec group SAP with this interface. This is the public side for an IPsec tunnel. Tunnels referencing this IPsec group in the private side may be created if their local IP is in the subnet of the interface subnet and the routing context specified matches with the one of the interface.

This context provides a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The “tag” will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 to 4095.

SAP Tunnels — sap tunnel-*id*.**private** | **public**:*tag* — This parameter associates a tunnel group SAP with this interface.

This context will provide a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The “tag” will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 to 4094.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

port-id — Specifies the physical port ID in the *slot/mda/port* format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 61/2/3 specifies port 3 on MDA 2 in slot 61.

Table 121 **Port ID Syntax**

null	*port-id* | lag-*id*
dot1q	{port-id | lag-id}:{qtag1 | cp-conn-prof-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 121 **Port ID Syntax**

qinq	{*port-id* | lag-*id*}:{*qtag1* | cp-*conn-prof-id*}.{*qtag2* | cp-*conn-prof-id*} cp: keyword *conn-prof-id*: 1 to 8000	
port-id	slot/mda/port [.channel]	
	eth-sat-id	esat-id/slot/port
		esat: keyword
		id: 1 to20
	pxc-id	psc-id.sub-port
		pxc psc-id.sub-port
		pxc: keyword
		id: 1 to 64
		sub-port: a, b
lag-id	lag-id	lag: keyword
		id: 1 to 800
qtag1	0 to 4094	
qtag2	* | null | 0 to 4094	

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels (7750 SR), the port ID must include the channel ID. A period "." separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

create — Keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap
- configure service vprn subscriber-interface group-interface sap

All

- configure service ies interface sap
- configure service vprn interface sap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context **[Tree]** (config>service>vprn>sub-if>grp-if sap)

Full Context configure service vprn subscriber-interface group-interface sap

Description This command creates a SAP for the interface.

The **no** form of this command removes the SAP.

Parameters *sap-id* — Specifies the SAP ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context **[Tree]** (config>service>vprn>if sap)

Full Context configure service vprn interface sap

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object. Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command. Channelized TDM ports are always access ports.

If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. The **no** form of this command causes the ptp-h-assist to be disabled.

Default No SAPs are defined.

Special Cases **VPRN —** A VPRN SAP must be defined on an Ethernet interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap ipsec-*id*.**private** | **public**:*tag* — This parameter associates an IPsec group SAP with this interface. This is the public side for an IPsec tunnel. Tunnels referencing this IPsec group in the private side may be created if their local IP is in the subnet of the interface subnet and the routing context specified matches with the one of the interface.

This context will provide a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The "tag" will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 to 4094.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

port-id — Specifies the physical port ID.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 6/2/3 specifies port 3 on MDA 2 in slot 6.

The *port-id* must reference a valid port type. When the *port-id* parameter represents SONET/SDH and TDM channels the port ID must include the channel ID. A period "." separates the physical port from the *channel-id*. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

create — Keyword used to create a SAP instance.

split-horizon-group *group-name* — Specifies the name of the split horizon group to which the SAP belongs.

Platforms All

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id>ppp sap)

Full Context debug service id ppp sap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables PPP debug output for the specified SAP, this command allow multiple instances.

The **no** form of this command disables debugging.

Parameters *sap-id* — Specifies the SAP ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sap

Syntax **sap** *sap-id*
no sap

Context **[Tree]** (config>service>vpls>site sap)

Full Context configure service vpls site sap

Description This command configures a SAP for the site.

The **no** form of this command removes the SAP ID from the configuration.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition

Platforms All

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id>mrp sap)

Full Context debug service id mrp sap

Description This command filters debug events and only shows events for the particular SAP.

The **no** form of this command removes the debug filter.

Parameters *sap-id* — The SAP ID.

Platforms All

sap

Syntax **sap** *sap-id*
no sap

Context **[Tree]** (config>service>epipe>site sap)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service epipe site sap

Description This command configures a SAP for the site.

The **no** form of this command removes the SAP ID from the configuration.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

Platforms All

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id sap)
[Tree] (debug>service>id>dhcp sap)
[Tree] (debug>service>id>stp sap)

Full Context debug service id dhcp sap
debug service id sap
debug service id stp sap

Description This command enables STP debugging for a specific SAP.

The **no** form of the command disables debugging.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

Platforms All

sap

Syntax **sap** [**split-horizon-group** *group-name*] [**create**] [**capture-sap**]
no sap *sap-id*

Context **[Tree]** (config>service>vpls>mac-move>primary-ports sap)
[Tree] (config>service>vpls>mac-move>secondary-ports sap)

Full Context configure service vpls mac-move primary-ports sap
configure service vpls mac-move secondary-ports sap

Description This command declares a specified SAP as a primary (or secondary) VPLS port.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id>arp-host sap)

Full Context debug service id arp-host sap

Description This command displays ARP host events for a particular SAP.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id>igmp-snooping sap)

Full Context debug service id igmp-snooping sap

Description This command shows IGMP packets for a specific SAP.

The **no** form of this command disables the debugging for the SAP.

Platforms All

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id>mld sap)

Full Context debug service id mld-snooping sap

Description This command shows MLD packets for a specific SAP.

The **no** form of this command disables the debugging for the SAP.

Platforms All

sap

Syntax [**no**] **sap** *sap-id*

Context **[Tree]** (debug>service>id>host-connectivity-verify sap)

Full Context debug service id host-connectivity-verify sap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular SAP.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sap

Syntax **sap** *card/mda/aa-svc:vlan* [**create**]
no sap

Context **[Tree]** (config>service>vprn>aa-if sap)

Full Context configure service vprn aa-interface sap

Description This commands specifies which ISA card and which VLAN is used by a given AA Interface.

Default no sap

Parameters *card/mda/aa-svc:vlan* — Specifies the AA ISA card slot/port and VLAN information.

create — Keyword used to create the AARP instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context **[Tree]** (config>service>ies>aa-interface sap)
[Tree] (config>service>vprn>aa-interface sap)

Full Context configure service ies aa-interface sap
configure service vprn aa-interface sap

Description This command configures the AA interface SAP.

Parameters *sap-id* — specifies the physical port identifier portion of the SAP definition.

create — creates the SAP instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

sap

Syntax **sap** *sap-id* [**create**] [**no-endpoint**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sap *sap-id* [**create**] **endpoint** *name*
no sap

Context **[Tree]** (config>mirror>mirror-dest sap)

Full Context configure mirror mirror-dest sap

Description This command creates a service access point (SAP) within a mirror destination service. The SAP is owned by the mirror destination service ID.

The SAP is defined with port and encapsulation parameters to uniquely identify the (mirror) SAP on the interface and within the box. The specified SAP may be defined on an Ethernet access port with a dot1q, null, or q-in-q encapsulation type.

Only one SAP can be created within a **mirror-dest** service ID. If the defined SAP has not been created on any service within the system, the SAP is created and the context of the CLI will change to the newly created SAP. In addition, the port cannot be a member of a multi-link bundle, APS group or IMA bundle.

If the defined SAP exists in the context of another service ID, **mirror-dest** or any other type, an error is generated.

Mirror destination SAPs can be created on Ethernet interfaces that have been defined as an access interface. If the interface is defined as network, the SAP creation returns an error.

When the **no** form of this command is used on a SAP created by a mirror destination service ID, the SAP with the specified port and encapsulation parameters is deleted.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

no-endpoint — Removes the association of a SAP or a sdp with an explicit endpoint name.

name — Specifies the name of the endpoint associated with the SAP.

Platforms All

sap

Syntax **sap** *sap-id* {[**egress**] [**ingress**]}
no sap *sap-id* [**egress**] [**ingress**]

Context **[Tree]** (config>mirror>mirror-source sap)

Full Context configure mirror mirror-source sap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables mirroring of traffic ingressing or egressing a service access port (SAP). A SAP that is defined within a mirror destination cannot be used in a mirror source. The mirror source SAP referenced by the *sap-id* is owned by the service ID of the service in which it was created. The SAP is only referenced in the mirror source name for mirroring purposes. The mirror source association does not need to be removed before deleting the SAP from its service ID. If the SAP is deleted from its service ID, the mirror association is removed from the mirror source.

More than one SAP can be associated within a single **mirror-source**. Each SAP has its own **ingress** and **egress** parameter keywords to define which packets are mirrored to the mirror destination.

The SAP must be valid and properly configured. If the associated SAP does not exist, an error occurs and the command will not execute.

The same SAP cannot be associated with multiple mirror source definitions for ingress packets.

The same SAP cannot be associated with multiple mirror source definitions for egress packets.

If a particular SAP is not associated with a mirror source name, then that SAP will not have mirroring enabled for that mirror source.

Note that the ingress and egress options cannot be supported at the same time on a CEM encap-type SAP. The options must be configured in either the ingress **or** egress contexts (applies to the 7750 SR and 7950 XRS).

The **no** form of this command disables mirroring for the specified SAP. All mirroring for that SAP on ingress and egress is terminated. Mirroring of packets on the SAP can continue if more specific mirror criteria is configured. If the **egress** or **ingress** parameter keywords are specified in the **no** command, only the ingress or egress mirroring condition is removed.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

egress — Specifies that packets egressing the SAP should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the SAP should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

Platforms All

sap

Syntax **sap** *sap-id* {[**ingress**] [**egress**]}
no sap *sap-id* [**ingress**] [**egress**]

Context **[Tree]** (config>li>li-source sap)

Full Context configure li li-source sap

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a service access point (SAP) within an LI configuration. The specified SAP must define a FastE, GigE, or XGigE, or XGigE access port with a dot1q, null, or q-in-q encapsulation type.

When the **no** form of this command is used on a SAP, the SAP with the specified port and encapsulation parameters is deleted.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

egress — Specifies that packets egressing the SAP should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the SAP should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

Platforms All

sap

Syntax **sap** *sap-id* {[**egress**] [**ingress**]}
no sap *sap-id* [**egress**] [**ingress**]

Context **[Tree]** (debug>mirror-source sap)

Full Context debug mirror-source sap

Description This command enables mirroring of traffic ingressing or egressing a service access port (SAP). A SAP that is defined within a mirror destination cannot be used in a mirror source. The mirror source SAP referenced by the *sap-id* is owned by the service ID of the service in which it was created. The SAP is only referenced in the mirror source name for mirroring purposes. The mirror source association does not need to be removed before deleting the SAP from its service ID. If the SAP is deleted from its service ID, the mirror association is removed from the mirror source.

More than one SAP can be associated within a single **mirror-source**. Each SAP has its own **ingress** and **egress** parameter keywords to define which packets are mirrored to the mirror destination.

The SAP must be valid and properly configured. If the associated SAP does not exist, an error occurs and the command will not execute.

The same SAP cannot be associated with multiple mirror source definitions for ingress packets.

The same SAP cannot be associated with multiple mirror source definitions for egress packets.

If a particular SAP is not associated with a mirror source name, then that SAP will not have mirroring enabled for that mirror source.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note that the ingress and egress options cannot be supported at the same time on a CEM encap-type SAP. The options must be configured in either the ingress **or** egress contexts (applies to the 7750 SR and 7950 XRS).

The **no** form of this command disables mirroring for the specified SAP. All mirroring for that SAP on ingress and egress is terminated. Mirroring of packets on the SAP can continue if more specific mirror criteria is configured. If the **egress** or **ingress** parameter keywords are specified in the **no** command, only the ingress or egress mirroring condition is removed.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

egress — Specifies that packets egressing the SAP should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the SAP should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

Platforms All

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context **[Tree]** (config>system>satellite>local-forward sap)

Full Context configure system satellite local-forward sap

Description This command configures a Service Access Point (SAP) used in satellite local forward instances defined in the system.

The **no** form of this command removes the satellite access point from the local-forward instance.

Parameters *eth-sat-id* — Specifies the satellite access point in the local-forward instance in the *esat-id*/*slot*/*port* format.

Values

esat	keyword
id	1 to 20

lag-id — Specifies the LAG identifier, expressed as an integer,

Values

lag	keyword
id	1 to 800

qtag1 — Specifies the qtag value.

Values 1 to 4094

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.20 sap-egress

sap-egress

Syntax **sap-egress** {*policy-id* | *policy-name*} [**create**] [**name** *name*]
no sap-egress {*policy-id* | *policy-name*}

Context **[Tree]** (config>qos sap-egress)

Full Context configure qos sap-egress

Description This command is used to create or edit a Service Egress QoS policy. The egress policy defines the SLA for service packets as they egress on the SAP.

Policies are templates that can be applied to multiple services as long as the scope of the policy is template. The queues defined in the policy are not instantiated until a policy is applied to a service.

Sap-egress policies determine queue mappings based on ingress DSCP, IP precedence, dot1p, and IPv4 or IPv6 match criteria. Multiple queues can be created per forwarding class and each queue can have different CIR or PIR parameters.

Egress SAP QoS policies allow the definition of queues and the mapping of forwarding classes to those queues. Each queue needs to have a relative CIR for determining its allocation of QoS resources during periods of congestion. A PIR can also be defined that forces a hard limit on the packets transmitted through the queue. When the forwarding class is mapped to the queue, a DSCP, IP precedence, or dot1p value can optionally be specified.

The sap-egress policy with *policy-id* 1 is the default sap-egress QoS policy and is applied to service egress SAPs when an explicit policy is not specified or removed. The default sap-egress policy cannot be modified or deleted.

By default, all forwarding classes map to queue 1.

Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all egress SAPs where this policy is applied. For this reason, when many changes are required on a policy, it is highly recommended that the policy be copied to a work area *policy-id*. That work-in-progress policy can be modified until complete, then written over the original policy-id. Use the **config qos copy** command to maintain policies in this manner.

The **no** form of this command deletes the sap-egress policy. A policy cannot be deleted until it is removed from all service SAPs where it is applied. When a sap-egress policy is removed from a SAP, the SAP will revert to the default sap-egress *policy-id* 1.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-id* — The *policy-id* uniquely identifies the policy on the router.

Values 1 to 65535

policy-name — The *policy-name* uniquely identifies the policy.

Values 64 characters maximum.

create — Required parameter when creating a SAP QoS egress policy.

name — Configures an optional policy name, up to 64 characters in length, which adds a name identifier to a given policy to then use that policy name in configuration references as well as display and use policy names in show commands throughout the system. This helps the service provider or administrator to identify and manage sap-egress policies within the SR OS platforms.

All sap-egress policies are required to assign a policy ID to initially create a policy. However, either the policy ID or the policy name can be used to identify and reference a given policy once it is initially created.

If a name is not specified at creation time, then SR OS assigns a string version of the *policy-id* as the name.

Values 64 characters maximum

Platforms All

sap-egress

Syntax **sap-egress** *src-pol dst-pol* [**overwrite**]

Context **[Tree]** (config>qos>copy sap-egress)

Full Context configure qos copy sap-egress

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters **overwrite** — Specifies to replace the existing destination policy. Everything in the existing destination policy will be overwritten with the contents of the source policy. If **overwrite** is not specified, an error will occur if the destination policy ID exists.

```
SR>config>qos# copy sap-egress 1 1010
MINOR: CLI Destination "1010" exists use {overwrite}.
SR>config>qos# copy sap-egress 1 1010 overwrite
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-pol dst-pol — Indicates that the source policy ID and the destination policy ID are SAP egress policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.

Values 1 to 65535

Platforms All

23.21 sap-host-limit

sap-host-limit

Syntax **sap-host-limit** *max-num-hosts-sap*
no sap-host-limit

Context **[Tree]** (config>service>ies>sub-if>grp-if>arp-host sap-host-limit)
[Tree] (config>service>vprn>sub-if>grp-if>arp-host sap-host-limit)

Full Context configure service ies subscriber-interface group-interface arp-host sap-host-limit
configure service vprn subscriber-interface group-interface arp-host sap-host-limit

Description This command configures the maximum number of ARP hosts per SAP.

The **no** form of this command reverts to the default.

Default sap-host-limit 1

Parameters *max-num-hosts-sap* — Specifies the maximum number of ARP hosts per SAP allowed on this interface.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 1 to 131071

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.22 sap-id

sap-id

Syntax **sap-id** *sap-id*
no sap-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident sap-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>host-identification sap-id)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification sap-id
configure subscriber-mgmt local-user-db ppp host host-identification sap-id

Description This command specifies the SAP ID to match for a host lookup. When the LUDB is accessed using a DHCPv4 server, the SAP-ID is matched against the Nokia vendor-specific sub-option in DHCP Option 82.

Note: This command is used only when **sap-id** is configured as one of the **match-list** parameters.

The **no** form of this command removes the SAP ID from the configuration.

Parameters *sap-id* — Specifies a SAP ID, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sap-id

Syntax [**no**] **sap-id**

Context **[Tree]** (config>service>vpls>sap>dhcp>option>vendor sap-id)
[Tree] (config>service>vprn>if>dhcp>option>vendor sap-id)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option>vendor sap-id)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option>vendor sap-id)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option>vendor sap-id)

Full Context configure service ies subscriber-interface group-interface dhcp option vendor-specific-option sap-id
configure service vpls sap dhcp option vendor-specific-option sap-id
configure service vprn interface dhcp option vendor-specific-option sap-id
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option sap-id
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option sap-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the sending of the SAP ID in the Nokia vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command disables the sending of the SAP ID in the Nokia vendor-specific sub-option of the DHCP relay packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option sap-id
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option sap-id
- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option sap-id

All

- configure service vpls sap dhcp option vendor-specific-option sap-id
- configure service vprn interface dhcp option vendor-specific-option sap-id

sap-id

Syntax **sap-id** *sap-string*
no sap-id

Context **[Tree]** (config>service>dynsvc>ladb>user>idx sap-id)

Full Context configure service dynamic-services local-auth-db user-name index sap-id

Description This command specifies the dynamic data service SAP that is created. A dynamic service SAP ID uniquely identifies a dynamic data service instance. For a local authenticated dynamic service data trigger, one of the dynamic service SAP IDs must be the data trigger SAP.

The **no** form of this command removes the **sap-id** from the configuration.

Parameters *sap-string* — Specifies a string representing the dynamic service SAP ID (only SAPs on Ethernet ports and LAGs are valid), up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.23 sap-ingress

sap-ingress

Syntax **sap-ingress** {*policy-id* | *policy-name*} [**create**] [**name** *name*]
no sap-ingress {*policy-id* | *policy-name*}

Context **[Tree]** (config>qos sap-ingress)

Full Context configure qos sap-ingress

Description This command is used to create or edit the ingress policy. The ingress policy defines the SLA enforcement that service packets receive as they ingress a SAP. SLA enforcement is accomplished through the definition of queues that have Forwarding Class (FC), Fair Information Rate (FIR), Committed Information Rate (CIR), Peak Information Rate (PIR), Committed Burst Size (CBS), and Maximum Burst Size (MBS) characteristics.

Policies in effect are templates that can be applied to multiple services as long as the **scope** of the policy is template. Queues defined in the policy are not instantiated until they are assigned to at least one forwarding class and a policy is applied to a service SAP.

It is possible that a SAP ingress policy will include the **dscp** map command, the **dot1p** map command, and an IP or MAC match criteria. When multiple matches occur for the traffic, the order of precedence will be used to arrive at the final action. The order of precedence is as follows:

1. 802.1p bits
2. DSCP
3. IP quintuple or MAC headers

The SAP ingress policy with *policy-id* 1 is a system-defined policy applied to services when no other policy is explicitly specified. The system SAP ingress policy cannot be modified or deleted. The default SAP ingress policy defines one unicast and one multipoint queue associated with all forwarding classes, with an FIR of zero, a CIR of zero, and a PIR of line rate.

Any changes made to the existing policy, using any of the sub-commands, are applied immediately to all services where this policy is applied. For this reason, when many changes are required on a policy, it is recommended that the policy be copied to a work area policy ID. That work-in-progress policy can be modified until complete, then written over the original policy-id. Use the **config>qos>copy** command to maintain policies in this manner.

The **no** form of this command deletes the SAP ingress policy. A policy cannot be deleted until it is removed from all services where it is applied.

Parameters *policy-id* — The *policy-id* uniquely identifies the policy.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

policy-name — The *policy-name* uniquely identifies the policy.

Values 64 characters maximum

create — Required parameter when creating a SAP QoS ingress policy.

name *name* — Configures an optional policy name, up to 64 characters in length, which adds a name identifier to a given policy to then use that policy name in configuration references as well as display and use policy names in show commands throughout the system. This helps the service provider/administrator to identify and manage sap-ingress policies within the SR OS platforms.

All sap-ingress policies are required to assign a policy ID to initially create a policy. However, either the policy ID or the policy name can be used to identify and reference a given policy once it is initially created.

If a name is not specified at creation time, then SR OS assigns a string version of the *policy-id* as the name.

Values 64 characters maximum

Platforms All

sap-ingress

Syntax **sap-ingress** *src-pol dst-pol* [**overwrite**]

Context **[Tree]** (config>qos>copy sap-ingress)

Full Context configure qos copy sap-ingress

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters **overwrite** — Specifies to replace the existing destination policy. Everything in the existing destination policy will be overwritten with the contents of the source policy. If **overwrite** is not specified, an error will occur if the destination policy ID exists.

```
SR>config>qos# copy sap-egress 1 1010
MINOR: CLI Destination "1010" exists use {overwrite}.
SR>config>qos# copy sap-egress 1 1010 overwrite
```

src-pol dst-pol — Indicates that the source policy ID and the destination policy ID are SAP ingress policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.24 sap-limit

sap-limit

Syntax **sap-limit** [*limit*]
no sap-limit

Context **[Tree]** (config>service>dynsvc>policy sap-limit)

Full Context configure service dynamic-services dynamic-services-policy sap-limit

Description This command specifies a limit for the number of dynamic data service instances (SAPs) that can be setup simultaneously using a given dynamic services policy.

A value of zero (0) means the policy is drained: existing dynamic data services can be modified and torn down but no new dynamic data services can be setup.

Default sap-limit 1

Parameters *limit* — Specifies the number of dynamic data service SAPs that can be setup simultaneously using this dynamic services policy.

Values 0 to 131072

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.25 sap-parameters

sap-parameters

Syntax **sap-parameters**

Context **[Tree]** (config>service>ies>sub-if>grp-if sap-parameters)
[Tree] (config>service>vprn>sub-if>grp-if sap-parameters)

Full Context configure service ies subscriber-interface group-interface sap-parameters
configure service vprn subscriber-interface group-interface sap-parameters

Description Commands in this context configure parameters that can be applied to automatically-generated internal SAPs.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.26 sap-session-index

sap-session-index

Syntax [**no**] **sap-session-index**

Context **[Tree]** (config>subscr-mgmt>auth-policy>include-radius-attribute sap-session-index)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute sap-session-index

Description This command includes **sap-session-index** attributes.

The **no** form of this command excludes **sap-session-index** attributes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.27 sap-session-limit

sap-session-limit

Syntax **sap-session-limit** *sap-session-limit*
no sap-session-limit

Context **[Tree]** (config>service>ies>sub-if>grp-if>pppoe sap-session-limit)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe sap-session-limit)

Full Context configure service ies subscriber-interface group-interface pppoe sap-session-limit
configure service vprn subscriber-interface group-interface pppoe sap-session-limit

Description This command specifies the number of PPPoE hosts per SAP allowed for this group-interface.

The **no** form of this command reverts to the default.

Default sap-session-limit 1

Parameters *sap-session-limit* — Specifies the number of PPPoE hosts per SAP allowed.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 1 to 131071

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sap-session-limit

Syntax **sap-session-limit** *sap-session-limit*
no sap-session-limit

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipoe-session sap-session-limit)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session sap-session-limit)

Full Context configure service ies subscriber-interface group-interface ipoe-session sap-session-limit
configure service vprn subscriber-interface group-interface ipoe-session sap-session-limit

Description This command specifies the number of IPoE sessions per SAP allowed for this group-interface.

The **no** form of this command reverts to the default.

Default sap-session-limit 1

Parameters *sap-session-limit* — Specifies the number of allowed IPoE sessions.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 1 to 131071 131071 on wlan-gw group interfaces

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.28 sap-template

sap-template

Syntax **sap-template** *sap-template*
no sap-template

Context **[Tree]** (config>service>vpls>wlan-gw sap-template)

Full Context configure service vpls wlan-gw sap-template

Description This command specifies the VPLS SAP template that is applied on the internal SAPs created for communication between the VPLS and the ISAs.

The **no** form of this command removes the SAP template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sap-template* — Specifies the existing SAP template to apply. The template is created in the **config>service>template** context.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

sap-template

Syntax **sap-template** *name* [**create**]
no sap-template *name*

Context **[Tree]** (config>subscr-mgmt sap-template)

Full Context configure subscriber-mgmt sap-template

Description This command configures a template that specifies parameters for automatically generated subscriber SAPs, for example, when creating CUPS sessions. A template with the name "default" is used if no specific name is provided, but this must be manually provisioned.

The **no** form of this command removes the template.

Parameters *name* — Specifies the name of the PFCP association, up to 32 characters.

create — Keyword used to create the SAP template.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.29 sap-template-binding

sap-template-binding

Syntax **sap-template-binding** *name/id*
no sap-template-binding

Context **[Tree]** (config>service>vpls>vpls-group sap-template-binding)

Full Context configure service vpls vpls-group sap-template-binding

Description This command configures the binding to a SAP template to be used to instantiate SAPs in the data VPLS using as input variables the VLAN IDs generated by the vid-range command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the binding and deletes the related SAP instances. The command will fail if any of the affected VPLS instances have either a provisioned SAP or an active MVRP declaration/registration or if the related vpls-group is in no shutdown state. Any changes to the **sap-template-binding** require the **vpls-group** to be in **shutdown** state. New control SAP additions to the management VPLS are allowed as long as data VPLS instantiations/removals for vpls-groups are not in progress. Control SAPs can be removed at any time generating the removal of related data SAPs from the data VPLS. The **shutdown** or **no shutdown** state for the control SAPs does not have any effect on data SAPs instantiated with this command.

Default no sap-template-binding

Parameters *name* — Specifies the name of the VPLS template

Values ASCII character string

id — Specifies the ID of the VPLS template

Values 1 to 8196

Platforms All

23.30 sat-type

sat-type

Syntax **sat-type** *sat-type* [**port-template** *template-name*]
no sat-type

Context **[Tree]** (config>system>satellite>eth-sat sat-type)
[Tree] (config>system>satellite>tdm-sat sat-type)

Full Context configure system satellite eth-sat sat-type
configure system satellite tdm-sat sat-type

Description This command configures the type of satellite variant for the associated satellite chassis.

The **no** form of the command deletes the **sat-type** configuration.

Default no sat-type

Parameters *sat-type* — Specifies the satellite type. Configuration of the following variants is supported:

es24-1gb-sfp — Specifies the 24xGE (SFP) + 4x10GE Ethernet satellite.

es48-1gb-sfp — Specifies the 48xGE (SFP) + 4x10GE Ethernet satellite.

es24-sass-1gb-sfp — Specifies the SAS-S 24xGE (SFP) + 4x10GE Ethernet satellite.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

es48-sass-1gb-sfp — Specifies the SAS-S 48xGE (SFP) + 4x10GE Ethernet satellite.

es24-1gb-tx — Specifies the 24xGE (copper) + 4x10GE Ethernet satellite.

es48-1gb-tx — Specifies the 48xGE (copper) + 4x10GE Ethernet satellite.

es24-1gb-tx — Specifies the 24-port copper + PoE Ethernet satellite.

es48-1gb-tx — Specifies the 48-port copper + PoE Ethernet satellite.

es64-10gb-sfpp+4-100gb-cfp4 — Specifies the 64x10GE + 4x100GE Ethernet satellite.

es64-10gb-sfpp+4-100gb-qsfp28 — Specifies the 64x10GE + 4xQSFP28 Ethernet satellite.

es24-sasmxp-1gb-sfp — Specifies the 7210 SAS-Mxp as an ethernet satellite.

ts4-choc3-sfp — Specifies the 4-port OC3 TDM satellite.

ts4-chstm1-sfp — Specifies the 4-port STM1 TDM satellite.

ts1-choc12-sfp — Specifies the 1-port OC12 TDM satellite.

ts1-chstm4-sfp — Specifies the 1-port STM4 TDM satellite.

template-name — Specifies the name for the associated port template.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure system satellite eth-sat sat-type

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure system satellite tdm-sat sat-type

23.31 satellite

satellite

Syntax **satellite**

Context **[Tree]** (config>system satellite)

Full Context configure system satellite

Description This command enables the satellite configuration context. Within the satellite context, the administrator can specify the configuration details for a satellite chassis that is hosted by the associated local system.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

satellite

Syntax **satellite**

Context **[Tree]** (admin satellite)

Full Context admin satellite

Description This command performs satellite operations.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.32 save

save

Syntax **save**

Context **[Tree]** (config>li save)

Full Context configure li save

Description This command is required to save LI configuration parameters.

Platforms All

save

Syntax **save** [*cflash-id*]

Context **[Tree]** (bof save)

Full Context bof save

Description This command uses the boot option parameters currently in memory and writes them from the boot option file to the specified compact flash.

The BOF must be located in the root directory of the internal or external compact flash drives local to the system and have the mandatory filename of *bof.cfg*.

If a location is not specified, the BOF is saved to the default compact flash drive (cf3:) on the active CPM (typically the CPM in slot A, but the CPM in slot B could also be acting as the active CPM). The slot name is not case-sensitive. You can use upper or lowercase “A” or “B”.

Command usage:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **bof save** — saves the BOF to the default drive (cf3:) on the active CPM (either in slot A or B)
- **bof save cf3:** — saves the BOF to cf3: on the active CPM (either in slot A or B)

To save the BOF to a compact flash drive on the standby CPM (for example, the redundant (standby) CPM is installed in slot B), specify -A or -B option.

Command usage:

- **bof save cf3-A:** — saves the BOF to cf3: on CPM in slot A whether it is active or standby
- **bof save cf3-B:** — saves the BOF to cf3: on CPM in slot B whether it is active or standby

The slot name is not case-sensitive. You can use upper or lowercase “A” or “B”.

The **bof save** and **show bof** commands allow you to save to or read from the compact flash of the standby CPM. Use the **show card** command to determine the active and standby CPM (A or B).

Default Saves must be explicitly executed. The BOF is saved to cf3: if a location is not specified.

Parameters *flash-id* — Specifies the compact flash ID where the *bof.cfg* is to be saved.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Default cf3:

Platforms All

save

Syntax **save** *file-url*

Context **[Tree]** (candidate save)

Full Context candidate save

Description This command saves the current candidate to a file.

Parameters *file-url* — Specifies the directory and filename.

save

Syntax **save** [**comment** *comment*] [**rescue**]

Context **[Tree]** (admin>rollback save)

Full Context admin rollback save

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description If the optional **rescue** keyword is not used, this command saves a rollback checkpoint at the location and with the filename specified by the rollback-location with a suffix of .rb. The previously saved checkpoints will have their suffixes incremented by one (.rb.1 becomes .rb.2, and so on). If there are already as many checkpoint files as the maximum number supported, then the last checkpoint file is deleted.

If the **rescue** keyword is used, then this command saves the current operational configuration as a rescue configuration at the location and with the filename specified by the rescue location. The filename will have the suffix .rc appended.

Parameters *comment-string* — Specifies a comment, up to 255 characters, that is associated with the checkpoint.

rescue — Saves the rescue checkpoint instead of a normal rollback checkpoint.

Platforms All

save

Syntax **save** [*file-url*] [**detail**] [**index**]

Context **[Tree]** (admin save)

Full Context admin save

Description This command saves the running configuration to a configuration file. For example:

```
A:ALA-1>admin# save ftp://test:test@192.168.x.xx/./100.cfg
Saving configuration .........Completed.
```

By default, the running configuration is saved to the primary configuration file.

Parameters *file-url* — Specifies the file URL location to save the configuration file.

Values

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-url | *remote-url*	
local-url	[*cflash-id/*][*file-path*] 200 chars max, including cflash-id directory length 99 chars max each
remote-url	[{ftp:// | tftp://}*login:pswd@remote-locn/*][*file-path*] 243 chars max directory length 99 chars max each
remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[*-interface*] *x:x:x:x:x:x:d.d.d.d*[*-interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - 32 chars max, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Default the primary configuration file location

detail — Saves both default and non-default configuration parameters.

index — Forces a save of the persistent index file regardless of the persistent status in the BOF file. The index option can also be used to avoid an additional boot required while changing your system to use the persistence indices.

Platforms All

23.33 save-deterministic-script

save-deterministic-script

Syntax **save-deterministic-script**

Context **[Tree]** (admin>nat save-deterministic-script)

Full Context admin nat save-deterministic-script

Description This command saves the script that calculates Deterministic NAT map entries.

Once the location for the Python deterministic NAT script is configured, the script is generated/updated every time deterministic NAT configuration is modified. However, the script must be manually exported to the remote location. This command triggers the export of the script to a remote location.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.34 saved-ind-prompt

saved-ind-prompt

Syntax [**no**] **saved-ind-prompt**

Context **[Tree]** (environment saved-ind-prompt)

Full Context environment saved-ind-prompt

Description This command enables saved indicator in the prompt. When changes are made to the configuration file a "*" appears in the prompt string indicating that the changes have not been saved. When an **admin save** command is executed the "*" disappears.

```
*A:ALA-48# admin save
Writing file to ftp://192.0.2.43/./sim48/sim48-config.cfg
Saving configuration .... Completed.
A:ALA-48#
```

Platforms All

23.35 scaling-profile

scaling-profile

Syntax **scaling-profile** *scaling-profile-id*

Context **[Tree]** (config>isa>nat-group scaling-profile)

Full Context configure isa nat-group scaling-profile

Description This command determines profiles for NAT scaling. Lower profile numbers allocate less resources, therefore, supporting lower scaling.

Contact your Nokia representative for more information about NAT scaling figures in each profile.

Default scaling-profile profile1

Parameters *scaling-profile-id* — Specifies the name of the profile, up to 32 characters.

Values ESA-VM supports three scaling profiles, while VSR-I supports only two.

- profile1 is a low scaling profile that requires 8 CPU cores and 32 GB of DRAM memory per ESA-VM

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- profile2 is a medium scaling profile that requires 11 CPU cores and 96 GB of DRAM memory per ESA-VM
- profile3 is a high scaling profile that requires 15 CPU cores and 115 GB of DRAM memory per ESA-VM

For the number of required CPU control cores on a VSR-I in relation to profiles, see to the Sysinfo section in the Virtualized Service Router Installation and Setup Guide.For the amount of required memory on VSR-I in relation to profiles, refer to Software Release Notes, section VM Memory Requirements by Function Mix.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.36 sched-class

sched-class

Syntax **sched-class** *sched-class* **group** *name* **[weight** *weight***]**
no sched-class *sched-class*

Context **[Tree]** (config>qos>hw-agg-shap-sched-plcy sched-class)

Full Context configure qos hw-agg-shaper-scheduler-policy sched-class

Description This command configures the scheduling class for the hardware aggregate shaper scheduler policy.

The **no** form of this command removes the scheduling class configuration.

Parameters *sched-class* — Specifies the scheduling class ID.

Values 3 to 6

name — Assigns the specified scheduling class to a group within the hardware aggregate shaper scheduler policy.

weight — Specifies the weight for a scheduling class within the specified group.

Values 3 to 8

Default 1

Platforms 7750 SR-1, 7750 SR-s

sched-class

Syntax **sched-class** *sched-class*
no sched-class

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>sap-egress>queue sched-class)

Full Context configure qos sap-egress queue sched-class

Description This command configures the scheduling class for the hardware aggregate shaper scheduler policy.

The **no** form of this command removes the scheduling class configuration.

Parameters *sched-class* — Specifies the scheduling class ID.

Values 3 to 6

Platforms 7750 SR-1, 7750 SR-s

23.37 sched-class-elevation

sched-class-elevation

Syntax **sched-class-elevation sched-class** *sched-class* **weight** *weight*
no sched-class-elevation sched-class *sched-class*

Context [Tree] (config>qos>sap-egress sched-class-elevation)

Full Context configure qos sap-egress sched-class-elevation

Description This command configures the scheduling class elevation.

The **no** form of this command removes the scheduling class elevation configuration.

Parameters *sched-class* — Specifies the scheduling class ID.

Values 3 to 6

weight — Specifies the weight for the scheduling class.

Values 3 to 8

Platforms 7750 SR-1, 7750 SR-s

23.38 sched-run-min-int

sched-run-min-int

Syntax **sched-run-min-int** *percent-of-default*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no sched-run-min-int

Context [Tree] (config>card>virt-sched-adj sched-run-min-int)

Full Context configure card virtual-scheduler-adjustment sched-run-min-int

Description This command overrides the default minimum time that must elapse before a virtual scheduler may redistribute bandwidth based on changes to the offered rates of member policers or queues. A minimum run interval is enforced to allow a minimum amount of "batching" queue changes before reacting to the changed rates. This minimum interval is beneficial since the periodic function of determining policer or queue offered rates is performed sequentially and the interval allows a number policer and queue rates to be determined prior to determining the distribution of bandwidth to the policers and queues.

The default minimum scheduler run interval is 0.5 seconds. The sched-run-min-int command uses a percent value to modify the default interval.

The **no** form of this command restores the default minimum scheduler run interval for all virtual schedulers on the card.

Default no sched-run-min-int

Parameters *percent-of-default* — Specifies that the percent-of-default parameter is required and is used to modify the default minimum scheduler run interval for all virtual schedulers on the card. Defining 100.00 percent is equivalent to removing the override (restoring the default) for the minimum scheduler run interval.

Values 0.01% to 1000.00%

Default 100.00%

Platforms All

23.39 schedule

schedule

Syntax [**no**] **schedule** *schedule-name* [**owner** *schedule-owner*]

Context [Tree] (config>system>cron schedule)

Full Context configure system cron schedule

Description This command configures the type of schedule to run, including one-time only (oneshot), periodic or calendar-based runs. All runs are determined by month, day of month or weekday, hour, minute and interval (seconds).

The **no** form of the command removes the context from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *schedule-name* — Specifies the name of the schedule. The name can be up to 32 characters.

schedule-owner — Specifies the owner name of the schedule. The name can be up to 32 characters.

Default TiMOS CLI

Platforms All

23.40 schedule-type

schedule-type

Syntax **schedule-type** *schedule-type*

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update schedule-type)

Full Context configure system security pki ca-profile auto-crl-update schedule-type

Description This command specifies the schedule type for auto CRL update. The system supports two types:

- **periodic**: — The system will download a CRL periodically at the interval configured via the **periodic-update-interval** command. For example, if the periodic-update-interval is 1 day, then the system will download a CRL every 1 day. The minimal periodic-update-interval is 1 hour.
- **next-update-based** — The system will download a CRL at the time = Next_Update_of_existing_CRL *minus* pre-update-time. For example, if the Next-Update of the existing CRL is 2015-06-30 06:00 and pre-update-time is 1 hour, then the system will start downloading at 2015-06-30, 05:00.

Default schedule-type next-update-based

Parameters *schedule-type* — Specifies the type of time scheduler to update the CRL.

Values periodic, next-update-based

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.41 scheduler

scheduler

Syntax **scheduler** *scheduler-name* **rate** *pir-rate* [**cir** *cir-rate*]
no scheduler *scheduler-name*

Context **[Tree]** (config>subscr-mgmt>sub-prof>egr>sched scheduler)
[Tree] (config>subscr-mgmt>sub-prof>ing>sched scheduler)

Full Context configure subscriber-mgmt sub-profile egress scheduler-policy scheduler
configure subscriber-mgmt sub-profile ingress scheduler-policy scheduler

Description This command provides a way to override parameters of the existing scheduler associated with the egress or ingress scheduler policy. A scheduler defines bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier).

The **no** form of this command reverts to the default.

Parameters *scheduler-policy-name* — Specify an existing scheduler policy name.

pir-rate — Specify the pir-rate, in kilobits, to override the administrative PIR used by the scheduler. When the **rate** command is executed, a valid PIR setting must be explicitly defined. Fractional values are not allowed and must be given as a positive integer.

Values 1 to 3200000000, max

cir-rate — The **cir** parameter overrides the administrative CIR used by the scheduler. When the **rate** command is executed, a CIR setting is optional. The sum keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues. Fractional values are not allowed and must be given as a positive integer.

Values 0 to 3200000000, sum, max

Default sum

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>service>vpls>sap>egress>sched-override scheduler)

Full Context configure service vpls sap egress scheduler-override scheduler

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command overrides specific attributes of the specified scheduler name.

A scheduler defines a bandwidth control that limits each child (other schedulers, policers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created has policers, queues or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword **create**), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause policers, queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context does not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

Step 1. The maximum number of schedulers has not been configured.

Step 2. The provided *scheduler-name* is valid.

Step 3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command does not execute, nor does the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error occurs, the command does not execute, and the CLI context does not change.

The **no** form of this command removes the scheduler name from the configuration.

Parameters *scheduler-name* — Specifies name of the scheduler

Values Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>port>ethernet>access>egr>qgrp>sched-override scheduler)
[Tree] (config>port>ethernet>access>ing>qgrp>sched-override scheduler)

Full Context configure port ethernet access egress queue-group scheduler-override scheduler
configure port ethernet access ingress queue-group scheduler-override scheduler

Description This command can be used to override specific attributes of the specified scheduler name. A scheduler defines bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers. The *scheduler-name* must exist in the applied scheduler policy.

The **no** form of this command removes the scheduler overrides for the specified scheduler and returns the scheduler's parent weight and CIR weight, and its PIR and CIR to the values configured in the applied scheduler policy.

Parameters *scheduler-name* — Specifies the name of the scheduler.

Values Valid names consist of any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — Creates a new scheduler for this port.

Platforms All

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>service>apipe>sap>egress>sched-override scheduler)
[Tree] (config>service>apipe>sap>ingress>sched-override scheduler)
[Tree] (config>service>cpipe>sap>egress>sched-override scheduler)
[Tree] (config>service>cpipe>sap>ingress>sched-override scheduler)
[Tree] (config>service>epipe>sap>egress>sched-override scheduler)
[Tree] (config>service>epipe>sap>ingress>sched-override scheduler)
[Tree] (config>service>fpipe>sap>egress>sched-override scheduler)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>fpipe>sap>ingress>sched-override scheduler)
[Tree] (config>service>ipipe>sap>egress>sched-override scheduler)
[Tree] (config>service>ipipe>sap>ingress>sched-override scheduler)

Full Context

configure service apipe sap egress scheduler-override scheduler
configure service apipe sap ingress scheduler-override scheduler
configure service cpipe sap egress scheduler-override scheduler
configure service cpipe sap ingress scheduler-override scheduler
configure service epipe sap egress scheduler-override scheduler
configure service epipe sap ingress scheduler-override scheduler
configure service fpipe sap egress scheduler-override scheduler
configure service fpipe sap ingress scheduler-override scheduler
configure service ipipe sap egress scheduler-override scheduler
configure service ipipe sap ingress scheduler-override scheduler

Description

This command can be used to override specific attributes of the specified scheduler name. A scheduler defines bandwidth controls that limit each child (other schedulers, policers, and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have policers, queues or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause policers, queues, or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided *scheduler-name* is valid.
3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the following criteria, a name syntax error will occur, the command will not execute, and the CLI context will not change.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *scheduler-name* — The name of the scheduler.

Values Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Default None. Each scheduler must be explicitly created.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress scheduler-override scheduler
- configure service fpipe sap ingress scheduler-override scheduler
- configure service cpipe sap ingress scheduler-override scheduler
- configure service fpipe sap egress scheduler-override scheduler

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress scheduler-override scheduler
- configure service apipe sap ingress scheduler-override scheduler

All

- configure service epipe sap egress scheduler-override scheduler
- configure service ipipe sap egress scheduler-override scheduler
- configure service ipipe sap ingress scheduler-override scheduler
- configure service epipe sap ingress scheduler-override scheduler

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>service>vprn>if>sap>egress>sched-override scheduler)
[Tree] (config>service>vprn>if>sap>ingress>sched-override scheduler)

Full Context configure service vprn interface sap egress scheduler-override scheduler
configure service vprn interface sap ingress scheduler-override scheduler

Description This command can be used to override specific attributes of the specified scheduler name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A scheduler defines a bandwidth controls that limit each child (other schedulers, policers, and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have policers, queues, or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

Step 1. The maximum number of schedulers has not been configured.

Step 2. The provided *scheduler-name* is valid.

Step 3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

Parameters *scheduler-name* — Specifies the name of the scheduler.

Values Valid names consist of any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

create — Specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>service>ies>if>sap>egress>sched-override scheduler)
[Tree] (config>service>ies>if>sap>ingress>sched-override scheduler)

Full Context configure service ies interface sap egress scheduler-override scheduler
configure service ies interface sap ingress scheduler-override scheduler

Description This command can be used to override specific attributes of the specified scheduler name.

A scheduler defines a bandwidth controls that limit each child (other schedulers, policers, and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have policers, queues, or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

Step 1. The maximum number of schedulers has not been configured.

Step 2. The provided *scheduler-name* is valid.

Step 3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *scheduler-name* — The name of the scheduler.

Values Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Default None. Each scheduler must be explicitly created.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

Platforms All

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>qos>scheduler-policy>tier scheduler)

Full Context configure qos scheduler-policy tier scheduler

Description This command creates a new scheduler or edits an existing scheduler within the scheduler policy tier. A scheduler defines bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however, the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce SLAs.

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

1. The maximum number of schedulers has not been configured.
2. The provided *scheduler-name* is valid.
3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs, the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

Parameters *scheduler-name* — Specifies the scheduler name.

Values Valid names consist of any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

Platforms All

scheduler

Syntax **scheduler** *scheduler-name* [**create**]
no scheduler *scheduler-name*

Context **[Tree]** (config>service>cust>multi-service-site>ingress>sched-override scheduler)
[Tree] (config>service>cust>multi-service-site>egress>sched-override scheduler)

Full Context configure service customer multi-service-site egress scheduler-override scheduler
configure service customer multi-service-site ingress scheduler-override scheduler

Description This command override specifics attributes of the specified scheduler name.

A scheduler defines bandwidth controls that limit each child (other schedulers, policers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have policers, queues or other schedulers defined as child associations. The scheduler can be a child which takes bandwidth from a scheduler in a higher tier. A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause policer, queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the *scheduler-name* exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the *scheduler-name* does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

Step 1. The maximum number of schedulers has not been configured.

Step 2. The provided *scheduler-name* is valid.

Step 3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

The **no** form of the command disables the scheduler override.

Parameters *scheduler-name* — Specifies the name of the scheduler.

Values Valid names consist of any string up to 32 characters in length, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given *scheduler-name*. If the **create** keyword is omitted, **scheduler-name** is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

Platforms All

scheduler

Syntax **scheduler** *scheduler-name* **rate** *pir-rate* [**cir** *cir-rate*]
no scheduler *scheduler-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>sla-prof>egress>sched scheduler)

Full Context configure subscriber-mgmt sla-profile egress scheduler-policy scheduler

Description This command provides a way to override parameters of the existing scheduler associated with the egress scheduler policy. A scheduler defines bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier).

The **no** form of this command reverts to the default.

Parameters *scheduler-name* — Specify an existing scheduler policy name up to 32 characters.

pir-rate — Specifies the PIR rate in kb/s. This parameter overrides the administrative PIR used by the scheduler. When the rate command is executed, a valid PIR setting must be explicitly defined. Fractional values are not allowed and must be given as a positive integer.

Values 1 to 3200000000, max

cir-rate — Specifies the CIR rate in kb/s. This parameter overrides the administrative CIR used by the scheduler. When the rate command is executed, a CIR setting is optional. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues. Fractional values are not allowed and must be given as a positive integer.

Values 0 to 3200000000, sum, max

Default sum

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.42 scheduler-override

scheduler-override

Syntax [**no**] **scheduler-override**

Context [Tree] (config>service>vpls>sap>egress scheduler-override)
[Tree] (config>service>vpls>sap>ingress scheduler-override)

Full Context configure service vpls sap egress scheduler-override
configure service vpls sap ingress scheduler-override

Description Commands in this context configure the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag returns the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes scheduler parameters from the configuration.

Platforms All

scheduler-override

Syntax [**no**] **scheduler-override**

Context **[Tree]** (config>port>ethernet>access>egr>qgrp scheduler-override)
[Tree] (config>port>ethernet>access>ing>qgrp scheduler-override)

Full Context configure port ethernet access egress queue-group scheduler-override
configure port ethernet access ingress queue-group scheduler-override

Description This command specifies the set of attributes whose values have been overridden by management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the ingress or egress queue group template.

The **no** form of this command removes all of the scheduler overrides and returns the scheduler's parent weight and CIR weight, and its PIR and CIR to the values configured in the applied scheduler policy.

Platforms All

scheduler-override

Syntax [**no**] **scheduler-override**

Context **[Tree]** (config>service>apipe>sap>egress scheduler-override)
[Tree] (config>service>apipe>sap>ingress scheduler-override)
[Tree] (config>service>cpipe>sap>egress scheduler-override)
[Tree] (config>service>cpipe>sap>ingress scheduler-override)
[Tree] (config>service>epipe>sap>egress scheduler-override)
[Tree] (config>service>epipe>sap>ingress scheduler-override)
[Tree] (config>service>fpipe>sap>egress scheduler-override)
[Tree] (config>service>fpipe>sap>ingress scheduler-override)
[Tree] (config>service>ipipe>sap>egress scheduler-override)
[Tree] (config>service>ipipe>sap>ingress scheduler-override)

Full Context configure service apipe sap egress scheduler-override
configure service apipe sap ingress scheduler-override
configure service cpipe sap egress scheduler-override
configure service cpipe sap ingress scheduler-override
configure service epipe sap egress scheduler-override
configure service epipe sap ingress scheduler-override
configure service fpipe sap egress scheduler-override
configure service fpipe sap ingress scheduler-override
configure service ipipe sap egress scheduler-override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ipipe sap ingress scheduler-override

Description This command specifies the set of attributes whose values have been overridden by management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap ingress scheduler-override
- configure service fpipe sap egress scheduler-override
- configure service cpipe sap egress scheduler-override
- configure service fpipe sap ingress scheduler-override

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress scheduler-override
- configure service apipe sap ingress scheduler-override

All

- configure service ipipe sap egress scheduler-override
- configure service epipe sap egress scheduler-override
- configure service epipe sap ingress scheduler-override
- configure service ipipe sap ingress scheduler-override

scheduler-override

Syntax [**no**] **scheduler-override**

Context **[Tree]** (config>service>ies>if>sap>egress scheduler-override)
[Tree] (config>service>ies>if>sap>ingress scheduler-override)

Full Context configure service ies interface sap egress scheduler-override
configure service ies interface sap ingress scheduler-override

Description This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

Platforms All

scheduler-override

Syntax [**no**] **scheduler-override**

Context **[Tree]** (config>service>vprn>if>sap>egress scheduler-override)
[Tree] (config>service>vprn>if>sap>ingress scheduler-override)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap egress scheduler-override
configure service vprn interface sap ingress scheduler-override

Description This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

Platforms All

scheduler-override

Syntax [**no**] **scheduler-override**

Context **[Tree]** (config>service>cust>multi-service-site>ingress scheduler-override)
[Tree] (config>service>cust>multi-service-site>egress scheduler-override)

Full Context configure service customer multi-service-site egress scheduler-override
configure service customer multi-service-site ingress scheduler-override

Description This command specifies the set of attributes whose values have been overridden by management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress and egress scheduler policy.

The **no** form of the command disables the override.

Platforms All

23.43 scheduler-parent

scheduler-parent

Syntax **scheduler-parent** *scheduler-name* [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*] [**cir-level** *cir-level*]
no scheduler-parent

Context **[Tree]** (config>qos>sap-egress>policer scheduler-parent)

Full Context configure qos sap-egress policer scheduler-parent

Description This command defines an optional parent scheduler that governs the available bandwidth given to a policer in addition to the PIR setting of the policer. When multiple schedulers, queues, or policers share a child status with the parent scheduler, the **weight** or **level** parameters define how this policer contends with the other children for the bandwidth of the parent. This command and the configuration of a SAP policer **port-parent** or **parent** arbiter are mutually exclusive.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Multiple schedulers can exist in different scheduler policies with the same *scheduler-name*; in this command, the associated *scheduler-name* pertains to a scheduler that should exist on the SAP as the policy is applied and the policer is created. When the policer is created on the SAP, the existence of the *scheduler-name* is dependent on a scheduler policy containing the *scheduler-name* being directly applied or indirectly applied (through a multiservice customer site) to the SAP. The policer accepts packets, but is not bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP. The SAP to which the policer belongs displays an orphan policer status with the SapEgressPolicerMismatch flag in the **show service sap-using** output. The orphaned state of the policer is automatically cleared when the *scheduler-name* becomes available on the SAP.

The parent scheduler can be made unavailable by the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the policer enters the orphaned state. The policer automatically returns to normal operation when the parent scheduler is available again.

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and no error message is returned. When a parent association has been removed, the former child policer attempts to operate based on its configured rate parameter.

Removing the parent association on the policer within the policy takes effect immediately on all policers using the SAP QoS policy.

Default no scheduler-parent

Parameters *scheduler-name* — Scheduler names are configured in the **config>qos>scheduler-policy>tier** context. There are no checks performed at the time of definition to ensure that the *scheduler-name* exists within an existing scheduler policy. For the policer to use the defined *scheduler-name*, the scheduler must exist on each SAP that the policer is created on. If a *scheduler-name* does not exist on the SAP, the policer operates in an orphaned state.

Values Any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Default None. Each parental association must be explicitly defined.

weight — Defines the relative weight of this policer in comparison with other child policers, queues, and schedulers when competing for bandwidth on the parent *scheduler-name* at the above-CIR priority level defined by the **level** parameter.

All weight values from all weighted active policers, queues, and schedulers with a common port parent are added together. Then, each individual active weight is divided by the total to determine the percentage of remaining bandwidth provided to the policer, queue, or scheduler after the higher priority level children have been serviced. A weight is considered to be active when the applicable policer, queue, or

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scheduler has not reached its maximum rate and still has packets to transmit. All child policers, queues, and schedulers with a weight of 0 are considered to have the lowest priority at the configured level and are not serviced until all non-zero weighted policers, queues, and schedulers at that level are operating at the maximum bandwidth or are idle.

Values 0 to 100

Default 1

level — Defines the level of hierarchy when compared with other policers, queues, and schedulers when competing for bandwidth on the parent *scheduler-name*.

Children of the parent scheduler with a lower priority will not receive bandwidth until all children with a higher priority have either reached their maximum bandwidth or are idle. Children with the same level are serviced in relation to their relative weights.

Values 1 to 8 (8 is the highest priority)

Default 1

cir-weight — Defines the relative weight of this policer in comparison with other child policers, queues, or schedulers competing for bandwidth on the parent *scheduler-name* at the within-CIR priority level defined by the **cir-level** parameter.

All **cir-weight** values from all weighted active policers, queues, and schedulers with a common parent are added together. Then, each individual active weight is divided by the total to determine the percentage of remaining bandwidth provided to the policer, queue, or scheduler after the higher priority level children have been serviced. A weight is considered to be active when the applicable policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit.

The weight is specified as an integer value from 0 to 100, with 100 being the highest weight. When the **cir-weight** parameter is set to a value of 0, the policer receives bandwidth only after the other children with a non-zero weight at this level.

Values 0 to 100

Default 1

cir-level — Defines the level of hierarchy when compared with other policers, queues, and schedulers that the policer uses to receive bandwidth for its within-CIR offered load. If the **cir-level** parameter is set to a value of 0 (the default value), the policer does not receive bandwidth during the schedulers within-CIR pass and the **cir-weight** parameter is ignored. If the **cir-level** parameter is 1 or greater, the **cir-weight** parameter is used.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-e, VSR

scheduler-parent

Syntax **scheduler-parent** *scheduler-name* [**weight** *weight*] [**level** *level*] [**cir-weight** *cir-weight*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[**cir-level** *cir-level*]
no scheduler-parent

Context **[Tree]** (config>qos>sap-ingress>policer scheduler-parent)

Full Context configure qos sap-ingress policer scheduler-parent

Description This command defines an optional parent scheduler that governs the available bandwidth given to a policer in addition to the PIR setting of the policer. When multiple schedulers, queues, or policers share a child status with the parent scheduler, the **weight** or **level** parameters define how this policer contends with the other children for the bandwidth of the parent. This command and the configuration of a SAP policer **scheduler-parent** or **parent** arbiter are mutually exclusive.

Multiple schedulers can exist in different scheduler policies with the same *scheduler-name*; in this command, the associated *scheduler-name* pertains to a scheduler that should exist on the SAP as the policy is applied and the policer is created. When the policer is created on the SAP, the existence of the *scheduler-name* is dependent on a scheduler policy containing the *scheduler-name* being directly applied or indirectly applied (through a multiservice customer site) to the SAP. The policer accepts packets, but is not bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP.

The parent scheduler can be made unavailable by the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the policer enters the orphaned state. The policer automatically returns to normal operation when the parent scheduler is available again.

The **no** form of this command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and no error message is returned. When a parent association has been removed, the former child policer attempts to operate based on its configured rate parameter.

Removing the parent association on the policer within the policy takes effect immediately on all policers using the SAP QoS policy.

Default no scheduler-parent

Parameters *scheduler-name* — Scheduler names are configured in the **config>qos>scheduler-policy>tier** context. There are no checks performed at the time of definition to ensure that the *scheduler-name* exists within an existing scheduler policy. For the policer to use the defined *scheduler-name*, the scheduler must exist on each SAP that the policer is created on. If a *scheduler-name* does not exist on the SAP, the policer operates in an orphaned state.

Values Any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Default None. Each parental association must be explicitly defined.

weight — Defines the relative weight of this policer in comparison with other child policers, queues, and schedulers when competing for bandwidth on the parent *scheduler-name* at the above-CIR priority level defined by the **level** parameter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All weight values from all weighted active policers, queues, and schedulers with a common port parent are added together. Then, each individual active weight is divided by the total to determine the percentage of remaining bandwidth provided to the policer, queue, or scheduler after the higher priority level children have been serviced. A weight is considered to be active when the applicable policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit. All child policers, queues, and schedulers with a weight of 0 are considered to have the lowest priority at the configured level and are not serviced until all non-zero weighted policers, queues, and schedulers at that level are operating at the maximum bandwidth or are idle.

Values 0 to 100

Default 1

level — Defines the level of hierarchy when compared with other policers, queues, and schedulers when competing for bandwidth on the parent *scheduler-name*.

Children of the parent scheduler with a lower priority will not receive bandwidth until all children with a higher priority have either reached their maximum bandwidth or are idle. Children with the same level are serviced in relation to their relative weights.

Values 1 to 8 (8 is the highest priority)

Default 1

cir-weight — Defines the relative weight of this policer in comparison with other child policers, queues, or schedulers competing for bandwidth on the parent *scheduler-name* at the within-CIR priority level defined by the **cir-level** parameter.

All **cir-weight** values from all weighted active policers, queues, and schedulers with a common parent are added together. Then, each individual active weight is divided by the total to determine the percentage of remaining bandwidth provided to the policer, queue, or scheduler after the higher priority level children have been serviced. A weight is considered to be active when the applicable policer, queue, or scheduler has not reached its maximum rate and still has packets to transmit.

The weight is specified as an integer value from 0 to 100, with 100 being the highest weight. When the **cir-weight** parameter is set to a value of 0, the policer receives bandwidth only after the other children with a non-zero weight at this level.

Values 0 to 100

Default 1

cir-level — Defines the level of hierarchy when compared with other policers, queues, and schedulers that the policer uses to receive bandwidth for its within-CIR offered load. If the **cir-level** parameter is set to a value of 0 (the default value), the policer does not receive bandwidth during the schedulers within-CIR pass and the **cir-weight** parameter is ignored. If the **cir-level** parameter is 1 or greater, the **cir-weight** parameter is used.

Values 0 to 8 (8 is the highest priority)

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.44 scheduler-policy

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context [Tree] (config>subscr-mgmt>sla-prof>egress scheduler-policy)

Full Context configure subscriber-mgmt sla-profile egress scheduler-policy

Description This command specifies a scheduler policy to associate to the sla profile. Scheduler policies are configured in the **configure>qos>scheduler>policy** context. Each scheduler policy is divided up into groups of schedulers based on the tier each scheduler is created under. A tier is used to give structure to the schedulers within a policy and define rules for parent scheduler associations. The policy defines the hierarchy and operating parameters for virtual schedulers.

The **no** form of this command removes the scheduler-policy-name from the configuration.

Parameters *scheduler-policy-name* — Specifies an existing scheduler policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context [Tree] (config>subscr-mgmt>sub-profile>egress scheduler-policy)
[Tree] (config>subscr-mgmt>sub-profile>ingress scheduler-policy)

Full Context configure subscriber-mgmt sub-profile egress scheduler-policy
configure subscriber-mgmt sub-profile ingress scheduler-policy

Description This command specifies a scheduler policy to associate to the subscriber profile. Scheduler policies are configured in the **configure>qos>scheduler>policy** context. Each scheduler policy is divided up into groups of schedulers based on the tier each scheduler is created under. A tier is used to give structure to the schedulers within a policy and define rules for parent scheduler associations. The policy defines the hierarchy and operating parameters for virtual schedulers.

The **no** form of this command reverts to the default.

Parameters *scheduler-policy-name* — Specify an existing scheduler policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>egress scheduler-policy)
[Tree] (config>service>ies>sub-if>grp-if>sap>ingress scheduler-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap>egress scheduler-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap>ingress scheduler-policy)
[Tree] (config>service>ies>sap>egress scheduler-policy)
[Tree] (config>service>ies>sap>ingress scheduler-policy)

Full Context configure service ies sap egress scheduler-policy
configure service ies sap ingress scheduler-policy
configure service ies subscriber-interface group-interface sap egress scheduler-policy
configure service ies subscriber-interface group-interface sap ingress scheduler-policy
configure service vprn subscriber-interface group-interface sap egress scheduler-policy
configure service vprn subscriber-interface group-interface sap ingress scheduler-policy

Description This command applies an existing scheduler policy to an ingress or egress scheduler used by ingress SAP queues or egress SAP policers and queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the **config>qos>scheduler-policy** *scheduler-policy-name* context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the SAP policers or queues associated with the customer site. Policers and queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have policers or queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more policers or queues. When the **no** form of this command executed, the customer site ingress or egress node will not contain an applied scheduler policy.

Parameters *scheduler-policy-name:* — Specifies the scheduler policy name to apply to an existing scheduler policy that was created in the **config>qos>scheduler-policy** *scheduler-policy-name* context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress queues or egress policers and queues created on associated SAPs.

Values Any existing valid scheduler policy name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no scheduler-policy

Context [Tree] (config>port>ethernet>access>egress>vport scheduler-policy)
[Tree] (config>port>sonet-sdh>path>access>egress>vport scheduler-policy)

Full Context configure port ethernet access egress vport scheduler-policy
configure port sonet-sdh path access egress vport scheduler-policy

Description This command specifies a scheduler policy to associate to the Vport. Scheduler policies are configured in the **configure>qos>scheduler>policy** context. Each scheduler policy is divided up into groups of schedulers based on the tier each scheduler is created under. A tier is used to give structure to the schedulers within a policy and define rules for parent scheduler associations. The policy defines the hierarchy and operating parameters for virtual schedulers.

The **no** form of this command removes the configured egress scheduler policy from the Vport.

The **agg-rate rate**, **port-scheduler-policy** and **scheduler-policy** commands are mutually exclusive. Changing between the use of a scheduler policy and the use of an agg-rate/ port-scheduler-policy involves removing the existing command and applying the new command.

The configuration of a scheduler policy under a Vport is mutually exclusive with the configuration of the egress-rate-modify parameter.

The **no** form of this command reverts to the default.

Parameters *scheduler-policy-name* — Specifies the *scheduler-policy-name* parameter applies an existing scheduler policy that was created in the **config>qos>scheduler-policy** *scheduler-policy-name* context to create the hierarchy of egress virtual schedulers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path access egress vport scheduler-policy

All

- configure port ethernet access egress vport scheduler-policy

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context [Tree] (config>service>vpls>sap>ingress scheduler-policy)
[Tree] (config>service>vpls>sap>egress scheduler-policy)
[Tree] (config>service>ies>if>sap>egress scheduler-policy)
[Tree] (config>service>ies>if>sap>ingress scheduler-policy)
[Tree] (config>service>vprn>if>sap>egress scheduler-policy)
[Tree] (config>service>vprn>if>sap>ingress scheduler-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies interface sap egress scheduler-policy
configure service ies interface sap ingress scheduler-policy
configure service vpls sap egress scheduler-policy
configure service vpls sap ingress scheduler-policy
configure service vprn interface sap egress scheduler-policy
configure service vprn interface sap ingress scheduler-policy

Description This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the **config>qos>scheduler-policy** *scheduler-policy-name* context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues and egress SAP policers and queues associated with the customer site. Policers and queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have policers or queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more policers or queues. When the **no scheduler-policy** command is executed, the customer site's ingress or egress node will not contain an applied scheduler policy.

Parameters *scheduler-policy-name* — Specifies that the *scheduler-policy-name* is applied to an existing scheduler policy that was created in the **config>qos>scheduler-policy** *scheduler-policy-name* context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

Values Any existing valid scheduler policy name.

Platforms All

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>egress scheduler-policy)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress scheduler-policy

Description This command configures the identifier of the egress scheduler policy associated with each wlan-gw tunnel of this interface.

The **no** form of this command removes the scheduler policy name from the configuration.

Parameters *scheduler-policy-name* — Specifies the identifier of the egress scheduler policy associated with each wlan-gw tunnel of this interface.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context **[Tree]** (config>port>ethernet>egress>queue-group scheduler-policy)
[Tree] (config>port>ethernet>ingress>queue-group scheduler-policy)
[Tree] (config>port>ethernet>network>egress>queue-group scheduler-policy)

Full Context configure port ethernet egress queue-group scheduler-policy
configure port ethernet ingress queue-group scheduler-policy
configure port ethernet network egress queue-group scheduler-policy

Description This command configures a scheduler policy for the egress queue group.

Parameters *scheduler-policy-name* — Specifies the scheduler policy name, up to 32 characters.

Platforms All

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context **[Tree]** (config>service>apipe>sap>ingress scheduler-policy)
[Tree] (config>service>apipe>sap>egress scheduler-policy)
[Tree] (config>service>cpipe>sap>ingress scheduler-policy)
[Tree] (config>service>cpipe>sap>egress scheduler-policy)
[Tree] (config>service>epipe>sap>ingress scheduler-policy)
[Tree] (config>service>epipe>sap>egress scheduler-policy)
[Tree] (config>service>fpipe>sap>ingress scheduler-policy)
[Tree] (config>service>fpipe>sap>egress scheduler-policy)
[Tree] (config>service>ipipe>sap>ingress scheduler-policy)
[Tree] (config>service>ipipe>sap>egress scheduler-policy)

Full Context configure service apipe sap egress scheduler-policy
configure service apipe sap ingress scheduler-policy
configure service cpipe sap egress scheduler-policy
configure service cpipe sap ingress scheduler-policy
configure service epipe sap egress scheduler-policy
configure service epipe sap ingress scheduler-policy
configure service fpipe sap egress scheduler-policy
configure service fpipe sap ingress scheduler-policy
configure service ipipe sap egress scheduler-policy
configure service ipipe sap ingress scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created when the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the **config>qos>scheduler-policy** *scheduler-policy-name* context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues associated with the customer site. Policers or queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have policers or queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more policers or queues. When the **no scheduler-policy** command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

Parameters *scheduler-policy-name* — The *scheduler-policy-name* parameter applies an existing scheduler policy that was created in the **config>qos>scheduler-policy** *scheduler-policy-name* context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues and to egress policers managed by HQoS created on associated SAPs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe sap egress scheduler-policy
- configure service fpipe sap ingress scheduler-policy
- configure service cpipe sap egress scheduler-policy
- configure service cpipe sap ingress scheduler-policy

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap egress scheduler-policy
- configure service apipe sap ingress scheduler-policy

All

- configure service ipipe sap ingress scheduler-policy
- configure service epipe sap ingress scheduler-policy
- configure service epipe sap egress scheduler-policy
- configure service ipipe sap egress scheduler-policy

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>service>vpls>sap>egress>encap-defined-qos>encap-group scheduler-policy)

Full Context configure service vpls sap egress encap-defined-qos encap-group scheduler-policy

Description This command configures the scheduler policy.

Platforms All

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name* [**create**]
no scheduler-policy *scheduler-policy-name*

Context **[Tree]** (config>qos scheduler-policy)

Full Context configure qos scheduler-policy

Description Each scheduler policy is divided up into groups of schedulers based on the tier each scheduler is created under. A tier is used to give structure to the schedulers within a policy and define rules for parent scheduler associations.

The **scheduler-policy** command creates a scheduler policy or allows editing of an existing policy. The policy defines the hierarchy and operating parameters for virtual schedulers. Creating a policy does not create the schedulers; it only provides a template for the schedulers to be created when the policy is associated with a SAP or multiservice site.

Each scheduler policy must have a unique name within the context of the system. Modifications made to an existing policy are executed on all schedulers that use the policy. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce SLAs.

If a *scheduler-policy-name* does not exist, it is assumed that an attempt is being made to create a new policy. The success of the command execution is dependent on the following:

1. The maximum number of scheduler policies has not been configured.
2. The provided scheduler-policy-name is valid.
3. The **create** keyword is entered with the command if the system is configured to require it (enabled in the **environment create** command).

When the maximum number of scheduler policies has been exceeded, a configuration error occurs, the command will not execute, and the CLI context will not change.

If the provided scheduler-policy-name is invalid according to the criteria below, a name syntax error occurs, the command will not execute, and the CLI context will not change.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *scheduler-policy-name* — The name of the scheduler policy.

Values Valid names consist of any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Platforms All

scheduler-policy

Syntax **scheduler-policy** *scheduler-policy-name*
no scheduler-policy

Context **[Tree]** (config>service>cust>multi-service-site>ingress scheduler-policy)
[Tree] (config>service>cust>multi-service-site>egress scheduler-policy)

Full Context configure service customer multi-service-site egress scheduler-policy
configure service customer multi-service-site ingress scheduler-policy

Description This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues or, at egress only, policers associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the **config>qos>scheduler-policy** *scheduler-policy-name* context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the SAP policers and queues associated with the customer site. Policers and queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler.

The SAPs that have ingress queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more policers and queues. When the **no scheduler-policy** command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

Parameters *scheduler-policy-name* — Applies an existing scheduler policy that was created in the **config>qos>scheduler-policy** *scheduler-policy-name* context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues and egress policers managed by HQoS created on associated SAPs.

Values Any existing valid scheduler policy name up to 32 characters in length.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scheduler-policy

Syntax **scheduler-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy scheduler-policy)

Full Context configure qos copy scheduler-policy

Description This command copies existing QoS policy entries for a QoS policy to another QoS policy.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

If **overwrite** is not specified, an error will occur if the destination policy exists.

Parameters *src-name dst-name* — Indicates that the source policy and the destination policy are scheduler policy. Specify the source policy that the copy command will attempt to copy from and specify the destination policy to which the command will copy a duplicate of the policy.

overwrite — Forces the destination policy name to be copied as specified. When forced, everything in the existing destination policy will be completely overwritten with the contents of the source policy.

Platforms All

23.45 scheduling-class

scheduling-class

Syntax **scheduling-class** *class* **rate** *rate*
scheduling-class *class* **weight** *weight-in-group*
no scheduling-class *class*

Context **[Tree]** (config>port>ethernet>egress>hs-sched-ovr scheduling-class)

Full Context configure port ethernet egress hs-scheduler-overrides scheduling-class

Description This command overrides the scheduling class configuration in the HS scheduler policy applied to the port egress. The scheduling class rate or weight within the WRR group can be overridden.

The **no** form of this command removes the scheduling class override parameters from the port egress configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *class* — Specifies the scheduling class.

Values 1 to 6

rate — Specifies the explicit maximum frame based bandwidth limit, in megabits per second, for this HS scheduler policy scheduling class. The **rate** keyword must be followed by either the keyword **max** or a rate specified in megabits per second.

Values 1 to 100000, max

The **max** keyword specifies that a limit is not enforced for the specified class. The **max** keyword is mutually exclusive to the rate value and when specified, must directly follow the **rate** keyword. Setting the rate of the class will fail when the class is currently a member of a group.

weight-in-group — Specifies the weight the HS scheduler policy should apply to this scheduling class within the group in which it belongs. The *weight-in-group* parameter must follow the **weight** keyword and is used to specify the relative weight of class to the other scheduling classes within the group. Setting the weight will fail if the scheduling class is not currently configured in a group.

Values 1 to 127

Platforms 7750 SR-7/12/12e

scheduling-class

Syntax **scheduling-class** *class-id*

Context **[Tree]** (config>service>apipe>sap>frame-relay scheduling-class)
[Tree] (config>service>epipe>sap>frame-relay scheduling-class)
[Tree] (config>service>fpipe>sap>frame-relay scheduling-class)
[Tree] (config>service>ipipe>sap>frame-relay scheduling-class)

Full Context configure service apipe sap frame-relay scheduling-class
configure service epipe sap frame-relay scheduling-class
configure service fpipe sap frame-relay scheduling-class
configure service ipipe sap frame-relay scheduling-class

Description This command specifies the scheduling class to use for this SAP.

Parameters *class-id* — Specifies the scheduling class to use for this SAP.

Values 0 to 3

Default 0

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ipipe sap frame-relay scheduling-class
- configure service epipe sap frame-relay scheduling-class
- configure service fpipe sap frame-relay scheduling-class

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe sap frame-relay scheduling-class

scheduling-class

Syntax **scheduling-class** *class-id*
no scheduling-class

Context **[Tree]** (config>service>vpls>sap>frame-relay scheduling-class)

Full Context configure service vpls sap frame-relay scheduling-class

Description This command specifies the scheduling class to use for this SAP. This object is only applicable for a SAP whose bundle type is set to MLFR.

Parameters *class-id* — Specifies the scheduling class

Values 0 to 3

Platforms All

scheduling-class

Syntax **scheduling-class** *class-id*
no scheduling-class

Context **[Tree]** (config>service>ies>if>sap>frame-relay scheduling-class)
[Tree] (config>service>vprn>if>sap>frame-relay scheduling-class)

Full Context configure service ies interface sap frame-relay scheduling-class
configure service vprn interface sap frame-relay scheduling-class

Description This command assigns a Frame Relay scheduling class for a Frame Relay SAP. The scheduling class dictates which queue the frame or frame fragments are stored in FRF.12 end-to-end fragmentation, FRF.12 UNI/NNI link fragmentation and MLFR applications.

Default scheduling-class 3

Parameters *class-id* — Specifies the Frame Relay scheduling class number.

Values 0 to 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

scheduling-class

Syntax **scheduling-class** *class-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no scheduling-class

Context [Tree] (config>service>vprn>if>sap scheduling-class)

Full Context configure service vprn interface sap scheduling-class

Description This command specifies the scheduling class to use for this SAP.

Parameters *class-id* — Specifies the scheduling class to use for this SAP.

Values 0 to 3

Default 0

scheduling-class

Syntax **scheduling-class** *class-id* **group** *group-id* [**weight** *weight-in-group*]
scheduling-class *class-id* **rate** *rate*
no scheduling-class *class-id*

Context [Tree] (config>qos>hs-scheduler-policy scheduling-class)

Full Context configure qos hs-scheduler-policy scheduling-class

Description This command configures the behavior of a specific scheduling class on all HSQ schedulers associated with the policy. The **scheduler-class** command performs one of two operations: it configures a maximum rate for the scheduling class or places the scheduling class into the weighted scheduling group. The two operations are mutually exclusive.

By default, none of the scheduling classes are members of the weighted scheduling group and each class is set to a rate limit of **max** (no rate limit applied).

Specifying Scheduling Class Rate (or Removing the Scheduling Class from Group) — If the **scheduling-class** command is executed with the **rate** keyword specified, either **max** or a specified rate value must follow. If a *class-id was* previously mapped into the weighted scheduling group, the class is removed from the group. However, if removing the class from the group causes the group to no longer have contiguous class members, the command fails with no effect on the specified class. A “non-contiguous grouping error” is returned. The lowest or highest members within a weighted group must be removed prior to removing the middle members. For example, if scheduling classes 3, 4, and 5 were members of weighted group 1, class 4 cannot be removed first.

This command using the **rate** keyword also fails when an override for the group weight is in place on the scheduling class within a scheduler associated with the policy. The override expects the class to be associated with a weighted scheduling group and the policy rate definition is attempting to remove the class from the group. An “override mismatch” error is generated, specifying the scheduling object where the override exists.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

After a rate has been successfully defined for a scheduling class, the specified rate is automatically updated on all HSQ scheduler instances associated with the scheduling policy. The exception is where the scheduler instance has a local override for the rate on the scheduling class.

Specifying Scheduling Class Weighted Group Membership — If the **scheduling-class** command is executed with the **group** keyword specified, the group ID value of 1 must follow. The corresponding optional **weight** keyword is used to specify the weight of the scheduling class within the group. If weight is not specified, the default weight of 1 is used. If the specified scheduling class is not contiguous with the other scheduling classes in the group, the command fails with no change to the current state of the scheduling class and a "non-contiguous grouping" error is returned, specifying the weighted scheduling group and the current group members.

The **scheduling-class** command fails using the **group** keyword when a rate override for the scheduling class exists on an HSQ scheduler instance associated with the policy. The rate override for the scheduling class indicates the class is directly attached to a strict priority level, conflicting with the policy **group** keyword trying to place the class in the specified group. The command fails without affecting the scheduling class definition on the policy and returns an error specifying the scheduling object where the override exists.

Other Override Constraints — The scheduling overrides cannot change or remove a scheduling class from a policy-defined weighted group membership.

The **no** form of the command returns the scheduling class represented by *class-id* to the default behavior. The default behavior for a scheduling class is to not be a member of the weighted scheduling class group and have a rate set to **max**. The **no scheduling-class** command fails if the scheduling class is currently a member of the weighted scheduling class group and a weight override is in effect on a scheduling object for the class, in which case an error is returned.

Parameters *class-id* — Specifies the scheduling class for HS scheduler policy. The *class-id* value is a required parameter that specifies which scheduling class the scheduling-class command is acting upon.

Values 1 to 6

group-id — Specifies the group this HS scheduler policy scheduling class belongs to. The **group** and the **rate** keywords are mutually exclusive when executing this command. A group ID value of 1 must follow the **group** keyword. The **group** keyword removes the class ID from its inherent strict scheduling level and places it into the specified group ID. The associated **weight** parameter is optional and is used to specify the weight of a class ID within the weighted scheduling class group. Specifying the **group** parameter while an override for the scheduling class exists for rate causes the **scheduling-class** command to fail.

Values 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

weight-in-group — Specifies the weight the HS scheduler policy should apply to this scheduling class within the group in which it belongs. This keyword is optional and must follow the **group** parameter when specified. The *weight-in-group* parameter must follow the **weight** keyword and is used to specify the relative weight of the *class-id* to the other scheduling classes within the group. If the group is specified without the **weight** parameter, a default weight of 1 is used.

Values 1 to 127

rate — Specifies the explicit maximum frame-based bandwidth limit, in megabits per second, for this HS scheduler policy scheduling class. The **rate** and **group** keywords are mutually exclusive. Either the **rate** or **group** keyword must be specified when executing this command. When specified, the **rate** keyword must be followed by either the keyword **max** or a rate specified in megabits per second. The specified rate can be overridden at the port Ethernet egress using the scheduler override functions. A newly-created HS scheduler policy defaults each scheduling class to have its rate set to **max** and the weighted scheduling class group has no members.

Values 1 to 100000, max

The **max** keyword specifies that a limit is not enforced for the specified class ID and that the class ID is not a member of a weighted scheduling class group. The **max** keyword and the *rate* value are mutually exclusive; when **max** is specified, it must directly follow the **rate** keyword. Setting the rate of the class fails when the class currently has a group weight override defined on a scheduling object.

Platforms 7750 SR-7/12/12e

23.46 schema-path

schema-path

Syntax **schema-path** *url-string*
no schema-path

Context **[Tree]** (config>system>management-interface schema-path)

Full Context configure system management-interface schema-path

Description This command defines a schema path where the SR OS YANG modules can be manually copied by the user prior to using a <get-schema> request.

By default, no schema path is configured, and the software upgrade process manages the YANG schema files to ensure they are synchronized with the software image on both the primary and standby CPM.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no schema-path

Parameters *url-string* — Specifies the schema path URL up to 180 characters. However, Nokia recommends that the string shall not exceed 135 characters to ensure that the <get-schema> request works properly with *all* schema files.

Platforms All

23.47 scope

scope

Syntax **scope** {**exclusive** | **template**}
no scope

Context **[Tree]** (config>service>mrp>mrp-policy scope)

Full Context configure service mrp mrp-policy scope

Description This command configures the filter policy scope as exclusive or template. If the scope of the policy is template and is applied to one or more services, the scope cannot be changed.

The **no** form of this command sets the scope of the policy to the default of template.

Default scope template

Parameters **exclusive** — When the scope of a policy is defined as exclusive, the policy can only be applied to a single entity (SAP or SDP). Attempting to assign the policy to a second entity will result in an error message. If the policy is removed from the entity, it will become available for assignment to another entity.

template — When the scope of a policy is defined as template, the policy can be applied to multiple SAPs or network ports.

Platforms All

scope

Syntax **scope** {**exclusive** | **template**}
no scope

Context **[Tree]** (config>qos>sap-ingress scope)

Full Context configure qos sap-ingress scope

Description This command configures the Service Ingress QoS policy scope as exclusive or template.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The policy's scope cannot be changed if the policy is applied to a service.

The **no** form of this command sets the scope of the policy to the default of **template**.

Default scope template

Parameters **exclusive** — When the scope of a policy is defined as exclusive, the policy can only be applied to one SAP. If a policy with an exclusive scope is assigned to a second SAP, an error message is generated. If the policy is removed from the exclusive SAP, it will become available for assignment to another exclusive SAP.

The system default policies cannot be put into the exclusive scope. An error will be generated if scope exclusive is executed in any policies with a policy-id equal to 1.

template — When the scope of a policy is defined as template, the policy can be applied to multiple SAPs on the router.

Default QoS policies are configured with template scopes. An error is generated when the template scope parameter to exclusive scope on default policies is modified.

Platforms All

scope

Syntax **scope** {**exclusive** | **template**}
no scope

Context **[Tree]** (config>qos>sap-egress scope)

Full Context configure qos sap-egress scope

Description Enter the scope of this policy. The scope of the policy cannot be changed if the policy is applied to one or more services.

The no form of this command sets the scope of the policy to the default of template.

Default scope template

Parameters **exclusive** — When the scope of a policy is defined as exclusive, the policy can only be applied to a single SAP. Attempting to assign the policy to a second SAP will result in an error message. If the policy is removed from the exclusive SAP, it will become available for assignment to another exclusive SAP.

The system default policies cannot be put into the exclusive scope. An error will be generated if scope exclusive is executed in any policies with a policy-id equal to 1.

template — When the scope of a policy is defined as template, the policy can be applied to multiple SAPs on the router.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scope

Syntax **scope** {**exclusive** | **template**}
no scope

Context **[Tree]** (config>qos>network scope)

Full Context configure qos network scope

Description This command configures the network policy scope as exclusive or template. The policy's scope cannot be changed if the policy is applied to an interface.

The **no** form of this command sets the scope of the policy to the default of **template**.

Default scope template

Parameters **exclusive** — When the scope of a policy is defined as exclusive, the policy can only be applied to one interface. If a policy with an exclusive scope is assigned to a second interface, an error message is generated. If the policy is removed from the exclusive interface, it will become available for assignment to another exclusive interface.

The system default policies cannot be put into the exclusive scope. An error will be generated if the **scope exclusive** command is executed in any policies with a policy-id equal to 1.

template — When the scope of a policy is defined as template, the policy can be applied to multiple interfaces on the router.

Default QoS policies are configured with template scopes. An error is generated if the template scope parameter is modified to exclusive scope on default policies.

Platforms All

scope

Syntax **scope** {**exclusive** | **template** | **embedded** | **system**}
scope {**exclusive** | **template**}
no scope

Context **[Tree]** (config>filter>ip-exception scope)
[Tree] (config>filter>ip-filter scope)
[Tree] (config>filter>ipv6-filter scope)
[Tree] (config>filter>mac-filter scope)

Full Context configure filter ip-exception scope
configure filter ip-filter scope
configure filter ipv6-filter scope
configure filter mac-filter scope

Description This command configures the filter policy scope as exclusive, template, embedded or system.

The scope of the policy cannot be changed when:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- the scope is **template** and the policy is applied to one or more services or network interfaces
- the scope is **embedded** and the policy is embedded by another policy

Changing the scope to/from system is only allowed when a policy is not active and the policy has no entries configured.

The **no** form of the command sets the scope of the policy to the default of **template**.

Default scope template

Parameters **exclusive** — Specifies that the policy can only be applied to a single entity. Attempting to assign the policy to a second entity will result in an error message.

template — Specifies that the policy can be applied to multiple entities.

embedded — Specifies that the policy cannot be applied directly. The policy defines embedded filter rules, which are embedded by other exclusive/template/system filter policies. The **embedded** scope is supported for IPv4 and IPv6 filter policies only.

system — Specifies that the policy defines system-wide filter rules. To apply system policy rules, activate system filter and chain exclusive/template ACL filter policy to the system filter. The **system** scope is supported for IPv4 and IPv6 filter policies only.

Platforms All

- configure filter ip-filter scope
- configure filter ipv6-filter scope
- configure filter mac-filter scope

VSR

- configure filter ip-exception scope

23.48 scp

scp

Syntax **scp** *local-file-url destination-file-url* [**router** *router-instance*] [**force**]
scp *local-file-url destination-file-url* [**force**] **service** *service-name*

Context **[Tree]** (file scp)

Full Context file scp

Description This command copies a local file to a remote host file system. It uses `ssh` for data transfer, and uses the same authentication and provides the same security as `ssh`. The following prompt appears:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

"Are you sure (y/n)?" The destination must specify a user and a host.

Parameters *local-file-url* — Specifies the local source file or directory.

Values

[*cflash-id/*] *file-path*	up to 200 characters
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

destination-file-url — Specifies the destination file.

Values

*destination-file-**: *user@hostname*:*file-path* - up to 255 characters	
user	up to 32 characters
hostname	[*dns-name* | *ipv4-address* | "["*ipv6-address*"]"]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
	x:x:x:x:x:x:d.d.d.d[-*interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface - up to 32 characters, mandatory for link local addresses
dns-name	up to 128 characters
file-path	up to 200 characters, directory length up to 99 characters

user — Specifies the SSH user.

hostname — Specifies the remote host IP address of DNS name.

file-path — Specifies the destination path.

router-instance — Specifies the router name or service ID used to specify the router instance.

Values

router-name	"Base", "management", "vpls-management"
vprn-service-id	1 to 2147483647

Default Base

force — Forces an immediate copy of the specified file. The command **file scp** *local-file-url destination-file-url* [**router** *router-instance*] **force** executes the command without displaying a user prompt message.

service-name — Specifies the service name used to identify the router instance. The service name can be a maximum of 64 characters long.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.49 scramble

scramble

Syntax [**no**] **scramble**

Context **[Tree]** (config>port>tdm>ds1>channel-group scramble)
[Tree] (config>port>tdm>ds3 scramble)
[Tree] (config>port>tdm>e1>channel-group scramble)
[Tree] (config>port>tdm>e3 scramble)

Full Context configure port tdm ds1 channel-group scramble
configure port tdm ds3 scramble
configure port tdm e1 channel-group scramble
configure port tdm e3 scramble

Description This command enables payload scrambling on channel groups.

Scrambling randomizes the pattern of 1s and 0s carried in a SONET frame. Rearranging or scrambling the pattern prevents continuous strings of all 1s or all 0s and meets the needs of physical layer protocols that rely on sufficient transitions between 1s and 0s to maintain clocking.

For ATM, this command enables or disables ATM cell-level payload scrambling/descrambling using x43+1 polynomial as defined in ITU-T I.432.1. Scrambling is enabled by default for the ATM path/channel. Note that this scrambling is done in addition to SONET/SDH frame scrambling/descrambling, which is always enabled in the framer.

The **no** form of this command disables scrambling.

Default no scramble

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

scramble

Syntax [**no**] **scramble**

Context **[Tree]** (config>port>sonet-sdh>path scramble)

Full Context configure port sonet-sdh path scramble

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables SONET/SDH payload scrambling. Scrambling randomizes the pattern of 1s and 0s carried in a SONET frame. Rearranging or scrambling the pattern prevents continuous strings of all 1s or all 0s and meets the needs of physical layer protocols that rely on sufficient transitions between 1s and 0s to maintain clocking.

For ATM, this command enables or disables ATM cell-level payload scrambling/descrambling using x43+1 polynomial as defined in ITU-T I.432.1. Scrambling is enabled by default for the ATM path/channel. Note that this scrambling is done in addition to SONET/SDH frame scrambling/descrambling, which is always enabled in the framer.

The **no** form of this command disables scrambling.

Default no scramble

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.50 script

script

Syntax **script** *script*

Context **[Tree]** (debug>dynsvc>scripts script)

Full Context debug dynamic-services scripts script

Description Commands in this context configure dynamic services script debugging for a specific script.

Parameters *script* — Specifies the script name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

script

Syntax **script** *script-name* [**owner** *script-owner*]
no script

Context **[Tree]** (config>system>script-control>script-policy script)
[Tree] (config>system>script-control script)

Full Context configure system script-control script
configure system script-control script-policy script

Description This command is used to configure a script to be run.

The **no** form of the command removes the script.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no script

Parameters *script-name* — Specifies the name of the script. Can be up to 32 characters.

script-owner — Specifies the name of the script owner. Can be up to 32 characters.

The owner is an arbitrary name and not necessarily a user name. Commands in the scripts are not authorized against the owner. The **configure system security cli-script authorization** *x* **cli-user** command determines the user context against which commands in the scripts are authorized.

Default "TiMOS CLI"

Platforms All

23.51 script-all-info

script-all-info

Syntax **script-all-info**

Context **[Tree]** (debug>python>py-script script-all-info)

Full Context debug python python-script script-all-info

Description This command enables the script-compile-error, script-export-variables, script-output, script-output-on-error, and script-runtime-error functionalities.

Platforms All

script-all-info

Syntax **script-all-info**

Context **[Tree]** (debug>subscr-mgmt>sub-ident-plcy script-all-info)

Full Context debug subscriber-mgmt sub-ident-policy script-all-info

Description This command enables the script-compile-error, script-export-variables, script-output, script-output-on-error, and script-runtime-error functionalities.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.52 script-compile-error

script-compile-error

Syntax [**no**] **script-compile-error**

Context **[Tree]** (debug>python>py-script script-compile-error)

Full Context debug python python-script script-compile-error

Description This command sends the traceback of the compile error to the logger. The traceback contains detailed information about where and why the compilation fails. The compilation takes place when the CLI user changes the admin state of the Python script from **shutdown** to **no shutdown**.

Platforms All

script-compile-error

Syntax [**no**] **script-compile-error**

Context **[Tree]** (debug>subscr-mgmt>sub-ident-plcy script-compile-error)

Full Context debug subscriber-mgmt sub-ident-policy script-compile-error

Description This command send the traceback of the compile error to the logger. The traceback contains detailed information about where and why the compilation fails. The compilation takes place when the CLI user changes the admin state of the Python URL from shutdown to no-shutdown.

The **no** form of this command disables debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.53 script-control

script-control

Syntax **script-control**

Context **[Tree]** (config>system script-control)

Full Context configure system script-control

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure command script parameters.

Platforms All

23.54 script-export-variables

script-export-variables

Syntax [**no**] **script-export-variables**

Context **[Tree]** (debug>python>py-script script-export-variables)

Full Context debug python python-script script-export-variables

Description This command sends the output variables of the Python script to the logger when the script ran successfully.

Platforms All

script-export-variables

Syntax [**no**] **script-export-variables**

Context **[Tree]** (debug>subscr-mgmt>sub-ident-plcy script-export-variables)

Full Context debug subscriber-mgmt sub-ident-policy script-export-variables

Description This command sends the result (the three output variables) of the Python script to the logger when the script ran successfully.

The **no** form of this command disables debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.55 script-output

script-output

Syntax [**no**] **script-output**

Context **[Tree]** (debug>python>py-script script-output)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug python python-script script-output

Description This command sends the output (such as from **print** statements) of the Python script to the logger.

Platforms All

script-output

Syntax [**no**] **script-output**

Context **[Tree]** (debug>subscr-mgmt>sub-ident-plcy script-output)

Full Context debug subscriber-mgmt sub-ident-policy script-output

Description This command sends the output (such as from 'print' statements) of the Python script to the logger.

The **no** form of this command disables debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.56 script-output-on-error

script-output-on-error

Syntax [**no**] **script-output-on-error**

Context **[Tree]** (debug>python>py-script script-output-on-error)

Full Context debug python python-script script-output-on-error

Description This command sends the output (such as traceback data) of the Python script to the logger, only when the script fails.

Platforms All

script-output-on-error

Syntax [**no**] **script-output-on-error**

Context **[Tree]** (debug>subscr-mgmt>sub-ident-plcy script-output-on-error)

Full Context debug subscriber-mgmt sub-ident-policy script-output-on-error

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sends the output (such as from print statements) of the Python script to the logger, but only when the script fails.

The **no** form of this command disables debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.57 script-parameters-1

script-parameters-1

Syntax **script-parameters-1** *param-string1*
no script-parameters-1

Context **[Tree]** (config>service>dynsvc>ladb>user>idx script-parameters-1)

Full Context configure service dynamic-services local-auth-db user-name index script-parameters-1

Description This command specifies the first part of parameters as input to the dynamic data service Python script. The concatenation of all four script-parameters strings are passed to the Python script and must be formatted as function-key <dictionary>. The function-key specifies which Python functions is called, and <dictionary> contains the actual parameters in a Python dictionary structure format. The **no** form of this command removes **script-parameters-1** from the configuration.

Parameters *param-string1* — Specifies a string representing parameters that are used as input for the dynamic service Python script, up to 250 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.58 script-parameters-2

script-parameters-2

Syntax **script-parameters-2** *param-string2*
no script-parameters-2

Context **[Tree]** (config>service>dynsvc>ladb>user>idx script-parameters-2)

Full Context configure service dynamic-services local-auth-db user-name index script-parameters-2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the second part of parameters as input to the dynamic data service Python script. The concatenation of all four script-parameters strings are passed to the Python script and must be formatted as function-key <dictionary>. The function-key specifies which Python functions is called, and <dictionary> contains the actual parameters in a Python dictionary structure format. The **no** form of this command removes the **script-parameters-2** from the configuration.

Parameters *param-string2* — Specifies a string representing parameters that are used as input for the dynamic service Python script, up to 250 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.59 script-parameters-3

script-parameters-3

Syntax **script-parameters-3** *param-string3*
no script-parameters-3

Context **[Tree]** (config>service>dynsvc>ladb>user>idx script-parameters-3)

Full Context configure service dynamic-services local-auth-db user-name index script-parameters-3

Description This command specifies the third part of parameters as input to the dynamic data service Python script. The concatenation of all four script-parameters strings are passed to the Python script and must be formatted as function-key <dictionary>. The function-key specifies which Python functions is called, and <dictionary> contains the actual parameters in a Python dictionary structure format. The **no** form of this command removes the **script-parameters-3** from the configuration.

Parameters *param-string3* — Specifies string representing parameters that are used as input for the dynamic service Python script, up to 250 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.60 script-parameters-4

script-parameters-4

Syntax **script-parameters-4** *param-string4*
no script-parameters-4

Context **[Tree]** (config>service>dynsvc>ladb>user>idx script-parameters-4)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service dynamic-services local-auth-db user-name index script-parameters-4

Description This command specifies the fourth part of parameters as input to the dynamic data service Python script. The concatenation of all four script-parameters strings are passed to the Python script and must be formatted as function-key <dictionary>. The function-key specifies which Python functions is called, and <dictionary> contains the actual parameters in a Python dictionary structure format. The **no** form of this command removes the **script-parameters-4** from the configuration.

Parameters *param-string4* — Specifies a string representing parameters that are used as input for the dynamic service Python script, up to 250 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.61 script-policy

script-policy

Syntax **script-policy** *name*
no script-policy

Context **[Tree]** (config>service>dynsvc>policy script-policy)

Full Context configure service dynamic-services dynamic-services-policy script-policy

Description This command specifies the radius script policy to be used to setup the dynamic data services. The script-policy configuration cannot be changed when there are active dynamic data services referencing the policy.

The **no** form of this command removes the script-policy from the configuration. This is only allowed when there are no active dynamic data services referencing this policy.

Parameters *name* — Specifies the RADIUS script policy name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

script-policy

Syntax **script-policy** *policy-name* [**owner** *policy-owner*]
no script-policy

Context **[Tree]** (config>system>cron>schedule script-policy)

Full Context configure system cron schedule script-policy

Description This command is used to configure the CLI script policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *policy-name* — Specifies the name of the policy. Can be up to 32 characters.

policy-owner — Specifies the name of the policy owner. Can be up to 32 characters.

The owner is an arbitrary name and not necessarily a user name. Commands in the scripts are not authorized against the owner. The **configure system security cli-script authorization** *x* **cli-user** command determines the user context against which commands in the scripts are authorized.

Default "TiMOS CLI"

Platforms All

script-policy

Syntax [**no**] **script-policy** *policy-name* [**owner** *policy-owner*]

Context **[Tree]** (config>system>script-control script-policy)

Full Context configure system script-control script-policy

Description This command is used to configure the CLI script policy.

Parameters *policy-name* — Specifies the name of the policy, up to 32 characters.

policy-owner — Specifies the name of the policy owner, up to 32 characters.

The owner is an arbitrary name and not necessarily a user name. Commands in the scripts are not authorized against the owner. The **configure system security cli-script authorization** *x* **cli-user** command determines the user context against which commands in the scripts are authorized.

Default "TiMOS CLI"

Platforms All

script-policy

Syntax **script-policy** *policy-name* [**owner** *policy-owner*]
no script-policy

Context **[Tree]** (config>log>event-handling>handler>action-list>entry script-policy)

Full Context configure log event-handling handler action-list entry script-policy

Description This command configures the script policy parameters to use for this EHS handler action-list entry. The associated script is launched when the handler is triggered.

Default no script-policy

Parameters *policy-name* — Specifies the script policy name. Can be up to 32 characters maximum.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

owner *policy-owner* — Specifies the script policy owner. Can be up to 32 characters maximum.

Default "TiMOS CLI"

Platforms All

23.62 script-runtime-error

script-runtime-error

Syntax [**no**] **script-runtime-error**

Context **[Tree]** (debug>python>py-script script-runtime-error)

Full Context debug python python-script script-runtime-error

Description This command generates log information when detecting a script runtime error.

Platforms All

script-runtime-error

Syntax [**no**] **script-runtime-error**

Context **[Tree]** (debug>subscr-mgmt>sub-ident-plcy script-runtime-error)

Full Context debug subscriber-mgmt sub-ident-policy script-runtime-error

Description This command sends the traceback of the Python script failure to the logger.

The **no** form of this command disables debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.63 script-url

script-url

Syntax **script-url** *primary-script-url*
no script-url

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>aaa>radius-scr-plcy>primary script-url)

Full Context configure aaa radius-script-policy primary script-url

Description This command configures the URL of the primary script.

The **no** form of this command removes the URL from the configuration.

Parameters *primary-script-url* — Specifies the URL of the secondary script to change RADIUS attributes of the RADIUS message.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

script-url

Syntax **script-url** *secondary-script-url*
no script-url

Context [Tree] (config>aaa>radius-scr-plcy>secondary script-url)

Full Context configure aaa radius-script-policy secondary script-url

Description Specifies the URL of the secondary script to change RADIUS attributes of the RADIUS message.

The **no** form of this command removes the URL from the configuration.

Parameters *secondary-script-url* — Specifies the URL of the secondary script to change RADIUS attributes of the RADIUS message.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

script-url

Syntax **script-url** *dhcp-script-url*
no script-url

Context [Tree] (config>subscr-mgmt>sub-ident-pol>primary script-url)
[Tree] (config>subscr-mgmt>sub-ident-pol>secondary script-url)
[Tree] (config>subscr-mgmt>sub-ident-pol>tertiary script-url)

Full Context configure subscriber-mgmt sub-ident-policy primary script-url
configure subscriber-mgmt sub-ident-policy secondary script-url
configure subscriber-mgmt sub-ident-policy tertiary script-url

Description This command specifies the URL of the identification scripts.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *dhcp-primary-script-url* — Specifies the URL of the primary identification script up to 180 characters.

dhcp-secondary-script-url — Specifies the URL of the secondary identification script up to 180 characters.

dhcp-tertiary-script-url — Specifies the URL of the tertiary identification script up to 180 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

script-url

Syntax **script-url** *script-url-name*
no script-url

Context **[Tree]** (config>app-assure>group>http-notif script-url)

Full Context configure application-assurance group http-notification script-url

Description This command configures the URL of the script used by the http notification policy.

The **no** form of this command removes the script URL from the http-notification policy.

Default no script-url

Parameters *script-url-name* — Specifies the string representing the URL of the script used in the http notification policy, up to 255 characters.

create — Keyword to create the script URL.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.64 scripts

scripts

Syntax **scripts**

Context **[Tree]** (debug>dynsvc scripts)

Full Context debug dynamic-services scripts

Description Commands in this context configure dynamic services script debugging.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

scripts

Syntax **scripts**
scripts event [**cli**] [**errors**] [**executed-cmd**] [**state-change**] [**warnings**]
scripts instance *instance* **event** [**cli**] [**errors**] [**executed-cmd**] [**state-change**] [**warnings**]

Context **[Tree]** (debug>vsd scripts)

Full Context debug vsd scripts

Description This command enables the debug of the VSD fully dynamic integration scripts.

Platforms All

23.65 scte30

scte30

Syntax **scte30**

Context **[Tree]** (config>service>ies>video-interface>adi scte30)
[Tree] (config>service>vprn>video-interface>adi scte30)

Full Context configure service ies video-interface adi scte30
configure service vprn video-interface adi scte30

Description Commands in this context configure SCTE 30 parameters.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

23.66 scte35-action

scte35-action

Syntax **scte35-action** {**forward** | **drop**}

Context **[Tree]** (config>service>ies>video-interface>channel scte35-action)
[Tree] (config>service>vprn>video-interface>channel scte35-action)

Full Context configure service ies video-interface channel scte35-action
configure service vprn video-interface channel scte35-action

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies whether the Society of Cable Telecommunications Engineers 35 (SCTE 35) cue avails in the stream need to be forwarded or not. When specified to forward, SCTE 35 messages will be forwarded downstream. When specified to drop, SCTE 35 messages will not be forwarded downstream. They will be still be processed for local splicing decisions.

Parameters **forward** — Forwards SCTE 35 messages downstream.

drop — Drops SCTE 35 messages.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

23.67 sctp-filter

sctp-filter

Syntax **sctp-filter** *sctp-filter-name*
no sctp-filter

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action sctp-filter)

Full Context configure application-assurance group policy app-qos-policy entry action sctp-filter

Description This command assigns an existing SCTP filter as an action on flows matching this AQP entry.

The **no** form of this command removes this SCTP filter from actions on flows matching this AQP entry.

Default no sctp-filter

Parameters *sctp-filter-name* — Specifies the name of the existing SCTP filter for this application assurance profile. The *sctp-filter-name* is configured in the **config>app-assure>group[:partition]>sctp-filter** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

sctp-filter

Syntax **sctp-filter** *sctp-filter-name*

Context **[Tree]** (config>app-assure>group>statistics>tca sctp-filter)

Full Context configure application-assurance group statistics threshold-crossing-alert sctp-filter

Description This command configures TCA generation for an SCTP filter.

Parameters *sctp-filter-name* — Specifies the name of the SCTP filter, up to 32 characters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

sctp-filter

Syntax **sctp-filter** *sctp-filter-name* [**create**]
no sctp-filter *sctp-filter-name*

Context **[Tree]** (config>app-assure>group sctp-filter)

Full Context configure application-assurance group sctp-filter

Description Commands in this context configure Stream Control Transmission Protocol (SCTP) parameters.

The **no** form of this command removes this filter.

Parameters *sctp-filter-name* — Specifies the SCTP filter name, up to 32 characters.

create — Keyword used to create the SCTP filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.68 sctp-filter-stats

sctp-filter-stats

Syntax [**no**] **sctp-filter-stats**

Context **[Tree]** (config>app-assure>group>statistics>aa-admit-deny sctp-filter-stats)

Full Context configure application-assurance group statistics aa-admit-deny sctp-filter-stats

Description This command configures whether to include or exclude SCTP filter admit-deny statistics in accounting records.

Default no sctp-filter-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.69 sd

sd

Syntax **sd**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if sd)

Full Context configure mcast-management multicast-info-policy video-policy video-interface sd

Description Commands in this context configure within a video interface policy the properties relating to requests received by the video interface for Standard Definition (SD) channel requests.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

23.70 sd-offset

sd-offset

Syntax **sd-offset** *offset-value*
no sd-offset

Context **[Tree]** (config>service>vprn>isis>if>level sd-offset)

Full Context configure service vprn isis interface level sd-offset

Description If the pre-FEC error rate of the associated DWDM port crosses the configured **sd-threshold**, this offset-value is added to the IS-IS interface metric. This parameter is only effective if the interface is associated with a DWDM port and the **sd-threshold** value is configured under that port.

The **no** form of this command reverts the offset value to 0.

Default no sd-offset

Parameters *offset-value* — Specifies the amount the interface metric is increased by if the **sd-threshold** is crossed.

Values 0 to 16777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sd-offset

Syntax **sd-offset** *sd-offset*
no sd-offset

Context **[Tree]** (config>router>isis>if>level sd-offset)

Full Context configure router isis interface level sd-offset

Description If the pre-FEC error rate of the associated DWDM port crosses the configured **sd-threshold**, this offset-value is added to the IS-IS interface metric. This parameter is only effective if the interface is associated with a DWDM port and the **sd-threshold** value is configured under that port.

The **no** form of this command reverts the offset value to 0.

Default no sd-offset

Parameters *sd-offset* — Specifies the amount the interface metric is increased by if the **sd-threshold** is crossed.

Values 0 to 16777215

Platforms All

23.71 sd-threshold

sd-threshold

Syntax **sd-threshold** *threshold* [**coefficient** *coefficient*]

Context **[Tree]** (config>port>otu sd-threshold)

Full Context configure port otu sd-threshold

Description This command defines the error rate at which to declare the signal degrade (SD) condition.

The parameters define an error rate of (*coefficient*/10) * 10E-*threshold*. For example, **sd-threshold 5 coefficient 20** defines an error rate of (20/10) * 10E-5, or 2 * 10E-5, or 0.000 02.

The SD threshold must be:

- greater than the SF threshold.
- 5 or higher before setting **sf-sd-method** to **bip8**.

The **coefficient** parameter is only used when **sf-sd-method** is set to **fec**. When **sf-sd-method** is set to **bip8**, **coefficient** is considered to have the value of 10.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *threshold* — Specifies the exponent for the SD threshold value.

Values 5 to 9 when **sf-sd-method** is **bip8**
3 to 9 when **sf-sd-method** is **fec**

Default 7

coefficient — Specifies the coefficient for the SD threshold value.

Values 10 to 99

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

sd-threshold

Syntax **sd-threshold** *errored-frames*
no sd-threshold

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame sd-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-frame sd-threshold

Description The option defines the number of errored frames within the configured window which indicates the port has gone beyond an acceptable error rate and should be considered degraded. This is a first level warning that a port may be suspect. This generates an information log event message only and will be recorded in the Port event index but has no port level actions when the error count is equal to or greater than the threshold. This value must be lower than or equal to the sf-threshold value.

The **no** value of this option disables the sd-threshold.

Default no sd-threshold

Parameters *errored-frames* — Specifies the number of errored frames within the configured window which indicates the port has become degraded.

Values 1 to 1000000

Platforms All

sd-threshold

Syntax **sd-threshold** *errored-frames*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame-period sd-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-period sd-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The option defines the number of errored frames within the configured window which indicates the port has gone beyond an acceptable error rate and should be considered degraded. This is a first level warning that a port may be suspect. This generates an information log event message only and will be recorded in the Port event index but has no port level actions when the error count is equal to or greater than the threshold. This value must be lower than or equal to the sf-threshold value.

The **no** value of this option disables the sd-threshold

Default no sd-threshold

Parameters *errored-frames* — Specifies the number of errored frames within the configured window which indicates the port has become degraded.

Values 1 to 1000000

Platforms All

sd-threshold

Syntax **sd-threshold** *errored-frames*
no sd-threshold

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame-seconds sd-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-seconds sd-threshold

Description This command defines the number of errored frame seconds within the configured window which indicates the port has gone beyond an acceptable error rate and should be considered degraded. This is a first level warning that a port may be suspect. This event is raised when the error count is equal to or greater than the configured threshold. This is an information log event message only and will be recorded in the Port event index but has no port level actions. This value must be lower than or equal to the sf-threshold value.

The **no** version of this command disables the sd-threshold.

Parameters *errored-frames* — Specifies the number of errored seconds within the configured window which indicates the port has become degraded.

Values 1 to 900

Platforms All

sd-threshold

Syntax **sd-threshold** *errored-symbols*
no sd-threshold

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-symbols sd-threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet efm-oam link-monitoring errored-symbols sd-threshold

Description This command defines the number of errored frames within the configured window which indicates the port has gone beyond an acceptable error rate and should be considered degraded. This is a first level warning that a port may be suspect. An event is raised when the error count is equal to or greater than this value. This is an information log event message only and will be recorded in the Port event index but has no port level actions. This value must be lower than or equal to the sf-threshold value. Specific to symbol errors, this value must be configured with the value that indicates anything less is acceptable and the port can be returned to service. If this value is not configured then manual operation is required to return the port to service.

The **no** value of this option means there is there is no automatic return to service.

Default no sd-threshold

Parameters *errored-symbols* — Specifies the number of errored symbols which indicates the port has become degraded.

Values 1 to1000000

Platforms All

sd-threshold

Syntax **sd-threshold** *threshold* [**multiplier** *multiplier*]
no sd-threshold

Context **[Tree]** (config>port>ethernet>sym-mon sd-threshold)

Full Context configure port ethernet symbol-monitor sd-threshold

Description This command specifies the error rate at which to declare the Signal Degrade condition on an Ethernet interface. The value represents M*10E-N a ratio of symbol errors over total symbols received over W seconds of the sliding window. The symbol errors on the interface are sampled once per second. A default of 10 seconds is used when there is no additional window-size configured. The multiplier keyword is optional. If the multiplier keyword is omitted or no sd-threshold is specified the multiplier will return to the default value of 1.

Default no sd-threshold

Parameters *threshold* — Specifies the rate of symbol errors.

Values 1 to 9

multiplier — Specifies the multiplier used to scale the symbol error ratio.

Values 1 to 9

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sd-threshold

Syntax **sd-threshold** *threshold* [**multiplier** *multiplier*]
no sd-threshold

Context **[Tree]** (config>port>ethernet>crc-monitor sd-threshold)

Full Context configure port ethernet crc-monitor sd-threshold

Description This command specifies the error rate at which to declare the Signal Degrade condition on an Ethernet interface. The value represents M*10E-N a ratio of errored frames over total frames received over W seconds of the sliding window. The CRC errors on the interface are sampled once per second. A default of 10 seconds is used when there is no additional window-size configured. The multiplier keyword is optional. If the multiplier keyword is omitted or **no sd-threshold** is specified the multiplier will return to the default value of 1.

Default no sd-threshold

Parameters *threshold* — Specifies the threshold value.

Values 1 to 9

multiplier — Specifies the multiplier value.

Values 1 to 9

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.72 sd-threshold-clear

sd-threshold-clear

Syntax **sd-threshold-clear** *threshold* [**coefficient** *coefficient*]

Context **[Tree]** (config>port>otu sd-threshold-clear)

Full Context configure port otu sd-threshold-clear

Description This command defines the signal degrade (SD) threshold clear value.

When the bit error rate falls below this value, the SD condition is cleared. The parameters define an error rate of (*coefficient*/10) * 10E-*threshold*. For example, **sd-threshold-clear 7 coefficient 10** defines an error rate of (10/10) * 10E-7, or 10E-7, or 0.000 000 1.

This SD threshold clear setting is valid only when **sf-sd-method** is set to **fec**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *threshold* — Specifies the exponent for the SD threshold clear value.

Values 3 to 10

Default 8

coefficient — Specifies the coefficient for the SD threshold clear value.

Values 10 to 99

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.73 sdp

sdp

Syntax **sdp** *sdp-id* [**sync-tag** *sync-tag*] [**create**]
no sdp *sdp-id*

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync sdp)

Full Context configure redundancy multi-chassis peer sync sdp

Description This command specifies the manually configured spoke SDPs to be synchronized with the multi-chassis peer and a synchronization tag to be used while synchronizing these spoke SDPs with the multi-chassis peer.

Manually configured spoke SDPs with the specified *sdp-id* are synchronized according to the synchronization tag. If synchronization is required only for a subset of the spoke SDPs using the configured SDP, the **range** sub-command should be used. The **range** command and the **sync-tag** parameters are mutually exclusive.

The synchronization of PIM snooping is only supported for manually configured spoke SDPs but is not supported for spoke SDPs configured within an endpoint.

The synchronization of PIM snooping is not supported on any of the following when used with the configured *sdp-id*:

- Mesh SDPs
- Spoke SDPs in non-VPLS services
- BGP-AD/BGP-VPLS (FEC 129) spoke SDPs
- Spoke SDPs configured in endpoints
- Pseudowire SAPs
- ESM-over-MPLS Pseudowires

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Non-existent spoke SDPs may be specified. If these spoke SDPs are created at a later time, then all states on the spoke SDPs are synchronized according to the synchronization tag and the synchronization protocols enabled.

A synchronization tag can be changed by entering the same command with a different synchronization tag. Changing the synchronization tag removes all states relating to the previous synchronization tag for the SDP and a new synchronization tag state is created.

Parameters *sdp-id* — Specifies the SDP of the spoke SDPs to be synchronized with the multi-chassis peer.

Values 1 to 32767

sync-tag — Specifies a synchronization tag, up to 32 characters, to be used when synchronizing with the multi-chassis peer.

create — Creates the SDP instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

sdp

Syntax **sdp** *sdp-id*
no sdp

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg sdp)

Full Context configure service system bgp-evpn ethernet-segment sdp

Description This command configures an *sdp-id* associated to the Ethernet-Segment. If the Ethernet-Segment is configured as **all-active**, then only a lag or PW port can be associated to the Ethernet-Segment. If the Ethernet-Segment is configured as **single-active**, then lag, port or sdp can be associated to the Ethernet-Segment. In any case, only one of the four objects can be configured in the Ethernet-Segment. A specified SDP can be part of only one Ethernet-Segment. Only user-configured SDPs can be added to an Ethernet-Segment.

Default no sdp

Parameters *sdp-id* — Specifies the IP address.

Values 1 to 17407

Platforms All

sdp

Syntax [**no**] **sdp** *sdp-id:vc-id*

Context **[Tree]** (config>service>vpls>pbb>backbone-vpls sdp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls pbb backbone-vpls sdp

Description This command configures attributes of a SDP binding on the B-VPLS service.

Parameters *sdp-id* — Specifies the SDP ID.

Values 1 to 17407

vc-id — Specifies the VC ID.

Values 1 to 4294967295

Platforms All

sdp

Syntax [**no**] **sdp** *sdp-id:vc-id*

Context **[Tree]** (debug>service>id>mrp sdp)

Full Context debug service id mrp sdp

Description This command filters debug events and only shows events for the particular SDP.

The **no** form of this command removes the debug filter.

Parameters *sdp-id* — Specifies the SDP ID for which to display information

Default All SDPs

Values 1 to 17407

vc-id — Displays information about the virtual circuit identifier.

Values 1 to 4294967295

Platforms All

sdp

Syntax [**no**] **sdp** *sdp-id:vc-id*

Context **[Tree]** (debug>service>id sdp)
[Tree] (debug>service>id>dhcp sdp)
[Tree] (debug>service>id>stp sdp)

Full Context debug service id dhcp sdp
debug service id sdp
debug service id stp sdp

Description This command enables STP debugging for a specific SDP.

The **no** form of the command disables debugging.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sdp-id:vc-id* — Specifies the SDP ID and VC ID.

Values sdp-id: 1 to 17407
vc-id: 1 to 4294967295

Platforms All

sdp

Syntax [**no**] **sdp** *sdp-id:vc-id*

Context **[Tree]** (debug>service>id>igmp-snooping sdp)

Full Context debug service id igmp-snooping sdp

Description This command shows IGMP packets for a specific SDP.

The **no** form of this command disables the debugging for the SDP.

Parameters *sdp-id* — Displays only IGMP snooping entries associated with the specified mesh SDP or spoke-SDP. For a spoke-SDP, the VC ID must be specified, for a mesh SDP, the VC ID is optional.

Values 1 to 17407

vc-id — Displays information for the specified virtual circuit ID on the SDP ID

Values 1 to 4294967295

Platforms All

sdp

Syntax [**no**] **sdp** *sdp-id:vc-id*

Context **[Tree]** (debug>service>id>mld sdp)

Full Context debug service id mld-snooping sdp

Description This command shows MLD packets for a specific SDP.

The **no** form of this command disables the debugging for the SDP.

Parameters *sdp-id* — Displays only MLD entries associated with the specified mesh SDP or spoke-SDP

Values 1 to 17407

vc-id — Displays information for the specified virtual circuit ID on the SDP ID

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sdp

Syntax **sdp** *sdp-id* [*delivery-type*] [**create**]
no sdp *sdp-id*

Context **[Tree]** (config>service sdp)

Full Context configure service sdp

Description This command creates or edits a Service Distribution Point (SDP). SDPs must be explicitly configured.

An SDP is a logical mechanism that ties a far-end router to a particular service without having to specifically define far-end SAPs. Each SDP represents a method to reach another router.

One method is IP Generic Router Encapsulation (GRE), which has no state in the core of the network. GRE does not specify a specific path to the far-end router. A GRE-based SDP uses the underlying IGP routing table to find the best next hop to the far-end router.

The second method is Multi-Protocol Label Switching (MPLS) encapsulation. A router supports both signaled and non-signaled Label Switched Paths (LSPs) through the network. Non-signaled paths are defined at each hop through the network. Signaled paths are communicated by protocol from end-to-end using Resource Reservation Protocol (RSVP). Paths may be manually defined or a constraint-based routing protocol (such as OSPF-TE or CSPF) can be used to determine the best path with specific constraints. An LDP LSP can also be used for an SDP when the encapsulation is MPLS. The use of an LDP LSP type or an RSVP/Static LSP type are mutually exclusive except when the mixed-lsp option is enabled on the SDP.

Segment routing is another MPLS tunnel type and is used to allow service binding to an SR tunnel programmed in TTM by OSPF or IS-IS. The SDP of type **sr-isis** or **sr-ospf** can be used with the **far-end** option. The **tunnel-far-end** option is not supported. In addition, the **mixed-lsp-mode** option does not support the **sr-isis** and **sr-ospf** tunnel types.

L2TPv3-over-IPv6 transport is also an option for 7750 SR and 7950 XR Ethernet Pipe (Epipe) Services. Like GRE, L2TPv3 is stateless in the core of the network, as well as on the service nodes as the L2TPv3 control plane functionality is disabled for this SDP type. A unique source and destination IPv6 address combined with TX and RX Cookie values are used to ensure that the SDP is bound to the correct service.

SDPs are created and then bound to services. Many services may be bound to a single SDP. The operational and administrative state of the SDP controls the state of the SDP binding to the service.

If the *sdp-id* does not exist, a new SDP is created. When creating an SDP, either the **gre, mpls, or l2tpv3** keyword must be specified. SDPs are created in the admin down state (**shutdown**) and the **no shutdown** command must be executed once all relevant parameters are defined and before the SDP can be used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If *sdp-id* exists, the current CLI context is changed to that SDP for editing and modification. For editing an existing SDP, neither the **gre, mpls**, or **l2tpv3** keyword is specified. If a keyword is specified for an existing *sdp-id*, an error is generated and the context of the CLI will not be changed to the specified *sdp-id*.

The **no** form of this command deletes the specified SDP. Before an SDP can be deleted, it must be administratively down (shutdown) and not bound to any services. If the specified SDP is bound to a service, the **no sdp** command will fail generating an error message specifying the first bound service found during the deletion process. If the specified *sdp-id* does not exist an error will be generated.

Parameters *sdp-id* — Specifies the SDP identifier.

Values 1 to 32767

gre — Specifies the SDP will use GRE to reach the far-end router. The GRE encapsulation of the MPLS service packet uses the base 4-byte header as per RFC 2890. The optional fields Checksum (plus Reserved field), Key, and Sequence Number are not inserted. Only one GRE SDP can be created to a given destination address. Multiple GRE SDPs to a single destination address serve no purpose as the path taken to reach the far end is determined by the IGP which will be the same for all SDPs to a given destination and there is no bandwidth reservation in GRE tunnels.

mpls — Specifies the SDP will use MPLS encapsulation and one or more LSP tunnels to reach the far-end device. Multiple MPLS SDPs may be created to a given destination device. Multiple MPLS SDPs to a single destination device are helpful when they use divergent paths.

l2tpv3 — Specifies the SDP will use L2TPv3-over-IPv6 encapsulation for the 7750 SR or 7950 XRS. One SDP is created per service, regardless of whether the far-end node is common or not. Unique local and far-end addresses are configured for every L2TPv3 SDP type. The local address must exist on the local node.

eth-gre-bridged — Configures the SDP as an L2oGRE tunnel that is terminated on an FPE-based PW port. Only the end-points of such a tunnel (the far-end IPv4/IPv6 address or local-end IPv4/IPv6 address) are allowed to be configured under this SDP.

Platforms All

23.74 sdp-exclude

sdp-exclude

Syntax [**no**] **sdp-exclude** *group-name*

Context **[Tree]** (config>service>pw-template sdp-exclude)

Full Context configure service pw-template sdp-exclude

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures SDP admin group constraints for a pseudowire template.

The admin group name must have been configured or the command is failed. The user can execute the command multiple times to include or exclude more than one admin group. The sdp-include and sdp-exclude commands can only be used with the **use-provisioned-sdp** or **prefer-provisioned-sdp** options. If the same group name is included and excluded within the same pseudowire template, only the exclude option will be enforced.

Any changes made to the admin group sdp-include and sdp-exclude constraints will only be reflected in existing spoke-sdps after the following command has been executed:

tools>perform>service>eval-pw-template>allow-service-impact

When the service is bound to the pseudowire template, the SDP selection rules will enforce the admin group constraints specified in the sdp-include and sdp-exclude commands.

In the SDP selection process, all provisioned SDPs with the correct far-end IP address, the correct tunnel-far-end IP address, and the correct service label signaling are considered. The SDP with the lowest admin metric is selected. If more than one SDP with the same lowest metric are found then the SDP with the highest sdp-id is selected. The type of SDP, GRE or MPLS (BGP/RSVP/LDP) is not a criterion in this selection.

The selection rule with SDP admin groups is modified such that the following admin-group constraints are applied upfront to prune SDPs that do not comply:

- if one or more **sdp-include** statement is part of the PW template, then an SDP that is a member of one or more of the included groups will be considered. With the **sdp-include** statement, there is no preference for an SDP that belongs to all included groups versus one that belongs to one or fewer of the included groups. All SDPs satisfying the admin-group constraint will be considered and the selection above based on the lowest metric and highest sdp-id is applied.
- if one or more **sdp-exclude** statement is part of the PW template, then an sdp that is a member of any of the excluded groups will not be considered.

SDP admin group constraints can be configured on all router services that makes use of the pseudowire template (BGP-AD VPLS service, BGP-VPLS service, and FEC129 VLL service). In the latter case, only support at a T-PE node is provided.

The **no** form of this command removes the SDP admin group constraints from the pseudowire template.

Parameters *group-name* — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.75 sdp-group

sdp-group

Syntax **sdp-group**

Context **[Tree]** (config>service sdp-group)

Full Context configure service sdp-group

Description This command configures the SDP membership in admin groups.

The user can enter a maximum of one (1) admin group name at once. The user can execute the command multiple times to add membership to more than one admin group. The admin group name must have been configured or the command is failed. Admin groups are supported on an SDP of type GRE and of type MPLS (BGP/RSVP/LDP). They are also supported on an SDP with the mixed-lsp-mode option enabled.

The **no** form of this command removes this SDP membership to the specified admin group.

Platforms All

23.76 sdp-id-range

sdp-id-range

Syntax **sdp-id-range from** *id* **to** *id*
no sdp-id-range

Context **[Tree]** (config>fwd-path-ext sdp-id-range)

Full Context configure fwd-path-ext sdp-id-range

Description This command reserves an SDP ID range used by the FPE based PW-Port and VXLAN termination applications.

Each configured FPE based PW-Port is associated with two internal SDPs (one in each direction) whose id(s) are allocated from the configured sdp-id-range.

When the FPE is associated to VXLAN termination, an internal SDP is allocated from the configured sdp-id-range and is used for R-VPLS services that terminate VXLAN IPv6. A spoke-sdp per VXLAN IPv6 R-VPLS service is created on that SDP for egress processing of the packets. Sdp-id-range cannot be modified if any of its IDs are currently in use.

Default no sdp-id-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **from** *id* — Specifies the start of the SDP ID range (inclusive).

Values 1 to 32767

to *id* — Specifies the end of the SDP ID range.

Values 1 to 32767

Platforms All

23.77 sdp-include

sdp-include

Syntax [**no**] **sdp-include** *group-name*

Context **[Tree]** (config>service>pw-template sdp-include)

Full Context configure service pw-template sdp-include

Description This command configures SDP admin group constraints for a pseudowire template.

The admin group name must have been configured or the command is failed. The user can execute the command multiple times to include or exclude more than one admin group. The sdp-include and sdp-exclude commands can only be used with the **use-provisioned-sdp** or **prefer-provisioned-sdp** options. If the same group name is included and excluded within the same pseudowire template, only the exclude option will be enforced.

Any changes made to the admin group sdp-include and sdp-exclude constraints will only be reflected in existing spoke-sdps after the following command has been executed:

tools>perform>service>eval-pw-template>allow-service-impact

When the service is bound to the pseudowire template, the SDP selection rules will enforce the admin group constraints specified in the sdp-include and sdp-exclude commands.

In the SDP selection process, all provisioned SDPs with the correct far-end IP address, the correct tunnel-far-end IP address, and the correct service label signaling are considered. The SDP with the lowest admin metric is selected. If more than one SDP with the same lowest metric are found then the SDP with the highest sdp-id is selected. The type of SDP, GRE or MPLS (BGP/RSVP/LDP) is not a criterion in this selection.

The selection rule with SDP admin groups is modified such that the following admin-group constraints are applied upfront to prune SDPs that do not comply:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- if one or more **sdp-include** statement is part of the PW template, then an SDP that is a member of one or more of the included groups will be considered. With the **sdp-include** statement, there is no preference for an SDP that belongs to all included groups versus one that belongs to one or fewer of the included groups. All SDPs satisfying the admin-group constraint will be considered and the selection above based on the lowest metric and highest sdp-id is applied.
- if one or more **sdp-exclude** statement is part of the PW template, then an sdp that is a member of any of the excluded groups will not be considered.

SDP admin group constraints can be configured on all router services that make use of the pseudowire template (BGP-AD VPLS service, BGP-VPLS service, and FEC129 VLL service). In the latter case, only support at a T-PE node is provided.

The **no** form of this command removes the SDP admin group constraints from the pseudowire template.

Default none

Parameters *group-name* — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.

Platforms All

23.78 sdp-mtu

sdp-mtu

Syntax **sdp-mtu** *orig-sdp-id* **size-inc** *start-octets end-octets* [**step** *step-size*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam sdp-mtu)

Full Context oam sdp-mtu

Description Performs MTU Path tests on an SDP to determine the largest path-mtu supported on an SDP. The **size-inc** parameter can be used to easily determine the **path-mtu** of a given SDP-ID. The forwarding class is assumed to be Best-Effort Out-of-Profile. The message reply is returned with IP/GRE encapsulation from the far-end router. OAM request messages sent within an IP/GRE SDP must have the 'DF' IP header bit set to 1 to prevent message fragmentation.

To terminate an **sdp-mtu** in progress, use the CLI break sequence <Ctrl-C>.

Special Cases **SDP Path MTU Tests —** SDP Path MTU tests can be performed using the **sdp-mtu size-inc** keyword to easily determine the **path-mtu** of a given SDP-ID. The forwarding class is assumed to be Best-Effort Out-of-Profile. The message reply is returned with IP/GRE encapsulation from the far-end router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

With each OAM Echo Request sent using the **size-inc** parameter, a response line is displayed as message output. The path MTU test displays incrementing packet sizes, the number sent at each size until a reply is received and the response message.

As the request message is sent, its size value is displayed followed by a period for each request sent of that size. Up to three requests are sent unless a valid response is received for one of the requests at that size. Once a response is received, the next size message is sent.

The response message indicates the result of the message request.

After the last reply has been received or response time out, the maximum size message replied to indicates the largest size OAM Request message that received a valid reply.

Parameters *orig-sdp-id* — Specifies the *sdp-id* to be used by **sdp-ping,** expressed as a decimal integer. The far-end address of the specified **sdp-id** is the expected *responder-id* within each reply received. The specified *sdp-id* defines the encapsulation of the SDP tunnel encapsulation used to reach the far end. This can be IP/GRE or MPLS. If *orig-sdp-id* is invalid or administratively down or unavailable, the SDP echo request message is not sent and an appropriate error message is displayed (once the **interval** timer expires, **sdp-ping** attempts to send the next request, if required).

Values 1 to 32767

start-octets — Specifies the beginning size in octets of the first message sent for an incremental MTU test, expressed as a decimal integer.

Values 40 to 9786

end-octets — Specifies the ending size in octets of the last message sent for an incremental MTU test, expressed as a decimal integer. The specified value must be greater than *start-octets*.

Values 40 to 9786

step-size — Specifies the number of octets to increment the message size request for each message sent for an incremental MTU test, expressed as a decimal integer. The next size message is not sent until a reply is received or three messages have timed out at the current size.

If the incremented size exceeds the *end-octets* value, no more messages are sent.

Values 1 to 512

Default 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout — Specifies the *timeout* parameter in seconds, expressed as a decimal integer. This value is used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

Values 1 to 10

Default 5

interval — Specifies the *interval* parameter in seconds, expressed as a decimal integer. This parameter is used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the *interval* is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

Output

Sample Output for SDP MTU Path Test

```
*A:Dut-A# oam sdp-mtu 1201 size-inc 512 3072 step 256
Size    Sent    Response
----------------------------
512     .        Success
768     .        Success
1024    .        Success
1280    .        Success
1536    .        Success
1792    .        Success
2048    .        Success
2304    .        Success
2560    .        Success
2816    .        Success
3072    .        Success

Maximum Response Size: 3072
*A:Dut-A#
```

Platforms

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.79 sdp-ping

sdp-ping

Syntax **sdp-ping** *orig-sdp-id* [**resp-sdp** *resp-sdp-id*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**count** *send-count*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam sdp-ping)
[Tree] (config>saa>test>type sdp-ping)

Full Context configure saa test type sdp-ping
oam sdp-ping

Description This command tests SDPs for uni-directional or round trip connectivity and performs SDP MTU Path tests.

The **sdp-ping** command accepts an originating SDP-ID and an optional responding SDP-ID. The size, number of requests sent, message time-out and message send interval can be specified. All **sdp-ping** requests and replies are sent with PLP OAM-Label encapsulation, as a *service-id* is not specified.

For round trip connectivity testing, the **resp-sdp** keyword must be specified. If **resp-sdp** is not specified, a uni-directional SDP test is performed.

To terminate an **sdp-ping** in progress, use the CLI break sequence <Ctrl-C>.

An **sdp-ping** response message indicates the result of the **sdp-ping** message request. When multiple response messages apply to a single SDP echo request/reply sequence, the response message with the highest precedence is displayed. Table 122 shows the response messages sorted by precedence.

Table 122 **sdp-ping Response Messages**

Result of Request	Displayed Response Message	Precedence
Request time out without reply	Request Timeout	1
Request not sent due to non-existent *orig-sdp-id*	Orig-SDP Non-Existent	2
Request not sent due to administratively down *orig-sdp-id*	Orig-SDP Admin-Down	3
Request not sent due to operationally down *orig-sdp-id*	Orig-SDP Oper-Down	4
Request terminated by user before reply or time out	Request Terminated	5
Reply received, invalid *origination-id*	Far End: Originator-ID Invalid	6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 122 **sdp-ping Response Messages**

Result of Request	Displayed Response Message	Precedence
Reply received, invalid *responder-id*	Far End: Responder-ID Error	7
Reply received, non-existent *resp-sdp-id*	Far End: Resp-SDP Non-Existent	8
Reply received, invalid *resp-sdp-id*	Far End: Resp-SDP Invalid	9
Reply received, *resp-sdp-id* down (admin or oper)	Far-end: Resp-SDP Down	10
Reply received, No Error	Success	11

Special Cases **Single Response Connectivity Tests —** A single response sdp-ping test provides detailed test results. See Table 123.

Upon request time out, message response, request termination, or request error the following local and remote information is displayed. Local and remote information is dependent upon the SDP ID existence and reception of reply.

Table 123 **sdp-ping Test Results**

Field	Description	Values
Request Result	The result of the **sdp-ping** request message.	Sent - Request Timeout
		Sent - Request Terminated
		Sent - Reply Received
		Not Sent - Non-Existent Local SDP-ID
		Not Sent - Local SDP-ID Down
Originating SDP-ID	The originating SDP-ID specified by **orig-sdp**.	orig-sdp-id
Originating SDP-ID Administrative State	The local administrative state of the originating SDP-ID. If the SDP-ID has been shut down, Admin-Down is displayed. If the originating SDP-ID is in the **no shutdown** state, Admin-Up is displayed. If the *orig-sdp-id* does not exist, Non-Existent is displayed.	Admin-Up
		Admin-Down
		Non-Existent
Originating SDP-ID Operating State	The local operational state of the originating SDP-ID. If *orig-sdp-id* does not exist, N/A is displayed.	Oper-Up
		Oper-Down
		—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 123 **sdp-ping Test Results**

Field	Description	Values
Originating SDP-ID Path MTU	The local **path-mtu** for *orig-sdp-id*. If *orig-sdp-id* does not exist locally, N/A is displayed.	orig-path-mtu
		—
Responding SDP-ID	The SDP-ID requested as the far-end path to respond to the **sdp-ping** request. If **resp-sdp** is not specified, the responding router does not use an SDP-ID as the return path and N/A is displayed.	resp-sdp-id
		—
Responding SDP-ID Path Used	Displays whether the responding router used the responding **sdp-id** to respond to the **sdp-ping** request. If *resp-sdp-id* is a valid, operational SDP-ID, it must be used for the SDP echo reply message. If the far-end uses the responding **sdp-id** as the return path, Yes is displayed. If the far-end does not use the responding **sdp-id** as the return path, No is displayed. If **resp-sdp** is not specified, N/A is displayed.	Yes
		No
		—
Responding SDP-ID Administrative State	The administrative state of the responding **sdp-id**. When *resp-sdp-id* is administratively down, Admin-Down is displayed. When *resp-sdp-id* is administratively up, Admin-Up is displayed. When *resp-sdp-id* exists on the far-end router but is not valid for the originating router, Invalid is displayed. When *resp-sdp-id* does not exist on the far-end router, Non-Existent is displayed. When **resp-sdp** is not specified, N/A is displayed.	Admin-Down
		Admin-Up
		Invalid
		Non-Existent
		—
Responding SDP-ID Operational State	The operational state of the far-end **sdp-id** associated with the return path for *service-id*. When a return path is operationally down, Oper-Down is displayed. If the return **sdp-id** is operationally up, Oper-Up is displayed. If the responding **sdp-id** is non-existent, N/A is displayed.	Oper-Up
		Oper-Down
		—
Responding SDP-ID Path MTU	The remote **path-mtu** for *resp-sdp-id*. If *resp-sdp-id* does not exist remotely, N/A is displayed	resp-path-mtu
		—
Local Service IP Address	The local system IP address used to terminate remotely configured **sdp-ids** (as the **sdp-id far-end** address). If an IP address has not been configured to be the system IP address, N/A is displayed.	system-ip-addr
		—
Local Service IP Interface Name	The name of the local system IP interface. If the local system IP interface has not been created, N/A is displayed.	system-interface-name
		—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 123 **sdp-ping Test Results**

Field	Description	Values
Local Service IP Interface State	The state of the local system IP interface. If the local system IP interface has not been created, Non-Existent is displayed.	Up
		Down
		Non-Existent
Expected Far End Address	The expected IP address for the remote system IP interface. This must be the **far-end** address configured for the *orig-sdp-id*.	orig-sdp-far-end-addr
		dest-ip-addr
		—
Actual Far End Address	The returned remote IP address. If a response is not received, the displayed value is N/A. If the far-end service IP interface is down or non-existent, a message reply is not expected.	resp-ip-addr
		—
Responders Expected Far End Address	The expected source of the originators **sdp-id** from the perspective of the remote router terminating the **sdp-id**. If the far-end cannot detect the expected source of the ingress **sdp-id**, N/A is displayed.	resp-rec-tunnel-far-end-addr
		—
Round Trip Time	The round trip time between SDP echo request and the SDP echo reply. If the request is not sent, times out or is terminated, N/A is displayed.	delta-request-reply
		—

Parameters *orig-sdp-id* — Specifies the SDP ID to be used by **sdp-ping,** expressed as a decimal integer. The far-end address of the specified SDP-ID is the expected *responder-id* within each reply received. The specified SDP-ID defines the encapsulation of the SDP tunnel encapsulation used to reach the far end. This can be IP/GRE or MPLS. If *orig-sdp-id* is invalid or administratively down or unavailable for some reason, the SDP Echo Request message is not sent and an appropriate error message is displayed (once the **interval** timer expires, **sdp-ping** attempts to send the next request if required).

Values 1 to 32767

resp-sdp-id — Specifies the return SDP-ID to be used by the far-end router for the message reply for round trip SDP connectivity testing. If *resp-sdp-id* does not exist on the far-end router, terminates on another router different than the originating router, or another issue prevents the far-end router from using *resp-sdp-id*, the SDP echo reply is sent using generic IP/GRE OAM encapsulation. The received forwarding class (as mapped on the ingress network interface for the far end) defines the forwarding class encapsulation for the reply message.

Values 1 to 32767

Default null. Use the non-SDP return path for message reply.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc-name — Specifies the parameter to be used to indicate the forwarding class of the SDP encapsulation. The actual forwarding class encoding is controlled by the network egress DSCP or LSP-EXP mappings.

The DSCP or LSP-EXP mappings on the receive network interface controls the mapping back to the internal forwarding class used by the far-end router that receives the message request. The egress mappings of the egress network interface on the far-end router controls the forwarding class markings on the return reply message.

The DSCP or LSP-EXP mappings on the receive network interface controls the mapping of the message reply at the originating router. This is displayed in the response message output upon receipt of the message reply.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | **out}** — Specifies the profile state of the SDP encapsulation.

Default out

octets — Specifies the **size** parameter in octets. This parameter is used to override the default message size for the **sdp-ping** request. Changing the message size is a method of checking the ability of an SDP to support a **path-mtu**. The size of the message does not include the SDP encapsulation, VC-Label (if applied) or any DLC headers or trailers.

When the OAM message request is encapsulated in an IP/GRE SDP, the IP 'DF' (Do Not Fragment) bit is set. If any segment of the path between the sender and receiver cannot handle the message size, the message is discarded. MPLS LSPs are not expected to fragment the message either, as the message contained in the LSP is not an IP packet.

Values 72 to 9786

Default 72

send-count — Specifies the number of messages to send. The **count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must have expired before the next message request is sent.

Values 1 to 100

Default 1

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of time out, the test is marked complete and no more packets is processed for any of those request probes.

Values 1 to 10

Default 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

Values 1 to 10

Default 1

Output

Single Response Round Trip Connectivity Test Sample Output

```
A:router1> sdp-ping 10 resp-sdp 22 fc ef
Request Result: Sent - Reply Received
RTT:30ms

Err  SDP-ID Info            Local     Remote
__   SDP-ID:                10        22
__   Administrative State:  Up        Up
__   Operative State:       Up        Up
__   Path MTU               4470      4470
__   Response SDP Used:               Yes

Err  System IP Interface Info
Local Interface Name: "ESR-System-IP-Interface (Up to 32 chars)…"
__   Local IP Interface State:          Up
__   Local IP Address:                  10.10.10.11
__   IP Address Expected By Remote:     10.10.10.11
__   Expected Remote IP Address:        10.10.10.10
__   Actual Remote IP Address:          10.10.10.10

Err   FC Mapping Info      Local        Remote
__    Forwarding Class     Assured      Assured
__    Profile              In           In
```

Multiple Response Connectivity Tests — When the connectivity test count is greater than one (1), a single line is displayed per SDP echo request send attempt.

The request number is a sequential number starting with 1 and ending with the last request sent, incrementing by one (1) for each request. This should not be confused with the *message-id* contained in each request and reply message.

A response message indicates the result of the message request. Following the response message is the round trip time value. If any reply is received, the round trip time is displayed.

After the last reply has been received or response timed out, a total is displayed for all messages sent and all replies received. A maximum, minimum and average round trip time is also displayed. Error response and timed out requests do not apply towards the average round trip time.

Multiple Response Round Trip Connectivity Test Sample Output

```
A:router1> sdp-ping 6 resp-sdp 101size 1514 count 5
Request        Response       RTT
----------     ----------     -------
     1         Success        10ms
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
     2         Success        15ms
     3         Success        10ms
     4         Success        20ms
     5         Success        5ms
Sent:    5    Received:    5
Min: 5ms       Max: 20ms      Avg: 12ms
```

Platforms All

23.80 seamless-bfd

seamless-bfd

Syntax **seamless-bfd**

Context **[Tree]** (config>bfd seamless-bfd)

Full Context configure bfd seamless-bfd

Description This command specifies the context for the configuration of a seamless BFD reflector.

Platforms All

seamless-bfd

Syntax **seamless-bfd**

Context **[Tree]** (config>router>bfd seamless-bfd)

Full Context configure router bfd seamless-bfd

Description This command specifies the context for the configuration of seamless BFD initiator parameters that are global to this router.

The **no** form of this command removes the context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.81 search

search

Syntax **search** *base-dn*
no search

Context **[Tree]** (config>system>security>ldap>server search)

Full Context configure system security ldap server search

Description This command configures the LDAP **search** command. The search *base-dn* tells the server which part of the external directory tree to search. The search DN uses the same LDAP attribute as *root-dn*. For example, to search a public-key for an SSH generated for a Nokia vendor, one might use “dc=public-key,dc=nokia,dc=com”.

The **no** version of this command removes the search DN; as such, no search is possible on the LDAP server.

Parameters *base-dn* — Specifies the base domain name used in the search, up to 512 characters.

Platforms All

23.82 secondary

secondary

Syntax **secondary**

Context **[Tree]** (config>aaa>radius-scr-plcy secondary)

Full Context configure aaa radius-script-policy secondary

Description Commands in this context configure a secondary script.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

secondary

Syntax **secondary**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol secondary)

Full Context configure subscriber-mgmt sub-ident-policy secondary

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure secondary identification script parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

secondary

Syntax **secondary** *ip-address[/mask]* [*netmask*] [**broadcast** {**all-ones** | **host-ones**}] [**igp-inhibit**] [**track-srrp** *srrp-instance*]
no secondary *ip-address[/mask]*

Context **[Tree]** (config>service>ies>if secondary)

Full Context configure service ies interface secondary

Description This command assigns a secondary IP address or IP subnet/broadcast address format to the interface.

The **no** form of this command reverts to the default.

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that is used in a logical and function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.254.

Note: A mask of 255.255.255.255 is reserved for system IP addresses.

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

broadcast — Overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones** which indicates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) is received by the IP interface. (Default: host-ones)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

all-ones — Specifies the broadcast address used by the IP interface for this IP address is 255.255.255.255, also known as the local broadcast.

host-ones — Specifies that the broadcast address used by the IP interface for this IP address is the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask-length* or *mask* with all the host bits set to binary one. This is the default broadcast address used by an IP interface. The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

igp-inhibit — Signals that the given secondary IP interface should not be recognized as a local interface by the running IGP. For OSPF and IS-IS, this means that the specified secondary IP interfaces are not injected and used as passive interfaces and are not advertised as internal IP interfaces into the IGP's link state database. For RIP, this means that these secondary IP interfaces do not source RIP updates.

track-srrp *srrp-instance* — Specifies the SRRP instance ID that this interface route needs to track.

Values 1 to 4294967295

Platforms All

secondary

Syntax **secondary** *ip-address*[/*mask*] [*netmask*] [**broadcast** {**all-ones** | **host-ones**}] [**igp-inhibit**] [**track-srrp** *srrp-instance*]
no secondary *ip-address*[/*mask*]

Context **[Tree]** (config>service>vprn>if secondary)
[Tree] (config>service>vprn>nw-if secondary)

Full Context configure service vprn interface secondary
configure service vprn network-interface secondary

Description This command assigns a secondary IP address to the interface. Up to 16 total primary and secondary IPv4 and IPv6 addresses can be assigned to network interfaces, and up to 256 to access interfaces. Each address can be configured in an IP address, IP subnet or broadcast address format.

Caution: Configurations must not exceed 16 secondary IP addresses when IPsec, GRE, L2TPv3, or IP in IP protocols are active on an access interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.254. A mask of 255.255.255.255 is reserved for system IP addresses.

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

broadcast — The optional **broadcast** parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones** which indicates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed. This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) will be received by the IP interface. *(Default: host-ones)*

all-ones — The **all-ones** keyword following the **broadcast** parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

host-ones — The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask-length* or *mask* with all the host bits set to binary one. This is the default used by an IP interface.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

igp-inhibit — The optional **igp-inhibit** parameter signals that the given secondary IP interface should not be recognized as a local interface by the running IGP. For OSPF and IS-IS, this means that the specified secondary IP interfaces will not be injected and used as passive interfaces and will not be advertised as internal IP interfaces into the IGP's link state database. For RIP, this means that these secondary IP interfaces will not source RIP updates.

track-srrp *srrp-instance* — Specifies the SRRP instance ID that this interface route needs to track.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

secondary

Syntax [**no**] **secondary** *path-name*

Context **[Tree]** (config>router>mpls>lsp secondary)

Full Context configure router mpls lsp secondary

Description This command specifies an alternative path that the LSP uses if the primary path is not available. This command is optional and is not required if the **config router mpls lsp** *lsp-name* **primary** *path-name* command is specified. After the switch over from the primary to the secondary, the system continuously tries to revert to the primary path. The switch back to the primary path is based on the **retry-timer** interval.

For RSVP-TE LSPs, up to eight secondary paths can be specified (or seven if a primary is configured). For SR-TE LSPs, up to three paths of any type (with a maximum of one primary) can be configured. By default, a secondary path is non-standby unless the **standby** keyword is configured. All non-standby secondary paths are considered equal and the first available path is used.

The system does not switch among secondary paths. The system starts the signaling (RSVP-TE) or programming (SR-TE) of all non-standby secondary paths at the same time. Retry counters are maintained for each unsuccessful attempt. After the retry limit is reached on a path, the system does not attempt to signal the path and administratively shuts down the path. The first successfully established non-standby secondary path is made the active path for the LSP.

The **no** form of this command removes the association between this *path-name* and *lsp-name*. All specific configurations for this association are deleted. The secondary path must be shut down prior to deleting it. The **no secondary** *path-name* command does not result in any action except a warning message on the console indicating that the secondary path is administratively up.

Parameters *path-name* — Specifies the case-sensitive alphanumeric name label for the LSP path, up to 64 characters.

Platforms All

secondary

Syntax **secondary** {*ip-address*/*mask* | *ip-address netmask*} [**broadcast** {**all-ones** | **host-ones**}] [**igp-inhibit**] [**track-srrp** *srrp-instance*]
no secondary {*ip-address/mask* | *ip-address netmask*}

Context **[Tree]** (config>router>if secondary)

Full Context configure router interface secondary

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command assigns additional IP addresses to the interface. Up to 16 total primary and secondary IPv4 and IPv6 addresses can be assigned to network interfaces, and up to 256 to access interfaces. Each address can be configured in an IP address, IP subnet, or broadcast address format.

Caution: Configurations must not exceed 16 secondary IP addresses when IPsec, GRE, L2TPv3, or IP in IP protocols are active on an access interface.

Parameters *ip-address* — Specifies the IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 to 223.255.255.255

/ — The forward slash is a parameter delimiter that separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-addr*, the "*/*" and the *mask-length* parameter. If a forward slash does not immediately follow the *ip-addr*, a dotted decimal mask must follow the prefix.

mask — Specifies the subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask* parameter. The *mask* parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Allowed values are integers in the range 1 to 32. A mask length of 32 is reserved for system IP addresses.

Values 1 to 32

netmask — Specifies the subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. A mask of 255.255.255.255 is reserved for system IP addresses.

Values 128.0.0.0 to 255.255.255.255

broadcast — The optional **broadcast** parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones,** which indicates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) will be received by the IP interface.

all-ones — The **all-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

host-ones — The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask* with all the host bits set to binary 1. This is the default broadcast address used by an IP interface.

igp-inhibit — The secondary IP address should not be recognized as a local interface by the running IGP.

srrp-instance — Specifies the SRRP instance ID that this interface route needs to track.

Platforms All

23.83 secondary-config

secondary-config

Syntax **secondary-config** *file-url*
no secondary-config

Context **[Tree]** (bof secondary-config)

Full Context bof secondary-config

Description This command specifies the name and location of the secondary configuration file.

The system attempts to use the configuration as specified in **secondary-config** if the primary config cannot be located. If the **secondary-config** file cannot be located, the system attempts to obtain the configuration from the location specified in the **tertiary-config**.

Note that if an error in the configuration file is encountered, the boot process aborts.

The **no** form of this command removes the **secondary-config** configuration.

Parameters *file-url* — Specifies the secondary configuration file location, expressed as a file URL.

Values

file-url	[*local-url* | *remote-url*] (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cflash-id cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

23.84 secondary-dns

secondary-dns

Syntax **secondary-dns** *ip-address*
no secondary-dns

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp secondary-dns)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp secondary-dns)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp secondary-dns
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp secondary-dns

Description This command configures the secondary DNS address to be returned via DHCP on WLAN-GW ISA.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the secondary DNS address.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

secondary-dns

Syntax **secondary-dns** *ip-address*
no secondary-dns

Context **[Tree]** (config>service>vprn>dns secondary-dns)

Full Context configure service vprn dns secondary-dns

Description This command configures the secondary DNS server for DNS name resolution. The secondary DNS server is used only if the primary DNS server does not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of this command removes the secondary DNS server from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no secondary-dns — No secondary DNS server is configured.

Parameters *ip-address* — The IP or IPv6 address of the secondary DNS server.

Values

ipv4-address -a.b.c.d

ipv6-address: x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x: [0 to FFFF]H
d: [0 to 255]D
interface - 32 characters max, for link local addresses.

Platforms All

secondary-dns

Syntax **secondary-dns** *ip-address*
no secondary-dns [*ip-address*]

Context **[Tree]** (bof secondary-dns)

Full Context bof secondary-dns

Description This command configures the secondary DNS server for DNS name resolution. The secondary DNS server is used only if the primary DNS server does not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of this command removes the secondary DNS server from the configuration.

Default no secondary-dns

Parameters *ip-address* — Specifies the IP or IPv6 address of the secondary DNS server.

Values

ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
interface	up to 32 characters for link local addresses

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: IPv6 is applicable to the 7750 SR and 7950 XRS only.

Platforms All

23.85 secondary-fast-retry-timer

secondary-fast-retry-timer

Syntax **secondary-fast-retry-timer** *seconds*
no secondary-fast-retry-timer

Context **[Tree]** (config>router>mpls secondary-fast-retry-timer)

Full Context configure router mpls secondary-fast-retry-timer

Description This command specifies the value used as the fast retry timer for a secondary path. If the first attempt to set up a secondary path fails due to a path error, the fast retry timer will be started for the secondary path so that the path can be retried sooner. If the next attempt also fails, further retries for the path will use the configured value for LSP retry timer.

If retry-timer for the LSP is configured to be less than the MPLS secondary-fast-retry-timer, all retries for the secondary path will use the LSP retry-timer.

The **no** form of this command reverts to the default.

Default no secondary-fast-retry-timer

Parameters *seconds* — Specifies the value (in seconds), used as the fast retry timer for a secondary path

Values 1 to 10

Platforms All

23.86 secondary-image

secondary-image

Syntax **secondary-image** *file-url*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no secondary-image

Context **[Tree]** (bof secondary-image)

Full Context bof secondary-image

Description This command specifies the secondary directory location for runtime image file loading.

The system attempts to load all runtime image files configured in the **primary-image** first. If this fails, the system attempts to load the runtime images from the location configured in the **secondary-image**. If the secondary image load fails, the tertiary image specified in **tertiary-image** is used.

All runtime image files (*.tim files) must be located in the same directory.

The **no** form of this command removes the **secondary-image** configuration.

Parameters *file-url* — Specifies the file URL; can be either local (this CPM) or a remote FTP server.

Values

file-url	{*local-url* | *remote-url*} (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

23.87 secondary-ip-address

secondary-ip-address

Syntax **secondary-ip-address** *ipv4-address*
no secondary-ip-address

Context **[Tree]** (config>router>bgp>orr>location secondary-ip-address)

Full Context configure router bgp optimal-route-reflection location secondary-ip-address

Description This command specifies the secondary IP address of a reference location used for BGP optimal route reflection. Up to three IPv4 addresses and three IPv6 addresses can be specified per location.

If the TE DB is unable to find a node in its topology database that matches the primary address, then the TE DB tries to find a node with the matching secondary address. If this attempt also fails, the TE DB then tries to find a node with the matching tertiary address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The IP addresses specified for a location should be topologically “close” to a set of clients that should all receive the same optimal path for that location.

The **no** form of this command removes the secondary IP address information.

Default no secondary-ip-address

Parameters *ipv4-address* — Specifies the secondary IPv4 address of a location, expressed in dotted decimal notation.

Values a.b.c.d

Platforms All

23.88 secondary-ipv6-address

secondary-ipv6-address

Syntax **secondary-ipv6-address** *ipv6-address*
no secondary-ipv6-address

Context **[Tree]** (config>router>bgp>orr>location secondary-ipv6-address)

Full Context configure router bgp optimal-route-reflection location secondary-ipv6-address

Description This command specifies the secondary IPv6 address of a reference location used for BGP optimal route reflection. Up to three IPv4 addresses and three IPv6 addresses can be specified per location.

If the TE DB is unable find a node in its topology database that matches a primary address of the location, then it tries to find a node matching a secondary address. If this attempt also fails, the TE DB tries to find a node matching a tertiary address.

The IP addresses specified for a location should be topologically “close” to a set of clients that should all receive the same optimal path for that location.

The **no** form of this command removes the secondary IPv6 address information.

Default no secondary-ipv6-address

Parameters *ipv6-address* — Specifies the secondary IPv6 address of a location.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.89 secondary-location

secondary-location

Syntax **secondary-location** *file-url*
no secondary-location

Context **[Tree]** (config>system>software-repository secondary-location)

Full Context configure system software-repository secondary-location

Description This command configures the secondary location for the files in the software repository. See the **software-repository** command description for more information.

The **no** form of the command removes the secondary location.

Parameters *file-url* — Specifies the secondary location to be used to access the files in the software repository.

Values

file url	*local-url* | *remote-url*	
local-url	[*cflash-id*/][*file-path*]	200 chars maximum, including cflash-id directory length 99 characters maximum each
remote-url	[{ftp://} *login:pswd@remote-locn*/][*file-path*]	
	243 characters maximum	
	directory length 99 characters maximum each	
	remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
	ipv4-address	*a.b.c.d*
	ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*]
		x:x:x:x:x:x:d.d.d.d[-*interface*]
		x - [0 to FFFF]H
		d - [0 to 255]D
		interface - 32 characters max, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:	

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.90 secondary-nbns

secondary-nbns

Syntax **secondary-nbns** *ip-address*
no secondary-nbns

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dhcp secondary-nbns)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dhcp secondary-nbns)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp secondary-nbns
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range dhcp secondary-nbns

Description This command configures the secondary NBNS address to be returned via DHCP on WLAN-GW ISA.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the secondary NBNS address.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.91 secondary-path

secondary-path

Syntax **secondary-path**

Context **[Tree]** (config>mcast-mgmt>bw-plcy>t2-paths secondary-path)

Full Context configure mcast-management bandwidth-policy t2-paths secondary-path

Description Commands in this context configure secondary path queue parameters. This command overrides the default path limit for the secondary path, which is one of the three ingress multicast paths into the switch fabric.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.92 secondary-ports

secondary-ports

Syntax **secondary-ports**

Context **[Tree]** (config>service>vpls>mac-move secondary-ports)
[Tree] (config>service>template>vpls-template>mac-move secondary-ports)

Full Context configure service template vpls-template mac-move secondary-ports
configure service vpls mac-move secondary-ports

Description This command opens configuration context for defining secondary vpls-ports. VPLS ports that were declared as primary prior to the execution of this command will be moved from primary port-level to secondary port-level. Changing a port to the tertiary level can only be done by first removing it from the primary port-level.

Platforms All

23.93 secondary-retry-limit

secondary-retry-limit

Syntax **secondary-retry-limit** {*number* | **infinite**}
no secondary-retry-limit

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth>use-last-adj-bw secondary-retry-limit)

Full Context configure router mpls lsp auto-bandwidth use-last-adj-bw secondary-retry-limit

Description This command configures the maximum number of retry attempts for secondary paths. After each successful attempt, the counter is reset to zero.

When the specified *number* is reached, no more attempts are made and the path is put into the shutdown state.

A value of 0 or **infinite** means that the system will retry forever.

The **no** form of this command reverts to the default.

Default no secondary-retry-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the number of retries.

Values 0 to 10000

Default 5

infinite — Specifies a retry limit of infinity.

23.94 secondary-shaper-hashing

secondary-shaper-hashing

Syntax [**no**] **secondary-shaper-hashing**

Context **[Tree]** (config>subscr-mgmt>sub-prof secondary-shaper-hashing)

Full Context configure subscriber-mgmt sub-profile secondary-shaper-hashing

Description This command enables LAG secondary shaper ID hashing. With this feature enabled, secondary shaper ID hashing can span multiple forwarding complexes on egress LAG. The default is to perform secondary shaper ID hashing on egress and requires all active LAG members to be on the same forwarding complex.

The **no** form of this command enables the default behavior.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.95 secondary-url

secondary-url

Syntax **secondary-url** *url*
no secondary-url

Context **[Tree]** (config>python>py-script secondary-url)

Full Context configure python python-script secondary-url

Description This command specifies the location of secondary Python script. The system supports three locations for each Python-script. Users can store scripts file on either a local CF card or a FTP server.

The **no** form of this command removes the URL.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **url** — Specifies the secondary URL of the Python script, up to 180 characters, either a local CF card URL or a FTP server URL.

Platforms All

23.96 secret

secret

Syntax **secret** *secret* [**hash** | **hash2** | **custom**]
no secret

Context **[Tree]** (config>router>wpp>portals>portal secret)
[Tree] (config>service>vprn>wpp>portals>portal secret)

Full Context configure router wpp portals portal secret
configure service vprn wpp portals portal secret

Description This command configures the secret that is used by WPPv2 to authenticate the messages between portal and BRAS.

The **no** form of this command removes the secret and hash from the configuration.

Parameters *secret* — Specifies the secret key to access the server, up to 64 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

secret

Syntax **secret** *secret* [**hash** | **hash2** | **custom**]
no secret

Context **[Tree]** (config>router>radius-proxy>server secret)
[Tree] (config>service>vprn>radius-proxy>server secret)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router radius-proxy server secret
configure service vprn radius-proxy server secret

Description This command configures the shared secret key. The RADIUS client must have the same key to communicate with the RADIUS-proxy server.

The **no** form of this command removes the parameters from the configuration.

Parameters **secret** *key* — Specifies the secret key up to 64 characters to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values hash-key: Up to 33 characters
hash2-key: Up to 55 characters.

hash — Specifies that the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

secret

Syntax **secret** *secret-key* | *hash-key* [**hash** | **hash2** | **custom**]
no secret

Context **[Tree]** (config>aaa>isa-radius-plcy>servers>server secret)

Full Context configure aaa isa-radius-policy servers server secret

Description This command configures the secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Default no secret

Parameters **hash** — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.97 section-trace

section-trace

Syntax **section-trace** {**increment-z0** | **byte** *value* | **string** *string*}

Context **[Tree]** (config>port>sonet-sdh section-trace)

Full Context configure port sonet-sdh section-trace

Description This command configures the section trace bytes in the SONET section header to inter-operate with some older versions of ADMs or regenerators that require an incrementing STM ID. You can explicitly configure an incrementing STM value rather than a static one in the SDH overhead by specifying the z0-increment.

This command is supported on TDM satellite.

Default section-trace byte *0x1*

Parameters *increment-z0* — Configures an incrementing STM ID instead of a static value.

value — Sets values in SONET header bytes.

Default 0x1

Values 0 to 255 or 0x00 to 0xFF

string — Specifies a text string that identifies the section. The string can be a maximum of 16 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.98 secure-nd

secure-nd

Syntax [**no**] **secure-nd**

Context **[Tree]** (config>service>ies>if>ipv6 secure-nd)

Full Context configure service ies interface ipv6 secure-nd

Description This command enables Secure Neighbor Discovery (SeND) on the IPv6 interface.

The **no** form of this command reverts to the default and disabled SeND.

Platforms All

secure-nd

Syntax [**no**] **secure-nd**

Context **[Tree]** (config>service>vprn>if>ipv6 secure-nd)

Full Context configure service vprn interface ipv6 secure-nd

Description This command enables Secure Neighbor Discovery (SeND) on the IPv6 interface.

The **no** form of this command reverts to the default and disabled SeND.

Platforms All

secure-nd

Syntax [**no**] **secure-nd**

Context **[Tree]** (config>router>if>ipv6 secure-nd)

Full Context configure router interface ipv6 secure-nd

Description This command enables Secure Neighbor Discovery (SeND) on the IPv6 interface.

The **no** form of this command reverts to the default and disabled SeND.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.99 secure-nd-export

secure-nd-export

Syntax **secure-nd-export**

Context **[Tree]** (admin>certificate secure-nd-export)

Full Context admin certificate secure-nd-export

Description This command exports IPv6 Secure Neighbor Discovery (SeND) certificates to the file cf[1..3]:\system-pki\secureNdKey in PKCS #7 DER format.

Platforms All

23.100 secure-nd-import

secure-nd-import

Syntax **secure-nd-import input** *url-string* **format** *input-format* [**password** *password*] [**key-rollover**]

Context **[Tree]** (admin>certificate secure-nd-import)

Full Context admin certificate secure-nd-import

Description This command imports IPv6 Secure Neighbor Discovery (SeND) certificates from a file, and saves them to cf[1..3]:\system-pki\secureNdKey in PKCS #7 DER format.

Parameters *url-string* — Specifies the name of an input file up to 99 characters.

Values

local-url	<cflash-id>\<file-path>
cflash-id	cf1:| cf2:| cf3:

input-format — Specifies the input file format.

Values pkcs12, pem, or der

password — Specifies the password to decrypt the input file if it is an encrypted PKCS#12 file.

Values 32 characters maximum

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.101 security

security

Syntax **security**

Context **[Tree]** (config>system security)

Full Context configure system security

Description Commands in this context configure a number of central security settings, such as DDoS protection, users, authorization profiles, and certificates. Access to these commands should be restricted to highly trusted users and device administrators.

Platforms All

23.102 security-association

security-association

Syntax **security-association** *security-entry-id* **authentication-key** *hex-string* **encryption-key** *hex-string* **spi** *spi* **transform** *transform-id* **direction** *direction*
no security-association *security-entry-id* **direction** *direction*

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>manual-keying security-association)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>manual-keying security-association)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel>manual-keying security-association)
[Tree] (config>router>if>ipsec>ipsec-tunnel>manual-keying security-association)

Full Context configure router interface ipsec ipsec-tunnel manual-keying security-association
configure service ies interface ipsec ipsec-tunnel manual-keying security-association
configure service vprn interface ipsec ipsec-tunnel manual-keying security-association
configure service vprn interface sap ipsec-tunnel manual-keying security-association

Description This command configures the information required for manual keying SA creation.

The **no** form of this command removes the **security-association** parameters from the configuration.

Parameters *security-entry-id* — Specifies the ID of an SA entry.

Values 1 to 16

authentication-key *hex-string* — Specifies an authentication key.

Values none or 0x0 to 0xFFFFFFFF...(max 128 hex nibbles)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

encryption-key *hex-string* — Specifies the key used for the encryption algorithm.

Values none or 0x0 to 0xFFFFFFFF...(max 64 hex nibbles)

spi *spi* — Specifies the Security Parameter Index (SPI) used to look up the instruction to verify and decrypt the incoming IPsec packets when the direction is inbound. When the direction is outbound, the SPI that will be used in the encoding of the outgoing packets. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.

Values 256 to 16383

transform *transform-id* — Specifies the transform entry that will be used by this SA entry. This object should be specified for all the entries created which are manual SAs. If the value is dynamic, then this value is irrelevant and will be zero.

Values 1 to 2048

direction — Specifies the direction of an IPsec tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel manual-keying security-association

VSR

- configure service vprn interface ipsec ipsec-tunnel manual-keying security-association
- configure router interface ipsec ipsec-tunnel manual-keying security-association
- configure service ies interface ipsec ipsec-tunnel manual-keying security-association

security-association

Syntax **security-association spi** *spi* **authentication-key** *authentication-key* **encryption-key** *encryption-key* [**crypto**]
no security-association spi *spi*

Context **[Tree]** (config>grp-encryp>encryp-keygrp security-association)

Full Context configure group-encryption encryption-keygroup security-association

Description This command is used to create a security association for a specific SPI value in a key group. The command is also used to enter the authentication and encryption key values for the security association, or to delete a security association.

The SPI value used for the security association is a node-wide unique value, meaning that no two security associations in any key group on the node may share the same SPI value.

Keys are entered in clear text. After configuration, they are never displayed in their original, clear text form. Keys are displayed in an encrypted form, which is indicated by the system-appended **crypto** keyword when an **info** or an **admin>save** command is run. For security reasons, keys encrypted on one node are not usable on other nodes (that is, keys are not exchangeable between nodes).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the security association and related key values from the list of security associations for the key group. If the **no** form of the command is attempted using the same SPI value that is configured for **active-outbound-sa**, then a warning is issued and the command is blocked. If the **no** form of the command is attempted on the last SPI in the key group and the key group is configured on a service, then the command is blocked.

Parameters *spi* — Specifies the SPI ID of the SPI being referenced for the security association.

Values 1 to 127

authentication-key — Specifies the authentication key for the SPI, in hexadecimal format. The number of characters in the hexadecimal string must be 64 or 128, depending on whether the authentication algorithm is set to sha256 or sha512, respectively.

encryption-key — Specifies the encryption key for the SPI, in hexadecimal format. The number of characters in the hexadecimal string must be 32 or 64, depending on whether the encryption algorithm is set to aes128 or aes256, respectively.

crypto — Displays the keys showing on the CLI **info** display in an encrypted form.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.103 security-param-index

security-param-index

Syntax **security-param-index** *security-parameter-index*
no security-param-index

Context **[Tree]** (config>test-oam>build-packet>header>ipsec-auth security-param-index)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipsec-auth security-param-index)

Full Context configure test-oam build-packet header ipsec-auth security-param-index
debug oam build-packet packet field-override header ipsec-auth security-param-index

Description This command defines the security index to be used in the IPsec header. This same context can be used for IPv4 and IPv6 packets.

The **no** form of this command removes the security parameter index value.

Default security-param-index 1

Parameters *security-parameter-index* — Specifies the IPsec security parameter index to be used in the IPsec header.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.104 security-parameter

security-parameter

Syntax **security-parameter** *sec*
no security-parameter

Context **[Tree]** (config>service>ies>if>ipv6>secure-nd security-parameter)

Full Context configure service ies interface ipv6 secure-nd security-parameter

Description This command configures the security parameter used in the generation of a Cryptographically Generated Address (CGA).

Parameters *sec* — Specifies the security parameter.

Values 0 to 1

Platforms All

security-parameter

Syntax **security-parameter** *sec*
[**no**] **security-parameter**

Context **[Tree]** (config>service>vprn>if>secure-nd security-parameter)

Full Context configure service vprn interface secure-nd security-parameter

Description This command configures the security parameter used in the generation of a Cryptographically Generated Address (CGA).

Parameters *sec* — Specifies the security parameter.

Values 0 to 1

security-parameter

Syntax **security-parameter** *sec*
no security-parameter

Context **[Tree]** (config>router>if>ipv6>secure-nd security-parameter)

Full Context configure router interface ipv6 secure-nd security-parameter

Description This command configures the security parameter used in the generation of a Cryptographically Generated Address (CGA).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sec* — Specifies the security parameter.

Values 0 to 1

Platforms All

23.105 security-policy

security-policy

Syntax **security-policy** *security-policy-id* [**create**]
no security-policy *security-policy-id*

Context **[Tree]** (config>router>ipsec security-policy)
[Tree] (config>service>vprn>ipsec security-policy)

Full Context configure router ipsec security-policy
configure service vprn ipsec security-policy

Description This command configures a security policy to use for an IPsec tunnel.

The **no** form of this command removes the security policy ID from the configuration.

Parameters *security-policy-id* — specifies a value to be assigned to a security policy.

Values 1 to 32768

create — Keyword used to create the security policy instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn ipsec security-policy

VSR

- configure router ipsec security-policy

security-policy

Syntax **security-policy** *security-policy-id* [**strict-match**]
no security-policy

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel security-policy)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel security-policy)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel security-policy)
[Tree] (config>router>if>ipsec>ipsec-tunnel security-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface ipsec ipsec-tunnel security-policy
configure service ies interface ipsec ipsec-tunnel security-policy
configure service vprn interface ipsec ipsec-tunnel security-policy
configure service vprn interface sap ipsec-tunnel security-policy

Description This command configures an IPsec security policy. The policy may then be associated with static IPsec tunnels defined in the same routing instance.

With **strict-match** parameter enabled, when a CREATE_CHILD exchange request is received for a static IPsec tunnel, and this request is not a re-key request, then ISA matches the received TSi and TSr with the configured security policy. This can be a match only when a received TS (in TSi or TSr) address range matches exactly with the subnet in a security policy entry.

If there is no match, then the setup fails, and TS_UNACCEPTABLE is sent.

If there is a match, but there is an existing CHILD_SA for the matched security policy, then the setup fails, and NO_PROPOSAL_CHOSEN.

If there is a match, and there is not CHILD_SA for the matched entry, then the subnet is sent in the matched security-policy entry as TSi and TSr, and the CHILD_SA is created.

Default no security-policy

Parameters *security-policy-id* — Specifies the IPsec security policy entry that the tunnel will use.

Values 1 to 32768

strict-match — Enables strict match of security-policy entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-tunnel security-policy

VSR

- configure service vprn interface ipsec ipsec-tunnel security-policy
- configure service ies interface ipsec ipsec-tunnel security-policy
- configure router interface ipsec ipsec-tunnel security-policy

23.106 seen-ip-radius-acct-policy

seen-ip-radius-acct-policy

Syntax **seen-ip-radius-acct-policy** *rad-acct-plcy-name*
no seen-ip-radius-acct-policy

Context **[Tree]** (config>app-assure>group>transit-ip-policy>radius seen-ip-radius-acct-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group transit-ip-policy radius seen-ip-radius-acct-policy

Description This command refers to a RADIUS accounting-policy to enable seen-IP notification.

The no form of this command removes the policy.

Default no seen-ip-radius-acct-policy

Parameters *rad-acct-plcy-name* — Specifies the RADIUS accounting policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.107 segment

segment

Syntax **segment** [1..11] [**create**]
no segment

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy>segment-list segment)

Full Context configure router segment-routing sr-policies static-policy segment-list segment

Description This command creates the context to configure a segment inside a segment-list of a statically-defined segment routing policy.

Each segment list can have up to 11 segments.

The **no** form of this command deletes the segment context.

Default no segment

Parameters **create** — Keyword used to create the list.

Platforms All

23.108 segment-list

segment-list

Syntax **segment-list** *segment-list*
no segment-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>saa>test>type-multi-line>lsp-ping>sr-policy segment-list)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy segment-list)

Full Context configure saa test type-multi-line lsp-ping sr-policy segment-list
configure saa test type-multi-line lsp-trace sr-policy segment-list

Description This command configures the segment list ID.

The **no** form of this command removes the configuration.

Parameters *segment-list* — Specifies the segment list number.

Values 1 to 32

Platforms All

segment-list

Syntax **segment-list** [1..32] [**create**]
no segment-list *list*

Context [Tree] (config>router>segment-routing>sr-policies segment-list)
[Tree] (config>router>segment-routing>sr-policies>static-policy segment-list)

Full Context configure router segment-routing sr-policies segment-list
configure router segment-routing sr-policies static-policy segment-list

Description This command creates the context to configure a segment list for the statically-defined segment routing policy.

Up to 32 segment lists are supported per policy.

The **no** form of this command deletes the segment list.

Parameters **create** — Keyword used to create the segment list.

Platforms All

23.109 segment-protection-type

segment-protection-type

Syntax **segment-protection-type** *protection-type*
no segment-protection-type

Context [Tree] (config>router>gmpls>lsp>working-path segment-protection-type)
[Tree] (config>router>gmpls>lsp>protect-path segment-protection-type)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router gmpls lsp protect-path segment-protection-type
configure router gmpls lsp working-path segment-protection-type

Description This command defines the requested segment recovery type for the gLSP path. This is the recovery capability requested by the router UNI-C to the UNI-N for recovery in segments of the optical network between ingress and egress UNI-N nodes.

The **no** form of this command removes the configured segment recovery, reverting to unprotected.

Default segment-protection-type unprotected

Parameters *protection-type* — Specifies the requested GMPLS segment recovery type.

Values unprotected | sbr | gr | sncp | prc

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.110 segment-routing

segment-routing

Syntax **segment-routing**

Context **[Tree]** (config>router>bgp segment-routing)

Full Context configure router bgp segment-routing

Description Commands in this context configure options related to BGP segment routing (prefix SID support).

Platforms All

segment-routing

Syntax **segment-routing**
no segment-routing

Context **[Tree]** (config>router>isis segment-routing)

Full Context configure router isis segment-routing

Description Commands in this context configure segment routing parameters within a given IGP instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Segment routing adds to IS-IS and OSPF routing protocols the ability to perform shortest path routing and source routing using the concept of abstract segment. A segment can represent a local prefix of a node, a specific adjacency of the node (interface or next-hop), a service context, or a specific explicit path over the network. For each segment, the IGP advertises an identifier referred to as Segment ID (SID).

When segment routing is used together with MPLS data plane, the SID is a standard MPLS label. A router forwarding a packet using segment routing will thus push one or more MPLS labels.

Segment routing using MPLS labels can be used in both shortest path routing applications and in traffic engineering applications. This feature implements the shortest path forwarding application.

After segment routing is successfully enabled in the IS-IS or OSPF instance, the router will perform the following operations:

1. Advertise the Segment Routing Capability Sub-TLV to routers in all areas/levels of this IGP instance. However, only neighbors with which it established an adjacency interprets the SID or label range information and use it for calculating the label to swap to or push for a given resolved prefix SID.
2. Advertise the assigned index for each configured node SID in the new prefix SID sub-TLV with the N-flag (node-SID flag) set. Then the segment routing module programs the incoming label map (ILM) with a pop operation for each local node SID in the data path.
3. Assign and advertise automatically an adjacency SID label for each formed adjacency over a network IP interface in the new adjacency SID sub-TLV. The segment routing module programs the incoming label map (ILM) with a pop operation, in effect with a swap to an implicit null label operation, for each advertised adjacency SID.
4. Resolve received prefixes and if a prefix SID sub-TLV exists, the Segment Routing module programs the ILM with a swap operation and also an LTN with a push operation both pointing to the primary/LFA NHLFE. An SR tunnel is also added to the TTM.

When the user enables segment routing in a given IGP instance, the main SPF and LFA SPF are computed normally and the primary next-hop and LFA backup next-hop for a received prefix are added to RTM without the label information advertised in the prefix SID sub-TLV.

Platforms All

segment-routing

Syntax [**no**] **segment-routing**

Context **[Tree]** (config>router>ospf segment-routing)
[Tree] (config>router>ospf3 segment-routing)

Full Context configure router ospf segment-routing
configure router ospf3 segment-routing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure segment routing parameters within an IGP instance.

Segment routing adds to IS-IS, OSPF, or OSPF3 routing protocols the ability to perform shortest path routing and source routing using the concept of abstract segment. A segment can represent a local prefix of a node, a specific adjacency of the node (interface or next hop), a service context, or a specific explicit path over the network. For each segment, the IGP advertises an identifier referred to as a segment ID (SID).

When segment routing is used together with the MPLS data plane, the SID is a standard MPLS label. A router forwarding a packet using segment routing will thus push one or more MPLS labels.

Segment routing using MPLS labels can be used in both shortest path routing applications and traffic engineering applications. This feature implements the shortest path forwarding application.

After segment routing is successfully enabled in the IS-IS, OSPF, or OSPF3 instance, the router will perform the following operations:

- Advertise the Segment Routing Capability sub-TLV to routers in all areas or levels of the IGP instance. However, only neighbors with which the IGP instance established an adjacency will interpret the SID and label range information and use it for calculating the label to swap to or push for a particular resolved prefix SID.
- Advertise the assigned index for each configured node SID in the new prefix SID sub-TLV with the N-flag (node SID flag) set. The segment routing module then programs the incoming label map (ILM) with a pop operation for each local node SID in the data path.
- Automatically assign and advertise an adjacency SID label for each formed adjacency over a network IP interface in the new adjacency SID sub-TLV. The segment routing module programs the incoming label map (ILM) with a pop operation, in effect with a swap to an implicit null label operation, for each advertised adjacency SID.
- Resolve received prefixes, and if a prefix SID sub-TLV exists, the segment routing module programs the ILM with a swap operation and programs an LSP ID to NHLFE (LTN) with a push operation, both pointing to the primary/LFA NHLFE. An SR tunnel is also added to the TTM.

When the user enables segment routing in an IGP instance, the main SPF and LFA SPF are computed normally and the primary next hop and LFA backup next hop for a received prefix are added to the RTM without the label information advertised in the prefix SID sub-TLV.

Platforms All

segment-routing

Syntax **segment-routing**

Context **[Tree]** (config>router segment-routing)

Full Context configure router segment-routing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a context to configure protocol-independent parameters relating to segment routing.

Platforms All

23.111 segment-routing-v6

segment-routing-v6

Syntax [**no**] **segment-routing-v6**

Context **[Tree]** (config>router>segment-routing segment-routing-v6)

Full Context configure router segment-routing segment-routing-v6

Description Commands in this context configure global SRv6 parameters.

The **no** form of this command deletes the context.

Default no segment-routing-v6

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

segment-routing-v6

Syntax [**no**] **segment-routing-v6**

Context **[Tree]** (config>router>isis segment-routing-v6)

Full Context configure router isis segment-routing-v6

Description Commands in this context configure SRv6 parameters specific to this IS-IS instance.

Note: This context has its own **shutdown** command.The **config>router>segment-routing>shutdown** command only applies to SR-MPLS and does not impact this context.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

segment-routing-v6

Syntax [**no**] **segment-routing-v6**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>bgp segment-routing-v6)
[Tree] (config>service>vprn>bgp-ipvpn segment-routing-v6)

Full Context configure router bgp segment-routing-v6
configure service vprn bgp-ipvpn segment-routing-v6

Description Commands in this context configure SRv6 parameters specific to this BGP or BGP-IPVPN instance.

The **no** form of this command deletes the context.

Default no segment-routing-v6

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

segment-routing-v6

Syntax **[no] segment-routing-v6**

Context [Tree] (config>router>bgp>group segment-routing-v6)
[Tree] (config>router>bgp>group>neighbor segment-routing-v6)

Full Context configure router bgp group neighbor segment-routing-v6
configure router bgp group segment-routing-v6

Description Commands in this context configure SRv6 parameters.

The **no** form of this command deletes the context.

Note: When configuring this command at the neighbor level, by default, the neighbor inherits route advertisement options from its BGP peer group. However, after this command is configured, there is no inheritance of any route advertisement options from the group level.

Default no segment-routing-v6

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

segment-routing-v6

Syntax **segment-routing-v6** *instance* [**create**]
no segment-routing-v6 *instance*

Context [Tree] (config>service>vprn segment-routing-v6)

Full Context configure service vprn segment-routing-v6

Description Commands in this context configure the SRv6 instance that is used in the service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the configured SRv6 instance.

Parameters *instance* — Specifies the SRv6 instance number enabled in the service.

Values 1, 2

create — Keyword used to create the SRv6 instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

segment-routing-v6

Syntax **segment-routing-v6** *instance* [**create**]
no segment-routing-v6 *instance*

Context **[Tree]** (config>service>epipe segment-routing-v6)

Full Context configure service epipe segment-routing-v6

Description Commands in this context configure the SRv6 instance that is used in the service.

The **no** form of this command removes the configured SRv6 instance.

Parameters *instance* — Specifies the SRv6 instance number enabled in the service.

Values 1

create — Keyword used to create the SRv6 instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

segment-routing-v6

Syntax **segment-routing-v6** [**bgp** *bgp-instance*] [**srv6-instance** *srv6-instance*] [**default-locator** *name*] [**create**]
no segment-routing-v6 [**bgp** *bgp-instance*]

Context **[Tree]** (config>service>epipe>bgp-evpn segment-routing-v6)

Full Context configure service epipe bgp-evpn segment-routing-v6

Description Commands in this context configure the SRv6 instance that is used in the service.

The **no** form of this command removes the configured SRv6 instance.

Parameters *bgp-instance* — Specifies the SRv6 instance that is configured in the service and associated to an EVPN control plane.

Values 1, 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

srv6-instance — Specifies the SRv6 instance ID that exists in the service and is associated to a BGP EVPN control plane.

Values 1

name — Specifies the locator that exists in the service SRv6 instance and is used as the default locator for the service, up to 64 characters.

create — Keyword used to create the SRv6 instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.112 sel-mcast-advertisement

sel-mcast-advertisement

Syntax [**no**] **sel-mcast-advertisement**

Context **[Tree]** (config>service>vpls>bgp-evpn sel-mcast-advertisement)

Full Context configure service vpls bgp-evpn sel-mcast-advertisement

Description This command enables the advertisement of BGP EVPN Selective Multicast Ethernet Tag (SMET) routes.

The **no** form of this command disables the advertisement of BGP EVPN SMET routes.

Default no sel-mcast-advertisement

Platforms All

23.113 selection-criteria

selection-criteria

Syntax **selection-criteria** [**best-port** | **highest-count** | **highest-weight**] [**slave-to-partner**] [**subgroup-hold-time** *hold-time*]
no selection-criteria

Context **[Tree]** (config>lag selection-criteria)

Full Context configure lag selection-criteria

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies which selection criteria should be used to select the active sub-group. If there is a tie for highest-count or highest-weight, the LAG will prefer the port with the lowest priority. If that does not break the tie, the currently active subgroup will stay active (that is, non-revertive behavior).

The **no** form of this command reverts to the default value.

Default selection-criteria highest-count

Parameters **highest-count** — Selects a sub-group with the highest number of eligible members as an active sub-group (not applicable to “power-off” mode of operations).

highest-weight — Selects a sub-group with the highest aggregate weight as an active subgroup (not applicable to “power-off” mode of operations). Aggregate weight is calculated as the sum of (65535 - port priority) all ports within a sub-group.

best-port — Selects a sub-group containing the port with highest priority port as an active subgroup. In case of equal port priorities, the sub-group containing the port with the lowest port-id is chosen.

slave-to-partner — The **slave-to-partner** keyword specifies that it, together with the selection criteria, should be used to select the active sub-group. An eligible member is a LAG-member link which can potentially become active. This means it is operationally up (not disabled) for use by the remote side. The **slave-to-partner** keyword can be used to control whether or not this latter condition is taken into account.

hold-time — Applicable with LACP enabled. Specifies the optional delay timer for switching to a newly selected active sub-group from the existing active sub-group. The timer delay applies only if the existing sub-group remains operationally up.

Values

not specified	Equivalent to specifying a value of 0. Specifies no delay and to switchover immediately to a new candidate active sub-group.
0 to 2000	Integer specifying the timer value in 10ths of a second.
infinite	Do not switchover from existing active sub-group if the subgroup remains UP. Manual switchover possible using tools perform lag force command.

Platforms All

23.114 selective

selective

Syntax **selective**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>mvpn>provider-tunnel selective)

Full Context configure service vprn mvpn provider-tunnel selective

Description Commands in this context specify selective provider tunnel parameters.

Platforms All

selective

Syntax **selective**

Context [Tree] (config>router>gtm>provider-tunnel selective)

Full Context configure router gtm provider-tunnel selective

Description Commands in this context configure selective provider tunnel parameters.

Platforms All

23.115 selective-label-ip-prioritization

selective-label-ip-prioritization

Syntax [**no**] **selective-label-ip-prioritization**

Context [Tree] (config>router>bgp selective-label-ip-prioritization)

Full Context configure router bgp selective-label-ip-prioritization

Description This command enables selective-label IP prioritization for BGP labeled IPv4 and IPv6 routes.

When this command is configured, every received labeled IPv4 and IPv6 route that is potentially usable by a local service is automatically prioritized for fast control plane reconvergence. When the reachability of a BGP next-hop changes, these labeled IPv4 and IPv6 routes are updated into the route table first, along with other routes manually tagged as high priority by import policies.

A /32 or /128 labeled unicast route (and associated BGP-LU tunnel) is determined to be potentially usable by a local service if one of the following conditions is met:

- the route matches the far-end address of a user-provisioned SDP of an Layer 2 service and the SDP is configured to use BGP tunnels as transport
- the route matches the BGP next-hop address of a BGP-EVPN or IP VPN route, and this VPN route is either imported into a local service or readvertised by the router acting as a next-hop-self route-reflector or a model-B ASBR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables selective-label IP prioritization for BGP.

Default no selective-label-ip-prioritization

Platforms All

23.116 selective-label-ipv4-install

selective-label-ipv4-install

Syntax [**no**] **selective-label-ipv4-install**

Context **[Tree]** (config>router>bgp selective-label-ipv4-install)
[Tree] (config>router>bgp>group selective-label-ipv4-install)
[Tree] (config>router>bgp>group>neighbor selective-label-ipv4-install)

Full Context configure router bgp group neighbor selective-label-ipv4-install
configure router bgp group selective-label-ipv4-install
configure router bgp selective-label-ipv4-install

Description This command enables selective download for BGP label-ipv4 routes.

When this command is configured so that it applies to a BGP session, label-ipv4 routes received on this session are marked as invalid if they are not needed for any eligible service. A /32 label-ipv4 route is determined to be required if one of the following applies:

1. It matches the far-end address of a manually configured or auto-created SDP Layer 2 VLL or VPLS service and the SDP is configured to use BGP tunnels as transport.
2. It matches the IPv4 BGP next hop of a BGP-EVPN route and this EVPN route is either imported into a VPLS service or re-advertised by the router acting as a next-hop-self route-reflector or a model-B ASBR.
3. It matches the IPv4 BGP next hop of a VPN-IPv4 route and this VPN-IP route is either imported into a VPRN service or re-advertised by the router acting as a next-hop-self route-reflector or a model-B ASBR.
4. It matches the IPv4 address in the IPv4-mapped IPv6 address of a VPN IPv6 route and this VPN-IP route is either imported into a VPRN service or re-advertised by the router acting as a next-hop-self route-reflector or a model-B ASBR.

The **no** form of this command at the top (**config>router>bgp**) level disables the selective installation functionality. The **no** form of this command at the **group** or **neighbor** level causes the setting to be inherited from a higher level configuration.

Default no selective-label-ipv4-install

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.117 selective-learned-fdb

selective-learned-fdb

Syntax [**no**] **selective-learned-fdb**

Context **[Tree]** (config>service>vpls selective-learned-fdb)

Full Context configure service vpls selective-learned-fdb

Description This command determines which line cards FDB entries are allocated on for MAC addresses in the VPLS service in which the command is configured.

By default, FDB entries for MAC addresses in VPLS services are allocated on all line cards in the system. Enabling **selective-learned-fdb** causes FDB entries to be allocated only on the line cards on which the service has a configured object, which includes all line cards:

- on which a SAP is configured
- which have ports configured in a LAG SAP
- which have ports configured in an Ethernet tunnel SAP
- which have ports configured on a network interface (which also may be on a LAG) when the service has a mesh or spoke-SDP, VXLAN or EVPN-MPLS configured

Only MAC addresses with a type “L” or “Evpn” in the **show** output displaying the FDB can be allocated selectively, unless a MAC address configured as a conditional static MAC address is learned dynamically on an object other than its monitored object; this can be displayed with type “L” or “Evpn” but is allocated as global because of the conditional static MAC configuration.

The **no** form of this command returns the FDB MAC address entry allocation mode to its default where FDB entries for MAC addresses are allocated on all line cards in the system.

Default no selective-learned-fdb

Platforms All

23.118 send

send

Syntax **send** {**broadcast** | **multicast** | **none** | **version-1** | **both**}
no send

Context **[Tree]** (config>service>vprn>rip send)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>rip>group send)
[Tree] (config>service>vprn>rip>group>neighbor send)
[Tree] (config>service>vprn>ripng send)
[Tree] (config>service>vprn>ripng>group send)
[Tree] (config>service>vprn>ripng>group>neighbor send)

Full Context configure service vprn rip group neighbor send
configure service vprn rip group send
configure service vprn rip send
configure service vprn ripng group neighbor send
configure service vprn ripng group send
configure service vprn ripng send

Description This command configures the type of RIP messages sent to RIP neighbors. This control can be issued at the global, group or interface level. The default behavior sends RIPv2 messages with the multicast (224.0.0.9) destination address.

If **version-1** is specified, the router only listens for and accepts packets sent to the broadcast address.

The **no** form of this command resets the type of messages sent back to the default value.

Default no send

Parameters *broadcast* — Send RIPv2 formatted messages to the broadcast address.

multicast — Send RIPv2 formatted messages to the multicast address.

none — Do not send any RIP messages (i.e. silent listener).

version-1 — Send RIPv1 formatted messages to the broadcast address.

both — Send both RIP v1 & RIP v2 updates to the broadcast address.

Platforms All

send

Syntax **send**

Context [Tree] (config>system>security>keychain>direction>uni send)

Full Context configure system security keychain direction uni send

Description This command specifies the send nodal context to sign TCP segments that are being sent by the router to another device.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

send

Syntax **send** *option-number*
no send

Context **[Tree]** (config>system>security>keychain>tcp-option-number send)

Full Context configure system security keychain tcp-option-number send

Description This command configures the TCP option number accepted in TCP packets sent.

Default send 254

Parameters *option-number* — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.

Values 253, 254, tcp-ao

Platforms All

send

Syntax **send** {**broadcast** | **multicast** | **none** | **version-1**}
no send

Context **[Tree]** (config>router>rip send)
[Tree] (config>router>rip>group send)
[Tree] (config>router>rip>group>neighbor send)

Full Context configure router rip group neighbor send
configure router rip group send
configure router rip send

Description This command specifies the type of RIP messages sent to RIP neighbors.

If **version-1** is specified, the router need only listen for and accept packets sent to the broadcast address.

This control can be issued at the global, group or interface level.

The **no** form of the command reverts to the default value.

Default send version-1

Parameters **broadcast** — Specifies send RIPv2 formatted messages to the broadcast address.

multicast — Specifies send RIPv2 formatted messages to the multicast address.

none — Specifies not to send any RIP messages (i.e. silent listener).

version-1 — Specifies send RIPv1 formatted messages to the broadcast address.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

send

Syntax **send** {**none** | **ripng** | **unicast**}
no send

Context **[Tree]** (config>router>ripng send)
[Tree] (config>router>ripng>group send)
[Tree] (config>router>ripng>group>neighbor send)

Full Context configure router ripng group neighbor send
configure router ripng group send
configure router ripng send

Description This command specifies if RIPng are sent to RIP neighbors or not and what type of IPv6 address is to be used to deliver the messages.

This control can be issued at the global, group or interface level.

The **no** form of the command reverts to the default value.

Default send ripng

Parameters **ripng** — Specifies RIPng messages to be sent to the standard multicast address (FF02::9).

none — Specifies not to send any RIPng messages (i.e. silent listener).

unicast — Specifies to send RIPng updates as unicast messages to the defined unicast address configured through the **unicast-address** command. This option is only allowed within the neighbor context.

Platforms All

23.119 send-accounting-response

send-accounting-response

Syntax [**no**] **send-accounting-response**

Context **[Tree]** (config>router>radius-proxy>server send-accounting-response)
[Tree] (config>service>vprn>radius-proxy>server send-accounting-response)

Full Context configure router radius-proxy server send-accounting-response
configure service vprn radius-proxy server send-accounting-response

Description This command results in the system to always generate RADIUS accounting-response to acknowledge RADIUS accounting-request received from the RADIUS client.

The **no** form of this command disables the command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.120 send-acct-stop-on-fail

send-acct-stop-on-fail

Syntax **send-acct-stop-on-fail** {[**on-request-failure**] [**on-reject**] [**on-accept-failure**]}
no send-acct-stop-on-fail

Context **[Tree]** (config>subscr-mgmt>auth-policy send-acct-stop-on-fail)

Full Context configure subscriber-mgmt authentication-policy send-acct-stop-on-fail

Description This command activates the reporting of RADIUS authentication failures of a PPPoE session to a RADIUS accounting server with an Accounting Stop message.

Three failure categories can be enabled separately:

- **on-request-failure**: All failure conditions between the sending of an Access-Request and the reception of an Access-Accept or Access-Reject.
- **on-reject**:
- **on-accept-failure**: All failure conditions that appear after receiving an Access-Accept and before successful instantiation of the host or session.

The RADIUS accounting policy to be used for sending the Accounting Stop messages must be obtained prior to RADIUS authentication via local user database pre-authentication.

The **no** form of this command reverts to the default.

Parameters **on-request-failure** — Specifies that an accounting stop message is sent when a RADIUS Access-Request message could not be sent (for example, there is no server configured, or timeout).

on-reject — Specifies that an accounting stop message is sent when an Access-Reject is received.

on-accept-failure — Specifies that an accounting stop message is sent a failure occurred after the reception of a RADIUS Access-Accept message (such as a duplicate IP address).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.121 send-bvpls-evpn-flush

send-bvpls-evpn-flush

Syntax [**no**] **send-bvpls-evpn-flush**

Context **[Tree]** (config>service>vpls>pbb send-bvpls-evpn-flush)

Full Context configure service vpls pbb send-bvpls-evpn-flush

Description This command triggers ISID-based C-MAC flush signaling in the PBB-EVPN. When the command is enabled in an I-VPLS service, a B-MAC/ISID route is sent for the I-VPLS ISID.

Default no send-bvpls-evpn-flush

Platforms All

23.122 send-bvpls-flush

send-bvpls-flush

Syntax **send-bvpls-flush** {[**all-but-mine**] [**all-from-me**]}
no send-bvpls-flush

Context **[Tree]** (config>service>vpls>pbb send-bvpls-flush)

Full Context configure service vpls pbb send-bvpls-flush

Description This command enables generation of LDP MAC withdrawal “flush-all-from-me” in the B-VPLS domain when the following triggers occur in the related IVPLS:

- MC-LAG failure
- Failure of a local SAP
- Failure of a local pseudowire/SDP binding

A failure means transition of link SAP/pseudowire to either down or standby status.

This command does not require send-flush-on-failure in B-VPLS to be enabled on an IVPLS trigger to send an MAC flush into the BVPLS.

Default no send-bvpls-flush

Parameters **all-but-mine** — Specifies to send an LDP flush all-but-mine and also sent into the B-VPLS. Both parameters can be set together.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

all-from-me — Specifies to send an LDP flush-all-from and when STP initiates a flush, it is sent into the B-VPLS using LDP MAC flush all-from-me. Both parameters can be set together.

Platforms All

23.123 send-chain

send-chain

Syntax [**no**] **send-chain**

Context **[Tree]** (config>ipsec>cert-profile>entry send-chain)

Full Context configure ipsec cert-profile entry send-chain

Description Commands in this context configure the send-chain in the **cert-profile entry**.

The configuration of this command is optional, by default system will only send the certificate specified by **cert** command in the selected entry to the peer. This command allows system to send additional CA certificates to the peer. These additional CA certificates must be in the certificate chain of the certificate specified by the **cert** command in the same entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

send-chain

Syntax [**no**] **send-chain**

Context **[Tree]** (config>system>security>tls>cert-profile>entry send-chain)

Full Context configure system security tls cert-profile entry send-chain

Description This command enables the sending of certificate authority (CA) certificates, and enters the context to configure send-chain information.

By default, the system only sends the TLS server certificate or TLS client certificate specified by the **cert** command. If CA certificates are to be sent using send-chain, they must be in the chain of certificates specified by the **config**>**system**>**security**>**pki**>**ca-profile** command. The specification of the send-chain is not necessary for a working TLS profile if the TLS peer has the CA certificate used to sign the server or client certificate in its own trust anchor.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For example, given a TLS client running on SR OS, the ROOT CA certificate resides on the TLS server, but the subsequent SUB-CA certificate needed to complete the chain resides within SR OS. The **send-chain** command allows these SUB-CA certificates to be sent from SR OS to the peer to be authenticated using the ROOT CA certificate that resides on the peer.

The **no** form of the command disables the send-chain.

Default no send-chain

Platforms All

23.124 send-count

send-count

Syntax **send-count** *send-count*
no send-count

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy send-count)

Full Context configure saa test type-multi-line lsp-ping sr-policy send-count

Description This command configures the number of messages to send. The *send-count* value is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message *interval* value must be expired before the next message request is sent.

The **no** form of this command reverts to the default value.

Default send-count 1

Parameters *send-count* — Specifies the send count in number of packets.

Values 1 to 100

Default 1

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.125 send-default

send-default

Syntax **send-default** [**ipv4**] [**ipv6**] [**export-policy** *export-policy*]
no send-default

Context **[Tree]** (config>router>bgp send-default)
[Tree] (config>router>bgp>group send-default)
[Tree] (config>router>bgp>group>neighbor send-default)

Full Context configure router bgp group neighbor send-default
configure router bgp group send-default
configure router bgp send-default

Description This command enables the advertisement of a default route. When this command is configured so that it applies to an IBGP or EBGP session, the default route for IPv4 and/or IPv6 is automatically added to the Adj_RIB-OUT of that peer. The advertised defaults are unrelated to any default routes that may be installed in the FIB of the local router.

When the command includes the **ipv4** parameter, an IPv4 default route (0/0) is generated.

When the command includes the **ipv6** parameter, an IPv6 default route (::/0) is generated.

If there is an active default route in the FIB of the local router and a BGP export policy allows that default route to be advertised so it conflicts with the **send-default** command, the artificially generated default overrides the advertisement of the installed default.

The artificially generated default route is not matched by BGP export policies. In order to modify its attributes, a route policy must be created for this purpose and it must be referenced by the **export-policy** parameter. Only the route modifications in the default-action of this policy are parsed and applied.

The **no** form of this command restores the default behavior. At the group and neighbor levels the default behavior is to inherit the configuration from a higher level. At the instance level the default behavior is to not generate nor inject a default route.

Default no send-default

Parameters **ipv4** — Includes the **ipv4** parameter.

ipv6 — Includes the **ipv6** parameter.

export-policy — Specifies the name of a route policy, up to 64 characters. Only the route modifications in the **default-action** context of this route policy are parsed. Those modifications change the attributes of the advertised default route.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.126 send-fib-population-packets

send-fib-population-packets

Syntax **send-fib-population-packets** *mode*
no send-fib-population-packets

Context [Tree] (config>service>ies>sub-if>grp-if>srrp send-fib-population-packets)
[Tree] (config>service>vprn>sub-if>grp-if>srrp send-fib-population-packets)

Full Context configure service ies subscriber-interface group-interface srrp send-fib-population-packets
configure service vprn subscriber-interface group-interface srrp send-fib-population-packets

Description This command configures the mode used to send Fib population packets. When SRRP becomes master it generates gratuitous ARPs (GARPs) used by the Layer 2 access network to populate the correct SRRP gateway.

The **no** form of this command disables sending FDB population packets.

Default send-fib-population-packets all

Parameters *mode* — Specifies on which VLANs the gratuitous ARPs are sent.

Values **all**: Generates, on SSRP master assignment, the GARPs on all VLANs

out-tag-only: Generates, on SRRP master assignment, the GARPs only on SAPs with unique outer VLAN and lowest VLAN tags

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.127 send-flush-on-bvpls-failure

send-flush-on-bvpls-failure

Syntax [**no**] **send-flush-on-bvpls-failure**

Context [Tree] (config>service>vpls>pbb send-flush-on-bvpls-failure)

Full Context configure service vpls pbb send-flush-on-bvpls-failure

Description This command enables the generation in the local I-VPLS of an LDP MAC flush-all-from-me following a failure of SAP/the whole endpoint/spoke-SDP in the related B-VPLS. The failure of mesh-SDP in B-VPLS does not generate the I-VPLS MAC flush.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the generation of LDP MAC flush in I-VPLS on failure of SAP/endpoint/spoke-SDP in the related B-VPLS.

Default no send-flush-on-bvpls-failure

Platforms All

23.128 send-flush-on-failure

send-flush-on-failure

Syntax [**no**] **send-flush-on-failure**

Context **[Tree]** (config>service>vpls send-flush-on-failure)

Full Context configure service vpls send-flush-on-failure

Description This command enables sending out flush-all-from-me messages to all LDP peers included in affected VPLS, in the event of physical port failures or “operationally down” events of individual SAPs. This feature provides an LDP-based mechanism for recovering a physical link failure in a dual-homed connection to a VPLS service. This method provides an alternative to RSTP solutions where dual homing redundancy and recovery, in the case of link failure, is resolved by RSTP running between a PE router and CE devices. If the endpoint is configured within the VPLS and send-flush-on-failure is enabled, flush-all-from-me messages will be sent out only when all spoke-SDPs associated with the endpoint go down.

This feature cannot be enabled on management VPLS.

Default no send-flush-on-failure

Platforms All

23.129 send-idr-after-eap-success

send-idr-after-eap-success

Syntax [**no**] **send-idr-after-eap-success**

Context **[Tree]** (config>ipsec>ike-policy send-idr-after-eap-success)

Full Context configure ipsec ike-policy send-idr-after-eap-success

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the system to add the Identification Responder (IDr) payload in the last IKE authentication response after an Extensible Authentication Protocol (EAP) Success packet is received. When disabled, the system will not include IDr payload.

The **no** form of this command disables sending the IDr payload in the last IKE.

Default send-idr-after-eap-success

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.130 send-imet-ir-on-ndf

send-imet-ir-on-ndf

Syntax **send-imet-ir-on-ndf**
no send-imet-ir-on-ndf

Context **[Tree]** (config>service>vpls>bgp-evpn>vxlan send-imet-ir-on-ndf)

Full Context configure service vpls bgp-evpn vxlan send-imet-ir-on-ndf

Description This command controls the advertisement of Inclusive Multicast Ethernet Tag (IMET) routes for ingress replication in the case where the PE is Non-DF for a specified network interconnect VXLAN virtual ES. When enabled, the router will advertise IMET-IR routes even if the PE is NDF. This attracts BUM traffic but also speeds up convergence in case of DF failure.

The **no** form of this command withdraws the advertisement of the IMET-IR route on the network interconnect VXLAN NDF router.

Default send-imet-ir-on-ndf

Platforms All

23.131 send-orf

send-orf

Syntax **send-orf** [*comm-id*]
no send-orf [*comm-id*]

Context **[Tree]** (config>router>bgp>outbound-route-filtering>extended-community send-orf)
[Tree] (config>router>bgp>group>outbound-route-filtering>extended-community send-orf)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>bgp>group>neighbor>outbound-route-filtering>extended-community send-orf)

Full Context configure router bgp group neighbor outbound-route-filtering extended-community send-orf
configure router bgp group outbound-route-filtering extended-community send-orf
configure router bgp outbound-route-filtering extended-community send-orf

Description This command instructs the router to negotiate the send capability in the BGP outbound route filtering (ORF) negotiation with a peer.

This command also causes the router to send a community filter, prefix filter, or AS path filter configured as an inbound filter on the BGP session to its peer as an ORF Action ADD.

The **no** form of this command causes the router to remove the send capability in the BGP ORF negotiation with a peer.

The **no** form also causes the router to send an ORF remove action for a community filter, prefix filter, or AS path filter configured as an inbound filter on the BGP session to its peer.

If the *comm-id* parameters are not exclusively route target communities then the router will extract appropriate route targets and use those. If, for some reason, the *comm-id* parameters specified contain no route targets, then the router will not send an ORF.

Default no send-orf

Parameters *comm-id* — Specifies up to 32 community policies, which must consist exclusively of route target extended communities. If it is not specified, then the ORF policy is automatically generated from configured route target lists, accepted client route target ORFs and locally configured route targets.

Values [**target:** {*ip-address*:*comm-val* | *2byte-asnumber*:*ext-comm-val* | *4byte-asnumber*:*comm-val*}

where:

- *ip-address* — a.b.c.d
- *comm-val* — 0 to 65535
- *2byte-asnumber* — 0 to 65535
- *ext-comm-val* — 0 to 4294967295
- *4byte-asnumber* — 0 to 4294967295

Platforms All

23.132 send-queries

send-queries

Syntax [**no**] **send-queries**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap>igmp-snooping send-queries)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping send-queries)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping send-queries)
[Tree] (config>service>vpls>sap>mld-snooping send-queries)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping send-queries)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping send-queries)

Full Context configure service vpls mesh-sdp igmp-snooping send-queries
configure service vpls mesh-sdp mld-snooping send-queries
configure service vpls sap igmp-snooping send-queries
configure service vpls sap mld-snooping send-queries
configure service vpls spoke-sdp igmp-snooping send-queries
configure service vpls spoke-sdp mld-snooping send-queries

Description This command specifies whether to send IGMP general query messages on the SAP or SDP.

When send-queries is configured, all type of queries generate ourselves are of the configured version. If a report of a version higher than the configured version is received, the report will get dropped and a new wrong version counter will get incremented. If send-queries is not configured, the version command has no effect. The version used will be the version of the querier. This implies that, for example, when we have a v2 querier, we will never send out a v3 group or group-source specific query when a host wants to leave a certain group.

If **mrouter-port** is enabled on this SAP or spoke SDP, the **send-queries** command parameter cannot be set.

The **no** form of this command disables the IGMP general query messages.

Default no send-queries

Platforms All

send-queries

Syntax [**no**] **send-queries**

Context [Tree] (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp send-queries)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping send-queries

Description This command specifies whether to send IGMP general query messages on the managed SAP. When send-queries is configured, all type of queries generated are of the configured version. If a report of a version higher than the configured version is received, the report will get dropped and a new wrong version counter will get incremented.

If send-queries is not configured, the version command has no effect. The version used on that SAP/SDP is the version of the querier. This implies that, for example, when there is a v2 querier, a v3 group or group-source specific query is never sent when a host wants to leave a certain group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

send-queries

Syntax [**no**] **send-queries**

Context **[Tree]** (config>service>pw-template>igmp-snooping send-queries)

Full Context configure service pw-template igmp-snooping send-queries

Description This command specifies whether to send IGMP general query messages.

When **send-queries** is configured, all type of queries generated are of the configured version. If a report of a version higher than the configured version is received, the report will get dropped and a new wrong version counter will get incremented.

If **send-queries** is not configured, the version command has no effect. The version used on that SAP or SDP will be the version of the querier. This implies that, for example, when we have a v2 querier, we will never send out a v3 group or group-source specific query when a host wants to leave a certain group.

Default no send-queries

Platforms All

23.133 send-refresh

send-refresh

Syntax **send-refresh** *seconds*
no send-refresh

Context **[Tree]** (config>service>vpls>proxy-arp send-refresh)
[Tree] (config>service>vpls>proxy-nd send-refresh)

Full Context configure service vpls proxy-arp send-refresh
configure service vpls proxy-nd send-refresh

Description If enabled, this command will make the system send a refresh at the configured time. A refresh message is an ARP-request message that uses 0s as sender's IP for the case of a proxy-ARP entry. For proxy-ND entries, a refresh is a regular NS message using the chassis-mac as MAC source-address.

Default no send-refresh

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the send-refresh in seconds.

Values 120 to 86400

Platforms All

23.134 send-release

send-release

Syntax [**no**] **send-release**

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>dhcp send-release)
[Tree] (config>service>ies>if>sap>ipsec-gw>dhcp6 send-release)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp send-release)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp6 send-release)

Full Context configure service ies interface sap ipsec-gw dhcp send-release
configure service ies interface sap ipsec-gw dhcp6 send-release
configure service vprn interface sap ipsec-gw dhcp send-release
configure service vprn interface sap ipsec-gw dhcp6 send-release

Description This command enables the system to send a DHCPv4/v6 release message when the IPsec tunnel is removed.

Default no send-release

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.135 send-to-ebgp

send-to-ebgp

Syntax **send-to-ebgp** *family* [*family*]
no send-to-ebgp

Context **[Tree]** (config>service>vprn>bgp>group>link-bandwidth send-to-ebgp)
[Tree] (config>service>vprn>bgp>group>neighbor>link-bandwidth send-to-ebgp)

Full Context configure service vprn bgp group link-bandwidth send-to-ebgp
configure service vprn bgp group neighbor link-bandwidth send-to-ebgp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures BGP to allow link-bandwidth extended community to be sent in routes advertised to EBGP peers in the scope of the command, as long the routes belong to one of the listed address families.

The link-bandwidth extended community is encoded as a non-transitive type. This means that by default it should not be attached to any route advertised to an EBGP peer and it should be discarded when received in any route from an EBGP peer. This command overrides the standard behavior.

Up to three families may be configured.

The **no** form of this command restores the default behavior of stripping the link-bandwidth extended community from any route advertised to an EBGP peer.

Default no send-to-ebgp

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

Platforms All

send-to-ebgp

Syntax **send-to-ebgp** *family* [*family*]
no send-to-ebgp

Context **[Tree]** (config>router>bgp>group>link-bandwidth send-to-ebgp)
[Tree] (config>router>bgp>group>neighbor>link-bandwidth send-to-ebgp)

Full Context configure router bgp group link-bandwidth send-to-ebgp
configure router bgp group neighbor link-bandwidth send-to-ebgp

Description This command configures BGP to allow link-bandwidth extended community to be sent in routes advertised to EBGP peers in the scope of the command, as long the routes belong to one of the listed address families.

The link-bandwidth extended community is encoded as a non-transitive type. This means that by default it should not be attached to any route advertised to an EBGP peer and it should be discarded when received in any route from an EBGP peer. This command overrides the standard behavior.

Up to six families may be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command restores the default behavior of stripping the link-bandwidth extended community from any route advertised to an EBGP peer.

Default no send-to-ebgp

Parameters *family* — Specifies the address families for which receiving the link-bandwidth extended community from EBGP peers should be supported.

Values ipv4 — Adds a link-bandwidth extended community to unlabeled unicast IPv4 routes.

label-ipv4 — Adds a link-bandwidth extended community to labeled-unicast IPv4 routes.

vpn-ipv4 — Adds a link-bandwidth extended community to IPv4 VPN (SAFI 128) routes.

ipv6 — Adds a link-bandwidth extended community to unlabeled unicast IPv6 routes.

label-ipv6 — Adds a link-bandwidth extended community to labeled-unicast IPv6 routes.

vpn-ipv6 — Adds a link-bandwidth extended community to IPv6 VPN (SAFI 128) routes.

Platforms All

23.136 send-tunnel-encap

send-tunnel-encap

Syntax **send-tunnel-encap** [**mpls**] [**mplsoudp**]
no send-tunnel-encap

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls send-tunnel-encap)
[Tree] (config>service>vpls>bgp-evpn>mpls send-tunnel-encap)
[Tree] (config>service>vprn>bgp-evpn>mpls send-tunnel-encap)
[Tree] (config>service>epipe>bgp-evpn>vxlan send-tunnel-encap)
[Tree] (config>service>vpls>bgp-evpn>vxlan send-tunnel-encap)

Full Context configure service epipe bgp-evpn mpls send-tunnel-encap
configure service epipe bgp-evpn vxlan send-tunnel-encap
configure service vpls bgp-evpn mpls send-tunnel-encap
configure service vpls bgp-evpn vxlan send-tunnel-encap
configure service vprn bgp-evpn mpls send-tunnel-encap

Description This command configures the encapsulation to be advertised with the EVPN routes for the service. The encapsulation is encoded in RFC5512-based tunnel encapsulation extended communities.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When used in the **bgp-evpn**>**mpls** context, the supported options are none (**no send-tunnel-encap**), **mpls**, **mplsoudp** or both.

When used in the **bgp-evpn**>**vxlan** context, the supported options are **send-tunnel-encap** (the router signals a VXLAN value) or **no send-tunnel-encap** (no encapsulation extended community is sent).

Default send-tunnel-encap mpls (in the **config**>**service**>**vpls**>**bgp-evpn**>**mpls** context)

send-tunnel-encap (in the **config**>**service**>**vpls**>**bgp-evpn**>**vxlan** context)

Parameters **mpls** — Specifies the MPLS-over-UDP encapsulation value in the RFC5512 encapsulation extended community.

mplsoudp — Specifies the MPLS encapsulation value in the RFC5512 encapsulation extended community.

Platforms All

23.137 sender-id

sender-id

Syntax **sender-id local** *local-name*
sender-id system
no sender-id

Context **[Tree]** (config>eth-cfm>system sender-id)

Full Context configure eth-cfm system sender-id

Description This command allows the operator to include the configured “system name” (chassis3) or a locally configured value in ETH-CFM PDUs sent from MEPs and MIPs. The operator may only choose one of these options to use for ETH-CFM. MEPs include the **sender-id** TLV for CCM (not sub second CCM enabled MEPs), LBM/LBR, and LTM/LTR. MIPs include this value in the LBR and LTR PDUs.

Note: LBR functions reflect all TLVs received in the LBM unchanged, including the SenderID TLV.

Parameters *local-name* — Specifies a local alphanumeric string different from the “system name” chassis(3) value that can be used for other means, up to 45 characters.

system — Allows ETH-CFM to use the configured “system name” value as the chassis(3).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.138 sensor-group

sensor-group

Syntax **sensor-group** *name* [**create**]
no sensor-group *name*

Context **[Tree]** (config>system>telemetry>sensor-groups sensor-group)

Full Context configure system telemetry sensor-groups sensor-group

Description Commands in this context configure sensor-related commands.

The **no** form of this command removes the configuration.

Parameters *name* — Specifies the sensor group name, up to 32 characters.

create — Keyword used to create a sensor group.

Platforms All

sensor-group

Syntax **sensor-group** *name*
no sensor-group

Context **[Tree]** (config>system>telemetry>persistent-subscriptions>subscription sensor-group)

Full Context configure system telemetry persistent-subscriptions subscription sensor-group

Description This command assigns an existing sensor group to the specified persistent subscription. If no valid paths exist in the sensor group, the configuration is accepted; however, no gRPC connection is established when persistent subscription is activated.

The **no** form of this command removes the configuration.

Parameters *name* — Specifies the sensor group name, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.139 sensor-groups

sensor-groups

Syntax **sensor-groups**

Context **[Tree]** (config>system>telemetry sensor-groups)

Full Context configure system telemetry sensor-groups

Description Commands in this context configure a sensor group.

Platforms All

23.140 sequence-group

sequence-group

Syntax **sequence-group** *group*
no sequence-group

Context **[Tree]** (config>li>x-interfaces>lics>lic>authentication sequence-group)

Full Context configure li x-interfaces lics lic authentication sequence-group

Description This command configures the sequence group for the X1 and X2 interfaces.

The **no** form of this command reverts to the default.

Parameters *group* — Specifies the group number.

Values 2 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.141 serial-notify

serial-notify

Syntax [**no**] **serial-notify**

Context **[Tree]** (debug>router>rpki-session>packet serial-notify)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router rpki-session packet serial-notify

Description This command enables debugging for serial notify RPKI packets.

The **no** form of this command disables debugging for serial notify RPKI packets.

Platforms All

23.142 serial-query

serial-query

Syntax [**no**] **serial-query**

Context **[Tree]** (debug>router>rpki-session>packet serial-query)

Full Context debug router rpki-session packet serial-query

Description This command enables debugging for serial query RPKI packets.

The **no** form of this command disables debugging for serial query RPKI packets.

Platforms All

23.143 server

server

Syntax **radius-accounting-server**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>server server)

Full Context configure subscriber-mgmt radius-accounting-policy radius-accounting-server server

Description Commands in this context define RADIUS server attributes under a given session authentication policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**port** *port-num*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[**coa-only**] [**pending-requests-limit** *limit*]
no server *index*

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server server)

Full Context configure subscriber-mgmt authentication-policy radius-authentication-server server

Description This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to sixteen RADIUS servers can be configured at any one time in a RADIUS authentication policy. Only five can be used for authentication, all other servers should be configured as coa-only servers. RADIUS servers are accessed in order from lowest to highest index for authentication or accounting requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.

The **no** form of this command removes the server index from the configuration.

Parameters *server-index* — Specifies the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 16 (a maximum of 5 authentication servers)

ip-address — Specifies the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

key — Specifies the secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values secret-key: Up to 20 characters.
hash-key: Up to 33 characters.
hash2-ke: Up to 55 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

port-num — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

coa-only — Specifies Change-of-Authorization Messages only. Servers that are marked with the coa-only flag will not be used for authentication, but they is able to accept RADIUS CoA messages, independent of the accept-authorization-change setting in the authentication policy.

For authentication purposes, the maximum number of servers is 5. All other servers may only be used as coa-only servers.

limit — Specifies the maximum number of outstanding RADIUS authentication requests for this authentication server.

Values 1 to 4096

Default The default value when not configured is 4096

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *ip-address*
no server

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host server)

Full Context configure subscriber-mgmt local-user-db ipoe host server

Description This command configures the IP address of the DHCP server to relay to.

The configured DHCP server IP address must reference one of the addresses configured under the DHCP CLI context of an IES/VPRN subscriber or group interface.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IP address of the DHCP server.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *ip-address*
no server

Context **[Tree]** (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay server)

Full Context configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay server

Description This command configures the IPv6 address of the DHCP6 server to relay to.

The configured DHCP6 server IPv6 address must reference one of the addresses configured under the DHCP6 CLI context of an IES/VPRN subscriber or group interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies up to eight IPv6 addresses of the DHCP6 server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** [**service** *service-id*] **name** *server-name*
no server

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>match-radprox-cache server)

Full Context configure subscriber-mgmt local-user-db ipoe host match-radius-proxy-cache server

Description This command specifies the name of radius-proxy-server and optionally id of the service that the radius-proxy-server resides in.

The **no** form of this command removes the parameters from the configuration.

Parameters **service** *service-id* — Specifies the ID or name of the service.

Values 1 to 214748365
svc-name up to 64 char maximum

name *server-name* — Specifies the name of radius-proxy-server up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *ipv6z-address* [*ipv6z-address*]
no server [*ipv6z-address*]

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6 server)

Full Context configure service ies interface ipv6 dhcp6 server

Description This command specifies a list of servers where DHCP6 requests are forwarded. The list of servers can be entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP6 relay to work. If there are multiple servers then the request is forwarded to all servers in the list.

The **no** form of this command reverts to the default.

Parameters *ipv6z-address* — Specifies up to eight non-global IPv4 addresses including a zone index as defined by the InetAddressIPv4z textual convention.

Values
ipv6z-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

server

Syntax **server** *server1* [*server2*]

Context **[Tree]** (config>service>ies>if>dhcp server)
[Tree] (config>service>vprn>if>dhcp server)
[Tree] (config>service>ies>sub-if>grp-if>dhcp server)

Full Context configure service ies interface dhcp server
configure service ies subscriber-interface group-interface dhcp server
configure service vprn interface dhcp server

Description This command specifies a list of servers where requests are forwarded. The list of servers can be entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP relay to work. If there are multiple servers then the request is forwarded to all servers in the list.

There can be a maximum of 8 DHCP servers configured.

The **no** form of this command reverts to the default.

Parameters *server* — Specifies up to eight DHCP server IP addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface dhcp server

All

- configure service vprn interface dhcp server
- configure service ies interface dhcp server

server

Syntax **server** *server-name*
no server

Context **[Tree]** (config>service>ies>sub-if>grp-if>local-address-assignment server)
[Tree] (config>service>ies>sub-if>local-address-assignment server)
[Tree] (config>service>vprn>sub-if>grp-if>local-address-assignment server)
[Tree] (config>service>vprn>sub-if>local-address-assignment server)

Full Context configure service ies subscriber-interface group-interface local-address-assignment server
configure service ies subscriber-interface local-address-assignment server

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface local-address-assignment server
configure service vprn subscriber-interface local-address-assignment server

Description This command designates a local DHCPv4 server for local pools management where IPv4 addresses for PPPoXv4 clients are allocated without the need for the internal DHCP relay-agent. Those addresses are tied to PPPoX sessions and they are de-allocated when the PPPoX session is terminated.

Parameters *server-name* — Specifies the name of the local DHCP server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**port** *port*] [**create**]
no server *server-index*

Context **[Tree]** (config>aaa>l2tp-acct-plcy>radius-acct-server server)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server server

Description This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.

The **no** form of this command removes the server from the configuration.

Parameters *server-index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 16 (a maximum of 5 accounting servers)

address ip-address — The IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

secret *key* — The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values secret-key — A string up to 20 characters.
hash-key — A string up to 33 characters.
hash2-key — A string up to 55 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

custom — Specifies the custom encryption to management interface.

port — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**port** *port*] [**create**]
no server *server-index*

Context **[Tree]** (config>app-assure>rad-acct-plcy>server server)

Full Context configure application-assurance radius-accounting-policy radius-accounting-server server

Description This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.

The **no** form of this command removes the server from the configuration.

Parameters *server-index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 16 (a maximum of 5 accounting servers)

ip-address — The IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

secret *key* — The secret key to access the RADIUS server. This secret key must match the password on the RADIUS server.

Values secret-key — A string up to 20 characters
hash-key — A string up to 33 characters

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2-key — A string up to 55 characters

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

port — Specifies the UDP port number on which to contact the RADIUS server for authentication.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *server-name*
no server

Context **[Tree]** (config>service>ies>sub-if>grp-if>lcl-addr-assign>ipv6 server)
[Tree] (config>service>vprn>sub-if>grp-if>lcl-addr-assign>ipv6 server)

Full Context configure service ies subscriber-interface group-interface local-address-assignment ipv6 server
configure service vprn subscriber-interface group-interface local-address-assignment ipv6 server

Description This command designates a local router DHCPv6 server for local pools management where IPv6 prefixes or address for PPPoXv6 clients or IPoEv6 clients are allocated without the need for the internal router DHCP relay-agent. Those addresses are tied to PPPoX or IPoE sessions and they are de-allocated when the PPPoX or IPoE session is terminated.

Parameters *server-name* — The name of the local router DHCPv6 server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *server-index* **name** *server-name*
no server *server-index*

Context **[Tree]** (config>aaa>radius-srv-plcy>servers server)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa radius-server-policy servers server

Description This command adds a RADIUS server.

The **no** form of this command removes a RADIUS server.

Parameters *index* — Specifies the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 5

server-name — Specifies the server name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *server-name* [**address** *ip-address*] [**secret** *key*] [**hash** | **hash2**| **custom**] [**create**]
no server *server-name*

Context **[Tree]** (config>router>radius-server server)
[Tree] (config>service>vprn>radius-server server)

Full Context configure router radius-server server
configure service vprn radius-server server

Description This command either specifies an external RADIUS server in the corresponding routing instance or enters configuration context of an existing server. The configured server could be referenced in the radius-server-policy.

The **no** form of this command removes the parameters from the server configuration.

Parameters *server-name* — Specifies the name of the external RADIUS server.

ip-address — Specifies the IPv4 or IPv6 IP address of the external RADIUS server.

key — Specifies the shared secret key of the external RADIUS server, up to 64 characters.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

server

Syntax **server** *server-name* [**create**] [**purpose** {[**accounting** | **authentication**]}] [**wlan-gw-group** *group-id*]
no server *server-name*

Context **[Tree]** (config>router>radius-proxy server)
[Tree] (config>service>vprn>radius-proxy server)

Full Context configure router radius-proxy server
configure service vprn radius-proxy server

Description This command creates a RADIUS-proxy server in the corresponding routing instance. The proxy server can be configured for the purpose of proxying authentication or accounting or both.

If a WLAN-GW ISA group is specified, then the RADIUS proxy server is instantiated on the set of ISAs in the specified wlan-gw group. The RADIUS messages from the AP are load-balanced to these ISAs. The ISA that processes the RADIUS message then hashes this message to the ISA that anchors the UE. The hash is based on UE MAC address (required to be present in the calling-station-id attribute) in the RADIUS message.

If the **create** parameter is not specified, then this command enters configuration context of the specified RADIUS-proxy server.

The **no** form of this command removes the server-name and parameters from the radius-proxy configuration.

Parameters *server-name* — Specifies the name of the RADIUS-proxy server.

create — Specifies that the system will create the specified RADIUS-proxy server.

purpose — Specifies the purpose the RADIUS-proxy server.

Values accounting — proxy accounting packets
authentication — proxy authentication packets

group-id — Specifies the WLAN-GW ISA group.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *ipv6-address* [*ipv6-address*]
no server [*ipv6-address* [*ipv6-address*]]

Context **[Tree]** (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client server)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client server)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client server
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client server

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This specifies the DHCPv6 servers that are used for requesting addresses.

The **no** form of this command removes the server. This cannot be executed while any DHCPv6 client application is not shut down.

Parameters *ipv6-address* — Specifies up to 8 unicast IPv6 addresses of a DHCP6 server.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *xmpp-server-name* [**domain-name** *fqdn*] [**username** *user-name*] [**password** *password*] [**create**] [**service-name** *service-name*]
server *xmpp-server-name* [**domain-name** *fqdn*] [**username** *user-name*] [**password** *password*] [**create**] [**router** *router-instance*]
no server *xmpp-server-name*

Context **[Tree]** (config>system>xmpp server)

Full Context configure system xmpp server

Description This command configures the XMPP server as well as the Jabber ID that the 7750 SR, 7450 ESS, or 7950 XRS will use for the XMPP communication with the server. The system uses DNS to resolve the configured domain-name.

no server *name* will remove all the dynamic configurations in all the services.

Parameters *xmpp-server-name* — Specifies the name of the server in lower-case letters.

fqdn — Specifies the Fully Qualified Domain Name of the server.

user-name — Specifies the user-name part of the Jabber ID.

password — Specifies the password part of the Jabber ID's user.

create — Keyword used to create the server instance.

router-instance — Specifies the router name or service ID used to identify the router instance.

Values

router-instance: *router-name* or *vprn-svc-id*

router-name	"Base", "management"
vprn-svc-id	1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**tls-client-profile** *profile*]
no server *index*

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius server)

Full Context configure service vprn aaa remote-servers radius server

Description This command adds a RADIUS server and configures the IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. For authentication requests, RADIUS servers are accessed in order from lowest to highest index until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

The **no** form of this command removes the server from the configuration.

Default no server

Parameters *index* — Specifies the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 5

ip-address — Specifies the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D

key — Specifies the secret key, up to 64 characters, that must match the password on the RADIUS server.

Values Up to 64 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

profile — Specifies the TLS profile name, up to 32 characters, for the RADIUS server.

Platforms All

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [{**hash** | **hash2** | **custom**}] [**port** *port*]
no server *index*

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus server)

Full Context configure service vprn aaa remote-servers tacplus server

Description This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.

Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.

The **no** form of this command removes the server from the configuration.

Default No TACACS+ servers are configured.

Parameters *index* — Specifies the index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.

Values 1 to 5

ip-address — Specifies the IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

key — Specifies the secret key, up to 128 characters, for access to the TACACS+ server. This secret key must match the password on the TACACS+ server.

Values Up to 128 characters in length.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

port — Specifies the port ID.

Values 0 to 65535

Platforms All

server

Syntax **server** *ipv6-address* [*ipv6-address*]
no server

Context **[Tree]** (config>service>vprn>router-advert>dns-options server)
[Tree] (config>service>vprn>router-advert>if>dns-options server)

Full Context configure service vprn router-advertisement dns-options server
configure service vprn router-advertisement interface dns-options server

Description This command specifies the IPv6 DNS servers to include in the RDNSS option in Router Advertisements. When specified at the router advertisement level this applies to all interfaces that have **include-dns** enabled, unless the interfaces have more specific **dns-options** configured.

Parameters *ipv6-address* — Specifies the IPv6 address of the DNS server(s), up to a maximum of four, specified as eight 16-bit hexadecimal pieces.

Platforms All

server

Syntax **server** *ip-address*[**:***port*] [**create**]
no server *ip-address*[**:***port*]

Context **[Tree]** (config>app-assure>group>url-filter>icap server)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group url-filter icap server

Description This command configures the IP address and server port of the ICAP server.

Parameters *ip-address[:port]* — Specifies the ICAP server IP address and port.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *ip-address* [*ip-address*] **router** *router-instance*
server *ip-address* [*ip-address*] **service-name** *service-name*
no server

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>dhcp server)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp server)

Full Context configure service ies interface sap ipsec-gw dhcp server
configure service vprn interface sap ipsec-gw dhcp server

Description This command specifies up to eight DHCPv4 server addresses for DHCPv4-based address assignment. If multiple server addresses are specified, the first advertised DHCPv6 address received is chosen.

Default no server

Parameters *ip-address* — Specifies up to eight unicast IPv4 addresses.

Values

ipv4-address	a.b.c.d

router-instance — Specifies the router instance ID used to reach the configured server address.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **server** *ip-address* **service-name** *service-name* variant can be used in all configuration modes.

Values {router-name | *vprn-svc-id*}

vprn-svc-id:	1 to 2147483647
router-name:	*router-name* is an alias for input only. The *router-name* gets replaced with an id automatically by SR OS in the configuration).

Default Base

service-name — Specifies the name of the IES or VPRN service used to reach the configured server address, up to 64 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** *ipv6-address* [*ipv6-address*] **router** *router-instance*
server *ipv6-address* [*ipv6-address*] **service-name** *service-name*
no server

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw>dhcp6 server)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp6 server)

Full Context configure service ies interface sap ipsec-gw dhcp6 server
configure service vprn interface sap ipsec-gw dhcp6 server

Description This command specifies up to eight DHCPv6 server addresses for DHCPv6-based address assignment. If multiple server addresses are specified, the first advertised DHCPv6 address received is chosen.

Default no server

Parameters *ipv6-address* — Specifies up to eight unicast global unicast IPv6 addresses.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

router-instance — Specifies the router instance ID used to reach the configured server address.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **server** *ip-address* **service-name** *service-name* variant can be used in all configuration modes.

Values {router-name | *vprn-svc-id*}

vprn-svc-id:	1 to 2147483647
router-name:	*router-name* is an alias for input only. The *router-name* gets replaced with an id automatically by SR OS in the configuration).

Default Base

service-name — Specifies the name of the IES or VPRN service used to reach the configured server address, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

server

Syntax **server** *server-index* [**create**]
no server *server-index*

Context **[Tree]** (config>aaa>isa-radius-plcy>servers server)

Full Context configure aaa isa-radius-policy servers server

Description This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried.

The **no** form of the command removes the server from the configuration.

Default none

Parameters *server-index* — The index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 10 (a maximum of 5 accounting servers)

create — Keyword used to create the server index.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server**

Context **[Tree]** (config>test-oam>twamp server)

Full Context configure test-oam twamp server

Description This command configures the node for TWAMP server functionality.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

server

Syntax **server** *server* [*server*]

Context **[Tree]** (config>router>if>dhcp server)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router interface dhcp server

Description This command specifies a list of servers where requests will be forwarded. The list of servers can be entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP relay to work. If there are multiple servers then the request is forwarded to all of the servers in the list. There can be a maximum of eight DHCP servers configured.

The flood command is applicable only in the VPLS case. There is a scenario with VPLS where the VPLS node only wants to add Option 82 information to the DHCP request to provider per-subscriber information, but it does not do full DHCP relay. In this case, the server is set to "flood". This means the DHCP request is still a broadcast and is sent through the VPLS domain. A node running at Layer 3 further upstream then can perform the full Layer 3 DHCP relay function.

Default no server

Parameters *server* — Specifies the DHCP server IP address. A maximum of eight servers can be specified in a single statement.

Platforms All

server

Syntax **server** *ipv6-address* [*ipv6-address*]
no server

Context **[Tree]** (config>router>router-advert>dns-options server)
[Tree] (config>router>router-advert>if>dns-options server)

Full Context configure router router-advertisement dns-options server
configure router router-advertisement interface dns-options server

Description This command specifies the IPv6 DNS servers to include in the RDNSS option in Router Advertisements. When specified at the router advertisement level this applies to all interfaces that have **include-dns** enabled, unless the interfaces have more specific **dns-options** configured.

Parameters *ipv6-address* — Specifies the IPv6 address of the DNS servers as eight 16-bit hexadecimal pieces. A maximum of four ipv6 addresses can be specified in a single statement.

Platforms All

server

Syntax **server** *pcp-server-name* [**create**]
no server *pcp-server-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>pcp-server server)

Full Context configure router pcp-server server

Description Commands in this context configure a PCP server.

The **no** form of this command deletes the specified PCP server.

Parameters *pcp-server-name* — Specifies the PCP server name, up to 32 characters.

create — Creates a PCP server before entering the context to configure it.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server

Syntax **server** [**router** *router-instance* | **service-name** *service-name*] {*ip-address* | *ipv6-address* | **ptp**} [**key-id** *key-id*] [**version** *version*] [**prefer**]
no server [**router** *router-instance* | **service-name** *service-name*] {*ip address* | *ipv6-address* | **ptp**}

Context [Tree] (config>system>time>ntp server)

Full Context configure system time ntp server

Description This command configures the node to operate in client mode with the NTP server specified in the address field of this command.

If the internal PTP process is to be used as a source of time for System Time and OAM time then it must be specified as a server for NTP. If PTP is specified, then the prefer parameter must also be specified. After PTP has established a UTC traceable time from an external grandmaster then it will always be the source for time into NTP, even if PTP goes into time holdover. PTP applies only to the 7450 ESS and 7750 SR.

Use of the internal PTP time source for NTP will promote the internal NTP server to stratum 1 level, which may impact the NTP network topology.

The **no** form of this command removes the server with the specified address from the configuration.

Parameters *router-instance* — Specifies the routing context that contains the interface in the form of *router-name* or *service-id*.

Values *router-name* — Base | Management
service-id — 1 to 2147483647

Default Base

service name — Specifies the service name for the VPRN. The name can be up to 64 characters. CPM routing instances are not supported.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address — Configures the IPv4 address of an external NTP server.

Values a.b.c.d

Default None

ipv6-address — Configures the IPv6 address of an external NTP server.

Values
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF] H
- d: [0 to 255] D

Default None

key-id — Specifies the key ID that identifies the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP server. If an NTP packet is received by this node, the authentication key-id, type, and key value must be valid, otherwise the packet will be rejected and an event/trap generated. This is an optional parameter.

Values 1 to 255

version — Configures the NTP version number that is expected by this node. This is an optional parameter.

Values 2 to 4

Default 4

ptp — Configures the internal PTP process as a time server into the NTP process. The **prefer** parameter is mandatory with this server option.

prefer — Specifies that, when configuring more than one peer, one remote system can be configured as the preferred peer. When a second peer is configured as preferred, then the new entry overrides the old entry.

Platforms All

server

Syntax **server**

Context **[Tree]** (config>system>security>ssh>key-re-exchange server)

Full Context configure system security ssh key-re-exchange server

Description This command enables the key re-exchange context for the SSH server.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**tls-client-profile** *profile*]
no server *index*

Context **[Tree]** (config>system>security>radius server)

Full Context configure system security radius server

Description This command adds a RADIUS server and configures the IP address, index, and key values.

Up to five RADIUS servers can be configured at any one time. For authentication requests, RADIUS servers are accessed in order from the lowest to highest index until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

The **no** form of this command removes the server from the configuration.

Default no server

Parameters *index* — Specifies the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 5

ip-address — Specifies the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D

key — Specifies the secret key to access the RADIUS server, up to 64 characters. This secret key must match the password on the RADIUS server.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

tls-client-profile — Specifies the TLS profile for the RADIUS server.

profile — Specifies the TLS profile name, up to 32 characters.

Platforms All

server

Syntax **server** *index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**port** *port*]
no server *index*

Context **[Tree]** (config>system>security>tacplus server)

Full Context configure system security tacplus server

Description This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.

Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.

The **no** form of this command removes the server from the configuration.

Parameters *index* — Specifies the index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.

Values 1 to 5

ip-address — Specifies the IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D

key — Specifies the secret key, up to 128 characters, to access the TACACS+ server. This secret key must match the password on the TACACS+ server.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

port — Specifies the port ID.

Values 0 to 65535

Platforms All

server

Syntax **server** *server-index* [**create**]
no server *server-index*

Context **[Tree]** (config>system>security>ldap server)

Full Context configure system security ldap server

Description This command configures an LDAP server. Up to five servers can be configured, which can then work in a redundant manner.

The **no** version of this command removes the server connection.

Parameters *server-index* — Specifies a unique LDAP server connection.

Values 1 to 5

Platforms All

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2** | **custom**] [**auth-port** *auth-port*] [**acct-port** *acct-port*] [**type** *server-type*]

Context **[Tree]** (config>system>security>dot1x>radius-plcy server)

Full Context configure system security dot1x radius-plcy server

Description This command adds a Dot1x server and configures the Dot1x server IP address, index, and key values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Up to five Dot1x servers can be configured at any one time. Dot1x servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other Dot1x servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

The **no** form of this command removes the server from the configuration.

Default no server

Parameters *server-index* — Specifies the index for the Dot1x server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index.

Values 1 to 5

ip-address — Specifies the IP address of the Dot1x server. Two Dot1x servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

key — Specifies the secret key, up to 128 characters, to access the Dot1x server. This secret key must match the password on the Dot1x server.

hash — Specifies the key is entered in an encrypted form. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

custom — Specifies the custom encryption to management interface.

acct-port — Specifies the UDP port number on which to contact the RADIUS server for accounting requests.

auth-port — Specifies a UDP port number to be used as a match criteria.

Values 1 to 65535

server-type — Specifies the server type.

Values authorization, accounting, combined

Platforms All

server

Syntax [**no**] **server** *ip-address* [*ip-address*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>dhcp>offer-selection server)
[Tree] (config>service>vprn>sub-if>dhcp>offer-selection server)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>offer-selection server)

Full Context configure service ies subscriber-interface group-interface dhcp offer-selection server
configure service vprn subscriber-interface dhcp offer-selection server
configure service vprn subscriber-interface group-interface dhcp offer-selection server

Description This command configures a DHCPv4 server destination for which a discover delay must be configured. Up to eight DHCPv4 server destinations can be configured.

The **no** form of this command removes the DHCPv4 server destination.

Parameters *ip-address* — Specifies the IPv4 address of the DHCP server, in dotted notation a.b.c.d.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

server

Syntax [**no**] **server** *ipv6-address* [*ipv6-address*]

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection server)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>advertise-selection server)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection server)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection server

Description This command configures a DHCPv6 server destination for which a solicit delay or a preference option value must be configured. Up to eight DHCPv6 server destinations can be configured.

The **no** form of this command removes the DHCPv6 server destination.

Parameters *ipv6-address* — Specifies the IPv6 address of the DHCPv6 server.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

server

Syntax **server** [*ip-address* | **fqdn**] [**port** *port*]
no server

Context **[Tree]** (config>system>security>pki>est-profile server)

Full Context configure system security pki est-profile server

Description Commands in this context configure EST server parameters.

The **no** form of the command reverts to the default value.

Parameters *ip-address* — Specifies the IP address of the server.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D

fqdn — Specifies to use the Fully Qualified Domain Name (FQDN) of the EST server, up to 255 characters.

port — Specifies the port number of the EST server.

Values 1 to 65535

Default 443

Platforms All

23.144 server-address

server-address

Syntax **server-address** *server-address* [**name** *server-name*]
no server-address *server-address*

Context **[Tree]** (config>app-assure>group>dns-ip-cache>dns-match server-address)

Full Context configure application-assurance group dns-ip-cache dns-match server-address

Description This command configures a DNS server address. DNS responses from this DNS server are used to populate the dns-ip-cache. Up to 64 server addresses can be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *server-address* — Specifies the IPv4 or IPv6 address of the DNS.

Values

ipv4-address	a.b.c.d[/mask]	
		mask - [1 to 32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length	
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D
	prefix-length	[1 to 128]

server-name — Specifies an optional server name for a given server address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server-address

Syntax **server-address {eq | neq}** *ip-address*
server-address {**eq** | **neq**} **ip-address** *masked-ip-address* **netmask** *netmask*
server-address {**eq** | **neq**} **dns-ip-cache** *dns-ip-cache-name*
server-address {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
no server-address

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry server-address)

Full Context configure application-assurance group policy app-filter entry server-address

Description This command configures the server address to use in application definition. The server IP address may be the source or destination, network or subscriber IP address and may include the use of netmasks.

The **no** form of this command restores the default (removes the server address from application criteria defined by this entry).

Default no server-address

Parameters **eq** — Specifies a comparison operator that the value configured and the value in the flow are equal.

neq — Specifies a comparison operator that the value configured differs from the value in the flow.

ip-address — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D
prefix-length [1..128]

netmask — Specifies an IPv4 or IPv6 address mask.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

masked-ip-address — Specifies a valid unicast IPv4 or IPv6 address.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit)
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D

dns-ip-cache-name — Specifies a DNS IP cache name, up to 32 characters.

ip-prefix-list-name — Specifies the name of an IP prefix list, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server-address

Syntax **server-address** *ip-address* [**version** *version-number*] [**normal** | **preferred**] [**interval** *seconds*]
no server-address *ip-address*

Context **[Tree]** (config>system>time>sntp server-address)

Full Context configure system time sntp server-address

Description This command creates an SNTP server for unicast client mode.

Parameters *ip-address* — Specifies the IP address of the SNTP server.

Values a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

version-number — Specifies the SNTP version supported by this server.

Values 1 to 3

Default 3

normal | preferred — Specifies the preference value for this SNTP server. When more than one time-server is configured, one server can have preference over others. The value for that server should be set to **preferred**. Only one server in the table can be a preferred server.

Default normal

seconds — Specifies the frequency at which this server is queried.

Values 64 to 1024

Default 64

Platforms All

23.145 server-cipher-list

server-cipher-list

Syntax **server-cipher-list protocol-version** *version*

Context **[Tree]** (config>system>security>ssh server-cipher-list)

Full Context configure system security ssh server-cipher-list

Description This command enables the configuration of the list of allowed ciphers by the SSH server.

Parameters *version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server only accepts connections from clients that support SSH protocol version 1 2 — Specifies that the SSH server accepts connections from clients supporting either SSH protocol version 2

Platforms All

server-cipher-list

Syntax **server-cipher-list** *name* [**create**]
no server-cipher-list *name*

Context **[Tree]** (config>system>security>tls server-cipher-list)

Full Context configure system security tls server-cipher-list

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates the cipher list that is compared against cipher lists sent by the client to the server in the client hello message. The list contains all ciphers that are supported and desired by SR OS for use in the TLS session. The first common cipher found in both the server and client cipher lists will be chosen. As such, the most desired ciphers should be added at the top of the list.

The **no** form of the command removes the cipher list.

Parameters *name* — Specifies the name of the server cipher list, up to 32 characters in length.

create — Keyword used to create the server cipher list.

Platforms All

23.146 server-id

server-id

Syntax **server-id duid-en hex** *hex-string*
server-id duid-en string *ascii-string*
server-id duid-ll
no server-id

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy server-id)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy server-id)
[Tree] (config>router>dhcp6>server server-id)
[Tree] (config>service>vprn>dhcp6>server server-id)

Full Context configure router dhcp6 local-dhcp-server server-id
configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server server-id
configure service vprn dhcp6 local-dhcp-server server-id
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server server-id

Description This command allows the operator to customize the **server-id** attribute of a DHCPv6 message (such as DHCPv6 advertise and reply). By default, the **server-id** uses DUID-ll derived from the chassis link layer address. Operators have the option to use a unique identifier by using the **duid-en** (vendor based on an enterprise number). There is a maximum length associated with the customizable hex-string and ascii-string.

The **no** form of this command reverts to the default.

Default server-id duid-ll

Parameters *hex-string* — Specifies a DUID system ID in a hex format.

Values 0x0 to 0xFFFFFFFF (maximum 116 hex nibbles)

ascii-string — Specifies a DUID system ID in an ASCII format, up to 58 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

duid-ll — Specifies that the DUID system ID is derived from the system link layer address.

duid-en — Specifies the enterprise number.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.147 server-ip

server-ip

Syntax **server-ip** {**eq** | **neq**} *ip-address*
no server-ip

Context **[Tree]** (debug>app-assure>group>traffic-capture>match server-ip)

Full Context debug application-assurance group traffic-capture match server-ip

Description This command configures debugging on a servicer IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.148 server-kex-list

server-kex-list

Syntax **server-kex-list**

Context **[Tree]** (config>system>security>ssh server-kex-list)

Full Context configure system security ssh server-kex-list

Description This command allows the user to configure SSH KEX algorithms for SR OS as an SSH server.

An empty list is the default list that the SSH KEX advertises. The default list contains the following:

diffie-hellman-group16-sha512

diffie-hellman-group14-sha256

diffie-hellman-group14-sha1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

diffie-hellman-group1-sha1

Platforms All

23.149 server-mac-list

server-mac-list

Syntax **server-mac-list**

Context **[Tree]** (config>system>security>ssh server-mac-list)

Full Context configure system security ssh server-mac-list

Description This command allows the user to configure SSH MAC algorithms for SR OS as an SSH server.

Platforms All

23.150 server-policy

server-policy

Syntax **server-policy** *policy-name*
no server-policy

Context **[Tree]** (config>service>dynsvc>acct-1 server-policy)
[Tree] (config>service>dynsvc>acct-2 server-policy)

Full Context configure service dynamic-services dynamic-services-policy accounting-1 server-policy
configure service dynamic-services dynamic-services-policy accounting-2 server-policy

Description This command configures the radius server policy to be used for dynamic data services RADIUS accounting.

The **no** form of this command removes the radius server policy from the configuration. This is only allowed when there are no active dynamic data services referencing this policy.

Parameters *policy-name* — Specifies the name of the radius server policy.

Values Up to 32 characters maximum

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

server-policy

Syntax **server-policy** *policy-name*
no server-policy

Context **[Tree]** (config>service>dynsvc>plcy>auth server-policy)

Full Context configure service dynamic-services dynamic-services-policy authentication server-policy

Description This command configures the RADIUS server policy to be used for RADIUS authentication of data-triggered dynamic services.

Local authentication and RADIUS authentication are mutually exclusive.

The **no** form of this command removes the server policy from the configuration and disables RADIUS authentication.

Parameters *policy-name* — Specifies a RADIUS server policy name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.151 server-port

server-port

Syntax **server-port** {**eq** | **neq** | **gt** | **lt**} *port-num*
server-port {**eq** | **neq**} **range** *start-port-num end-port-num*
server-port {**eq**} {*port-num* | **range** *start-port-num end-port-num*} {**first-packet-trusted** | **first-packet-validate**}
server-port {**eq** | **neq**} **port-list** *port-list-name*
server-port {**eq**} **port-list** *port-list-name* {**first-packet-trusted** | **first-packet-validate**}
no server-port

Context **[Tree]** (config>app-assure>group>policy>app-filter>entry server-port)

Full Context configure application-assurance group policy app-filter entry server-port

Description This command specifies the server TCP or UDP port number to use in the application definition.

The **no** form of this command restores the default (removes server port number from application criteria defined by this app-filter entry).

Default no server-port (the server port is not used in the application definition)

Parameters **eq** — Specifies that the value configured and the value in the flow are equal.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

neq — Specifies that the value configured differs from the value in the flow.

gt — Specifies all port numbers greater than server-port-number match.

lt — Specifies all port numbers less than server-port-number match.

port-list-name — Specifies a named port list containing a set or range of ports.

port-num — Specifies a valid server port number.

Values 0 to 65535

start-port-num, end-port-num — Specifies the starting or ending port number.

Values 0 to 65535

Server Port Options: — The following options are available:

- **No option specified:** TCP/UDP port applications with full signature verification:
  - AA ensures that other applications that can be identified do not run over a well-known port.
  - Application-aware policy applied once signature-based identification completes (likely requiring several packets).
- **first-packet-validate:** TCP/UDP trusted port applications with signature verification:
  - Application identified using well known TCP/UDP port based filters and re-identified once signature identification completes.
  - AA policy applied from the first packet of a flow while continuing signature-based application identification. Policy re-evaluated once the signature identification completes, allowing to detect improper/unexpected applications on a well-known port.
- **first-packet-trusted:** TCP/UDP trusted port applications - no signature verification:
  - Application identified using well known TCP/UDP port based filters only.
  - Application Aware policy applied from the first packet of a flow.
  - No signature processing assumes operator/customer trusts that no other applications can run on the well-known TCP/UDP port (statistics collected against trusted_tcp or trusted_udp protocol).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

server-port

Syntax **server-port** {**eq** | **neq**} *port-num*
no server-port

Context **[Tree]** (debug>app-assure>group>traffic-capture>match server-port)

Full Context debug application-assurance group traffic-capture match server-port

Description This command configures debugging on a server port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.152 server-shutdown

server-shutdown

Syntax [**no**] **server-shutdown**

Context **[Tree]** (config>system>security>ssh server-shutdown)

Full Context configure system security ssh server-shutdown

Description This command enables the SSH servers running on the system.

Default no server-shutdown

Platforms All

23.153 server-timeout

server-timeout

Syntax **server-timeout** *seconds*
no server-timeout

Context **[Tree]** (config>port>ethernet>dot1x server-timeout)

Full Context configure port ethernet dot1x server-timeout

Description This command configures the period during which the router waits for the RADIUS server to respond to its access request message. When this timer expires, the router will re-send the access request message, up to the specified number times.

The **no** form of this command returns the value to the default.

Default server-timeout 30

Parameters *seconds* — Specifies the server timeout period, in seconds.

Values 1 to 300

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.154 server-tls-profile

server-tls-profile

Syntax **server-tls-profile** *name* [**create**]
no server-tls-profile *name*

Context **[Tree]** (config>system>security>tls server-tls-profile)

Full Context configure system security tls server-tls-profile

Description This command creates a TLS server profile. This profile can be used by applications that support TLS for encryption. The applications should not send any PDUs until the TLS handshake has been successful.

The **no** form of the command removes the TLS server profile.

Parameters *name* — Specifies the name of the TLS server profile, up to 32 characters in length.

create — Keyword used to create the TLS server profile.

Platforms All

23.155 server6

server6

Syntax **server6** *ipv6-address*
no server6

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host server6)

Full Context configure subscriber-mgmt local-user-db ipoe host server6

Description This command allows DHCP6 server selection based on the host entry in LUDB.

The configured DHCP6 server IP address must reference one of the v6 addressees configured under the **config>service>vprn>sub-if>grp-if>ipv6>dhcpv6>relay** or **config>service>ies>sub-if>grp-if>ipv6>dhcpv6>relay** context.

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the retailer service ID.

Values

ipv6-address:	x:x:x:x:x:x:x:x	(eight 16-bit pieces)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.156 servers

servers

Syntax **servers**

Context **[Tree]** (config>aaa>radius-srv-plcy servers)

Full Context configure aaa radius-server-policy servers

Description Commands in this context configure radius-server-policy parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.157 service

service

Syntax **service** *service-id*
no service

Context **[Tree]** (config>service>vpls>sap>msap-defaults service)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>msap-defaults service)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>msap-defaults service)

Full Context configure service vpls sap msap-defaults service
configure subscriber-mgmt local-user-db ipoe host msap-defaults service
configure subscriber-mgmt local-user-db ppp host msap-defaults service

Description This command sets default service for all subscribers created based on trigger packets received on the given capture SAP in case the corresponding VSA is not included in the RADIUS authentication response. This command is applicable to capture SAP only.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — Specifies the service ID as an integer or a name.

Values *service-id* - 1 to 2147483648
service-name - up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt local-user-db ipoe host msap-defaults service
- configure subscriber-mgmt local-user-db ppp host msap-defaults service

All

- configure service vpls sap msap-defaults service

service

Syntax **service** *service-id*
no service

Context **[Tree]** (config>service>vprn>sub-if>grp-if>bonding-parameters>connection service)
[Tree] (config>service>ies>sub-if>grp-if>bonding-parameters>connection service)

Full Context configure service ies subscriber-interface group-interface bonding-parameters connection service
configure service vprn subscriber-interface group-interface bonding-parameters connection service

Description This command binds a specified service to this connection. ESM subscribers created under this service are eligible for bonding in this group interface and are identified by the provisioned connection ID. All connections in one bonding context must use subscriber interfaces in separate router instances.

The **no** form of this command removes the service from this bonding context, which can only be done when bonding is administratively disabled.

Parameters *service-id* — Specifies the service ID of the service containing this subscriber interface.

service

Syntax **service**

Context **[Tree]** (config>cflowd>collector>exp-filter>if-list service)

Full Context configure cflowd collector export-filter interface-list service

Description Commands in this context configure which service interfaces' flow data is being sent to this collector

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

service

Syntax **service** *service-id* **preference** *preference*
no service *service-id*

Context **[Tree]** (config>router>dns>redirect-vprn service)

Full Context configure router dns redirect-vprn service

Description This command configures the VPRN DNS redirection for the specified service.

The **no** form of this command removes the service from the VPRN DNS resolution configuration.

Parameters *service-id* — Specifies the unique service identification number or string identifying the service in the service domain.

Values *service-id*: 1 to 2147483647
svc-name: 64 characters maximum

preference — Specifies the service preference.

Values 0 to 255

Platforms All

service

Syntax [**no**] **service** *service-id*

Context **[Tree]** (config>log>services-all-events service)

Full Context configure log services-all-events service

Description This command enables access to the entire system-wide set of log events (VPRN and non-VPRN) in the logs configured within the management VPRN specified by the service ID.

The **no** form of the command enables the display of VPRN events only.

Parameters *service-id* — Identifies the VPRN.

Values {*id* | *svc-name*}

id: 1 to 2147483647
svc-name: up to 64 characters

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

service

Syntax **service** *service-id*
service name *service-name*
no service

Context **[Tree]** (config>system>security>pki>ca-profile>ocsp service)

Full Context configure system security pki ca-profile ocsp service

Description This command specifies the service or routing instance that used to contact OCSP responder. This applies to OCSP responders that either configured in CLI or defined in AIA extension of the certificate to be verified.

The responder-url will also be resolved by using the DNS server configured in the configured routing instance.

With VPRN services, the system checks whether the specified service ID or service name is an existing VPRN service at the time of CLI configuration. Otherwise the configuration fails.

Parameters *service-id* — Specifies an existing service ID to be used in the match criteria.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **service name** *service-name* variant can be used in all configuration modes.

Values service-id: 1 to 2147483647 base-router: 0

name *service-name* — Identifies the service, up to 64 characters.

Platforms All

23.158 service-carving

service-carving

Syntax **service-carving**

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg service-carving)

Full Context configure service system bgp-evpn ethernet-segment service-carving

Description Commands in this context configure service-carving in the Ethernet-Segment. The service-carving algorithm determines which PE is the Designated Forwarder (DF) in a specified Ethernet Segment and for a specific service.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.159 service-category

service-category

Syntax **service-category** *service-category*

Context **[Tree]** (config>qos>atm-td-profile service-category)

Full Context configure qos atm-td-profile service-category

Description This command is used to configure an ATM service category attribute of an ATM traffic descriptor profile per ATM Forum Traffic Management Specification Version 4.1.

The router supports the ATM service categories on ATM-capable MDAs listed in Table 124.

Table 124 **ATM Service Categories**

Service Category	Description
CBR	Constant Bit Rate
rt-VBR	Real time Variable Bit Rate
nrt-VBR	Non-real time Variable Bit Rate
UBR	Unspecified Bit Rate without Minimum Desired Cell Rate (defined by specifying service category to be UBR, and MIR of 0)
UBR (with MIR)	Unspecified Bit Rate with non-zero Minimum Desired Cell Rate (defined by specifying service category to be UBR, and MIR > 0)

Changing the service category of a profile will reset all traffic attributes to their defaults (see the **config>qos>atm-td-profile traffic** command) and will cause reprogramming of the data path (with a small impact on user traffic) and a reset of VC statistics for all VCs using this traffic descriptor profile.

Default service-category ubr

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.160 service-context-id

service-context-id

Syntax **service-context-id** *name*
no service-context-id

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy>include-avp service-context-id)

Full Context configure subscriber-mgmt diameter-application-policy gy include-avp service-context-id

Description This command configures the value of the service context ID AVP.

The **no** form of this command returns the command to the default setting.

Parameters *name* — Specifies the service context ID AVP value, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.161 service-id

service-id

Syntax **service-id** *service-id*
no service-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident service-id)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification service-id

Description This command specifies the service ID to match for a host lookup. When the LUDB is accessed using a DHCPv4 server, the SAP ID is matched against the Nokia vendor-specific sub-option in DHCP Option 82.

The **no** form of this command removes the service ID from the configuration.

Parameters *service-id* — Specifies an existing service ID or service name.

Values *service-id* — 1 to 2147483647
service-name — up to 64 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

service-id

Syntax [**no**] **service-id**

Context **[Tree]** (config>service>vpls>sap>dhcp>option>vendor service-id)
[Tree] (config>service>vprn>if>dhcp>option>vendor service-id)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option>vendor service-id)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option>vendor service-id)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option>vendor-specific-option service-id)

Full Context configure service ies subscriber-interface group-interface dhcp option vendor-specific-option service-id
configure service vpls sap dhcp option vendor-specific-option service-id
configure service vprn interface dhcp option vendor-specific-option service-id
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option service-id
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option service-id

Description This command enables the sending of the service ID in the Nokia vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command disables the sending of the service ID in the Nokia vendor-specific sub-option of the DHCP relay packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option service-id
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option service-id
- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option service-id

All

- configure service vpls sap dhcp option vendor-specific-option service-id
- configure service vprn interface dhcp option vendor-specific-option service-id

service-id

Syntax [**no**] **service-id**

Context **[Tree]** (config>router>if>dhcp>option>vendor-specific-option service-id)

Full Context configure router interface dhcp option vendor-specific-option service-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the sending of the service ID in the Nokia vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command disables the sending of the service ID in the Nokia vendor-specific sub-option of the DHCP relay packet.

Default no service-id

Platforms All

service-id

Syntax **service-id** *service-id*
no service-id

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring>ibc service-id)
[Tree] (config>redundancy>mc>peer>mcr>l3-ring>ibc service-id)

Full Context configure redundancy multi-chassis peer mc-ring l3-ring in-band-control-path service-id
configure redundancy multi-chassis peer mc-ring ring in-band-control-path service-id

Description This command specifies the service ID if the interface used for the inband control connection belongs to a VPRN service. If not specified, the service-id is zero and the interface must belong to the Base router. This command supersedes the configuration of a service name.

The no form of this command removes the service ID from the IBC configuration.

Parameters *service-id* — Specifies a service ID or an existing service name.

Values 1 to 214748364 - Only supported in 'classic' configuration-mode (**configure>system>management-interface>configuration-mode classic**)

Platforms All

service-id

Syntax **service-id** *service-id*
no service-id

Context **[Tree]** (config>redundancy>mc>peer>mcr>node>cv service-id)
[Tree] (config>redundancy>mc>peer>mcr>l3-ring>node>cv service-id)

Full Context configure redundancy multi-chassis peer mc-ring l3-ring ring-node connectivity-verify service-id
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify service-id

Description This command specifies the service ID of the SAP used for the ring-node connectivity verification of this ring node. This command supersedes the configuration of a service name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command removes the service ID from the CV configuration.

Default no service-id

Parameters *service-id* — Specifies the service ID or an existing service name.

Values 1 to 2147483647- Only supported in “classic” configuration mode (**configure system management-interface configuration-mode classic**)

Platforms All

service-id

Syntax **service-id**

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg service-id)

Full Context configure service system bgp-evpn ethernet-segment service-id

Description This command enables the **service-id** context within the virtual **ethernet-segment** configuration.

Platforms All

23.162 service-id-lag-hashing

service-id-lag-hashing

Syntax [**no**] **service-id-lag-hashing**

Context **[Tree]** (config>system>load-balancing service-id-lag-hashing)

Full Context configure system load-balancing service-id-lag-hashing

Description This command enables enhanced VLL LAG service ID hashing. This command improves the LAG spraying of VLL service packets and is applied only when both ECMP and LAG hashing are performed by the same router. By default, the ECMP interface and LAG link for all packets on the VLL service are selected based on a direct modulo operation of the service ID. This command enhances distribution and hashes the service ID prior to the LAG link modulo operation when an ECMP link modulo operation is performed.

The **no** form of the command preserves the default behavior of VLL LAG service ID hashing.

Default no service-id-lag-hashing

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.163 service-id-range

service-id-range

Syntax **service-id-range start** *service-id* **end** *service-id*
no service-id-range

Context **[Tree]** (config>service>md-auto-id service-id-range)

Full Context configure service md-auto-id service-id-range

Description This command specifies the range of IDs used by SR OS to automatically assign an ID to services that are created in model-driven interfaces without an ID explicitly specified by the user or client.

A service created with an explicitly-specified ID cannot use an ID in this range. In the classic CLI and SNMP, the ID range cannot be changed while objects exist inside the previous or new range. In MD interfaces, the range can be changed, which causes any previously existing objects in the previous ID range to be deleted and re-created using a new ID in the new range.

The **no** form of this command removes the range values.

See the **config>service md-auto-id** command for further details.

Default no service-id-range

Parameters **start** *service-id* — Specifies the lower value of the ID range. The value must be less than or equal to the **end** value.

Values 1 to 2147483647

end *service-id* — Specifies the upper value of the ID range. The value must be greater than or equal to the **start** value.

Values 1 to 2147483647

Platforms All

23.164 service-mtu

service-mtu

Syntax **service-mtu** *octets*
no service-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls service-mtu)
[Tree] (config>service>template>vpls-template service-mtu)

Full Context configure service template vpls-template service-mtu
configure service vpls service-mtu

Description This command configures the service payload (Maximum Transmission Unit – MTU), in bytes, for the service. This MTU value overrides the service-type default MTU. The **service-mtu** defines the payload capabilities of the service. It is used by the system to validate the SAP and SDP binding's operational state within the service.

The service MTU and a SAP's service delineation encapsulation overhead (4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP will be placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP will be able to transition to the operative state.

When binding an SDP to a service, the service MTU is compared to the path MTU associated with the SDP. The path MTU can be administratively defined in the context of the SDP. The default or administrative path MTU can be dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path. If the service MTU is larger than the path MTU, the SDP binding for the service will be placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding will be placed in an operational state.

If a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, then all associated SAP and SDP binding operational states are automatically re-evaluated.

For i-VPLS and Epipes bound to a b-VPLS, the service-mtu must be at least 18 bytes smaller than the b-VPLS service MTU to accommodate the PBB header.

The **no** form of this command returns the default **service-mtu** for the indicated service type to the default value.

Default service-mtu 1514

Parameters *octets* — The following table displays MTU values for specific VC types

VC-Type	Example Service MTU	Advertised MTU
Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VPLS	1514	1500
VPLS (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500
VLAN (qinq with preserved bottom qtag)	1518	1504

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The size of the MTU in octets, expressed as a decimal integer

Values 1 to 9194

Platforms All

service-mtu

Syntax **service-mtu** *octets*
no service-mtu

Context **[Tree]** (config>service>apipe service-mtu)
[Tree] (config>service>cpipe service-mtu)
[Tree] (config>service>epipe service-mtu)
[Tree] (config>service>fpipe service-mtu)
[Tree] (config>service>ipipe service-mtu)

Full Context configure service apipe service-mtu
configure service cpipe service-mtu
configure service epipe service-mtu
configure service fpipe service-mtu
configure service ipipe service-mtu

Description This command configures the service payload in bytes, for the service. The configured Maximum Transmission Unit (MTU) value overrides the service-type default MTU. The **service-mtu** command defines the payload capabilities of the service. It is used by the system to validate the operational state of the SAP and SDP binding within the service.

The service MTU and a SAP's service delineation encapsulation overhead (4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, the SAP is placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP transitions to the operative state.

When binding an SDP to a service, the service MTU is compared to the path MTU associated with the SDP. The path MTU can be administratively defined in the context of the SDP. The default or administrative path MTU can be dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path. If the service MTU is larger than the path MTU, the SDP binding for the service is placed in an inoperative state. If the service MTU is equal to or less than the path MTU, the SDP binding is placed in an operational state.

If a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, all associated SAP and SDP binding operational states are automatically reevaluated.

Binding operational states are automatically reevaluated.

For I-VPLS and Epipes bound to a B-VPLS, the service MTU must be at least 18 bytes smaller than the B-VPLS service MTU to accommodate the PBB header.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Because this connects a Layer 2 to a Layer 3 service, adjust the service MTU under the Epipe service. The MTU that is advertised from the Epipe side is service MTU minus EtherHeaderSize.

Note: In the **configure**>**service**>**epipe** context, the **adv-service-mtu** command can be used to override the configured MTU value used in T-LDP signaling to the far-end of an Epipe spoke-sdp. The **adv-service-mtu** command is also used to validate the value signaled by the far-end PE. For more information, see **adv-service-mtu** command.

The **no** form of this command returns the default **service-mtu** for the indicated service type to the default value.

By default, if **no service-mtu** is configured, the MTU value is (1514 - 14) = 1500.

Default no service-mtu 1508 (for Apipe, Fpipe)

no service-mtu 1500 (for Ipipe)

no service-mtu 1524 (for Epipe)

Table 125 lists the MTU values for specific VC types.

Table 125 **MTU Values**

SAP VC-Type	Example: Service MTU	Advertised MTU
Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VPLS	1514	1500
VPLS (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500
VLAN (qinq with preserved bottom qtag)	1518	1504

Parameters *octets* — Specifies the MTU size in octets, expressed as a decimal integer.

Values 1 to 9782
1 to 9800 (for Epipe only)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service fpipe service-mtu
- configure service cpipe service-mtu

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service apipe service-mtu

All

- configure service epipe service-mtu
- configure service ipipe service-mtu

23.165 service-name

service-name

Syntax **service-name** *service-name*
no service-name

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>host-ident service-name)

Full Context configure subscriber-mgmt local-user-db ppp host host-identification service-name

Description This command specifies the service name tag in PADI and/or PADR packets to match for PPPoE hosts.

Note: This command is only used when **service-name** is configured as one of the **match-list** parameters.

The **no** form of this command removes the service-name from the configuration.

Parameters *service-name* — Specifies a PPPoE service name, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

service-name

Syntax **service-name** *service-name*
no service-name

Context **[Tree]** (config>redundancy>mc>peer>mcr>ring>ibc service-name)
[Tree] (config>redundancy>mc>peer>mc>l3-ring>ibc service-name)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring ibc service-name
configure redundancy multi-chassis peer mc-ring ring in-band-control-path service-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the service name if the interface used for the inband control connection belongs to a VPRN service. If not specified the interface must belong to the Base router. This command supersedes the configuration of a service ID.

The **no** form of this command removes the service name from the IBC configuration.

Default no service-name

Parameters *service-name* — Specifies the service name, up to 64 characters.

Platforms All

service-name

Syntax **service-name** *service-name*
no service-name

Context **[Tree]** (config>redundancy>mc>peer>mcr>node>cv service-name)
[Tree] (config>redundancy>mc>peer>mcr>l3-ring>cv service-name)

Full Context configure redundancy multi-chassis peer mc-ring l3-ring ring-node connectivity-verify service-name
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify service-name

Description This command specifies the service name of the SAP used for ring-node connectivity verification of this ring node. This command supersedes the configuration of a service ID.

The **no** form of this command removes the service name from the CV configuration.

Default no service-name

Parameters *service-name* — Specifies a service name, up to 64 characters.

Platforms All

23.166 service-range

service-range

Syntax **service-range** *service-id service-id*
no service-range

Context **[Tree]** (config>service>dynsvc service-range)

Full Context configure service dynamic-services service-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the service ID range that is reserved for dynamic data service creation. The range cannot overlap with existing static configured services. Once configured with active dynamic services in the range, the service range can only be extended at the end.

The **no** form of this command removes the service-range from the configuration. This is only allowed when there are no active dynamic data services.

When **no service-range** is specified, the setup of dynamic data services fails.

Parameters *service-id* — Specifies the start and end service IDs to define the service range for dynamic services.

Values 1 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

service-range

Syntax **service-range** *svc-id* **to** *svc-id*
no service-range

Context **[Tree]** (config>service>vsd service-range)

Full Context configure service vsd service-range

Description This command configures the range of service identifiers that the system allows for dynamic services configured by python, when the Nuage VSD sends the service configuration parameters for the VSD fully-dynamic integration model.

Parameters *svc-id* — Specifies the start and end service identifier values.

Values 1 to 2147483647

Platforms All

service-range

Syntax **service-range** *svc-id* [**to** *svc-id*]
no service-range *svc-id*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>service-id service-range)

Full Context configure service system bgp-evpn ethernet-segment service-id service-range

Description This command associates a specified service range to a virtual ES, along with the **network-interconnect-vxlan** command. Up to eight service ranges per VXLAN instance can be configured, where the ranges may overlap. The service range may be configured before the service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the association of the service range to the virtual ES for the configured VXLAN instance.

Parameters *svc-id* — Specifies which service range will be associated with the virtual Ethernet Segment.

Values 1 to 2147483647

Platforms All

service-range

Syntax **service-range** *startid-endid* [**start-vlan-id** *startvid*]
no service-range

Context **[Tree]** (config>service>vpls>vpls-group service-range)

Full Context configure service vpls vpls-group service-range

Description This command configures the service ID and implicitly the VLAN ID ranges to be used as input variables for related VPLS and SAP templates to pre-provision “data” VPLS instances and related SAPs using the service ID specified in the command. If the **start-vlan-id** is not specified then the service-range values are used for vlan-ids. The data SAPs will be instantiated on all the ports used to specify SAP instances under the related control VPLS.

Modifications of the service id and vlan ranges are allowed with the following restrictions.

- service-range increase can be achieved in two ways:
  - Allowed when vpls-group is in shutdown state
  - By creating a new vpls-group
- service-range decrease can be achieved in two ways:
  - Allowed when vpls-group is in shutdown state; when **shutdown** command is executed the associated service instances are deleted.
  - Allowed when vpls-group is in no shutdown state and has completed successfully instantiating services.
  - In both cases, only the services that do not have user configured SAPs will be deleted. Otherwise the above commands are rejected. Existing declarations or registrations do not prevent service deletion.
- start-vlan-id change can be achieved in two ways:
  - Allowed when vpls-group is in shutdown state
  - At the time of range decrease by increasing the start-vlan-id which can be done when vpls-group is in no shutdown state and has completed successfully instantiating services

The **no** form of this command removes the specified ranges and deletes the pre-provisioned VPLS instances and related SAPs. The command will fail if any of the VPLS instances in the affected ranges have a provisioned SAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no service-range

Parameters *startid-endid* — Specifies the range of service IDs

Values 1 to 2147483647

startvid — Specifies the starting VLAN ID; it provides a way to set aside a service ID range that is not the same as the VLAN range and allows for multiple MVRP control-VPLSs to control same VLAN range on different ports.

Values 1 to 4094

Platforms All

23.167 services-all-events

services-all-events

Syntax **services-all-events**

Context **[Tree]** (config>log services-all-events)

Full Context configure log services-all-events

Description Commands in this context control which log events are present in VPRN logs.

By default, the event streams for VPRN logs contain only events that are associated with the particular VPRN.

Access to the entire system-wide set of events (VPRN and non-VPRN) can be enabled using the **services-all-events** command.

Platforms All

23.168 serving-network

serving-network

Syntax **serving-network mcc** *mcc-value* **mnc** *mnc-value*
no serving-network

Context **[Tree]** (config>subscr-mgmt>gtp serving-network)

Full Context configure subscriber-mgmt gtp serving-network

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the Operator Identifier part (MCC and MNC) of the APN.

The **no** form of this command removes the values from the profile.

Default no serving-network

Parameters *mcc-value* — Specifies the Mobile Country Code (MCC) portion of the Serving Network.

Values 3 digits

mnc-value — Specifies the Mobile Network Code (MNC) portion of the Serving Network.

Values 2 or 3 digits

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.169 session

session

Syntax **session**

Context **[Tree]** (config>isa>video-group>watermark session)

Full Context configure isa video-group watermark session

Description Commands in this context configure watermark parameters based on the session.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

session

Syntax **session** *session-name* [**test-family** [**ethernet** | **ip** | **mpls**] [**session-type** {**proactive** | **on-demand**}] **create**]
no session *session-name*

Context **[Tree]** (config>oam-pm session)

Full Context configure oam-pm session

Description This command creates the individual session containers that houses the test specific configuration parameters. Since this session context provides only a container abstract to house the individual test functions, it cannot be shut down. Individual tests sessions within the container may be shut down. No values, parameters, or configuration within this context may be changed if any individual test is active. Changes may only be made when all tests within the context are shut down. The only exception to this is the description value.

The **no** form of this command deletes the session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *session-name* — Specifies the session name, up to 32 characters.

test-family — Indicates the type family and sets the context for the individual parameters.

Values **ethernet** — Specifies that the test is based on the Ethernet layer.

ip — Specifies that the test is based on the IP layer.

mpls — Specifies that the test is based on the MPLS layer.

session-type — Specifies how to set the Type bit in the Flags byte, and influences how different test criteria may be applied to the individual test. Not all test families carry this information in the PDU.

Values **proactive** — Sets the type to always on, with an immediate start and no stop.

on-demand — Sets the type to on-demand, with an immediate start and no stop, or a stop based on the offset.

Default proactive

create — Creates the PM session.

Platforms All

23.170 session-accounting

session-accounting

Syntax **session-accounting** [**interim-update**] [**host-update**]
no session-accounting

Context **[Tree]** (config>subscr-mgmt>acct-plcy session-accounting)

Full Context configure subscriber-mgmt radius-accounting-policy session-accounting

Description This command enables per session accounting mode. In per session accounting mode, the acct-session-id is generated per session. This acct-session-id is uniformly included in all accounting messages (START/INTERIM-UPDATE/STOP) and it can be included in RADIUS Access-Request message.

This accounting mode of operation can be used only in PPPoE environment with dual-stack host in which case both hosts (IPv4 and IPv6) are considered part of the same session. In addition to regular interim-updates, *triggered* interim-updates are sent by a host joining or leaving the session.

When an IPv4/v6 address is allocated, or released from a dual-stack host, a triggered interim-update message is immediately sent. This triggered interim-update message reflects the change in the IP address. The triggered interim-update has no effect on the interval at which the regular interim updates are scheduled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Accounting counters are based on the queue counters and as such are aggregated for all host sharing the queues within an sla-profile instance.

CoA and LI is supported based on the acct-session-id of the session.

The **no** form of this command reverts to the default.

Parameters **interim-update** — Specifies to enable interim updates. Without this keyword only START and STOP accounting messages are generated when the session is established or terminated. This is equivalent to a time-based accounting where only the duration of the session is required.

host-update — Indicates that host updates messages are sent. INTERIM-UPDATE messages can be generated (volume based accounting) by selecting this keyword.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.171 session-assign-method

session-assign-method

Syntax **session-assign-method** {**weighted** | **weighted-random**}
no session-assign-method

Context **[Tree]** (config>router>l2tp session-assign-method)
[Tree] (config>service>vprn>l2tp session-assign-method)

Full Context configure router l2tp session-assign-method
configure service vprn l2tp session-assign-method

Description This command configures the session assignment method.

The **no** form of this command reverts to the default value.

Default no session-assign-method

Parameters **weighted** — Specifies that the sessions are shared between the available tunnels. If necessary, new tunnels are set up until the maximum number is reached. The distribution aims at an equal ratio of the actual number of sessions to the maximum number of sessions.

weighted-random — Enhances the weighted algorithm such that when there are multiple tunnels with an equal number of sessions (equal weight), LAC randomly selects a tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

session-assign-method

Syntax **session-assign-method** {**existing-first** | **weighted** | **weighted-random**}
no session-assign-method

Context **[Tree]** (config>router>l2tp>group session-assign-method)
[Tree] (config>service>vprn>l2tp>group session-assign-method)

Full Context configure router l2tp group session-assign-method
configure service vprn l2tp group session-assign-method

Description This command specifies how new sessions are assigned to one of the set of suitable tunnels that are available or could be made available.

The **no** form of this command reverts to the default value.

Default session-assign-method existing-first

Parameters **existing-first** — Specifies that all new sessions are placed by preference in the existing tunnels.

weighted — Specifies that the sessions are shared between the available tunnels. If necessary, new tunnels are set up until the maximum number is reached. The distribution aims at an equal ratio of the actual number of sessions to the maximum number of sessions.

weighted-random — Enhances the weighted algorithm such that when there are multiple tunnels with an equal number of sessions (equal weight), LAC randomly selects a tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.172 session-filter

session-filter

Syntax **session-filter** *session-filter-name*
no session-filter

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action session-filter)

Full Context configure application-assurance group policy app-qos-policy entry action session-filter

Description This command specifies the Application-Assurance session filter that will be evaluated. If no session filters are specified then no session filters will be evaluated.

Default no session-filter

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *session-filter-name* — Specifies the session filter to be applied.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

session-filter

Syntax **session-filter** *session-filter-name* [**create**]
no session-filter *session-filter-name*

Context **[Tree]** (config>app-assure>group session-filter)

Full Context configure application-assurance group session-filter

Description This command creates a session filter.

Parameters *session-filter-name* — Creates a session filter name up to 32 characters.

create — Keyword used to create the session filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

session-filter

Syntax **session-filter** *session-filter-name*

Context **[Tree]** (config>app-assure>group>statistics>tca session-filter)

Full Context configure application-assurance group statistics threshold-crossing-alert session-filter

Description This command configures TCA generation for a session filter.

Parameters *session-filter-name* — Specifies the name of the session filter, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.173 session-filter-stats

session-filter-stats

Syntax [**no**] **session-filter-stats**

Context **[Tree]** (config>app-assure>group>statistics>aa-admit-deny session-filter-stats)

Full Context configure application-assurance group statistics aa-admit-deny session-filter-stats

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures whether to include or exclude session filter admit-deny statistics in accounting records.

Default no session-filter-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.174 session-hold-time

session-hold-time

Syntax **session-hold-time remaining-lease-time**
session-hold-time *seconds*
no session-hold-time

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile session-hold-time)

Full Context configure subscriber-mgmt gtp peer-profile session-hold-time

Description This command configures, in seconds, the time that a GTP session context is held after the corresponding UE is disconnected. If the same UE re-connects to this system before this time has elapsed, its GTP session context is re-used. When the timer expires, the GTP session context is cleared.

The **no** form of this command reverts to the default.

Default session-hold-time 30

Parameters **remaining-lease-time** — Specifies that the timer is equal to the UE's DHCP remaining lease time.

seconds — Specifies the time, in seconds, to hold a GTP session after its UE is disconnected.

Values 0 to 3600

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.175 session-id

session-id

Syntax **session-id** *session-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no session-id

Context [Tree] (config>li>li-source>nat>classic-lsn-sub session-id)
[Tree] (config>li>li-source>nat>dslite-lsn-sub session-id)
[Tree] (config>li>li-source>nat>ethernet-header session-id)
[Tree] (config>li>li-source>nat>l2-aware-sub session-id)
[Tree] (config>li>li-source>nat>nat64-lsn-sub session-id)

Full Context configure li li-source nat classic-lsn-sub session-id
configure li li-source nat dslite-lsn-sub session-id
configure li li-source nat ethernet-header session-id
configure li li-source nat l2-aware-sub session-id
configure li li-source nat nat64-lsn-sub session-id

Description This command configures the session ID that is inserted into the packet header for all mirrored packets of the associated LI source entry. This session ID can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs.

The session ID is only valid and used for mirror services that are configured with **ip-udp-shim** routable encapsulation (**config>mirror>mirror-dest>encap>ip-gre-shim**).

For all types of li-source entries (filter, nat, sap, or subscriber), when the mirror service is configured with **ip-udp-shim** routable encapsulation, a session-id field (as part of the routable encapsulation) is always present in the mirrored packets. If there is no *session-id* configured for an **li-source** entry, then the default value is inserted. When a mirror service is configured with **ip-gre** routable encapsulation, no *session-id* is inserted and none should be specified against the **li-source** entries.

The **no** form of this command removes the *session-id* from the configuration which results in the default value being used.

Default no session-id (an id of 0, or no id)

Parameters *session-id* — Specifies the value to insert into the header of the mirrored packets.

Values 1 to 4,294,967,295 (32b)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

session-id

Syntax **session-id** [*session-id*]
no session-id

Context [Tree] (config>li>li-source>wlan-gw session-id)

Full Context configure li li-source wlan-gw session-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the session ID inserted in the packet header for all mirrored packets of the associated li-source. When the mirror-service is configured with the **ip-udp-shim** routable encapsulation, session-id field (as part of the routable encapsulation) is always present in the mirrored packets. The session-id can be used by the LIG to identify a particular LI session to which the packet belongs.

Parameters *session-id* — Specifies the session ID inserted in the LI header.

Values 1 to 4294967295

session-id

Syntax **session-id** *session-id*
no session-id

Context **[Tree]** (config>test-oam>build-packet>header>l2tp session-id)
[Tree] (debug>oam>build-packet>packet>field-override>header>l2tp session-id)

Full Context configure test-oam build-packet header l2tp session-id
debug oam build-packet packet field-override header l2tp session-id

Description This command defines the session ID to be used in the L2TP header.

The **no** form of this command removes the session ID value.

Default session-id 0

Parameters *session-id* — Specifies the L2TP session ID to be used in the L2TP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.176 session-id-format

session-id-format

Syntax **session-id-format** {**description** | **number**}
no session-id-format

Context **[Tree]** (config>subscr-mgmt>acct-plcy session-id-format)

Full Context configure subscriber-mgmt radius-accounting-policy session-id-format

Description This command specifies the format for the acct-session-id attribute used in RADIUS accounting requests.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Default session-id-format description

Parameters **description** — Specifies to use a string containing following information: <subscriber>@<sap-id>@<SLA-profile>_<creation-time>

number — Specifies to use a unique number generated by the OS to identify a given session.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.177 session-key

session-key

Syntax **session-key sap mac** [**cid**] [**rid**]
no session-key

Context **[Tree]** (config>subscr-mgmt>ipoe-plcy session-key)

Full Context configure subscriber-mgmt ipoe-session-policy session-key

Description This command configures the key to logically group subscriber hosts that belong to the same dual stack end device in an IPoE session.

The SAP and MAC address are always part of the IPoE session key. Optionally the Circuit-Id/ Interface-Id or Remote-Id can be added to the session key.

The **no** form of this command reverts to the default.

Default session-key sap mac

Parameters **sap** — Includes the SAP as part of the IPoE session key. The **sap** parameter is mandatory and cannot be removed from the key.

mac — Includes the MAC address as part of the IPoE session key. The **mac** parameter is mandatory and cannot be removed from the key.

cid — Optionally adds the DHCPv4 Relay Agent Circuit-Id (Option 82, sub Option 1) and DHCPv6 Interface-Id (Option 18) field to the IPoE session key.

rid — Optionally adds the DHCPv4 Relay Agent Remote-Id (Option 82, sub Option 2) and DHCPv6 Remote-Id (Option 37) field to the IPoE session key. For DHCPv6, the enterprise number is excluded from the key.

sap and **mac** are mandatory parameters while **cid** and **rid** are optional and mutually exclusive. Valid IPoE session key parameters are: **sap mac**, **sap mac cid** and **sap mac rid**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.178 session-limit

session-limit

Syntax **session-limit** *session-limit*
session-limit unlimited
no session-limit

Context **[Tree]** (config>router>l2tp session-limit)
[Tree] (config>router>l2tp>group session-limit)
[Tree] (config>router>l2tp>group>tunnel session-limit)
[Tree] (config>service>vprn>l2tp session-limit)
[Tree] (config>service>vprn>l2tp>group session-limit)
[Tree] (config>service>vprn>l2tp>group>tunnel session-limit)

Full Context configure router l2tp group session-limit
configure router l2tp group tunnel session-limit
configure router l2tp session-limit
configure service vprn l2tp group session-limit
configure service vprn l2tp group tunnel session-limit
configure service vprn l2tp session-limit

Description This command configures the session limit.

This command configures the L2TP session limit for the router. The value controls how many L2TP sessions will be allowed within a given context (system, group, tunnel).

L2TP is connection-oriented. The L2TP Network Server (LNS) and LAC maintain state for each call that is initiated or answered by an LAC. An L2TP session is created between the LAC and LNS when an end-to-end PPP connection is established between a remote system and the LNS. Datagrams related to the PPP connection are sent over the tunnel between the LAC and LNS. There is a one-to-one relationship between established L2TP sessions and their associated calls.

The **no** form of this command removes the value from the configuration.

Default no session-limit

Parameters *session-limit* — Specifies the allowed number of sessions within the given context.

Values 1 to 131071

unlimited — Specifies to use the maximum number of sessions available.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

session-limit

Syntax **session-limit** *session-limit*
no session-limit

Context [Tree] (config>service>ies>sub-if>grp-if>pppoe session-limit)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe session-limit)
[Tree] (config>service>ies>sub-if>pppoe session-limit)
[Tree] (config>service>vprn>sub-if>pppoe session-limit)
[Tree] (config>service>ies>sub-if>grp-if>ppp session-limit)
[Tree] (config>service>vprn>sub-if>grp-if>ppp session-limit)

Full Context configure service ies subscriber-interface group-interface ppp session-limit
configure service ies subscriber-interface group-interface pppoe session-limit
configure service ies subscriber-interface pppoe session-limit
configure service vprn subscriber-interface group-interface ppp session-limit
configure service vprn subscriber-interface group-interface pppoe session-limit
configure service vprn subscriber-interface pppoe session-limit

Description This command specifies the number of PPPoE hosts allowed for this group interface.

The **no** form of this command reverts to the default.

Default session-limit 1

Parameters *session-limit* — Specifies the number of PPPoE hosts allowed.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 1 to 131071
1 to 262143 (retail subscriber interface)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

session-limit

Syntax **session-limit** *session-limit*
no session-limit

Context [Tree] (config>service>ies>sub-if>grp-if>ipoe-session session-limit)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session session-limit)
[Tree] (config>service>ies>sub-if>ipoe-session session-limit)
[Tree] (config>service>vprn>sub-if>ipoe-session session-limit)

Full Context configure service ies subscriber-interface group-interface ipoe-session session-limit
configure service ies subscriber-interface ipoe-session session-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface ipoe-session session-limit
configure service vprn subscriber-interface ipoe-session session-limit

Description This command specifies the number of IPoE sessions allowed for this group interface or retail subscriber interface.

The **no** form of this command reverts to the default.

Default session-limit 1

Parameters *session-limit* — Specifies the number of allowed IPoE sessions.

Note: The operational maximum value may be smaller due to equipped hardware dependencies.

Values 1 to 131071
1 to 500000 (retail subscriber interface)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

session-limit

Syntax **session-limit** *limit*

Context **[Tree]** (config>li>x-interfaces>x3 session-limit)

Full Context configure li x-interfaces x3 session-limit

Description This command configures the number of X3 sessions that the system should initiate to the LIC.

The **no** form of this command reverts to the default.

Default session-limit 32

Parameters *limit* — Specifies the session limit.

Values 1 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.179 session-limits

session-limits

Syntax **session-limits**

Context **[Tree]** (config>isa>wlan-gw-group>nat session-limits)

Full Context configure isa wlan-gw-group nat session-limits

Description Commands in this context configure session limits for the ISA WLAN gateway NAT group.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

session-limits

Syntax **session-limits**

Context **[Tree]** (config>isa>nat-group session-limits)

Full Context configure isa nat-group session-limits

Description Commands in this context configure session limits for the ISA NAT group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

session-limits

Syntax **session-limits**

Context **[Tree]** (config>service>nat>firewall-policy session-limits)
[Tree] (config>service>nat>nat-policy session-limits)
[Tree] (config>service>nat>up-nat-policy session-limits)

Full Context configure service nat firewall-policy session-limits
configure service nat nat-policy session-limits
configure service nat up-nat-policy session-limits

Description Commands in this context configure session limits for the NAT policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy session-limits
- configure service nat up-nat-policy session-limits

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service nat firewall-policy session-limits

session-limits

Syntax [**no**] **session-limits**

Context **[Tree]** (config>subscr-mgmt>sla-profile session-limits)
[Tree] (config>subscr-mgmt>sub-profile session-limits)

Full Context configure subscriber-mgmt sla-profile session-limits
configure subscriber-mgmt sub-profile session-limits

Description Commands in this context configure session limits per SLA profile instance or per subscriber.

The **no** form of this command removes the configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.180 session-messages

session-messages

Syntax [**no**] **session-messages**

Context **[Tree]** (debug>diam>application>policy session-messages)

Full Context debug diameter application policy session-messages

Description This command debugs session messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.181 session-optimized-stop

session-optimized-stop

Syntax [**no**] **session-optimized-stop**

Context **[Tree]** (config>subscr-mgmt>sub-prof>rad-acct session-optimized-stop)

Full Context configure subscriber-mgmt sub-profile radius-accounting session-optimized-stop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command optimizes a RADIUS Accounting Stop message for a PPPoE session termination (specifically for session accounting mode when the host update is enabled). By default when a PPPoE session terminates, the system removes a dual stack host in sequence, one host at a time. Therefore, the system will generate a RADIUS accounting interim for each host termination until only the final host is left. The final host will generate a final accounting stop message. Enabling this command will trigger a single Stop RADIUS accounting message and include information of all hosts without the host updates.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.182 session-parameters

session-parameters

Syntax **session-parameters**

Context **[Tree]** (config>router>ldp session-parameters)

Full Context configure router ldp session-parameters

Description Commands in this context configure peer specific parameters.

Platforms All

23.183 session-qer

session-qer

Syntax **session-qer**

Context **[Tree]** (config>subscr-mgmt>sla-prof>pfcp session-qer)

Full Context configure subscriber-mgmt sla-profile pfcp-mappings session-qer

Description Commands in this context configure the mapping of the GBR/MBR IEs present in a per-session QER without a QER correlation ID. A QER that contains a QER correlation ID does not use the QER mapping because it is assumed not to be a per-session construct.If a signaled PFCP QER rate applies to all data-plane rules, it is interpreted as the session QER rate and is mapped to the QoS overrides in the configuration. Examples of such QER rates are APN-AMBR for 4G FWA sessions and session-AMBR for 5G FWA sessions.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.184 session-time

session-time

Syntax [**no**] **session-time**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes session-time)

Full Context configure aaa isa-radius-policy acct-include-attributes session-time

Description This command enables the inclusion of the session-time attributes.

The **no** form of the command excludes session-time attributes.

Default no session-time

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.185 session-timeout

session-timeout

Syntax **session-timeout** *timeout*
no session-timeout

Context **[Tree]** (config>subscr-mgmt>ppp-policy session-timeout)

Full Context configure subscriber-mgmt ppp-policy session-timeout

Description This command defines the time before the PPP session is terminated.

A RADIUS specified session-timeout (attribute [27] Session-Timeout) overrides the CLI configured value.

The **no** form of this command reverts to the default.

Parameters *timeout* — Specifies the session timeout in seconds.

Values 1 to 31104000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

session-timeout

Syntax **session-timeout** *timeout*
no session-timeout

Context **[Tree]** (config>subscr-mgmt>ipoe-plcy session-timeout)

Full Context configure subscriber-mgmt ipoe-session-policy session-timeout

Description This command defines the time in seconds between 1 second and 360 days before the IPoE session is disconnected. The default value is unlimited session timeout.

The **no** form of this command reverts to the default.

Parameters *timeout* — Specifies the session timeout in seconds.

Values 1 to 31104000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.186 set-time

set-time

Syntax **set-time** *date time*

Context **[Tree]** (admin set-time)

Full Context admin set-time

Description This command sets the local system time.

The time entered should be accurate for the time zone configured for the system. The system will convert the local time to UTC before saving to the system clock which is always set to UTC. This command does not take into account any daylight saving offset if defined.

If SNTP or NTP is enabled (no shutdown) then this command cannot be used.

Parameters *date* — Specifies the local date and time accurate to the minute in the YYYY/MM/DD format.

Values *YYYY* is the four-digit year
MM is the two-digit month
DD is the two-digit date

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

time — Specifies the time (accurate to the second) in the *hh*:*mm[:ss]* format. If no seconds value is entered, the seconds are reset to :00.

Values *hh* is the two-digit hour in 24 hour format (00=midnight, 12=noon)*mm* is the two-digit minute

Default 0

Platforms All

23.187 set-tos

set-tos

Syntax **set-tos** [**0**..**255**]
no set-tos

Context **[Tree]** (config>service>vprn>nat>inside>nat64 set-tos)
[Tree] (config>router>nat>inside>nat64 set-tos)

Full Context configure router nat inside nat64 set-tos
configure service vprn nat inside nat64 set-tos

Description This command specifies the value of the IPv4 ToS field. When enabled, the NAT64 node ignores IPv6 traffic-class and sets IPv4 ToS to the supplied ToS value in the translated IPv4 packet.

The **no** form of the command reverts to the default.

Default set-tos 0

Parameters [**0**..**255**] — Sets the IPv4 ToS to a fixed value the IPv6 Traffic Class and set the IPv4 ToS to a fixed value and ignores the IPv6 traffic class.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.188 setup-role

setup-role

Syntax **setup-role** {**active** | **passive**}

Context **[Tree]** (config>router>lmp>peer>control-channel setup-role)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router lmp peer control-channel setup-role

Description This command specifies whether this node takes the active or the passive role in establishing the LMP session to the peer over a GMPLS UNI.

Default setup-role active

Parameters **active** — The router takes the active role.

passive — The router takes the passive role.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.189 setup-timeout

setup-timeout

Syntax **setup-timeout access-accept** *timeout*
no setup-timeout

Context **[Tree]** (config>service>dynsvc>timers setup-timeout)

Full Context configure service dynamic-services timers setup-timeout

Description This command specifies the time that dynamic data services setup requests from a RADIUS Access-Accept are hold in an internal work queue waiting to be processed. If after the timeout, the dynamic data service setup request is still in the queue (meaning it is not setup), then the dynamic service setup request is removed from the queue and the setup fails.

The **no** form of this command reverts to the default value of 30 seconds.

Default no setup-timeout

Parameters *timeout* — Specifies the setup-timeout, in seconds, for setup requests of dynamic services received via Access-Accept.

Values 2 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.190 severity

severity

Syntax **severity** {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *severity-level*
no severity

Context **[Tree]** (config>service>vprn>log>filter>entry>match severity)

Full Context configure service vprn log filter entry match severity

Description This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command.

The **no** form of this command removes the severity match criterion.

Default no severity

Parameters **eq | neq | lt | lte | gt | gte** — Specifies the type of match. Valid operators are listed below.

Values

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

severity-name — The ITU severity level name. Table 126 lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 126 **Severity Levels**

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Values cleared, intermediate, critical, major, minor, warning

Platforms All

severity

Syntax **severity** *syslog-severity*

Context **[Tree]** (config>app-assure>group>evt-log>syslog severity)

Full Context configure application-assurance group event-log syslog severity

Description This command configures the syslog message severity level threshold.

Default severity info

Parameters *syslog-severity* — Specifies the severity level for the syslog message.

Values emergency, alert, critical, error, warning, notice, info, debug

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

severity

Syntax **severity** {**eq** | **neq** | **lt** | **lte** | **gt** | **gte**} *severity-level*
no severity

Context **[Tree]** (config>log>filter>entry>match severity)

Full Context configure log filter entry match severity

Description This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the severity match criterion.

Parameters **eq | neq | lt | lte | gt | gte** — Specifies the match type. Valid operators are listed in Table 127.

Table 127 **Valid Operators**

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

severity-name — Specifies the ITU severity level name. Table 128 lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

Table 128 **ITU Severity Information**

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Values cleared, intermediate, critical, major, minor, warning

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.191 severity-level

severity-level

Syntax **severity-level** *syslog-level*

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy severity-level)

Full Context configure service nat syslog syslog-export-policy severity-level

Description This command configures the severity level.

For more information, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. The **config>log>syslog>level** hierarchy also applies to this context.

Default severity-level info

Parameters *syslog-level* — Specifies the severity level.

Values emergency, alert, critical, error, warning, notice, info, debug

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.192 sf-offset

sf-offset

Syntax **sf-offset** *offset-value*
no sf-offset

Context **[Tree]** (config>service>vprn>isis>if>level sf-offset)

Full Context configure service vprn isis interface level sf-offset

Description If the pre-FEC error rate of the associated DWDM port crosses the configured **sf-threshold**, this offset-value is added to the IS-IS interface metric. This parameter is only effective if the interface is associated with a DWDM port and the **sf-threshold** value is configured under that port.

The **no** form of this command reverts the offset value to 0.

Default no sf-offset

Parameters *offset-value* — Specifies the amount the interface metric is increased by if the **sf-threshold** is crossed.

Values 0 to 16777215

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

sf-offset

Syntax **sf-offset** *offset-value*
no sf-offset

Context **[Tree]** (config>router>isis>if>level sf-offset)

Full Context configure router isis interface level sf-offset

Description If the pre-FEC error rate of the associated DWDM port crosses the configured **sf-threshold**, this offset-value is added to the IS-IS interface metric. This parameter is only effective if the interface is associated with a DWDM port and the **sf-threshold** value is configured under that port.

The **no** form of this command reverts the offset value to 0.

Default no sf-offset

Parameters *offset-value* — Specifies the amount the interface metric is increased by if the **sf-threshold** is crossed.

Values 0 to 16777215

Platforms All

23.193 sf-sd-method

sf-sd-method

Syntax **sf-sd-method** {**bip8** | **fec**}

Context **[Tree]** (config>port>otu sf-sd-method)

Full Context configure port otu sf-sd-method

Description This command specifies the method used to determine the signal failure (SF) and signal degrade (SD) alarms. When the **bip8** method is selected, the SM-BIP8 errors are used. When the **fec** method is selected, the FEC corrected bits are used.

The following rules must be followed:

- The port's OTU must be enabled to set or change the **sf-sd-method**.
- The FEC mode must be **enhanced** or **g709** before setting **sf-sd-method** to **fec**.
- The SF threshold must be 5 or higher before setting **sf-sd-method** to **bip8**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default sf-sd-method fec

Parameters **bip8** — Specifies that SM-BIP8 errors are used to declare the presence of the SF and SD conditions.

fec — Specifies that FEC corrected bit errors are used to declare the presence of the SF and SD conditions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.194 sf-threshold

sf-threshold

Syntax **sf-threshold** *threshold* [**coefficient** *coefficient*]

Context **[Tree]** (config>port>otu sf-threshold)

Full Context configure port otu sf-threshold

Description This command defines the error rate at which to declare the signal failure (SF) condition.

The parameters define an error rate of (*coefficient*/10) * 10E-*threshold*. For example, **sf-threshold 5 coefficient 20** defines an error rate of (20/10) * 10E-5, or 2 * 10E-5, or 0.000 02.

The SF threshold must be the following:

- less than the SD threshold
- 5 or higher before setting **sf-sd-method** to **bip8**

The **coefficient** parameter is only used when **sf-sd-method** is set to **fec**. When **sf-sd-method** is set to **bip8**, **coefficient** is considered to have the value of 10.

Parameters *threshold* — Specifies the exponent for the SF threshold value.

Values 3 to 6 when **sf-sd-method** is **bip8**
3 to 8 when **sf-sd-method** is **fec**

Default 5

coefficient — Specifies the coefficient for the SF threshold value.

Values 10 to 99

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sf-threshold

Syntax **sf-threshold** *errored-frames*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame sf-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-frame sf-threshold

Description The option defines the number of frame errors within the configured window which indicates the port has exceeded an acceptable error rate. A log event will be raised, and the port will be taken out of service by default. Configuration options exist to take additional actions when the error rate exceeds the threshold. These actions are defined using the **local-sf-action** configuration. This event can only be cleared through manual intervention that affects the state of the port.

Parameters *errored-frames* — The number of errored frames within the configured window which indicates the port has become unusable.

Values 1 to 1000000

Default 1

Platforms All

sf-threshold

Syntax **sf-threshold** *errored-frames*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame-period sf-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-period sf-threshold

Description This command defines the number of frame errors within the configured window which indicates the port has exceeded an acceptable error rate. A log event will be raised, and the port will be taken out of service by default. Configuration options exist to take additional actions when the error rate exceeds the threshold. These actions are defined using the local-sf-action configuration. This event can only be cleared through manual intervention that affects the state of the port.

Default sf-threshold 1

Parameters *errored-frames* — Specifies the number of errored frames within the configured window which indicates the port has become unusable.

Values 1 to 1000000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sf-threshold

Syntax **sf-threshold** *errored-seconds*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame-seconds sf-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-seconds sf-threshold

Description This command defines the number of errors seconds within the configured window which indicates the port has exceeded an acceptable error rate. A log event will be raised, and the port will be taken out of service by default. Configuration options exist to take additional actions when the error rate exceeds the threshold. These actions are defined using the **local-sf-action** configuration. This event can only be cleared through manual intervention that affects the state of the port.

Parameters *errored-seconds* — Specifies the number of errored seconds within the configured window which indicates the port has become unusable.

Values 1 to 900

Platforms All

sf-threshold

Syntax **sf-threshold** *errored-symbols*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-symbols sf-threshold)

Full Context configure port ethernet efm-oam link-monitoring errored-symbols sf-threshold

Description This command defines the number of symbol errors within the configured window which indicates the port has exceeded an acceptable error rate. A log event will be raised, and the port will be taken out of service by default. Configuration options exist to take additional actions when the error rate exceeds the threshold. These actions are defined using the local-sf-action configuration.

Parameters *errored-symbols* — Specifies the number of errored-symbols which indicates the port has become unusable.

Values 1 to 1000000

Platforms All

sf-threshold

Syntax **sf-threshold** *threshold* [**multiplier** *multiplier*]
no sf-threshold

Context **[Tree]** (config>port>ethernet>sym-mon sf-threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet symbol-monitor sf-threshold

Description This command specifies the error rate at which to declare the Signal Fail condition on an Ethernet interface. The value represents M*10E-N symbol errors over total symbols received over W seconds of the sliding window. The symbol errors on the interface are sampled once per second. A default of 10 seconds is used when there is no additional window-size configured. The multiplier keyword is optional. If the multiplier keyword is omitted or no sf-threshold is specified, the multiplier will return to the default value of 1.

Default no sf-threshold

Parameters *threshold* — Specifies the rate of symbol errors.

Values 1 to 9

multiplier — Specifies the multiplier used to scale the symbol error ratio.

Values 1 to 9

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

sf-threshold

Syntax **sf-threshold** *threshold* [**multiplier** *multiplier*]
no sf-threshold

Context **[Tree]** (config>port>ethernet>crc-monitor sf-threshold)

Full Context configure port ethernet crc-monitor sf-threshold

Description This command specifies the error rate at which to declare the Signal Fail condition on an Ethernet interface. The value represents M*10E-N errored frames over total frames received over W seconds of the sliding window. The CRC errors on the interface are sampled once per second. A default of 10 seconds is used when there is no additional window-size configured. The multiplier keyword is optional. If the multiplier keyword is omitted or **no sf-threshold** is specified the multiplier will return to the default value of 1.

Default no sf-threshold

Parameters *threshold* — Specifies the threshold value.

Values 1 to 9

multiplier — Specifies the multiplier value.

Values 1 to 9

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.195 sf-threshold-clear

sf-threshold-clear

Syntax **sf-threshold-clear** *threshold* [**coefficient** *coefficient*]

Context **[Tree]** (config>port>otu sf-threshold-clear)

Full Context configure port otu sf-threshold-clear

Description This command defines the signal failure (SF) threshold clear value.

When the bit error rate falls below this value, the SF condition is cleared. The parameters define an error rate of (*coefficient*/10) * 10E-*threshold*. For example, **sf-threshold-clear 7 coefficient 10** defines an error rate of (10/10) * 10E-7, or 10E-7, or 0.000 000 1.

This SF threshold clear setting is valid only when **sf-sd-method** is set to **fec**.

Parameters *threshold* — Specifies the exponent for the SF threshold clear value.

Values 3 to 9

Default 6

coefficient — Specifies the coefficient for the SF threshold clear value.

Values 10 to 99

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.196 sflow

sflow

Syntax [**no**] **sflow**

Context **[Tree]** (config>port>ethernet sflow)

Full Context configure port ethernet sflow

Description This command enables sFlow data collection for a port and its SAPs that support sFlow data collection.

The **no** form of this of this command disables sFlow.

Default no sflow

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7750 SR, 7750 SR-s, 7950 XRS

sflow

Syntax **sflow**

Context **[Tree]** (config sflow)

Full Context configure sflow

Description Commands in this context configure sflow agent parameters.

Platforms 7750 SR, 7750 SR-s, 7950 XRS

23.197 sfm

sfm

Syntax **sfm** *sfm-name*
no sfm *sfm-name*

Context **[Tree]** (config sfm)

Full Context configure sfm

Description Commands in this context configure the specified SFM.

The **no** form of this command removes the SFM configuration for the specified SFM.

Parameters *sfm-name* —

Values 1 to 4

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-2s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

23.198 sfm-loss-threshold

sfm-loss-threshold

Syntax **sfm-loss-threshold** *num-sfm*
no sfm-loss-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>switch-fabric sfm-loss-threshold)

Full Context configure system switch-fabric sfm-loss-threshold

Description This command sets the number of SFMs that are permitted to fail before the system goes into SFM overload state. This command is only applicable on the 7750 SR-7s and the 7750 SR-14s. Users can select the SFM limit based on the number possible for the system minus one. For the 7750 SR-7s this is a value of 3 and for the 7750 SR-14s this is a value of 7.

For networks that can accommodate more SFM failures than the default value, this command allows the selection of the number of SFMs to fail prior to the system going into SFM overload state.

The **no** form of this command reverts the threshold to the default value.

Default 7750 SR-7s: sfm-loss-threshold 1

7750 SR-14s: sfm-loss-threshold 2

Parameters *num-sfm* — Specifies the number of SFMs permitted to fail before SFM overload state.

Values 1 to 7

Platforms 7750 SR-7s, 7750 SR-14s

23.199 sfm-type

sfm-type

Syntax **sfm-type** *sfm-type*
no sfm *sfm-type*

Context [Tree] (config>sfm sfm-type)

Full Context configure sfm sfm-type

Description This command provisions the SFM.

The **no** form of this command deprovisions the SFM.

Default no sfm *sfm-type*

Parameters *sfm-type* — Specifies the SFM card type.

Values Depending on the SR hardware platform.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-2s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.200 sg

sg

Syntax **sg** [**group** *grp-addr* [**source** *src-addr*]]
no sg

Context **[Tree]** (debug>service>id>video-interface sg)

Full Context debug service id video-interface sg

Description This command enables channel debugging.

Parameters **group** *grp-addr* — Specifies the multicast channel address.

source *src-addr* — Specifies the source address.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

23.201 sgsn-mcc-mnc

sgsn-mcc-mnc

Syntax [**no**] **sgsn-mcc-mnc**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp sgsn-mcc-mnc)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp sgsn-mcc-mnc

Description This command enables the inclusion of the 3GPP-SGSN-MCC-MNC AVP, which contains the MCC and MNC as configured under **configure subscriber-mgmt gtp serving-network**.

The **no** form of this command disables the inclusion of the AVP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.202 sgt-qos

sgt-qos

Syntax **sgt-qos**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router sgt-qos)
[Tree] (config>service>vprn sgt-qos)

Full Context configure router sgt-qos
configure service vprn sgt-qos

Description Commands in this context configure DSCP/dot1p remarking for self-generated traffic.

Platforms All

23.203 shallow-inspection

shallow-inspection

Syntax [**no**] **shallow-inspection**

Context [Tree] (config>app-assure>group shallow-inspection)

Full Context configure application-assurance group shallow-inspection

Description This command disables all Layer 7 signature-based flow inspection.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.204 sham-link

sham-link

Syntax **sham-link** *ip-int-name ip-address*

Context [Tree] (config>service>vprn>ospf>area sham-link)

Full Context configure service vprn ospf area sham-link

Description This command is similar to a virtual link with the exception that metric must be included in order to distinguish the cost between the MPLS-VPRN link and the backdoor.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-int-name* — The local interface name used for the sham-link. This is a mandatory parameter and interface names must be unique within the group of defined IP interfaces for **config>router>if**, **config>service>ies>if** and **config>service>vprn>if** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters, the entire string must be enclosed between double quotes. If the IP interface name does not exist or does not have an IP address configured, an error message will be returned.

ip-address — The IP address of the sham-link neighbor in IP address dotted decimal notation. This parameter is the remote peer of the sham link's IP address used to set up the sham-link. This is a mandatory parameter and must be a valid IP address.

Platforms All

23.205 sham-neighbor

sham-neighbor

Syntax **sham-neighbor** [*ip-address*]
no sham-neighbor

Context **[Tree]** (debug>router>ospf sham-neighbor)

Full Context debug router ospf sham-neighbor

Description This command enables debugging of the OSPFv2 sham-link neighbor.

Parameters *ip-address* — Debugs the sham-link neighbor identified by this IP address.

Platforms All

23.206 shape-multi-client-only

shape-multi-client-only

Syntax [**no**] **shape-multi-client-only**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>egress shape-multi-client-only)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress shape-multi-client-only

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the egress shaping is only enabled for a wlan-gw tunnel while there are multiple UE (User Equipment) using it.

The **no** form of this command disables the egress shaping.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.207 shaper

shaper

Syntax [**no**] **shaper**

Context **[Tree]** (config>service>sdp>binding>pw-port>egress shaper)

Full Context configure service sdp binding pw-port egress shaper

Description This command enables the egress shaping option for use by a pseudowire port.

The **no** form of the command disables the egress shaping option.

Default no shaper

Platforms All

shaper

Syntax [**no**] **shaper**

Context **[Tree]** (config>service>epipe>pw-port>egress shaper)

Full Context configure service epipe pw-port egress shaper

Description Commands in this context configure PW-port shaper parameters.

Platforms All

23.208 shaping

shaping

Syntax **shaping** {**per-retailer** | **per-tunnel**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no shaping

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>egress shaping)

Full Context configure service ies subscriber-interface group-interface wlan-gw egress shaping

Description This command configures the granularity of the egress shaping for wlan-gw on this group interface.

The **no** form of this command removes the parameter from the configuration.

Parameters **per-tunnel** — Specifies that a separate shaper is applied to each wlan-gw tunnel.

per-retailer — Specifies that a separate shaper is applied to each retailer Mobile Network Operator's fraction of the wlan-gw tunnel payload.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shaping

Syntax [**no**] **shaping**

Context **[Tree]** (config>qos>atm-td-profile shaping)

Full Context configure qos atm-td-profile shaping

Description This command enables cell level shaping when the ATM traffic descriptor profile is applied to an ATM SAP queue. Shaping is only applied in the egress queue of the ATM SAP. Shaping cannot be enabled on an ATM SAP with the UBR service category.

The **no** form of this command disables shaping.

Default The default is determined by the service category. Table 129 lists which defaults apply for shaping depending on the service and UBR/UBR+MIR category.

Table 129 **Default Shaping Values**

Applicable Service Category	Default Shaping Value	Comments
UBR	disabled	Shaping cannot be enabled
CBR	enabled	Shaping cannot be disabled when the profile is applied to ATM SAP on ATM MDA
rt-VBR	enabled	Shaping cannot be disabled when applied to ATM SAP on ATM MDA

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 129 **Default Shaping Values**

Applicable Service Category	Default Shaping Value	Comments
nrt-VBR	enabled	—

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

23.209 shared-circuit-id

shared-circuit-id

Syntax [**no**] **shared-circuit-id**

Context **[Tree]** (config>service>ies>sub-if>grp-if shared-circuit-id)
[Tree] (config>service>vprn>sub-if>grp-if shared-circuit-id)

Full Context configure service ies subscriber-interface group-interface shared-circuit-id
configure service vprn subscriber-interface group-interface shared-circuit-id

Description If configured, circuit-id in DHCPv4 Option82 is used to authenticate DHCPv6. If DHCPv6 is received before DHCPv4, it is dropped. Also, a SLAAC host is created based on DHCPv4 authentication if RADIUS returns IPv6 framed-prefix. The IPv6oE host is deleted if the linked IPv4oE host is deleted due to DHCP release or lease time-out. The linkage between IPv4 and IPv6 is based on SAP and MAC address. The sharing of circuit-id from DHCPv4 for authentication of DHCPv6 (or SLAAC) allows 7750 SR to work around lack of support for LDRA on access nodes.

The **no** form of this command reverts to the default.

23.210 shared-queue

shared-queue

Syntax **shared-queue** *policy-name* [**create**]
no shared-queue *policy-name*

Context **[Tree]** (config>qos shared-queue)

Full Context configure qos shared-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context modify the QoS default shared-queue policy.

Parameters *policy-name* — The name of the default shared-queue policy.

Values default

Platforms All

shared-queue

Syntax **shared-queue** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy shared-queue)

Full Context configure qos copy shared-queue

Description This command copies an existing **shared-queue** to another **shared-queue**. The **copy** command is a configuration level maintenance tool used to create new entries using an existing mapping policy name. If **overwrite** is not specified, an error occurs if the destination policy exists.

Parameters *src-name* — Specifies the existing source **shared-queue**, up to 32 characters, from which the **copy** command attempts to copy.

dst-name — Specifies the destination **shared-queue**, up to 32 characters, to which the copy command attempts to copy.

overwrite — Use this parameter when the **shared-queue** *dst-name* already exists. If it does, everything in the existing destination **shared-queue** *dst-name* is completely overwritten with the contents of the **shared-queue** *src-name*. The **overwrite** parameter must be specified or else the following error message is returned:

```
MINOR: CLI Destination "sqtest10" exists - use {overwrite}.
```

If **overwrite** is specified, the function of copying from source to destination occurs in a “break before make” manner and therefore should be handled with care.

Platforms All

23.211 shared-radius-filter-wmark

shared-radius-filter-wmark

Syntax **shared-radius-filter-wmark low** *low-watermark* **high** *high-watermark*
no shared-radius-filter-wmark

Context **[Tree]** (config>filter>ip-filter shared-radius-filter-wmark)
[Tree] (config>filter>ipv6-filter shared-radius-filter-wmark)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter ip-filter shared-radius-filter-wmark
configure filter ipv6-filter shared-radius-filter-wmark

Description This command configures the low and high watermark for the number of RADIUS shared filters reporting

Default no shared-radius-filter-wmark

Parameters *low-watermark* — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be raised by the agent.

Values 0 to 8000

high-watermark — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be cleared by the agent.

Values 1 to 8000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.212 shared-resources

shared-resources

Syntax **shared-resources**

Context **[Tree]** (config>isa>aa-grp shared-resources)

Full Context configure isa application-assurance-group shared-resources

Description Commands in this context configure the shared resources pool.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.213 shcv-policy

shcv-policy

Syntax **shcv-policy** *name* [**create**]
no shcv-policy *name*

Context **[Tree]** (config>subscr-mgmt shcv-policy)

Full Context configure subscriber-mgmt shcv-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a Subscriber Host Connectivity Verification (SHCV) policy. An SHCV policy can be applied to both the subscriber management group interface and VPLS instances. All SHCV-related features inside a group interface and a VPLS service follows the configuration specified in the SHCV policy. The SHCV policy and the SHCV configuration on a group interface are mutually exclusive. Only one can be applied to the group interface.

The **no** form of this command removes the policy name from the configuration.

Parameters *name* — Specifies the name of the SHCV policy, up to 32 characters.

create — Keyword required to create the configuration context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shcv-policy

Syntax **shcv-policy** *name*
no shcv-policy

Context **[Tree]** (config>service>vprn>sub-if>grp-if shcv-policy)
[Tree] (config>service>ies>sub-if>grp-if shcv-policy)

Full Context configure service ies subscriber-interface group-interface shcv-policy
configure service vprn subscriber-interface group-interface shcv-policy

Description This command references the SHCV policy to be used for both IPv4 and IPv6 subscriber hosts. The policy name must already exist in the **config>subscr-mgmt** context.

The **no** form of this command removes the policy name from the service configuration.

Parameters *name* — Specifies an existing SHCV policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.214 shcv-policy-ipv4

shcv-policy-ipv4

Syntax **shcv-policy-ipv4** *name*
no shcv-policy-ipv4

Context **[Tree]** (config>service>vpls shcv-policy-ipv4)
[Tree] (config>service>vpls>sap shcv-policy-ipv4)
[Tree] (config>service>ies>if shcv-policy-ipv4)
[Tree] (config>service>ies>sub-if>grp-if shcv-policy-ipv4)
[Tree] (config>service>vprn>if shcv-policy-ipv4)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if shcv-policy-ipv4)

Full Context configure service ies interface shcv-policy-ipv4
configure service ies subscriber-interface group-interface shcv-policy-ipv4
configure service vpls sap shcv-policy-ipv4
configure service vpls shcv-policy-ipv4
configure service vprn interface shcv-policy-ipv4
configure service vprn subscriber-interface group-interface shcv-policy-ipv4

Description This command specifies the Subscriber Host Connectivity Verification (SHCV) policy to be used exclusive for IPv4 subscriber hosts. The shcv-policy name must already exist in the **config>subscr-mgmt** context.

The **no** form of this command removes the policy name from the service configuration.

Parameters *name* — Specifies an existing SHCV policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.215 shcv-policy-ipv6

shcv-policy-ipv6

Syntax **shcv-policy-ipv6** *name*
no shcv-policy-ipv6

Context [Tree] (config>service>ies>if shcv-policy-ipv6)
[Tree] (config>service>ies>sub-if>grp-if shcv-policy-ipv6)
[Tree] (config>service>vprn>if shcv-policy-ipv6)
[Tree] (config>service>vprn>sub-if>grp-if shcv-policy-ipv6)

Full Context configure service ies interface shcv-policy-ipv6
configure service ies subscriber-interface group-interface shcv-policy-ipv6
configure service vprn interface shcv-policy-ipv6
configure service vprn subscriber-interface group-interface shcv-policy-ipv6

Description This command references the Subscriber Host Connectivity Verification (SHCV) policy to be used exclusive for IPv6 subscriber hosts. The policy name must already exist in the **config>subscr-mgmt** context.

The **no** form of this command removes the policy name from the service configuration.

Parameters *name* — Specifies an existing SHCV policy name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.216 shell

shell

Syntax **shell -password** *password*
no shell

Context **[Tree]** (environment shell)

Full Context environment shell

Description This command enables and disables the shell.

Parameters *password* — Specifies the password to enter the shell, up to 256 characters.

Platforms All

23.217 short-duration-flow-count

short-duration-flow-count

Syntax [**no**] **short-duration-flow-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-cntr short-duration-flow-count)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-counters short-duration-flow-count

Description This command includes the short duration flow count in the AA subscriber's custom record. This command only applies to the 7750 SR.

The **no** form of this command excludes the short duration flow count.

Default no short-duration-flow-count

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.218 short-sequence

short-sequence

Syntax [**no**] **short-sequence**

Context **[Tree]** (config>port>multilink-bundle short-sequence)

Full Context configure port multilink-bundle short-sequence

Description This command specifies that the Multi-link Point to Point Protocol (MLPPP) bundle should use short (12 bit) sequence numbers instead of the default 24-bit sequence number. This command is only valid for MLPPP bundles.

The **no** form of this command disables the short-sequence feature.

Default no short-sequence

Platforms 7450 ESS, 7750 SR-7/12/12e

23.219 short-sequence-numbers

short-sequence-numbers

Syntax [**no**] **short-sequence-numbers**

Context **[Tree]** (config>subscr-mgmt>ppp-policy>mlppp short-sequence-numbers)
[Tree] (config>router>l2tp>group>mlppp short-sequence-numbers)
[Tree] (config>router>l2tp>group>tunnel>mlppp short-sequence-numbers)
[Tree] (config>service>vprn>l2tp>group>mlppp short-sequence-numbers)
[Tree] (config>service>vprn>l2tp>group>tunnel>mlppp short-sequence-numbers)

Full Context configure router l2tp group mlppp short-sequence-numbers
configure router l2tp group tunnel mlppp short-sequence-numbers
configure service vprn l2tp group mlppp short-sequence-numbers
configure service vprn l2tp group tunnel mlppp short-sequence-numbers
configure subscriber-mgmt ppp-policy mlppp short-sequence-numbers

Description This command enables a peer request to send short sequence numbers. This command is applicable to LAC and LNS. By default, MLPPPoX negotiates 24bit long sequence numbers. This command allows this to be changed to shorter, 12-bit sequence numbers.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.220 shortcut-local-ttl-propagate

shortcut-local-ttl-propagate

Syntax [**no**] **shortcut-local-ttl-propagate**

Context **[Tree]** (config>router>ldp shortcut-local-ttl-propagate)
[Tree] (config>router>mpls shortcut-local-ttl-propagate)

Full Context configure router ldp shortcut-local-ttl-propagate
configure router mpls shortcut-local-ttl-propagate

Description This command configures the TTL handling of locally generated packets for all LSP shortcuts originating on this ingress LER. It applies to all LDP or RSVP LSPs that are used to resolve static routes, BGP routes, and IGP routes.

The user can enable or disable the propagation of the TTL from the header of an IP packet into the header of the resulting MPLS packet independently for local and transit packets forwarded over an LSP shortcut.

Local IP packets include ICMP Ping, traceroute, and OAM packets, that are destined to a route that is resolved to the LSP shortcut. Transit IP packets are all IP packets received on any IES interface and destined to a route that is resolved to the LSP shortcut

By default, the feature propagates the TTL from the header of locally generated IP packets into the label stack of the resulting MPLS packets forwarded over the LSP shortcut. This is referred to as Uniform mode.

When the **no** form of this command is enabled, TTL propagation is disabled on all locally generated IP packets, including ICMP Ping, traceroute, and OAM packets, that are destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack. This is referred to as Pipe mode.

Default shortcut-local-ttl-propagate

Platforms All

23.221 shortcut-transit-ttl-propagate

shortcut-transit-ttl-propagate

Syntax [**no**] **shortcut-transit-ttl-propagate**

Context **[Tree]** (config>router>ldp shortcut-transit-ttl-propagate)
[Tree] (config>router>mpls shortcut-transit-ttl-propagate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ldp shortcut-transit-ttl-propagate
configure router mpls shortcut-transit-ttl-propagate

Description This command configures the TTL handling of transit packets for all LSP shortcuts originating on this ingress LER. It applies to all LDP or RSVP LSPs that are used to resolve static routes, BGP routes, and IGP routes.

The user can enable or disable the propagation of the TTL from the header of an IP packet into the header of the resulting MPLS packet independently for local and transit packets forwarded over an LSP shortcut.

By default, the feature propagates the TTL from the header of transit IP packets into the label stack of the resulting MPLS packets forwarded over the LSP shortcut. This is referred to as Uniform mode.

When the **no** form of the command is enabled, TTL propagation is disabled on all transit IP packets received on any IES interface and destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack. This is referred to as Pipe mode.

Default shortcut-transit-ttl-propagate

Platforms All

23.222 shortcut-tunnel

shortcut-tunnel

Syntax **shortcut-tunnel**

Context **[Tree]** (config>router>bgp>next-hop-resolution shortcut-tunnel)

Full Context configure router bgp next-hop-resolution shortcut-tunnel

Description This command creates the context to configure the tunnel types that can be used to resolve unlabeled IPv4 and IPv6 BGP routes.

The following tunnel types are supported for resolving IPv4 routes and IPv6 routes with IPv4-mapped IPv6 next-hop addresses: bgp, ldp, rsvp, sr-isis, sr-ospf, sr-policy and sr-te. In this context:

- **bgp** — refers to IPv4 tunnels created by receiving BGP label-unicast IPv4 routes for /32 IPv4 prefixes.
- **ldp** — refers to /32 and shorter length LDP FEC prefixes imported into the tunnel table. For IPv4 NLRI, BGP selects the LDP FEC that is the longest-prefix-match (LPM) of the BGP next-hop address. For IPv6 NLRI, BGP selects the /32 FEC that is an exact match of the BGP next-hop address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **rsvp** — refers to RSVP tunnels in the tunnel table to IPv4 destinations. This option allows BGP to use the best metric RSVP LSP to the address of the BGP next-hop. This address can correspond to the system interface or to another loopback interface of the remote BGP router. In the case of multiple RSVP LSPs with the same lowest metric, BGP selects the LSP with the lowest tunnel id.
- **sr-isis** — refers to segment routing tunnels (shortest path) to IPv4 destinations reachable by the IS-IS protocol. This option allows BGP to use the segment routing tunnel in the tunnel table submitted by the lowest preference IS-IS instance or (in case of a tie) the lowest numbered IS-IS instance.
- **sr-ospf** — refers to segment routing tunnels (shortest path) to IPv4 destinations reachable by the OSPF protocol. This option allows BGP to use the segment routing tunnel in the tunnel table submitted by the lowest preference OSPF instance or (in case of a tie) the lowest numbered OSPF instance.
- **sr-policy** — refers to segment routing policies with an IPv4 endpoint that are statically configured in the local router or learned through BGP routes (AFI 1/SAFI 73). For BGP to resolve the next hop of an unlabeled IPv4 or IPv6 route using a segment routing policy the highest numbered color extended community attached to the IPv4 or IPv6 route must match the color of the segment routing policy.
- **sr-te** — refers to traffic engineered (TE) segment routing tunnels. This option allows BGP to use the best metric SR-TE tunnel to the address of the BGP next-hop. In the case of multiple SR-TE tunnels with the same lowest metric, BGP selects the tunnel with the lowest tunnel id.
- **udp** — refers to MPLSoUDPoIPv4 tunnels set up by action of the BGP import policies.

The following tunnel types are supported for resolving IPv6 routes with IPv6 next-hops that are not IPv4-mapped IPv6 addresses: ldp, sr-isis, and sr-policy. In this context:

- **ldp** — refers to /128 LDP FEC prefixes in the tunnel table. BGP selects the /128 FEC that is an exact match of the BGP next-hop address.
- **sr-isis** — refers to segment routing tunnels (shortest path) to IPv6 destinations reachable by the IS-IS protocol. This option allows BGP to use the segment routing tunnel in the tunnel table submitted by the lowest preference IS-IS instance or (in case of a tie) the lowest numbered IS-IS instance.
- **sr-policy** — refers to segment routing policies with a null IPv4 endpoint (0.0.0.0) that are statically configured in the local router or learned through BGP routes (AFI 1/SAFI 73). For BGP to resolve the next hop of an IPv6 route using a segment routing policy the highest numbered color extended community attached to the IPv6 route must match the color of the segment routing policy and its color bits must be set to '01' or '10'.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.223 show-ipsec-keys

show-ipsec-keys

Syntax [**no**] **show-ipsec-keys**

Context **[Tree]** (config>ipsec show-ipsec-keys)

Full Context configure ipsec show-ipsec-keys

Description This command enables user to optionally include IKE-SA or CHILD-SA keys in the output of **debug ipsec** or **admin ipsec display-key**.

The **no** form of this command disallows the user from including keys in the output.

Default no show-ipsec-keys

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.224 show-request

show-request

Syntax **show-request** [**ca** *ca-profile-name*]

Context **[Tree]** (admin>certificate>cmpv2 show-request)

Full Context admin certificate cmpv2 show-request

Description This command displays current the CMPv2 pending request toward the specified CA. If there is no pending request, the last pending request is displayed including the status (success/fail/rejected) and the receive time of last CMPv2 message from server.

The following information is included in the output:

- Request type, original input parameter (password is not displayed), checkAfter and reason in of last PollRepContent, time of original command input.

Parameters *ca-profile-name* — Specifies a ca-profile name, up to 32 characters. If not specified, the system will display pending requests of all ca-profiles.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.225 shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>grpc-tunnel>tunnel shutdown)
[Tree] (config>system>grpc-tunnel>tunnel>handler shutdown)
[Tree] (config>system>grpc-tunnel>destination-group>tcp-keepalive shutdown)
[Tree] (config>li>x-interfaces shutdown)
[Tree] (config>system>cron>sched shutdown)
[Tree] (config>system>satellite>local-forward>sap shutdown)
[Tree] (config>system>satellite>port-template shutdown)
[Tree] (config>system>time>ntp shutdown)
[Tree] (config>system>time>sntp shutdown)
[Tree] (config>system>script-control>script-policy shutdown)
[Tree] (config>system>script-control>script shutdown)
[Tree] (config>system>sync-if-timing>ref1 shutdown)
[Tree] (config>system>sync-if-timing>ref2 shutdown)
[Tree] (config>system>sync-if-timing>synce shutdown)
[Tree] (config>system>sync-if-timing>ptp shutdown)
[Tree] (config>system>sync-if-timing>bits>input shutdown)
[Tree] (config>system>sync-if-timing>bits>output shutdown)
[Tree] (config>system>persistence>app-assure shutdown)
[Tree] (config>system>persistence>dhcp-server shutdown)
[Tree] (config>system>persistence>nat-port-forward shutdown)
[Tree] (config>system>persistence>python-policy-cache shutdown)
[Tree] (config>system>persistence>subscriber-mgmt shutdown)
[Tree] (config>system>ptp>ptsf>monitor shutdown)
[Tree] (config>system>telemetry>destination-group>tcp-keepalive shutdown)
[Tree] (config>system>telemetry>persistent-subscriptions>subscription shutdown)
[Tree] (config>system>lldp shutdown)
[Tree] (config>system>switch-fabric>failure-recovery shutdown)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy>efh shutdown)
[Tree] (config>eth-tunnel>path shutdown)
[Tree] (config>eth-tunnel shutdown)
[Tree] (config>service>vprn>mvpn>pt>inclusive>p2mp-sr shutdown)
[Tree] (config>service>vprn>mvpn>pt>selective>multistream-spmsi shutdown)
[Tree] (config>service>vprn>mvpn>pt>selective>p2mp-sr shutdown)
[Tree] (config>router>gmpls>lsp shutdown)
[Tree] (config>router>gmpls shutdown)
[Tree] (config>gmpls-tun-grp>member shutdown)
[Tree] (config>gmpls-tun-grp shutdown)
[Tree] (config>router>mpls>static-lsp shutdown)
[Tree] (config>router>mpls>fwd-policies>fwd-policy>egress-statistics shutdown)
[Tree] (config>router>mpls>fwd-policies>fwd-policy>ingress-statistics shutdown)
[Tree] (config>service>epipe>nat-outside shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>test-oam>mpls-dm shutdown)
[Tree] (config>oam-pm>streaming>delay-template shutdown)
[Tree] (config>router>fad>flex-algo shutdown)
[Tree] (config>system>telemetry>notification-bundling shutdown)

Full Context

configure eth-tunnel path shutdown
configure eth-tunnel shutdown
configure gmpls-tun-grp member shutdown
configure gmpls-tun-grp shutdown
configure li x-interfaces shutdown
configure oam-pm streaming delay-template shutdown
configure router flexible-algorithm-definitions flex-algo shutdown
configure router gmpls lsp shutdown
configure router gmpls shutdown
configure router mpls forwarding-policies forwarding-policy egress-statistics shutdown
configure router mpls forwarding-policies forwarding-policy ingress-statistics shutdown
configure router mpls static-lsp shutdown
configure service epipe nat-outside shutdown
configure service vprn mvpn provider-tunnel inclusive p2mp-sr shutdown
configure service vprn mvpn provider-tunnel selective multistream-spmsi shutdown
configure service vprn mvpn provider-tunnel selective p2mp-sr shutdown
configure subscriber-mgmt diameter-application-policy gy extended-failure-handling shutdown
configure system cron schedule shutdown
configure system grpc-tunnel destination-group tcp-keepalive shutdown
configure system grpc-tunnel tunnel handler shutdown
configure system grpc-tunnel tunnel shutdown
configure system lldp shutdown
configure system persistence application-assurance shutdown
configure system persistence dhcp-server shutdown
configure system persistence nat-port-forward shutdown
configure system persistence python-policy-cache shutdown
configure system persistence subscriber-mgmt shutdown
configure system ptp ptsf monitor-ptsf-unusable shutdown
configure system satellite local-forward sap shutdown
configure system satellite port-template shutdown
configure system script-control script shutdown
configure system script-control script-policy shutdown
configure system switch-fabric failure-recovery shutdown
configure system sync-if-timing bits input shutdown
configure system sync-if-timing bits output shutdown
configure system sync-if-timing ptp shutdown
configure system sync-if-timing ref1 shutdown
configure system sync-if-timing ref2 shutdown
configure system sync-if-timing synce shutdown
configure system telemetry destination-group tcp-keepalive shutdown
configure system telemetry notification-bundling shutdown
configure system telemetry persistent-subscriptions subscription shutdown
configure system time ntp shutdown
configure system time sntp shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure test-oam mpls-dm shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure li x-interfaces shutdown
- configure system ptp ptsf monitor-ptsf-unusable shutdown
- configure system sync-if-timing synce shutdown
- configure system satellite port-template shutdown
- configure system sync-if-timing bits output shutdown
- configure system sync-if-timing bits input shutdown
- configure oam-pm streaming delay-template shutdown
- configure system sync-if-timing ref1 shutdown
- configure eth-tunnel shutdown
- configure system satellite local-forward sap shutdown
- configure eth-tunnel path shutdown
- configure system sync-if-timing ptp shutdown
- configure test-oam mpls-dm shutdown
- configure system sync-if-timing ref2 shutdown

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt diameter-application-policy gy extended-failure-handling shutdown

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service epipe nat-outside shutdown

7450 ESS, 7750 SR-7, 7950 XRS

- configure system switch-fabric failure-recovery shutdown

7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router gmpls lsp shutdown
- configure router gmpls shutdown
- configure gmpls-tun-grp shutdown
- configure gmpls-tun-grp member shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

All

- configure service vprn mvpn provider-tunnel selective p2mp-sr shutdown
- configure service vprn mvpn provider-tunnel inclusive p2mp-sr shutdown
- configure system grpc-tunnel tunnel handler shutdown
- configure system time ntp shutdown
- configure router flexible-algorithm-definitions flex-algo shutdown
- configure system cron schedule shutdown
- configure system lldp shutdown
- configure system grpc-tunnel tunnel shutdown
- configure system script-control script-policy shutdown
- configure system telemetry notification-bundling shutdown
- configure service vprn mvpn provider-tunnel selective multistream-spmsi shutdown
- configure system grpc-tunnel destination-group tcp-keepalive shutdown
- configure system time sntp shutdown
- configure router mpls forwarding-policies forwarding-policy ingress-statistics shutdown
- configure system script-control script shutdown
- configure system telemetry destination-group tcp-keepalive shutdown
- configure system telemetry persistent-subscriptions subscription shutdown
- configure router mpls static-lsp shutdown
- configure router mpls forwarding-policies forwarding-policy egress-statistics shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vprn>mvpn>pt>selective>multistream-spmsi shutdown)

Full Context configure service vprn mvpn provider-tunnel selective multistream-spmsi shutdown

Description This commands enables multi-stream S-PSMI. At least one group must be active in a policy.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>aaa>radius-scr-plcy>primary shutdown)
[Tree] (config>aaa>radius-scr-plcy>secondary shutdown)
[Tree] (config>router>radius-proxy>cache shutdown)
[Tree] (config>router>radius-proxy>server>cache shutdown)
[Tree] (config>router>radius-proxy>server shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>radius-proxy>server>cache shutdown)
[Tree] (config>service>vprn>radius-proxy>server shutdown)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw shutdown)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-mgr>dhcp6-client>slaac shutdown)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-mgr>dhcp6-client>slaac shutdown)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-mgr>dhcp6-client>ia-na shutdown)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-mgr>dhcp6-client>ia-na shutdown)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-mgr>dhcp6-client>dhcpv4-nat shutdown)
[Tree] (config>service>vprn>sub-if>wlan-gw>pool-mgr>dhcp6-client>dhcpv4-nat shutdown)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>brg shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>brg shutdown)
[Tree] (config>service>ies>sub-if>grp-if>brg shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>brg shutdown)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-ranges>range>vrgw>brg shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-ranges>range>vrgw>brg shutdown)
[Tree] (config>service>vprn>mvpn>provider-tunnel>inclusive>bier shutdown)
[Tree] (config>service>vprn>mvpn>provider-tunnel>selective>bier shutdown)
[Tree] (config>service>vprn>mvpn>pt>inclusive>rsvp>lsp-template shutdown)
[Tree] (config>service>vprn>mvpn>pt>inclusive>mldp shutdown)
[Tree] (config>service>vprn>mvpn>pt>selective>rsvp shutdown)
[Tree] (config>service>vprn>mvpn>pt>selective>mldp shutdown)
[Tree] (config>router>lmp>peer>control-channel shutdown)
[Tree] (config>router>lmp>peer shutdown)
[Tree] (config>router>lmp>te-link shutdown)
[Tree] (config>router>lmp shutdown)
[Tree] (config>router>gmpls>lsp>working-path shutdown)
[Tree] (config>router>gmpls>lsp>protect-path shutdown)
[Tree] (config>router>gmpls>te-link shutdown)
[Tree] (config>router>mpls>mpls-tp>transit-path shutdown)
[Tree] (config>isa>video-group shutdown)
[Tree] (config>service>ies>video-interface shutdown)
[Tree] (config>service>vpls>video-interface shutdown)
[Tree] (config>service>vprn>video-interface shutdown)
[Tree] (config>router>igmp shutdown)
[Tree] (config>router>igmp>group-interface shutdown)
[Tree] (config>router>igmp>if shutdown)
[Tree] (config>router>igmp>tunnel-interface shutdown)
[Tree] (config>router>igmp>interface>mcac>mc-constraints shutdown)
[Tree] (config>router>mcac>if-policy shutdown)
[Tree] (config>router>mcac>policy>bundle shutdown)
[Tree] (config>router>mld>grp-if>mcac>mc-constraints shutdown)
[Tree] (config>router>mld shutdown)
[Tree] (config>router>mld>group-interface shutdown)
[Tree] (config>router>mld>if shutdown)
[Tree] (config>router>pim>interface>mcac>mc-constraints shutdown)
[Tree] (config>router>msdp shutdown)
[Tree] (config>router>msdp>peer shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>msdp>group shutdown)
[Tree] (config>router>pim shutdown)
[Tree] (config>router>pim>interface shutdown)
[Tree] (config>router>pim>rp>bsr-candidate shutdown)
[Tree] (config>router>pim>rp>ipv6>bsr-candidate shutdown)
[Tree] (config>router>pim>rp>ipv6>embedded-rp shutdown)
[Tree] (config>router>pim>rp>ipv6>rp-candidate shutdown)
[Tree] (config>router>pim>rp>rp-candidate shutdown)
[Tree] (config>cflowd shutdown)
[Tree] (config>cflowd>collector shutdown)
[Tree] (config>router shutdown)
[Tree] (config>router>if shutdown)
[Tree] (config>router>if>eth-cfm>mep shutdown)
[Tree] (config>router>mtrace2 shutdown)
[Tree] (config>router>origin-validation>rpki-session shutdown)
[Tree] (config>router>static-route-entry>black-hole shutdown)
[Tree] (config>router>static-route-entry>indirect shutdown)
[Tree] (config>router>static-route-entry>next-hop shutdown)
[Tree] (config>system>management-interface>cli>md-cli>environment>progress-indicator shutdown)

Full Context

configure aaa radius-script-policy primary shutdown
configure aaa radius-script-policy secondary shutdown
configure cflowd collector shutdown
configure cflowd shutdown
configure isa video-group shutdown
configure router gmpls lsp protect-path shutdown
configure router gmpls lsp working-path shutdown
configure router gmpls te-link shutdown
configure router interface eth-cfm mep shutdown
configure router interface shutdown
configure router igmp group-interface shutdown
configure router igmp interface shutdown
configure router igmp interface mcac mc-constraints shutdown
configure router igmp shutdown
configure router igmp tunnel-interface shutdown
configure router lmp peer control-channel shutdown
configure router lmp peer shutdown
configure router lmp shutdown
configure router lmp te-link shutdown
configure router mcac if-policy shutdown
configure router mcac policy bundle shutdown
configure router mld group-interface shutdown
configure router mld group-interface mcac mc-constraints shutdown
configure router mld interface shutdown
configure router mld shutdown
configure router mpls mpls-tp transit-path shutdown
configure router msdp group shutdown
configure router msdp peer shutdown
configure router msdp shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router mtrace2 shutdown
configure router origin-validation rpki-session shutdown
configure router pim interface mcac mc-constraints shutdown
configure router pim interface shutdown
configure router pim rp bsr-candidate shutdown
configure router pim rp ipv6 bsr-candidate shutdown
configure router pim rp ipv6 embedded-rp shutdown
configure router pim rp ipv6 rp-candidate shutdown
configure router pim rp rp-candidate shutdown
configure router pim shutdown
configure router radius-proxy cache shutdown
configure router radius-proxy server cache shutdown
configure router radius-proxy server shutdown
configure router shutdown
configure router static-route-entry black-hole shutdown
configure router static-route-entry indirect shutdown
configure router static-route-entry next-hop shutdown
configure service ies subscriber-interface group-interface brg shutdown
configure service ies subscriber-interface group-interface wlan-gw ranges range brg shutdown
configure service ies subscriber-interface group-interface wlan-gw shutdown
configure service ies subscriber-interface group-interface wlan-gw vlan-ranges range vrgw brg shutdown
configure service ies subscriber-interface wlan-gw pool-mgr dhcp6-client dhcpv4-nat shutdown
configure service ies subscriber-interface wlan-gw pool-mgr dhcp6-client ia-na shutdown
configure service ies subscriber-interface wlan-gw pool-mgr dhcp6-client slaac shutdown
configure service ies video-interface shutdown
configure service vpls video-interface shutdown
configure service vprn mvpn provider-tunnel inclusive bier shutdown
configure service vprn mvpn provider-tunnel selective bier shutdown
configure service vprn mvpn provider-tunnel inclusive mldp shutdown
configure service vprn mvpn pt inclusive rsvp lsp-template shutdown
configure service vprn mvpn provider-tunnel selective mldp shutdown
configure service vprn mvpn provider-tunnel selective rsvp shutdown
configure service vprn radius-proxy server cache shutdown
configure service vprn radius-proxy server shutdown
configure service vprn subscriber-interface group-interface brg shutdown
configure service vprn subscriber-interface group-interface wlan-gw ranges range brg shutdown
configure service vprn subscriber-interface group-interface wlan-gw shutdown
configure service vprn subscriber-interface group-interface wlan-gw vlan-ranges range vrgw brg shutdown
configure service vprn subscriber-interface wlan-gw pool-mgr dhcp6-client dhcpv4-nat shutdown
configure service vprn subscriber-interface wlan-gw pool-mgr dhcp6-client ia-na shutdown
configure service vprn subscriber-interface wlan-gw pool-mgr dhcp6-client slaac shutdown
configure service vprn video-interface shutdown
configure system management-interface cli md-cli environment progress-indicator shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system-generated configuration files.

The **no** form of this command places the entity into an administratively enabled state.

Default no shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router mpls mpls-tp transit-path shutdown
- configure router interface eth-cfm mep shutdown

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn radius-proxy server shutdown
- configure router radius-proxy server shutdown
- configure router mld group-interface mcac mc-constraints shutdown
- configure aaa radius-script-policy secondary shutdown
- configure router radius-proxy server cache shutdown
- configure service vprn subscriber-interface group-interface brg shutdown
- configure router mld group-interface shutdown
- configure service vprn radius-proxy server cache shutdown
- configure aaa radius-script-policy primary shutdown
- configure router igmp group-interface shutdown
- configure service ies subscriber-interface group-interface brg shutdown

7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

- configure service vpls video-interface shutdown
- configure service ies video-interface shutdown
- configure service vprn video-interface shutdown
- configure isa video-group shutdown

7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router gmpls lsp working-path shutdown
- configure router gmpls lsp protect-path shutdown
- configure router lmp peer shutdown
- configure router lmp peer control-channel shutdown
- configure router lmp te-link shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router shutdown
- configure router lmp shutdown
- configure router gmpls te-link shutdown

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface wlan-gw shutdown
- configure service vprn subscriber-interface group-interface wlan-gw shutdown

All

- configure router igmp tunnel-interface shutdown
- configure router pim rp bsr-candidate shutdown
- configure router mcac policy bundle shutdown
- configure router mcac if-policy shutdown
- configure router pim interface mcac mc-constraints shutdown
- configure router pim rp rp-candidate shutdown
- configure cflowd shutdown
- configure router pim interface shutdown
- configure router origin-validation rpki-session shutdown
- configure router pim rp ipv6 rp-candidate shutdown
- configure router static-route-entry black-hole shutdown
- configure router static-route-entry next-hop shutdown
- configure router msdp shutdown
- configure cflowd collector shutdown
- configure service vprn mvpn provider-tunnel selective mldp shutdown
- configure router pim shutdown
- configure system management-interface cli md-cli environment progress-indicator shutdown
- configure router msdp peer shutdown
- configure router mtrace2 shutdown
- configure service vprn mvpn provider-tunnel inclusive bier shutdown
- configure router igmp interface shutdown
- configure service vprn mvpn provider-tunnel selective bier shutdown
- configure router mld shutdown
- configure service vprn mvpn provider-tunnel selective rsvp shutdown
- configure router static-route-entry indirect shutdown
- configure router pim rp ipv6 bsr-candidate shutdown
- configure router msdp group shutdown
- configure service vprn mvpn provider-tunnel inclusive mldp shutdown
- configure router igmp shutdown
- configure router igmp interface mcac mc-constraints shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router interface shutdown
- configure router mld interface shutdown
- configure router pim rp ipv6 embedded-rp shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>shcv-policy>trigger shutdown)

Full Context configure subscriber-mgmt shcv-policy trigger shutdown

Description This command administratively disables the SHCV triggers.

The **no** form of this command administratively enables the the SHCV triggers.

Default no shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>shcv-policy>periodic shutdown)

Full Context configure subscriber-mgmt shcv-policy periodic shutdown

Description This command administratively disables the periodic connectivity verification.

The **no** form of this command administratively enables the periodic connectivity verification.

Default no shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vpls>sap>ipoe-session shutdown)
[Tree] (config>service>ies>sub-if>grp-if>ipoe-session shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session shutdown)

Full Context configure service ies subscriber-interface group-interface ipoe-session shutdown
configure service vpls sap ipoe-session shutdown
configure service vprn subscriber-interface group-interface ipoe-session shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **shutdown** command enables or disables IPoE session management on a group interface or capture SAP.

A **shutdown** of the IPoE session CLI hierarchy on a group-interface clears all active IPoE sessions on that interface, resulting in a deletion of all corresponding subscriber hosts.

On wlan-gw group interfaces it is not possible to disable an IPoE session.

The **no** form of this command reverts to the default.

Default shutdown no shutdown on wlan-gw group interfaces

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>ies shutdown)
[Tree] (config>service>ies>aarp-interface shutdown)
[Tree] (config>service>ies>aarp-interface>spoke-sdp shutdown)
[Tree] (config>service>ies>if shutdown)
[Tree] (config>service>ies>if>dhcp shutdown)
[Tree] (config>service>ies>if>dhcp>proxy-server shutdown)
[Tree] (config>service>ies>if>sap>eth-cfm shutdown)
[Tree] (config>service>ies>if>sap>static-host shutdown)
[Tree] (config>service>ies>if>spoke-sdp shutdown)
[Tree] (config>service>ies>if>spoke-sdp>control-channel-status shutdown)
[Tree] (config>service>ies>if>vrrp shutdown)
[Tree] (config>service>ies>redundant-interface shutdown)
[Tree] (config>service>ies>sub-if>dhcp shutdown)
[Tree] (config>service>ies>sub-if>grp-if shutdown)
[Tree] (config>service>ies>sub-if>grp-if>dhcp shutdown)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy-server shutdown)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>router-advertisements shutdown)
[Tree] (config>service>ies>sub-if>grp-if>pppoe shutdown)
[Tree] (config>service>ies>sub-if>grp-if>sap shutdown)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host shutdown)
[Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt shutdown)

Full Context configure service ies aarp-interface shutdown
configure service ies aarp-interface spoke-sdp shutdown
configure service ies interface dhcp proxy-server shutdown
configure service ies interface dhcp shutdown
configure service ies interface sap eth-cfm shutdown
configure service ies interface sap static-host shutdown
configure service ies interface shutdown
configure service ies interface spoke-sdp control-channel-status shutdown
configure service ies interface spoke-sdp shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface vrrp shutdown
configure service ies redundant-interface shutdown
configure service ies shutdown
configure service ies subscriber-interface dhcp shutdown
configure service ies subscriber-interface group-interface dhcp shutdown
configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server shutdown
configure service ies subscriber-interface group-interface ipv6 router-advertisements shutdown
configure service ies subscriber-interface group-interface pppoe shutdown
configure service ies subscriber-interface group-interface sap shutdown
configure service ies subscriber-interface group-interface sap static-host shutdown
configure service ies subscriber-interface group-interface sap sub-sla-mgmt shutdown
configure service ies subscriber-interface group-interface shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface pppoe shutdown
- configure service ies subscriber-interface group-interface sap sub-sla-mgmt shutdown
- configure service ies subscriber-interface group-interface sap static-host shutdown
- configure service ies subscriber-interface group-interface ipv6 router-advertisements shutdown
- configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server shutdown
- configure service ies subscriber-interface group-interface sap shutdown
- configure service ies redundant-interface shutdown
- configure service ies subscriber-interface group-interface shutdown
- configure service ies interface sap static-host shutdown
- configure service ies subscriber-interface dhcp shutdown
- configure service ies subscriber-interface group-interface dhcp shutdown

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies aarp-interface spoke-sdp shutdown
- configure service ies aarp-interface shutdown

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies interface vrrp shutdown
- configure service ies interface dhcp shutdown
- configure service ies interface spoke-sdp shutdown
- configure service ies interface dhcp proxy-server shutdown
- configure service ies shutdown
- configure service ies interface shutdown
- configure service ies interface spoke-sdp control-channel-status shutdown

Special Cases

IES — The default administrative status of an IES service is down. While the service is down, all its associated virtual router interfaces will be operationally down. The administrative state of the service is not reflected in the administrative state of the virtual router interface.

For example if:

1) An IES service is operational and an associated interface is shut down. 2) The IES service is administratively shutdown and brought back up. 3) The interface shutdown will remain in administrative shutdown state.

A service is regarded as operational provided that one IP Interface is operational.

Shutting down a subscriber interface will operationally shut down all child group interfaces and SAPs. Shutting down a group interface will operationally shut down all SAPs that are part of that group-interface.

IES IP Interfaces — When the IP interface is shutdown, it enters the administratively and operationally down states. For a SAP bound to the IP interface, no packets are transmitted out the SAP and all packets received on the SAP will be dropped while incrementing the packet discard counter.

shutdown

Syntax [**no**] **shutdown**

Context

[Tree] (config>subscr-mgmt>sub-ident-pol>primary shutdown)
[Tree] (config>subscr-mgmt>sub-ident-pol>secondary shutdown)
[Tree] (config>subscr-mgmt>sub-ident-pol>tertiary shutdown)
[Tree] (config>service>vpls>sap>sub-sla-mgmt shutdown)
[Tree] (config>service>vpls>gsmp shutdown)
[Tree] (config>service>vpls>gsmp>group shutdown)
[Tree] (config>service>vpls>gsmp>group>neighbor shutdown)
[Tree] (config>service>vprn>redundant-interface shutdown)
[Tree] (config>service>vprn>red-if>spoke-sdp shutdown)
[Tree] (config>service>vprn>subscriber-interface shutdown)
[Tree] (config>service>vprn>sub-if>grp-if shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>srrp shutdown)
[Tree] (config>service>ies>subscriber-interface shutdown)
[Tree] (config>service>ies>sub-if>grp-if>arp-host shutdown)
[Tree] (config>service>ies>sub-if>grp-if>wpp shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>wpp shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>wpp>portals shutdown)
[Tree] (config>redundancy>multi-chassis>peer shutdown)
[Tree] (config>redundancy>multi-chassis>peer>mc-lag shutdown)
[Tree] (config>redundancy>multi-chassis>peer>sync shutdown)
[Tree] (config>subscr-mgmt>sub-mcac-policy shutdown)
[Tree] (config>aaa>route-downloader shutdown)
[Tree] (config>aaa>diam-peer-plcy>peer shutdown)
[Tree] (config>aaa>diam-peer-plcy>proxy shutdown)
[Tree] (config>aaa>wpp>portal-groups>portal-group shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>data-trigger shutdown)
[Tree] (config>service>ies>sub-if>grp-if>data-trigger shutdown)
[Tree] (config>service>ies>sub-if>grp-if>gtp-parameters shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>gtp-parameters shutdown)
[Tree] (config>service>ies>sub-if>grp-if>srrp shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>srrp shutdown)
[Tree] (config>aaa>diam>node>peer shutdown)

Full Context

configure aaa diameter node peer shutdown
configure aaa diameter-peer-policy peer shutdown
configure aaa diameter-peer-policy proxy shutdown
configure aaa route-downloader shutdown
configure aaa wpp portal-groups portal-group shutdown
configure redundancy multi-chassis peer mc-lag shutdown
configure redundancy multi-chassis peer shutdown
configure redundancy multi-chassis peer sync shutdown
configure service ies subscriber-interface group-interface arp-host shutdown
configure service ies subscriber-interface group-interface data-trigger shutdown
configure service ies subscriber-interface group-interface gtp-parameters shutdown
configure service ies subscriber-interface group-interface srrp shutdown
configure service ies subscriber-interface group-interface wpp shutdown
configure service ies subscriber-interface shutdown
configure service vpls gsmp group neighbor shutdown
configure service vpls gsmp group shutdown
configure service vpls gsmp shutdown
configure service vpls sap sub-sla-mgmt shutdown
configure service vprn redundant-interface spoke-sdp shutdown
configure service vprn redundant-interface shutdown
configure service vprn subscriber-interface group-interface data-trigger shutdown
configure service vprn subscriber-interface group-interface gtp-parameters shutdown
configure service vprn subscriber-interface group-interface shutdown
configure service vprn subscriber-interface group-interface srrp shutdown
configure service vprn subscriber-interface group-interface wpp portals shutdown
configure service vprn subscriber-interface group-interface wpp shutdown
configure service vprn subscriber-interface shutdown
configure subscriber-mgmt sub-ident-policy primary shutdown
configure subscriber-mgmt sub-ident-policy secondary shutdown
configure subscriber-mgmt sub-ident-policy tertiary shutdown
configure subscriber-mgmt sub-mcac-policy shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

Shutting down a subscriber interface on a 7750 SR will operationally shut down all child group interfaces and SAPs. Shutting down a group interface on a 7750 SR will operationally shut down all SAPs that are part of that group-interface.

The **no** form of this command puts an entity into the administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure subscriber-mgmt sub-mcac-policy shutdown

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure aaa route-downloader shutdown
- configure aaa diameter-peer-policy peer shutdown
- configure service vprn subscriber-interface group-interface wpp shutdown
- configure service vprn redundant-interface spoke-sdp shutdown
- configure subscriber-mgmt sub-ident-policy secondary shutdown
- configure service vprn subscriber-interface group-interface shutdown
- configure service ies subscriber-interface group-interface arp-host shutdown
- configure service vprn subscriber-interface group-interface data-trigger shutdown
- configure aaa diameter-peer-policy proxy shutdown
- configure service vpls sap sub-sla-mgmt shutdown
- configure aaa wpp portal-groups portal-group shutdown
- configure service ies subscriber-interface group-interface srrp shutdown
- configure subscriber-mgmt sub-ident-policy tertiary shutdown
- configure subscriber-mgmt sub-ident-policy primary shutdown
- configure service vprn subscriber-interface shutdown
- configure aaa diameter node peer shutdown
- configure service vprn redundant-interface shutdown
- configure service ies subscriber-interface group-interface data-trigger shutdown
- configure service ies subscriber-interface group-interface wpp shutdown
- configure service vprn subscriber-interface group-interface srrp shutdown
- configure service ies subscriber-interface shutdown

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls gsmp group shutdown
- configure redundancy multi-chassis peer shutdown
- configure redundancy multi-chassis peer mc-lag shutdown
- configure redundancy multi-chassis peer sync shutdown
- configure service vpls gsmp shutdown
- configure service vpls gsmp group neighbor shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vprn shutdown)
[Tree] (config>service>vprn>aaa>remote-servers>radius shutdown)
[Tree] (config>service>vprn>aarp-interface shutdown)
[Tree] (config>service>vprn>aarp-interface>spoke-sdp shutdown)
[Tree] (config>service>vprn>bgp shutdown)
[Tree] (config>service>vprn>bgp>group shutdown)
[Tree] (config>service>vprn>bgp>group>neighbor shutdown)
[Tree] (config>service>vprn>bgp-evpn>mpls shutdown)
[Tree] (config>service>vprn>bgp-ipvpn>mpls shutdown)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 shutdown)
[Tree] (config>service>vprn>gsmp shutdown)
[Tree] (config>service>vprn>gsmp>group shutdown)
[Tree] (config>service>vprn>gsmp>group>neighbor shutdown)
[Tree] (config>service>vprn>igmp shutdown)
[Tree] (config>service>vprn>igmp-trk shutdown)
[Tree] (config>service>vprn>igmp>grp-if>mcac>mc-constraints shutdown)
[Tree] (config>service>vprn>igmp>if shutdown)
[Tree] (config>service>vprn>igmp>if>mcac shutdown)
[Tree] (config>service>vprn>igmp>if>mcac>mc-constraints shutdown)
[Tree] (config>service>vprn>if shutdown)
[Tree] (config>service>vprn>if>ipv6>vrrp shutdown)
[Tree] (config>service>vprn>if>sap shutdown)
[Tree] (config>service>vprn>if>sap>static-host shutdown)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel shutdown)
[Tree] (config>service>vprn>if>vrrp shutdown)
[Tree] (config>service>vprn>isis shutdown)
[Tree] (config>service>vprn>isis>if shutdown)
[Tree] (config>service>vprn>l2tp shutdown)
[Tree] (config>service>vprn>l2tp>tunnel shutdown)
[Tree] (config>service>vprn>l2tpv3 shutdown)
[Tree] (config>service>vprn>log>log-id shutdown)
[Tree] (config>service>vprn>mld>grp-if>mcac>mc-constraints shutdown)
[Tree] (config>service>vprn>mld>if>mcac>mc-constraints shutdown)
[Tree] (config>service>vprn>msdp shutdown)
[Tree] (config>service>vprn>msdp>group shutdown)
[Tree] (config>service>vprn>msdp>group>peer shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>msdp>peer shutdown)
[Tree] (config>service>vprn>mvpn>provider-tunnel>inclusive>pim shutdown)
[Tree] (config>service>vprn>ntp shutdown)
[Tree] (config>service>vprn>nw-if shutdown)
[Tree] (config>service>vprn>nw-if>eth-cfm>mep shutdown)
[Tree] (config>service>vprn>ospf shutdown)
[Tree] (config>service>vprn>ospf>area>if shutdown)
[Tree] (config>service>vprn>ospf3 shutdown)
[Tree] (config>service>vprn>ospf3>area>if shutdown)
[Tree] (config>service>vprn>ospf3>area>virtual-link shutdown)
[Tree] (config>service>vprn>ospf>area>virtual-link shutdown)
[Tree] (config>service>vprn>ospf>area>sham-link shutdown)
[Tree] (config>service>vprn>pim shutdown)
[Tree] (config>service>vprn>pim>if shutdown)
[Tree] (config>service>vprn>pim>if>mcac>mc-constraints shutdown)
[Tree] (config>service>vprn>pim>rp>bsr-candidate shutdown)
[Tree] (config>service>vprn>pim>rp>ipv6>bsr-candidate shutdown)
[Tree] (config>service>vprn>pim>rp>ipv6>embedded-rp shutdown)
[Tree] (config>service>vprn>pim>rp>ipv6>rp-candidate shutdown)
[Tree] (config>service>vprn>red-if shutdown)
[Tree] (config>service>vprn>red-if>spoke-sdp shutdown)
[Tree] (config>service>vprn>red-if>spoke-sdp>control-channel-status shutdown)
[Tree] (config>service>vprn>rip shutdown)
[Tree] (config>service>vprn>rip>group shutdown)
[Tree] (config>service>vprn>rip>group>neighbor shutdown)
[Tree] (config>service>vprn>router-advert>if shutdown)

Full Context

configure service vprn aaa remote-servers radius shutdown
configure service vprn aarp-interface shutdown
configure service vprn aarp-interface spoke-sdp shutdown
configure service vprn bgp group neighbor shutdown
configure service vprn bgp group shutdown
configure service vprn bgp shutdown
configure service vprn bgp-evpn mpls shutdown
configure service vprn bgp-ipvpn mpls shutdown
configure service vprn bgp-ipvpn segment-routing-v6 shutdown
configure service vprn gsmp group neighbor shutdown
configure service vprn gsmp group shutdown
configure service vprn gsmp shutdown
configure service vprn interface ipv6 vrrp shutdown
configure service vprn interface sap ipsec-tunnel shutdown
configure service vprn interface sap shutdown
configure service vprn interface sap static-host shutdown
configure service vprn interface shutdown
configure service vprn interface vrrp shutdown
configure service vprn igmp group-interface mcac mc-constraints shutdown
configure service vprn igmp interface mcac mc-constraints shutdown
configure service vprn igmp interface mcac shutdown
configure service vprn igmp interface shutdown
configure service vprn igmp shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn igmp-host-tracking shutdown
configure service vprn isis interface shutdown
configure service vprn isis shutdown
configure service vprn l2tp shutdown
configure service vprn l2tp tunnel shutdown
configure service vprn l2tpv3 shutdown
configure service vprn log log-id shutdown
configure service vprn mld group-interface mcac mc-constraints shutdown
configure service vprn mld interface mcac mc-constraints shutdown
configure service vprn msdp group peer shutdown
configure service vprn msdp group shutdown
configure service vprn msdp peer shutdown
configure service vprn msdp shutdown
configure service vprn mvpn provider-tunnel inclusive pim shutdown
configure service vprn ntp shutdown
configure service vprn nw-if eth-cfm mep shutdown
configure service vprn network-interface shutdown
configure service vprn ospf area interface shutdown
configure service vprn ospf area sham-link shutdown
configure service vprn ospf area virtual-link shutdown
configure service vprn ospf shutdown
configure service vprn ospf3 area interface shutdown
configure service vprn ospf3 area virtual-link shutdown
configure service vprn ospf3 shutdown
configure service vprn pim interface mcac mc-constraints shutdown
configure service vprn pim interface shutdown
configure service vprn pim rp bsr-candidate shutdown
configure service vprn pim rp ipv6 bsr-candidate shutdown
configure service vprn pim rp ipv6 embedded-rp shutdown
configure service vprn pim rp ipv6 rp-candidate shutdown
configure service vprn pim shutdown
configure service vprn redundant-interface shutdown
configure service vprn redundant-interface spoke-sdp control-channel-status shutdown
configure service vprn redundant-interface spoke-sdp shutdown
configure service vprn rip group neighbor shutdown
configure service vprn rip group shutdown
configure service vprn rip shutdown
configure service vprn router-advertisement interface shutdown
configure service vprn shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command places the entity into an administratively enabled state.

If the AS number was previously changed, the BGP AS number inherits the new value.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface mcac mc-constraints shutdown
- configure service vprn interface sap static-host shutdown
- configure service vprn mld group-interface mcac mc-constraints shutdown
- configure service vprn igmp-host-tracking shutdown
- configure service vprn redundant-interface spoke-sdp shutdown
- configure service vprn l2tp shutdown
- configure service vprn redundant-interface shutdown
- configure service vprn redundant-interface spoke-sdp control-channel-status shutdown

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn aarp-interface spoke-sdp shutdown
- configure service vprn aarp-interface shutdown
- configure service vprn interface sap ipsec-tunnel shutdown

7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service vprn bgp-ipvpn segment-routing-v6 shutdown

All

- configure service vprn ospf area interface shutdown
- configure service vprn ospf3 area interface shutdown
- configure service vprn msdp group shutdown
- configure service vprn igmp shutdown
- configure service vprn msdp group peer shutdown
- configure service vprn ntp shutdown
- configure service vprn bgp-ipvpn mpls shutdown
- configure service vprn bgp shutdown
- configure service vprn interface ipv6 vrrp shutdown
- configure service vprn interface vrrp shutdown
- configure service vprn interface sap shutdown
- configure service vprn log log-id shutdown
- configure service vprn ospf shutdown
- configure service vprn msdp shutdown
- configure service vprn bgp group shutdown
- configure service vprn rip group neighbor shutdown
- configure service vprn ospf area virtual-link shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn ospf area sham-link shutdown
- configure service vprn pim shutdown
- configure service vprn gsmp group shutdown
- configure service vprn rip group shutdown
- configure service vprn isis interface shutdown
- configure service vprn msdp peer shutdown
- configure service vprn gsmp group neighbor shutdown
- configure service vprn igmp interface mcac mc-constraints shutdown
- configure service vprn network-interface shutdown
- configure service vprn router-advertisement interface shutdown
- configure service vprn mld interface mcac mc-constraints shutdown
- configure service vprn pim rp ipv6 embedded-rp shutdown
- configure service vprn gsmp shutdown
- configure service vprn ospf3 shutdown
- configure service vprn pim interface shutdown
- configure service vprn shutdown
- configure service vprn pim rp bsr-candidate shutdown
- configure service vprn ospf3 area virtual-link shutdown
- configure service vprn bgp-evpn mpls shutdown
- configure service vprn igmp interface shutdown
- configure service vprn bgp group neighbor shutdown
- configure service vprn pim rp ipv6 rp-candidate shutdown
- configure service vprn aaa remote-servers radius shutdown
- configure service vprn interface shutdown
- configure service vprn mvpn provider-tunnel inclusive pim shutdown
- configure service vprn pim rp ipv6 bsr-candidate shutdown
- configure service vprn isis shutdown
- configure service vprn pim interface mcac mc-constraints shutdown
- configure service vprn rip shutdown

Special Cases

Service Admin State — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

A service is regarded as operational providing that one IP Interface SAP and one SDP is operational.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

VPRN BGP and RIP — This command disables the BGP or RIP instance on the given IP interface. Routes learned from a neighbor that is shutdown are immediately removed from the BGP or RIP database and RTM. If BGP or RIP is globally shutdown, then all RIP group and neighbor interfaces are shutdown operationally. If a BGP or RIP group is shutdown, all member neighbor interfaces are shutdown operationally. If a BGP or RIP neighbor is shutdown, just that neighbor interface is operationally shutdown.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>ies>if>sap shutdown)
[Tree] (config>service>vpls shutdown)
[Tree] (config>service>vpls>wlan-gw shutdown)
[Tree] (config>service>vpls>sap shutdown)
[Tree] (config>service>vpls>sap>arp-host shutdown)
[Tree] (config>service>vpls>mesh-sdp shutdown)
[Tree] (config>service>vpls>spoke-sdp shutdown)
[Tree] (config>service>vprn shutdown)

Full Context configure service ies interface sap shutdown
configure service vpls mesh-sdp shutdown
configure service vpls sap arp-host shutdown
configure service vpls sap shutdown
configure service vpls shutdown
configure service vpls spoke-sdp shutdown
configure service vpls wlan-gw shutdown
configure service vprn shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system-generated configuration files.

Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vpls sap arp-host shutdown

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls wlan-gw shutdown

All

- configure service ies interface sap shutdown
- configure service vpls sap shutdown
- configure service vpls mesh-sdp shutdown
- configure service vpls shutdown
- configure service vprn shutdown
- configure service vpls spoke-sdp shutdown

Special Cases

Service Admin State — Bindings to an SDP within the service are put into the out-of-service state when the service is **shutdown**. While the service is shut down, all customer packets are dropped and counted as discards for billing and debugging purposes.

Service Operational State — A service is regarded as operational providing that two SAPs or if one SDP are operational.

SDP (global) — When an SDP is shut down at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding are discarded and counted as dropped packets.

SDP (service level) — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

SDP Keepalives — Enables SDP connectivity monitoring keepalive messages for the SDP ID. Default state is disabled (**shutdown**) in which case the operational state of the SDP-ID is not affected by the keepalive message state.

VPLS SAPs and SDPs — SAPs are created in a VPLS and SDPs are bound to a VPLS in the administratively up default state. The created SAP attempts to enter the operationally up state. An SDP attempts to go into the in-service state once bound to the VPLS.

shutdown

Syntax [**no**] **shutdown**

Context
[Tree] (config>service>vpls>bind>evpn-mcast-gateway shutdown)
[Tree] (config>service>vpls>bgp-ad shutdown)
[Tree] (config>service>vpls>eth-cfm>mep shutdown)
[Tree] (config>service>vpls>igmp-snooping shutdown)
[Tree] (config>service>vpls>igmp-snooping>mvr shutdown)
[Tree] (config>service>vpls>interface shutdown)
[Tree] (config>service>vpls>mac-move shutdown)
[Tree] (config>service>vpls>mac-notification shutdown)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>mld-snooping shutdown)
[Tree] (config>service>vpls>mld-snooping>mvr shutdown)
[Tree] (config>service>vpls>mrp shutdown)
[Tree] (config>service>vpls>mrp>mvrp shutdown)
[Tree] (config>service>vpls>sap>dhcp>proxy shutdown)
[Tree] (config>service>vpls>sap>eth-cfm>mep shutdown)
[Tree] (config>service>vpls>sap>igmp-snooping>mcac>mc-constraints shutdown)
[Tree] (config>service>vpls>sap>mld-snooping>mcac>mc-constraints shutdown)
[Tree] (config>service>vpls>sap>l2tpv3-session shutdown)
[Tree] (config>service>vpls>sap>spb shutdown)
[Tree] (config>service>vpls>sap>stp shutdown)
[Tree] (config>service>vpls>spb>level shutdown)
[Tree] (config>service>vpls>spoke-sdp shutdown)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep shutdown)
[Tree] (config>service>vpls>spoke-sdp>spb shutdown)
[Tree] (config>service>vpls>spoke-sdp>stp shutdown)
[Tree] (config>service>vpls>stp shutdown)

Full Context

configure service vpls bgp-ad shutdown
configure service vpls allow-ip-int-bind evpn-mcast-gateway shutdown
configure service vpls eth-cfm mep shutdown
configure service vpls igmp-snooping mvr shutdown
configure service vpls igmp-snooping shutdown
configure service vpls interface shutdown
configure service vpls mac-move shutdown
configure service vpls mac-notification shutdown
configure service vpls mesh-sdp eth-cfm mep shutdown
configure service vpls mld-snooping mvr shutdown
configure service vpls mld-snooping shutdown
configure service vpls mrp mvrp shutdown
configure service vpls mrp shutdown
configure service vpls sap dhcp proxy-server shutdown
configure service vpls sap eth-cfm mep shutdown
configure service vpls sap igmp-snooping mcac mc-constraints shutdown
configure service vpls sap l2tpv3-session shutdown
configure service vpls sap mld-snooping mcac mc-constraints shutdown
configure service vpls sap spb shutdown
configure service vpls sap stp shutdown
configure service vpls spb level shutdown
configure service vpls spoke-sdp eth-cfm mep shutdown
configure service vpls spoke-sdp shutdown
configure service vpls spoke-sdp spb shutdown
configure service vpls spoke-sdp stp shutdown
configure service vpls stp shutdown

Description

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vpls mesh-sdp eth-cfm mep shutdown
- configure service vpls sap eth-cfm mep shutdown
- configure service vpls spoke-sdp eth-cfm mep shutdown
- configure service vpls eth-cfm mep shutdown

All

- configure service vpls sap mld-snooping mcac mc-constraints shutdown
- configure service vpls mrp mvrp shutdown
- configure service vpls allow-ip-int-bind evpn-mcast-gateway shutdown
- configure service vpls igmp-snooping mvr shutdown
- configure service vpls mac-notification shutdown
- configure service vpls mld-snooping mvr shutdown
- configure service vpls interface shutdown
- configure service vpls spoke-sdp spb shutdown
- configure service vpls sap dhcp proxy-server shutdown
- configure service vpls sap igmp-snooping mcac mc-constraints shutdown
- configure service vpls sap spb shutdown
- configure service vpls igmp-snooping shutdown
- configure service vpls spoke-sdp shutdown
- configure service vpls sap stp shutdown
- configure service vpls stp shutdown
- configure service vpls mrp shutdown
- configure service vpls bgp-ad shutdown
- configure service vpls mld-snooping shutdown
- configure service vpls mac-move shutdown
- configure service vpls spoke-sdp stp shutdown
- configure service vpls sap l2tpv3-session shutdown

Special Cases **Service Admin State —** Bindings to an SDP within the service will be put into the out-of-service state when the service is shut down. While the service is shut down, all customer packets are dropped and counted as discards for billing and debugging purposes.

Service Operational State — A service is regarded as operational providing that two SAPs or one SDP is operational.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

SDP (global) — When an SDP is shut down at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

SDP (service level) — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

SDP Keepalives — Enables SDP connectivity monitoring keepalive messages for the SDP ID. Default state is disabled (shutdown), in which case the operational state of the SDP ID is not affected by the keepalive message state.

VPLS SAPs and SDPs — SAPs are created in a VPLS and SDPs are bound to a VPLS in the administratively up default state. The created SAP will attempt to enter the operationally up state. An SDP will attempt to go into the in-service state when bound to the VPLS.

Routed VPLS with forward-ipv4-multicast-to-ip-int and IGMP Snooping — To enable IGMP snooping (configured using **igmp-snooping no shutdown**) in a routed VPLS supporting the forwarding of multicast traffic from the VPLS to the IP interface (configured using **forward-ipv4-multicast-to-ip-int**), it is necessary to enable IGMP on the routed VPLS IP interface.

Routed VPLS with forward-ipv6-multicast-to-ip-int and MLD Snooping — To enable MLD snooping (configured using **mld-snooping no shutdown**) in a routed VPLS supporting the forwarding of multicast traffic from the VPLS to the IP interface (configured using forward-ipv6-multicast-to-ip-int) it is necessary to enable MLD on the routed VPLS IP interface.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vpls>spb shutdown)
[Tree] (config>service>vpls>spoke-sdp>spb shutdown)
[Tree] (config>service>vpls>mrp>mmrp shutdown)

Full Context configure service vpls mrp mmrp shutdown
configure service vpls spb shutdown
configure service vpls spoke-sdp spb shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within.

The **no** form of this command administratively enables an entity.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

SPB Interface — In the config>service>vpls>spb> context, the command disables the IS-IS interface. By default, the IS-IS interface is disabled (shutdown).

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>pppoe shutdown)

Full Context configure service vprn subscriber-interface group-interface pppoe shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>card shutdown)
[Tree] (config>card>fp>ingress>mcast-path-management shutdown)
[Tree] (config>card>mda shutdown)
[Tree] (config>card>xiom shutdown)
[Tree] (config>card>xiom>mda shutdown)
[Tree] (config>interface-group-handler shutdown)
[Tree] (config>lag shutdown)
[Tree] (config>lag>eth-cfm>mep shutdown)
[Tree] (config>port shutdown)
[Tree] (config>port>ethernet shutdown)
[Tree] (config>port>ethernet>dwl shutdown)
[Tree] (config>port>ethernet>efm-cfm>mep shutdown)
[Tree] (config>port>ethernet>efm-oam shutdown)
[Tree] (config>port>ethernet>ssm shutdown)
[Tree] (config>port>ethernet>symbol-monitor shutdown)
[Tree] (config>port>otu shutdown)
[Tree] (config>port>sonet-sdh>path shutdown)
[Tree] (config>port>tdm>ds1 shutdown)
[Tree] (config>port>tdm>ds1>channel-group shutdown)
[Tree] (config>port>tdm>ds3 shutdown)
[Tree] (config>port>tdm>e1 shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>port>tdm>e1>channel-group shutdown)
[Tree] (config>port>tdm>e3 shutdown)
[Tree] (config>port>ml-bundle>ima>test-pattern-procedure shutdown)
[Tree] (config>port>sonet-sdh>path>atm>ilmi shutdown)
[Tree] (config>port>sonet-sdh>path>atm>ilmi shutdown)
[Tree] (config>port>ethernet>dampening shutdown)
[Tree] (config>port>ethernet>eth-cfm>mep shutdown)
[Tree] (config>port>ethernet>efm-oam shutdown)
[Tree] (config>port-xc>pxc shutdown)
[Tree] (config>redundancy>mc>peer>mcr shutdown)
[Tree] (config>redundancy>mc>peer>mcr>ring shutdown)
[Tree] (config>redundancy>mc>peer>mcr>node>cv shutdown)
[Tree] (config>redundancy>multi-chassis>peer>mc-endpoint shutdown)

Full Context

configure card fp ingress mcast-path-management shutdown
configure card mda shutdown
configure card shutdown
configure card xiom mda shutdown
configure card xiom shutdown
configure interface-group-handler shutdown
configure lag eth-cfm mep shutdown
configure lag shutdown
configure port ethernet dampening shutdown
configure port ethernet down-when-looped shutdown
configure port ethernet efm-cfm mep shutdown
configure port ethernet efm-oam shutdown
configure port ethernet eth-cfm mep shutdown
configure port ethernet shutdown
configure port ethernet ssm shutdown
configure port ethernet symbol-monitor shutdown
configure port multilink-bundle ima test-pattern-procedure shutdown
configure port otu shutdown
configure port shutdown
configure port sonet-sdh path atm ilmi shutdown
configure port sonet-sdh path shutdown
configure port tdm ds1 channel-group shutdown
configure port tdm ds1 shutdown
configure port tdm ds3 shutdown
configure port tdm e1 channel-group shutdown
configure port tdm e1 shutdown
configure port tdm e3 shutdown
configure port-xc pxc shutdown
configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify shutdown
configure redundancy multi-chassis peer mc-ring ring shutdown
configure redundancy multi-chassis peer mc-ring shutdown
configure redundancy multi-chassis peer mc-endpoint shutdown

Description

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The operational state of the entity is disabled as well as the operational state of any entities contained within.

This command is supported on TDM satellite.

The **no** form of this command administratively enables an entity.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port ethernet symbol-monitor shutdown
- configure port sonet-sdh path shutdown
- configure lag eth-cfm mep shutdown
- configure port ethernet eth-cfm mep shutdown

7450 ESS, 7750 SR-7/12/12e

- configure port multilink-bundle ima test-pattern-procedure shutdown

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 shutdown
- configure port tdm ds1 shutdown
- configure port tdm e1 channel-group shutdown
- configure port tdm e1 shutdown
- configure port tdm ds1 channel-group shutdown
- configure port tdm e3 shutdown

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure port sonet-sdh path atm ilmi shutdown

7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

- configure card fp ingress mcast-path-management shutdown

7750 SR-s

- configure card xiom shutdown
- configure card xiom mda shutdown

All

- configure card mda shutdown
- configure interface-group-handler shutdown
- configure redundancy multi-chassis peer mc-endpoint shutdown
- configure port shutdown
- configure port-xc pxc shutdown
- configure port ethernet ssm shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify shutdown
- configure port ethernet efm-oam shutdown
- configure lag shutdown
- configure port ethernet dampening shutdown
- configure port ethernet down-when-looped shutdown
- configure redundancy multi-chassis peer mc-ring ring shutdown
- configure card shutdown

Special Cases **card —** Specifies the default state for a card is **no shutdown**.

interface group handler (IGH) — Specifies the default state for an IGH is **shutdown**.

mda — Specifies the default state for a mda is **no shutdown**.

lag — Specifies the default state for a Link Aggregation Group (LAG) is **shutdown**.

port — Specifies the default state for a port is **shutdown**.

path — Specifies the default state for a SONET/SDH path is **shutdown**.

xiom — Specifies the default state for an XIOM is **no shutdown**.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>aaa>l2tp-acct-plcy shutdown)

Full Context configure aaa l2tp-accounting-policy shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>mcast-mgmt>mcast-rprt-dest shutdown)

Full Context configure mcast-management mcast-reporting-dest shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>python>py-policy>cache shutdown)
[Tree] (config>python>python-script shutdown)

Full Context configure python python-policy cache shutdown
configure python python-script shutdown

Description Shutting down a Python script triggers the system to load and compile the script from the configured location(s). Since the system supports three locations, the primary, secondary and tertiary, the system will try to load the Python script in that order.

Shutting down a Python script will disable the Python script and cause the corresponding packet to pass through without any modification.

The **no** form of this command enables the cache or policy script.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vpls>sap>dyn-svc shutdown)

Full Context configure service vpls sap dynamic-services shutdown

Description This command disables or enables data-triggered dynamic services on this **capture-sap**.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>dynsvc>ladb shutdown)

Full Context configure service dynamic-services local-auth-db shutdown

Description This command disables or enables the local authentication database. When disabled, the database cannot be used for authentication.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>dynsvc>ladb>user shutdown)

Full Context configure service dynamic-services local-auth-db user-name shutdown

Description This command disables or enables a user name entry in the local authentication database. When disabled, the entry is not matched.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>svlan-statistics shutdown)

Full Context configure subscriber-mgmt svlan-statistics shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system-generated configuration files.

The **no** form of this command places the entity into an administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>evpn shutdown)
[Tree] (config>subscr-mgmt>isa-svc-chain>vas-filter shutdown)

Full Context configure subscriber-mgmt isa-service-chaining evpn shutdown
configure subscriber-mgmt isa-service-chaining vas-filter shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system-generated configuration files.

The **no** form of this command puts an entity into the administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>ccrt-replay shutdown)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy>ccrt-replay shutdown)

Full Context configure subscriber-mgmt diameter-application-policy gx ccrt-replay shutdown
configure subscriber-mgmt diameter-application-policy gy ccrt-replay shutdown

Description This command, enables or disables the CCR-T replay function for all Gx or Gy sessions that belong to the diameter application policy. Sessions in CCR-T replay are dropped when **ccrt-replay** is shut down.

The **no** form of this command enables the CCR-T replay function.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>bonding-parameters shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>bonding-parameters shutdown)

Full Context configure service ies subscriber-interface group-interface bonding-parameters shutdown
configure service vprn subscriber-interface group-interface bonding-parameters shutdown

Description The **shutdown** command administratively disables the entity. When a bonding context is shut down, all bonding subscribers are removed and no new bonding subscribers can be created in this context. The bonding configuration can be altered.

When a bonding context is placed in **no shutdown**, bonding subscribers can be created with connections in the specified subscriber interfaces. The specified FPE and connections can no longer be changed in this mode.

Default shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>rtr-sol shutdown)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-sol shutdown)

Full Context configure service ies subscriber-interface group-interface ipv6 router-solicit shutdown

Description This command enables SLAAC triggered host creation.

The **no** form of this command disables SLAAC triggered host creation.

Default no shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (debug>diam>diam-peer-plcy>avp-match shutdown)

Full Context debug diameter diameter-peer-policy avp-match shutdown

Description This command enables or disables the **avp-match** *id* criteria for filtering debug output based on AVP value matching.

A shutdown of the **avp-match** *id* clears the learned diameter session ID.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>health-check>test-account shutdown)

Full Context configure aaa radius-server-policy servers health-check test-account shutdown

Description This command disables the test account that probes the RADIUS server.

The **no** form of this command enables the capability.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax **shutdown** *sap-id* [**create**]
no shutdown *sap-id*

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>l2-access-points>l2-ap shutdown)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>l2-access-points>l2-ap shutdown)

Full Context configure service ies subscriber-interface group-interface wlan-gw l2-access-points l2-ap shutdown
configure service vprn subscriber-interface group-interface wlan-gw l2-access-points l2-ap shutdown

Description This command administratively enables this SAP to begin accepting Layer 2 packets for WIFI offloading.

The **no** form of this command disables this SAP.

Default shutdown

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>pfcp-association shutdown)

Full Context configure subscriber-mgmt pfcp-association shutdown

Description This command administratively enables or disables the PFCP association.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When administratively enabled, the system will try to maintain an active PFCP association with the configured peer. While no association is established, it will continue to retry setting up the association using the **association-setup-retry** configuration.

Shutting down a subscriber interface on a 7750 SR operationally shuts down all child group interfaces and SAPs. Shutting down a group interface on a 7750 SR operationally shuts down all SAPs that are part of that group interface.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>pwr-mgmt>peq shutdown)

Full Context configure system power-management peq shutdown

Description This command administratively enables/disables the APEQ. This command is supported in the 7750 SR-S OS and 7950 XRS only.

Platforms 7750 SR-12e, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>card>fp>egress>wred-queue-control shutdown)

Full Context configure card fp egress wred-queue-control shutdown

Description This command enables or disables egress WRED queue support on the forwarding plane. By default, WRED queue support is disabled (shutdown). While disabled, the various wred-queue-control commands may be executed on the forwarding plane and SAP egress QoS policies and egress queue group templates with wred-queue enabled may be applied to egress SAPs and port, respectively. The forwarding plane will allocate WRED pools to the WRED queues and the appropriate WRED mega-pool size and CBS reserve size will be calculated, but the WRED mega-pool will be empty and all buffers will be allocated to the default mega-pool. Each WRED queue will be mapped to its appropriate default pool.

Once the **no shutdown** command is executed, the calculated WRED mega-pool buffers will be moved from the default mega-pool to the WRED mega-pool. The WRED mega-pool CBS reserve size will be applied and each egress WRED queue will be moved from its default mega-pool buffer pool to its WRED pool within the WRED mega-pool hierarchy.

The **no** form of this command enables WRED queuing on an egress forwarding plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>macsec>connectivity-association shutdown)

Full Context configure macsec connectivity-association shutdown

Description This command shuts down the CA profile. All ports that are using this profile will not transmit PDUs as this command shuts down the MACsec for this profile.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>port>ethernet>efm-oam>link-monitoring shutdown)

Full Context configure port ethernet efm-oam link-monitoring shutdown

Description This command enables the link monitoring function. Issuing a no shutdown will start the process. Issuing a shutdown will clear any previously established negative conditions that were a result of the link monitoring process on this port and all collected data. This also controls the advertising capabilities.

The **no** form of this command activates the link monitoring function.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame shutdown)
[Tree] (config>port>ethernet>efm-oam>link-mon>errored-frame-period shutdown)
[Tree] (config>port>ethernet>efm-oam>link-mon>errored-frame-seconds shutdown)
[Tree] (config>port>ethernet>efm-oam>link-mon>errored-symbols shutdown)

Full Context configure port ethernet efm-oam link-monitoring errored-frame shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port ethernet efm-oam link-monitoring errored-frame-period shutdown
configure port ethernet efm-oam link-monitoring errored-frame-seconds shutdown
configure port ethernet efm-oam link-monitoring errored-symbols shutdown

Description This command enables or disables the local counting, thresholding and actions associated with this type of local monitor. Peer received errors are not controlled by this command. Reaction to peer messaging is defined in the peer-rdi-rx hierarchy.

The **no** form of this command activates the local monitoring function and actions for the event.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>port>ethernet>dot1x>macsec>sub-port shutdown)

Full Context configure port ethernet dot1x macsec sub-port shutdown

Description This command shuts down the MACsec under this sub-port specifically, including MKA negotiation. In the shutdown state, this port is not MACsec capable and all PDUs will be transmitted and expected without encryption and authentication.

The **no** form of this command puts the port in MACsec-enabled mode. A valid CA, different than any other CA configured on any other sub-port of this port and also a *max-peer* value larger than 0 must be configured. In MACsec-enabled mode, packets are sent in clear text until the MKA session is up, and if the **rx-must-be-encrypted** is set on the port, all incoming packets with no MACsec encapsulations are dropped.

Default shutdown

Platforms All

shutdown

Syntax **shutdown**
no shutdown

Context **[Tree]** (config>lag>bfd>family shutdown)

Full Context configure lag bfd family shutdown

Description This command disables micro BFD sessions for this address family.

The **no** form of this command re-enables micro BFD sessions for this address family.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>sdp shutdown)
[Tree] (config>service>sdp>class-forwarding shutdown)
[Tree] (config>service>sdp>keep-alive shutdown)
[Tree] (config>service>pw-routing>hop shutdown)
[Tree] (config>service>pw-template>stp shutdown)
[Tree] (config>service>sdp>binding>pw-port shutdown)
[Tree] (config>eth-ring>path shutdown)
[Tree] (config>eth-tunnel>path>eth-cfm>mep shutdown)

Full Context configure eth-ring path shutdown
configure eth-tunnel path eth-cfm mep shutdown
configure service pw-routing hop shutdown
configure service pw-template stp shutdown
configure service sdp binding pw-port shutdown
configure service sdp class-forwarding shutdown
configure service sdp keep-alive shutdown
configure service sdp shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure eth-tunnel path eth-cfm mep shutdown
- configure eth-ring path shutdown

All

- configure service sdp keep-alive shutdown
- configure service sdp class-forwarding shutdown
- configure service sdp binding pw-port shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service sdp shutdown
- configure service pw-template stp shutdown

Special Cases

Service Admin State — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

SDP (global) — When an SDP is shutdown at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

SDP (service level) — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

SDP Keepalives — Enables SDP connectivity monitoring keepalive messages for the SDP ID. Default state is disabled (shutdown) in which case the operational state of the SDP-ID is not affected by the keepalive message state.

shutdown

Syntax **shutdown**
[**no**] **shutdown**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls shutdown)
[Tree] (config>service>epipe>bgp-evpn>vxlan shutdown)
[Tree] (config>service>vpls>bgp-evpn>mpls shutdown)
[Tree] (config>service>vpls>bgp-evpn>srv6 shutdown)
[Tree] (config>service>vpls>bgp-evpn>vxlan shutdown)

Full Context
configure service epipe bgp-evpn mpls shutdown
configure service epipe bgp-evpn vxlan shutdown
configure service vpls bgp-evpn mpls shutdown
configure service epipe bgp-evpn segment-routing-v6 shutdown
configure service vpls bgp-evpn vxlan shutdown

Description This command controls the administrative state of EVPN-MPLS or EVPN-VXLAN in the service.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service epipe bgp-evpn segment-routing-v6 shutdown

All

- configure service vpls bgp-evpn mpls shutdown
- configure service vpls bgp-evpn vxlan shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service epipe bgp-evpn mpls shutdown
- configure service epipe bgp-evpn vxlan shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vpls>provider-tunnel>inclusive shutdown)

Full Context configure service vpls provider-tunnel inclusive shutdown

Description This command administratively enables and disables the service.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vpls>proxy-arp shutdown)
[Tree] (config>service>vpls>proxy-nd shutdown)

Full Context configure service vpls proxy-arp shutdown
configure service vpls proxy-nd shutdown

Description This command enables and disables the proxy-ARP and proxy-nd functionality. ARP/GARP/ND messages will be snooped and redirected to the CPM for lookup in the proxy-ARP/proxy-ND table. The proxy-ARP/proxy-ND table is populated with IP->MAC pairs received from different sources (EVPN, static, dynamic). When the **shutdown** command is issued, it flushes the dynamic/EVPN dup proxy-ARP/proxy-ND table entries and instructs the system to stop snooping ARP/ND frames. All the static entries are kept in the table as *inactive*, regardless of their previous *Status*.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vsd>domain shutdown)

Full Context configure service vsd domain shutdown

Description This command enables or disables a domain. A description must be provided before no shutdown is executed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg shutdown)

Full Context configure service system bgp-evpn ethernet-segment shutdown

Description This command changes the administrative status of the Ethernet-Segment.

The user can do **no shutdown** only when esi, multi-homing and lag/port/sdp are configured. If the Ethernet-Segment or the corresponding lag/port/sdp shutdown, the Ethernet-Segment route and the AD per-ES routes will be withdrawn. No changes are allowed when the Ethernet-Segment is **no shutdown**.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>xmpp>server shutdown)

Full Context configure system xmpp server shutdown

Description This command enables or disables the communication with a specified XMPP server. When the xmpp server is properly configured, **no shutdown** instructs the system to establish a TCP session with the XMPP server through the management interface first. If it fails to establish communication, the 7750 SR, 7450 ESS, or 7950 XRS uses an in-band communication and its system IP as source IP address. Shutdown does not remove the dynamic configurations.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>apipe shutdown)
[Tree] (config>service>apipe>sap shutdown)
[Tree] (config>service>apipe>spoke-sdp shutdown)
[Tree] (config>service>cpipe shutdown)
[Tree] (config>service>cpipe>sap shutdown)
[Tree] (config>service>cpipe>spoke-sdp shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>epipe shutdown)
[Tree] (config>service>epipe>site shutdown)
[Tree] (config>service>epipe>sap shutdown)
[Tree] (config>service>epipe>sap>l2tpv3-session shutdown)
[Tree] (config>service>epipe>sap>eth-cfm>mep shutdown)
[Tree] (config>service>epipe>spoke-sdp shutdown)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep shutdown)
[Tree] (config>service>fpipe shutdown)
[Tree] (config>service>fpipe>sap shutdown)
[Tree] (config>service>fpipe>spoke-sdp shutdown)
[Tree] (config>service>ipipe shutdown)
[Tree] (config>service>ipipe>sap shutdown)
[Tree] (config>service>ipipe>spoke-sdp shutdown)
[Tree] (config>service>epipe>pw-port shutdown)

Full Context

configure service apipe sap shutdown
configure service apipe shutdown
configure service apipe spoke-sdp shutdown
configure service cpipe sap shutdown
configure service cpipe shutdown
configure service cpipe spoke-sdp shutdown
configure service epipe pw-port shutdown
configure service epipe sap eth-cfm mep shutdown
configure service epipe sap l2tpv3-session shutdown
configure service epipe sap shutdown
configure service epipe shutdown
configure service epipe site shutdown
configure service epipe spoke-sdp eth-cfm mep shutdown
configure service epipe spoke-sdp shutdown
configure service fpipe sap shutdown
configure service fpipe shutdown
configure service fpipe spoke-sdp shutdown
configure service ipipe sap shutdown
configure service ipipe shutdown
configure service ipipe spoke-sdp shutdown

Description

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described as follows in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe spoke-sdp shutdown
- configure service epipe sap eth-cfm mep shutdown
- configure service fpipe shutdown
- configure service epipe spoke-sdp eth-cfm mep shutdown
- configure service cpipe shutdown
- configure service cpipe sap shutdown
- configure service fpipe sap shutdown
- configure service cpipe spoke-sdp shutdown

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp shutdown
- configure service apipe shutdown
- configure service apipe sap shutdown

All

- configure service epipe sap shutdown
- configure service ipipe shutdown
- configure service ipipe sap shutdown
- configure service epipe spoke-sdp shutdown
- configure service ipipe spoke-sdp shutdown
- configure service epipe shutdown
- configure service epipe site shutdown
- configure service epipe sap l2tpv3-session shutdown
- configure service epipe pw-port shutdown

Special Cases

Service Admin State — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

Service Operational State — A service is regarded as operational providing that at least one SAP and one SDP are operational or if two SAPs are operational.

SDP (global) — When an SDP is shutdown at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

SDP (service level) — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>epipe>bgp-vpws shutdown)

Full Context configure service epipe bgp-vpws shutdown

Description This command administratively enables/disables the local BGP VPWS instance. On de-activation an MP-UNREACH-NLRI is sent for the local NLRI.

The **no** form of this command enables the BGP VPWS addressing and the related BGP advertisement. The associated BGP VPWS MP-REACH-NLRI will be advertised in an update message and the corresponding received NLRIs must be considered to instantiate the data plane.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>ipipe>eth-legacy-fault-notification shutdown)

Full Context configure service ipipe eth-legacy-fault-notification shutdown

Description This command enables or disables the propagation of fault from the Ethernet segment to the legacy connection using PPP, MLPPP and HDLC for an Ipipe service. Issuing a “no shutdown” will activate the feature. Issuing a “shutdown” will deactivate the feature and stop fault notification from the Ethernet to PPP, MLPPP and HDLC protocols.

The **no** form of this command activates the ethernet legacy fault propagation.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vpls>bgp-vpls shutdown)

Full Context configure service vpls bgp-vpls shutdown

Description This command administratively enables/disables the local BGP VPLS instance. On de-activation an MP-UNREACH-NLRI must be sent for the local NLRI.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command enables the BGP VPLS addressing and the related BGP advertisement. The associated BGP VPLS MP-REACH-NLRI will be advertised in an update message and the corresponding received NLRIs must be considered to instantiate the data plane. RT, RD usage: same as in the BGP AD solution, if the values are not configured here, the value of the VPLS-id from under the bgp-ad node is used. If VPLS-id value is not configured either the MH site cannot be activated – i.e. no shutdown returns an error. Same applies if a pseudowire template is not specified under the BGP node.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>ies>if>ipv6>secure-nd shutdown)

Full Context configure service ies interface ipv6 secure-nd shutdown

Description This command enables or disables Secure Neighbor Discovery (SeND) on the interface.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus shutdown)

Full Context configure service vprn aaa remote-servers tacplus shutdown

Description This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables the protocol which is the default state.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>static-route-entry>black-hole shutdown)
[Tree] (config>service>vprn>static-route-entry>grt shutdown)
[Tree] (config>service>vprn>static-route-entry>indirect shutdown)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel shutdown)
[Tree] (config>service>vprn>static-route-entry>next-hop shutdown)

Full Context configure service vprn static-route-entry black-hole shutdown
configure service vprn static-route-entry grt shutdown
configure service vprn static-route-entry indirect shutdown
configure service vprn static-route-entry ipsec-tunnel shutdown
configure service vprn static-route-entry next-hop shutdown

Description This command causes the static route to be placed in an administratively down state and removed from the active route-table

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context [Tree] (config>service>vprn>if>secure-nd shutdown)

Full Context configure service vprn interface secure-nd shutdown

Description This command enables or disables Secure Neighbor Discovery (SeND) on the interface.

shutdown

Syntax [**no**] **shutdown**

Context [Tree] (config>router>gmpls>path shutdown)

Full Context configure router gmpls path shutdown

Description This command disables GMPLS LSPs using the path. All services using these GMPLS LSPs are affected. Paths are created in the **shutdown** state.

The **no** form of this command administratively enables the path. All LSPs, where this path is defined as primary or defined as standby secondary, are (re)established.

Default no shutdown

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>gmpls>peer shutdown)

Full Context configure router gmpls peer shutdown

Description This command disables or enables RSVP adjacency with the neighboring UNI-N peer node.

Default shutdown

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>ldp shutdown)
[Tree] (config>router>ldp>if-params>if shutdown)
[Tree] (config>router>ldp>if-params>if>ipv4 shutdown)
[Tree] (config>router>ldp>if-params>if>ipv6 shutdown)
[Tree] (config>router>ldp>targ-session>peer shutdown)
[Tree] (config>router>ldp>targ-session>peer-template shutdown)
[Tree] (config>router>ldp>egr-stats>fec-prefix shutdown)
[Tree] (config>router>ldp>aggregate-prefix-match shutdown)

Full Context configure router ldp aggregate-prefix-match shutdown
configure router ldp egress-statistics fec-prefix shutdown
configure router ldp interface-parameters interface ipv4 shutdown
configure router ldp interface-parameters interface ipv6 shutdown
configure router ldp interface-parameters interface shutdown
configure router ldp shutdown
configure router ldp targeted-session peer shutdown
configure router ldp targeted-session peer-template shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted. For an LDP interface, the **shutdown** command exists under the main interface context and under each of the interface IPv4 and IPv6 contexts.

- **shutdown** under the **interface** context brings down both IPv4 and IPv6 Hello adjacencies and stops Hello transmission in both contexts.
- **shutdown** under the **interface** IPv4 or IPv6 contexts brings down the Hello adjacency and stops Hello transmission in that context only.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The user can also delete the entire IPv4 or IPv6 context under the interface with the **no ipv4** or **no ipv6** command which in addition to bringing down the Hello adjacency will delete the configuration.

The **no** form of this command administratively enables an entity.

Unlike other commands and parameters where the default state is not indicated in the configuration file, the **shutdown** and **no shutdown** states are always indicated in system generated configuration files.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>ldp>targeted-session>auto-tx>ipv4 shutdown)
[Tree] (config>router>ldp>targeted-session>auto-rx>ipv4 shutdown)

Full Context configure router ldp targeted-session auto-rx ipv4 shutdown
configure router ldp targeted-session auto-tx ipv4 shutdown

Description This command administratively disables the capabilities associated with automatically sending targeted Hello messages through the **auto-tx** command or processing targeted Hello messages through the **auto-rx** command.

The **no** form of this command administratively enables the capabilities associated with the **auto-tx** and **auto-rx** commands.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls shutdown)
[Tree] (config>router>mpls>interface shutdown)
[Tree] (config>router>mpls>ingr-stats>p2mp-template-lsp shutdown)
[Tree] (config>router>mpls>ingr-stats>p2p-template-lsp shutdown)
[Tree] (config>router>mpls>lsp>primary shutdown)
[Tree] (config>router>mpls>lsp>primary-p2mp-instance shutdown)
[Tree] (config>router>mpls>lsp>secondary shutdown)
[Tree] (config>router>mpls>lsp>egress-statistics shutdown)
[Tree] (config>router>mpls>lsp-template>egress-statistics shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls ingress-statistics p2mp-template-lsp shutdown
configure router mpls ingress-statistics p2p-template-lsp shutdown
configure router mpls interface shutdown
configure router mpls lsp egress-statistics shutdown
configure router mpls lsp primary shutdown
configure router mpls lsp primary-p2mp-instance shutdown
configure router mpls lsp secondary shutdown
configure router mpls lsp-template egress-statistics shutdown
configure router mpls shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The **config**>**router**>**mpls**>**ingr-stats**>**p2mp-template-lsp**>**shutdown** command is supported on the 7750 SR, 7950 XRS, and with VPLS only on the 7450 ESS.

The **config**>**router**>**mpls**>**lsp**>**primary-p2mp-instance**>**shutdown** is not supported on the 7450 ESS.

MPLS is not enabled by default and must be explicitly enabled (**no shutdown**).

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>pce-initiated-lsp>sr-te shutdown)

Full Context configure router mpls pce-initiated-lsp sr-te shutdown

Description This command administratively enables or disables the **sr-te** context for PCE initiated LSPs. A shutdown of the **sr-te** context under **pce-initiated-lsp** causes an error to be generated for new PCInitate messages, and existing PCE-initiated LSPs are taken to the **oper-down** state.

The **no** form of this command administratively enables the **sr-te** context for PCE initiated LSP.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>if>label-map shutdown)

Full Context configure router mpls interface label-map shutdown

Description This command disables the label map definition. This drops all packets that match the specified *in-label* specified in the **label-map** *in-label* command.

The **no** form of this command administratively enables the defined label map action.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>lsp shutdown)
[Tree] (config>router>mpls>lsp-template shutdown)

Full Context configure router mpls lsp shutdown
configure router mpls lsp-template shutdown

Description This command disables the existing LSP including the primary and any standby secondary paths.

To shutdown only the primary enter the **config router mpls lsp** *lsp-name* **primary** *path-name* **shutdown** command.

To shutdown a specific standby secondary enter the **config router mpls lsp** *lsp-name* **secondary** *path-name* **shutdown** command. The existing configuration of the LSP is preserved.

Use the **no** form of this command to restart the LSP. LSPs are created in a shutdown state. Use this command to administratively bring up the LSP.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>rib-api>mpls shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router rib-api mpls shutdown

Description This command disables the programming of tunnel and label FIB entries by the RIB-API gRPC service. It causes all existing tunnel and label FIB entries to be de-programmed from the data path, but they remain in the control plane database.

The **no** form of this command enables the programming of tunnel and label FIB entries by the RIB-API gRPC service.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>path shutdown)

Full Context configure router mpls path shutdown

Description This command disables the existing LSPs using this path. All services using these LSPs are affected. Binding information, however, is retained in those LSPs. Paths are created in the **shutdown** state.

The **no** form of this command administratively enables the path. All LSPs, where this path is defined as primary or defined as standby secondary, are (re)established.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>pcep>pcc shutdown)
[Tree] (config>router>pcep>pce shutdown)

Full Context configure router pcep pcc shutdown
configure router pcep pce shutdown

Description This command administratively disables the PCC or PCE process.

The following PCE parameters can only be modified when the PCEP session is shut down:

- **local-address**
- **keepalive**
- **dead-timer**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **unknown-message-rate** PCE parameter can be modified without shutting down the PCEP session.

The following PCC parameters can only be modified when the PCEP session is shut down:

- **local-address**
- **keepalive**
- **dead-timer**
- **peer**

The following PCC parameters can be modified without shutting down the PCEP session:

- **report-path-constraints**
- **unknown-message-rate**

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>rsvp shutdown)
[Tree] (config>router>rsvp>interface shutdown)

Full Context configure router rsvp interface shutdown
configure router rsvp shutdown

Description This command disables the RSVP protocol instance or the RSVP-related functions for the interface. The RSVP configuration information associated with this interface is retained. When RSVP is administratively disabled, all the RSVP sessions are torn down. The existing configuration is retained.

The **no** form of this command administratively enables RSVP on the interface.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy>nh-grp shutdown)

Full Context configure router mpls forwarding-policies forwarding-policy next-hop-group shutdown

Description This command shuts down an NHG entry in a forwarding policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an NHG is shut down, it is removed from the data path entry of the forwarding policy.

The **no** form of this command brings up an NHG entry in a forwarding policy.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy shutdown)

Full Context configure router mpls forwarding-policies forwarding-policy shutdown

Description This command shuts down the forwarding policy.

The **no** form of this command enables the forwarding policy.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>mpls>fwd-policies shutdown)

Full Context configure router mpls forwarding-policies shutdown

Description This command shuts down the **forwarding-policies** context; causing all forwarding policies to be removed from the data path, however they remain in the MPLS forwarding database.

The **no** form of this command enables the **forwarding-policies** context.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>app-assure>aarp shutdown)
[Tree] (config>app-assure>group>aa-sub-cong shutdown)
[Tree] (config>app-assure>group>cflowd shutdown)
[Tree] (config>app-assure>group>cflowd>collector shutdown)
[Tree] (config>app-assure>group>cflowd>comp shutdown)
[Tree] (config>app-assure>group>cflowd>comp>template>dynamic-fields shutdown)
[Tree] (config>app-assure>group>cflowd>rtp-perf shutdown)
[Tree] (config>app-assure>group>cflowd>rtp-perf>audio-template>dynamic-fields shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>app-assure>group>cflowd>rtp-perf>video-template>dynamic-fields shutdown)
[Tree] (config>app-assure>group>cflowd>rtp-perf>voice-template>dynamic-fields shutdown)
[Tree] (config>app-assure>group>cflowd>tcp-perf shutdown)
[Tree] (config>app-assure>group>cflowd>tcp-perf>template>dynamic-fields shutdown)
[Tree] (config>app-assure>group>cflowd>volume shutdown)
[Tree] (config>app-assure>group>cflowd>volume>template>dynamic-fields shutdown)
[Tree] (config>app-assure>group>certificate-profile shutdown)
[Tree] (config>app-assure>group>dns-ip-cache shutdown)
[Tree] (config>app-assure>group>event-log shutdown)
[Tree] (config>app-assure>group>gtp shutdown)
[Tree] (config>app-assure>group>http-enrich shutdown)
[Tree] (config>app-assure>group>http-error-redirect shutdown)
[Tree] (config>app-assure>group>http-notification shutdown)
[Tree] (config>app-assure>group>http-redirect shutdown)
[Tree] (config>app-assure>group>policer>tod-override shutdown)
[Tree] (config>app-assure>group>policy>app-filter>entry shutdown)
[Tree] (config>app-assure>group>policy>app-qos-policy>entry shutdown)
[Tree] (config>app-assure>group>policy>custom-protocol shutdown)
[Tree] (config>app-assure>group>statistics>protocol shutdown)
[Tree] (config>app-assure>group>tethering-detection shutdown)
[Tree] (config>app-assure>group>transit-ip-policy>dhcp shutdown)
[Tree] (config>app-assure>group>transit-ip-policy>radius shutdown)
[Tree] (config>app-assure>group>transit-ip-policy>transit-auto-create shutdown)
[Tree] (config>app-assure>group>url-filter shutdown)
[Tree] (config>app-assure>group>url-filter>icap>server shutdown)
[Tree] (config>app-assure>group>url-list shutdown)
[Tree] (config>app-assure>group>wap1x shutdown)
[Tree] (config>app-assure>protocol shutdown)
[Tree] (config>isa>aa-grp shutdown)
[Tree] (config>service>ies>aa-interface shutdown)
[Tree] (config>service>ies>aa-interface>sap shutdown)
[Tree] (config>service>vprn>aa-interface shutdown)
[Tree] (config>service>vprn>aa-interface>sap shutdown)

Full Context

configure application-assurance aarp shutdown
configure application-assurance group aa-sub-congestion-detection shutdown
configure application-assurance group certificate-profile shutdown
configure application-assurance group cflowd collector shutdown
configure application-assurance group cflowd comprehensive shutdown
configure application-assurance group cflowd comprehensive template dynamic-fields shutdown
configure application-assurance group cflowd rtp-performance audio-template dynamic-fields shutdown
configure application-assurance group cflowd rtp-performance shutdown
configure application-assurance group cflowd rtp-performance video-template dynamic-fields shutdown
configure application-assurance group cflowd rtp-performance voice-template dynamic-fields shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure application-assurance group cflowd shutdown
configure application-assurance group cflowd tcp-performance shutdown
configure application-assurance group cflowd tcp-performance template dynamic-fields shutdown
configure application-assurance group cflowd volume shutdown
configure application-assurance group cflowd volume template dynamic-fields shutdown
configure application-assurance group dns-ip-cache shutdown
configure application-assurance group event-log shutdown
configure application-assurance group gtp shutdown
configure application-assurance group http-enrich shutdown
configure application-assurance group http-error-redirect shutdown
configure application-assurance group http-notification shutdown
configure application-assurance group http-redirect shutdown
configure application-assurance group policer tod-override shutdown
configure application-assurance group policy app-filter entry shutdown
configure application-assurance group policy app-qos-policy entry shutdown
configure application-assurance group policy custom-protocol shutdown
configure application-assurance group statistics protocol shutdown
configure application-assurance group tethering-detection shutdown
configure application-assurance group transit-ip-policy dhcp shutdown
configure application-assurance group transit-ip-policy radius shutdown
configure application-assurance group transit-ip-policy transit-auto-create shutdown
configure application-assurance group url-filter icap server shutdown
configure application-assurance group url-filter shutdown
configure application-assurance group url-list shutdown
configure application-assurance group wap1x shutdown
configure application-assurance protocol shutdown
configure isa application-assurance-group shutdown
configure service ies aa-interface sap shutdown
configure service ies aa-interface shutdown
configure service vprn aa-interface sap shutdown
configure service vprn aa-interface shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>app-assure>group>transit-ip>diameter shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group transit-ip-policy diameter shutdown

Description This command removes all transit AA subscribers created via Diameter on this transit AA subscriber IP policy and clears all corresponding Diameter sessions.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>isa>aa-grp>overload-sub-quarantine shutdown)

Full Context configure isa application-assurance-group overload-sub-quarantine shutdown

Description This command disables the overload subscriber detection algorithm in the ISA group for the purpose of quarantining an overloaded subscriber. It is possible to manually quarantine an AA subscriber even when this command is disabled (**shutdown**).

The **no** form of this command enables the overload subscriber detection algorithm in the ISA group. When enabled, each ISA monitors the traffic on a continuous basis to identify AA subscribers that occupy more than their fair share of ISA resources and need to be quarantined.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (debug>app-assure>group>traffic-capture shutdown)

Full Context debug application-assurance group traffic-capture shutdown

Description This command administratively disables traffic capture.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (debug>app-assure>group>http-host-recorder shutdown)
[Tree] (debug>app-assure>group>port-recorder shutdown)

Full Context debug application-assurance group http-host-recorder shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug application-assurance group port-recorder shutdown

Description This commands allows to stop or start the http-host-recorder. To reset the recorded values execute shutdown followed by **no** shutdown.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>esa shutdown)
[Tree] (config>esa>vm shutdown)

Full Context configure esa shutdown
configure esa vm shutdown

Description This command administratively disables the instance. The operational state of the instance is disabled, as well as the operational state of any entities contained within. When disabled, the instance does not change, reset, or remove any configuration settings or statistics.

The **no** form of this command administratively enables the instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>ipsec>cert-profile shutdown)
[Tree] (config>ipsec>client-db shutdown)
[Tree] (config>ipsec>client-db>client shutdown)
[Tree] (config>isa shutdown)
[Tree] (config>isa>aa-group shutdown)
[Tree] (config>isa>tunnel-grp shutdown)
[Tree] (config>redundancy>multi-chassis>peer>mc-ipsec>tunnel-group shutdown)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel shutdown)
[Tree] (config>service>ies>if>sap>ip-tunnel shutdown)
[Tree] (config>service>ies>if>sap>ipsec-gw shutdown)
[Tree] (config>service>ies>if>sap>ipsec-gw>dhcp shutdown)
[Tree] (config>service>ies>if>sap>ipsec-gw>dhcp6 shutdown)
[Tree] (config>service>ies>if>sap>ipsec-gw>lcl-addr-assign shutdown)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel shutdown)
[Tree] (config>service>vprn>if>sap>ip-tunnel shutdown)
[Tree] (config>service>vprn>if>sap>ipsec-gw shutdown)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp shutdown)
[Tree] (config>service>vprn>if>sap>ipsec-gw>dhcp6 shutdown)
[Tree] (config>service>vprn>if>sap>ipsec-gw>lcl-addr-assign shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context

configure ipsec cert-profile shutdown
configure ipsec client-db client shutdown
configure ipsec client-db shutdown
configure isa aa-group shutdown
configure isa shutdown
configure isa tunnel-group shutdown
configure redundancy multi-chassis peer mc-ipsec tunnel-group shutdown
configure service ies interface ipsec ipsec-tunnel shutdown
configure service ies interface sap ip-tunnel shutdown
configure service ies interface sap ipsec-gw dhcp shutdown
configure service ies interface sap ipsec-gw dhcp6 shutdown
configure service ies interface sap ipsec-gw local-address-assignment shutdown
configure service ies interface sap ipsec-gw shutdown
configure service vprn interface ipsec ipsec-tunnel shutdown
configure service vprn interface sap ip-tunnel shutdown
configure service vprn interface sap ipsec-gw dhcp shutdown
configure service vprn interface sap ipsec-gw dhcp6 shutdown
configure service vprn interface sap ipsec-gw local-address-assignment shutdown
configure service vprn interface sap ipsec-gw shutdown

Description

This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Platforms

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies interface sap ipsec-gw local-address-assignment shutdown
- configure ipsec cert-profile shutdown
- configure service ies interface sap ipsec-gw dhcp shutdown
- configure service vprn interface sap ipsec-gw shutdown
- configure service vprn interface sap ipsec-gw local-address-assignment shutdown
- configure redundancy multi-chassis peer mc-ipsec tunnel-group shutdown
- configure ipsec client-db shutdown
- configure service ies interface sap ipsec-gw dhcp6 shutdown
- configure service vprn interface sap ipsec-gw dhcp shutdown
- configure isa tunnel-group shutdown
- configure service ies interface sap ipsec-gw shutdown
- configure service vprn interface sap ipsec-gw dhcp6 shutdown
- configure ipsec client-db client shutdown

All

- configure service ies interface sap ip-tunnel shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface sap ip-tunnel shutdown

VSR

- configure service ies interface ipsec ipsec-tunnel shutdown
- configure service vprn interface ipsec ipsec-tunnel shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update shutdown)

Full Context configure system security pki ca-profile auto-crl-update shutdown

Description This command disables the auto CRL update.

The **no** form of this command enables an auto CRL update. Upon **no shutdown**, if the configured CRL file does not exist, is invalid or is expired or if the schedule-type is next-update-based and current time passed (Next-Update_of_existing_CRL - pre-update-time), then system will start downloading CRL right away.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>isa>lns-group shutdown)

Full Context configure isa lns-group shutdown

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context

[Tree] (config>aaa>isa-radius-plcy>servers>server shutdown)
[Tree] (config>isa>nat-group shutdown)
[Tree] (config>router>firewall>domain shutdown)
[Tree] (config>router>nat>inside>deterministic>prefix shutdown)
[Tree] (config>router>nat>inside>dual-stack-lite shutdown)
[Tree] (config>router>nat>inside>nat64 shutdown)
[Tree] (config>router>nat>inside>redundancy>subscriber-identification shutdown)
[Tree] (config>router>nat>inside>subscriber-id shutdown)
[Tree] (config>router>nat>outside>pool shutdown)
[Tree] (config>router>nat>outside>pool>address-range shutdown)
[Tree] (config>router>nat>outside>pool>redundancy shutdown)
[Tree] (config>service>ipfix>ipfix-export-policy>collector shutdown)
[Tree] (config>service>vprn>mtrace2 shutdown)
[Tree] (config>service>vprn>nat>inside>nat64 shutdown)
[Tree] (config>service>vprn>nat>outside>pool shutdown)
[Tree] (config>service>vprn>nat>outside>pool>address-range shutdown)
[Tree] (config>service>vprn>nat>outside>pool>redundancy shutdown)

Full Context

configure aaa isa-radius-policy servers server shutdown
configure isa nat-group shutdown
configure router firewall domain shutdown
configure router nat inside deterministic prefix shutdown
configure router nat inside dual-stack-lite shutdown
configure router nat inside nat64 shutdown
configure router nat inside redundancy subscriber-identification shutdown
configure router nat inside subscriber-id shutdown
configure router nat outside pool address-range shutdown
configure router nat outside pool redundancy shutdown
configure router nat outside pool shutdown
configure service ipfix ipfix-export-policy collector shutdown
configure service vprn mtrace2 shutdown
configure service vprn nat inside nat64 shutdown
configure service vprn nat outside pool address-range shutdown
configure service vprn nat outside pool redundancy shutdown
configure service vprn nat outside pool shutdown

Description

This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Platforms

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure isa nat-group shutdown
- configure router nat inside dual-stack-lite shutdown
- configure router nat inside deterministic prefix shutdown
- configure service vprn nat outside pool redundancy shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure router nat inside nat64 shutdown
- configure service vprn nat outside pool shutdown
- configure aaa isa-radius-policy servers server shutdown
- configure router nat outside pool shutdown
- configure service vprn nat inside nat64 shutdown
- configure router nat outside pool redundancy shutdown

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure router firewall domain shutdown

All

- configure service ipfix ipfix-export-policy collector shutdown
- configure service vprn mtrace2 shutdown

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>nat>map-domain>mapping-rule shutdown)

Full Context configure service nat map-domain mapping-rule shutdown

Description This command enables or disables a rule within a MAP domain. A MAP rule can be enabled (**no shutdown**) only when all parameters within the rule are defined. Disabling a rule within an instantiated MAP domain will withdraw the rule IPv4 routes and disable forwarding for the rule.

Interactions:

config>service>vprn>nat>map>map-domain *domain-name*

config>service>router>nat>map>map-domain *domain-name*

Shutdown of an instantiated MAP rule disables the rule (the rule routes will be withdrawn and forwarding will be disabled).

Default shutdown

Platforms VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>nat>map-domain shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service nat map-domain shutdown

Description This command enables or disables a MAP domain. A MAP domain can be enabled (**no shutdown**) only when the DMR prefix is configured. Disabling an instantiated domain will withdraw all routes associated with it.

Interactions:

config>service>vprn>nat>map>map-domain *domain-name*

config>service>router>nat>map>map-domain *domain-name*

Shutdown of a MAP domain template disables the instantiated MAP domain (the routes will be withdrawn and forwarding will be disabled).

Default shutdown

Platforms VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>bier shutdown)
[Tree] (config>router>bier>template shutdown)

Full Context configure router bier shutdown
configure router bier template shutdown

Description This command shuts down BIER or a BIER template.

The **no** form of this command enables BIER or the BIER template.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>gtm>provider-tunnel>inclusive>rsvp shutdown)
[Tree] (config>router>gtm>provider-tunnel>selective>rsvp shutdown)

Full Context configure router gtm provider-tunnel inclusive rsvp shutdown
configure router gtm provider-tunnel selective rsvp shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state.

The **no** form of this command places the entity into an administratively enabled state.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>p2mp-sr-tree shutdown)
[Tree] (config>router>p2mp-sr-tree>p2mp-policy shutdown)
[Tree] (config>router>p2mp-sr-tree>p2mp-policy>p2mp-candidate-path shutdown)
[Tree] (config>router>p2mp-sr-tree>replication-segment shutdown)
[Tree] (config>router>p2mp-sr-tree>replication-segment>next-hop-id shutdown)

Full Context configure router p2mp-sr-tree p2mp-policy p2mp-candidate-path shutdown
configure router p2mp-sr-tree p2mp-policy shutdown
configure router p2mp-sr-tree replication-segment next-hop-id shutdown
configure router p2mp-sr-tree replication-segment shutdown
configure router p2mp-sr-tree shutdown

Description This command administratively disables an entity for the P2MP SR tree. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

When the operational state of an entity is disabled, the operational state of any entities contained within are also disabled. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (shutdown) state. When a **no shutdown** command is entered, the service becomes administratively up, then attempts to enter the operationally up state.

The **no** form of this command places the entity into an administratively enabled state.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>mirror>mirror-dest shutdown)
[Tree] (config>mirror>mirror-source shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>mirror>mirror-dest>spoke-sdp>egress shutdown)
[Tree] (config>li>li-source shutdown)
[Tree] (config>li>log>log-id shutdown)
[Tree] (config>service>vprn>ip-mirror-interface shutdown)
[Tree] (config>service>vprn>ip-mirror-interface>spoke-sdp shutdown)
[Tree] (config>service>ies>if>ping-template shutdown)
[Tree] (config>service>vprn>if>ping-template shutdown)

Full Context

configure li li-source shutdown
configure li log log-id shutdown
configure mirror mirror-dest shutdown
configure mirror mirror-dest spoke-sdp egress shutdown
configure mirror mirror-source shutdown
configure service ies interface ping-template shutdown
configure service vprn interface ping-template shutdown
configure service vprn ip-mirror-interface shutdown
configure service vprn ip-mirror-interface spoke-sdp shutdown

Description

The **shutdown** command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

The **no** form of this command puts an entity into the administratively enabled state.

Default

See Special Cases below.

Platforms

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface ping-template shutdown
- configure service ies interface ping-template shutdown

All

- configure li li-source shutdown
- configure service vprn ip-mirror-interface spoke-sdp shutdown
- configure mirror mirror-dest shutdown
- configure service vprn ip-mirror-interface shutdown
- configure mirror mirror-source shutdown
- configure li log log-id shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Special Cases

Mirror Destination — When a mirror destination service ID is shutdown, mirrored packets associated with the service ID are not accepted from the mirror source or remote source router. The associated mirror source is put into an operationally down mode. Mirrored packets are not transmitted out of the SAP or SDP. Each mirrored packet is silently discarded. If the mirror destination is a SAP, the SAP's discard counters are incremented.

The **shutdown** command places the mirror destination service or mirror source into an administratively down state. The **mirror-dest** service ID must be shut down in order to delete the service ID, SAP or SDP association from the system.

The default state for a mirror destination service ID is **shutdown**. A **no shutdown** command is required to enable the service.

Mirror Source — Mirror sources do not need to be shutdown in order to remove them from the system.

When a mirror source is **shutdown**, mirroring is terminated for all sources defined locally for the mirror destination service ID. If the **remote-source** command has been executed on the mirror destination associated with the shut down mirror source, mirroring continues for remote sources.

The default state for a mirror source for a given mirror-dest service ID is **no shutdown**. A **shutdown** command is required to disable mirroring from that mirror-source.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (debug>mirror-source shutdown)

Full Context debug mirror-source shutdown

Description This command enables mirror source debugging.

The **no** form of this command clears mirror source information.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>oam-pm>bin-group shutdown)
[Tree] (config>oam-pm>session>ethernet>dmm shutdown)
[Tree] (config>oam-pm>session>ethernet>slm shutdown)
[Tree] (config>oam-pm>session>ethernet>lmm shutdown)
[Tree] (config>oam-pm>session>ethernet>lmm>availability shutdown)
[Tree] (config>oam-pm>session>ip>twamp-light shutdown)
[Tree] (config>oam-pm>session>measurement-interval>event-mon shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>saa>test shutdown)
[Tree] (config>test-oam>ldp-treetrace shutdown)
[Tree] (config>test-oam>twamp>server shutdown)
[Tree] (config>test-oam>twamp>server>prefix shutdown)

Full Context
configure oam-pm bin-group shutdown
configure oam-pm session ethernet dmm shutdown
configure oam-pm session ethernet lmm availability shutdown
configure oam-pm session ethernet lmm shutdown
configure oam-pm session ethernet slm shutdown
configure oam-pm session ip twamp-light shutdown
configure oam-pm session measurement-interval event-mon shutdown
configure saa test shutdown
configure test-oam ldp-treetrace shutdown
configure test-oam twamp server prefix shutdown
configure test-oam twamp server shutdown

Description
This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Entities are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the entity becomes administratively up and then tries to enter the operationally up state.

The **no** form of this command administratively enables the entity.

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light shutdown
- configure test-oam twamp server shutdown

All

- configure oam-pm session ethernet slm shutdown
- configure test-oam ldp-treetrace shutdown
- configure saa test shutdown
- configure oam-pm session ethernet lmm availability shutdown
- configure oam-pm bin-group shutdown
- configure oam-pm session ethernet lmm shutdown
- configure oam-pm session ethernet dmm shutdown

shutdown

Syntax [**no**] **shutdown**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>twamp-light>reflector shutdown)
[Tree] (config>service>vprn>twamp-light>reflector shutdown)

Full Context configure router twamp-light reflector shutdown
configure service vprn twamp-light reflector shutdown

Description This command disables or enables TWAMP Light functionality within the context where the configuration exists, either the base router instance or the service. Enabling the base router context enables the IES prefix list since the IES service uses the configuration under the base router instance.

The **no** form of this command allows the router instance or the service to accept TWAMP Light packets for processing.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context [Tree] (config>bfd>seamless-bfd>reflector shutdown)

Full Context configure bfd seamless-bfd reflector shutdown

Description This command specifies the administrative state of the seamless BFD reflector.

The **no** form of this command administratively enables the reflector. A discriminator must be configured before the **no shutdown** command is invoked.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context [Tree] (config>qos>slope-policy>exceed-slope shutdown)
[Tree] (config>qos>slope-policy>highplus-slope shutdown)
[Tree] (config>qos>slope-policy>high-slope shutdown)
[Tree] (config>qos>slope-policy>low-slope shutdown)

Full Context configure qos slope-policy exceed-slope shutdown
configure qos slope-policy high-slope shutdown
configure qos slope-policy highplus-slope shutdown
configure qos slope-policy low-slope shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables or disables the administrative status of the Random Early Detection slope.

By default, all slopes are shutdown and have to be explicitly enabled (**no shutdown**).

The **no** form of this command administratively enables the RED slope.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>filter>redirect-policy shutdown)
[Tree] (config>filter>redirect-policy>destination shutdown)
[Tree] (config>filter>log>summary shutdown)

Full Context configure filter log summary shutdown
configure filter redirect-policy destination shutdown
configure filter redirect-policy shutdown

Description Administratively enables/disabled (AdminUp/AdminDown) an entity. Downing an entity does not change, reset or remove any configuration settings or statistics. Many objects must be shutdown before they may be deleted.

The **shutdown** command administratively downs an entity. Administratively downing an entity changes the operational state of the entity to down.

Unlike other commands and parameters where the default state will not be indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

The **no** form of the command puts an entity into the administratively enabled state.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>if>ipv6>secure-nd shutdown)

Full Context configure router interface ipv6 secure-nd shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables or disables Secure Neighbor Discovery (SeND) on the interface.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>pcp-server>server shutdown)

Full Context configure router pcp-server server shutdown

Description This command administratively enables the PCP server.

The **no** form of this command administratively disables the PCP server.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>open-flow>of-switch shutdown)

Full Context configure open-flow of-switch shutdown

Description This command administratively enables or disables the OpenFlow switch instance. Disabling the switch purges all flowtable entries.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>if>vrrp shutdown)
[Tree] (config>router>if>ipv6>vrrp shutdown)
[Tree] (config>vrrp>policy shutdown)

Full Context configure router interface ipv6 vrrp shutdown
configure router interface vrrp shutdown
configure vrrp policy shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables an entity.

Default no shutdown

Platforms All

Special Cases **Non-Owner Virtual Router —** Non-owner virtual router instances can be administratively shutdown. This allows the termination of VRRP participation in the virtual router and stops all routing and other access capabilities with regards to the virtual router IP addresses. Shutting down the virtual router instance provides a mechanism to maintain the virtual routers without causing false backup/master state changes.

If the **shutdown** command is executed, no VRRP advertisement messages are generated and all received VRRP advertisement messages are silently discarded with no processing.

By default, virtual router instances are created in the **no shutdown** state.

Whenever the administrative state of a virtual router instance transitions, a log message is generated.

Whenever the operational state of a virtual router instance transitions, a log message is generated.

Owner Virtual Router — An owner virtual router context does not have a **shutdown** command. To administratively disable an owner virtual router instance, use the **shutdown** command within the parent IP interface node which administratively downs the IP interface.

shutdown

Syntax [**no**] **shutdown** [**active**] [**standby**]
[**no**] **shutdown** [*cflash-id*]

Context **[Tree]** (file shutdown)

Full Context file shutdown

Description This command shuts down (unmounts) the specified CPM(s).

Use the **no shutdown** [**active**] [**standby**] command to enable one or both CPM.

Use the **no shutdown** [*cflash-id*] command to enable a compact flash (cf1:, cf2:, or cf3:) on the CPM/CCM. The **no shutdown** command can be issued for a specific slot when no compact flash is present. When a flash card is installed in the slot, the card will be activated upon detection.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In redundant systems, use the **no shutdown** command on cf3: on both SF/CPMs or CCMs in order to facilitate synchronization. See the **config>redundancy synchronize** command.

Note: The **shutdown** command must be issued prior to removing a flash card. If no parameters are specified, then the drive referred to by the current working directory will be shut down.

LED Status Indicators

Table 130 lists the possible states for the compact flash and their LED status indicators.

Table 130 **LED Status Indicators**

State	Description
Operational	If a compact flash is present in a drive and operational (no shutdown), the respective LED is lit green. The LED flickers when the compact flash is accessed. **Note:** Do not remove the compact flash during a read/write operation.
Flash defective	If a compact flash is defective, the respective LED blinks amber to reflect the error condition and a trap is raised.
Flash drive shut down	When the compact flash drive is shut down and a compact flash present, the LED is lit amber. In this state, the compact flash can be ejected.
No compact flash present, drive shut down	If no compact flash is present and the drive is shut down the LED is unlit.
No compact flash present, drive enabled	If no compact flash is present and the drive is not shut down the LED is unlit.
Ejecting a compact flash	The compact flash drive should be shut down before ejecting a compact flash card. The LED should turn to solid (not blinking) amber. This is the only mode to safely remove the flash card. If a compact flash drive is not shut down before a compact flash is ejected, the LED blinks amber for approximately 5 seconds before shutting off.

The **shutdown** or **no shutdown** state is not saved in the configuration file. Following a reboot all compact flash drives are in their default state.

Default no shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *cflash-id* — Specifies the compact flash slot ID to be shut down or enabled. If *cflash-id* is specified, the drive is shut down or enabled. If no *cflash-id* is specified, the drive referred to by the current working directory is assumed. If a slot number is not specified, then the active CPM is assumed.

Values cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Default the current compact flash device

active — Specifies that all drives on the active CPM are shutdown or enabled.

standby — Specifies that all drives on the standby CPM are shutdown or enabled.

When both **active** and **standby** keywords are specified, then all drives on both CPM are shutdown.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>satellite>eth-sat shutdown)
[Tree] (config>system>satellite>tdm-sat shutdown)

Full Context configure system satellite eth-sat shutdown
configure system satellite tdm-sat shutdown

Description This command disables the associated satellite.

If the associated satellite is active, the satellite will not be reset but all satellite client ports will be shut down.

If the satellite is not active but attempts to associate with the host, the satellite chassis will be brought up according to the satellite configuration but all client ports will be shut down.

The **no** form of this command removes the shutdown state and all client ports on active satellites will be brought back up.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure system satellite eth-sat shutdown

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure system satellite tdm-sat shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>alarm-contact-input shutdown)

Full Context configure system alarm-contact-input shutdown

Description This command disables tracking of state changes associated with the alarm contact input. The system does not generate or clear the alarms for the alarm contact input while tracking is disabled. The system clears existing alarms when the **shutdown** command is executed.

The **no** form of this command enables tracking of state changes associated with the alarm contact input.

Default shutdown

Platforms 7750 SR-a

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>ptp>peer shutdown)

Full Context configure system ptp peer shutdown

Description This command disables or enables a specific PTP peer. Shutting down a peer sends cancel unicast negotiation messages on any established unicast sessions. When shutdown, all received packets from the peer are ignored.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last enabled peer cannot be shutdown. This prevents the user from having PTP enabled without any peer configured and enabled.

Default no shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>ptp>port shutdown)

Full Context configure system ptp port shutdown

Description This command disables or enables a specific PTP port. When shutdown, all PTP Ethernet messages are dropped on the IOM They will not be counted in the PTP message statistics. No PTP packets are transmitted by the node toward this port.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last enabled port or peer cannot be shutdown. This prevents the user from having PTP enabled without any means to synchronize the local clock to a parent clock.

Default no shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>management-interface>remote-management shutdown)
[Tree] (config>system>management-interface>remote-management>manager shutdown)

Full Context configure system management-interface remote-management manager shutdown
configure system management-interface remote-management shutdown

Description This command administratively disables remote management.

The **no** form of this command administratively enables remote management.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>alarms shutdown)

Full Context configure system alarms shutdown

Description This command enables or disables the Facility Alarm functionality. When enabled, the Facility Alarm sub-system tracks active and cleared facility alarms and controls the Alarm LEDs on the CPMs. When Facility Alarm functionality is enabled, the alarms are viewed using the show system alarms command(s).

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>log>log-id shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>log>accounting-policy shutdown)
[Tree] (config>log>event-handling>handler shutdown)
[Tree] (config>log>event-handling>handler>action-list>entry shutdown)
[Tree] (config>log>event-trigger>event shutdown)
[Tree] (config>log>event-trigger>event>trigger-entry shutdown)

Full Context configure log accounting-policy shutdown
configure log event-handling handler action-list entry shutdown
configure log event-handling handler shutdown
configure log event-trigger event shutdown
configure log event-trigger event trigger-entry shutdown
configure log log-id shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables an entity.

Default no shutdown

Platforms All

Special Cases **log-id —** When a log ID is shut down, no events are collected for the entity. This leads to the loss of event data.

accounting-policy — When an accounting policy is shut down, no accounting data is written to the destination log ID. Counters in the billing data reflect totals, not increments, so when the policy is re-enabled (**no shutdown**) the counters include the data collected during the period the policy was shut down.

shutdown

Syntax [**no**] **shutdown**

Context [Tree] (config>system>netconf shutdown)

Full Context configure system netconf shutdown

Description This command disables the NETCONF server. The **shutdown** command is blocked if there are any active NETCONF sessions. Use the **admin disconnect** command to disconnect all NETCONF sessions before shutting down the NETCONF service.

Platforms All

shutdown

Syntax [**no**] **shutdown**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context
[Tree] (config>system>security>mgmt-access-filter>ip-filter shutdown)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter shutdown)
[Tree] (config>sys>sec>cpm>ip-filter shutdown)
[Tree] (config>system>security>keychain shutdown)
[Tree] (config>system>security>keychain>direction>bi>entry shutdown)
[Tree] (config>system>security>keychain>direction>uni>receive>entry shutdown)
[Tree] (config>system>security>keychain>direction>uni>send>entry shutdown)
[Tree] (config>system>security>dot1x shutdown)
[Tree] (config>system>security>dot1x>radius-plcy shutdown)
[Tree] (config>sys>sec>cpm>ipv6-filter shutdown)
[Tree] (cfg>sys>sec>cpm>mac-filter>entry shutdown)

Full Context
configure system security cpm-filter mac-filter entry shutdown
configure system security cpm-filter ip-filter shutdown
configure system security cpm-filter ipv6-filter shutdown
configure system security dot1x radius-plcy shutdown
configure system security dot1x shutdown
configure system security keychain direction bi entry shutdown
configure system security keychain direction uni receive entry shutdown
configure system security keychain direction uni send entry shutdown
configure system security keychain shutdown
configure system security management-access-filter ip-filter shutdown
configure system security management-access-filter ipv6-filter shutdown

Description
This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command puts an entity into the administratively enabled state.

Default
no shutdown

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure system security cpm-filter ip-filter shutdown
- configure system security cpm-filter ipv6-filter shutdown

All

- configure system security management-access-filter ip-filter shutdown
- configure system security management-access-filter ipv6-filter shutdown
- configure system security dot1x shutdown
- configure system security keychain direction uni send entry shutdown
- configure system security dot1x radius-plcy shutdown
- configure system security keychain shutdown
- configure system security keychain direction uni receive entry shutdown
- configure system security keychain direction bi entry shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>pki>ca-profile shutdown)

Full Context configure system security pki ca-profile shutdown

Description Use this command to enable or disable the ca-profile. The system verifies the configured cert-file and crl-file. If the verification fails, then the **no shutdown** command fails.

The ca-profile in a **shutdown** state cannot be used in certificate authentication.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>ssh>key-re-exchange>client shutdown)
[Tree] (config>system>security>ssh>key-re-exchange>server shutdown)

Full Context configure system security ssh key-re-exchange client shutdown
configure system security ssh key-re-exchange server shutdown

Description This command stops the key exchange. It sets the minutes and bytes to infinity so there will not be any key exchange during the PDU transmission.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>tacplus shutdown)

Full Context configure system security tacplus shutdown

Description This command administratively disables the TACACS+ protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables the protocol which is the default state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>ldap shutdown)
[Tree] (config>system>security>ldap>server shutdown)

Full Context configure system security ldap server shutdown
configure system security ldap shutdown

Description In the **ldap** context, this command enables or disabled LDAP protocol operations.

In the **server** context, this command enables or disables the LDAP server. To perform **no shutdown**, an LDAP server address is required. To change the address, the user first needs to shut down the server.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>grpc>gnmi shutdown)

Full Context configure system grpc gnmi shutdown

Description This command stops the gNMI service.

The **no** form of this command starts the gNMI service.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>grpc>rib-api shutdown)

Full Context configure system grpc rib-api shutdown

Description This command stops the RibApi gRPC service, deletes all programmed RIB entries (stale and non-stale), but does not close the TCP connections.

The **no** form of this command restarts the RibApi gRPC service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>grpc shutdown)

Full Context configure system grpc shutdown

Description This command stops the gRPC server. This closes all of the associated TCP connections and immediately purges all RIB entries that were programmed using the RibApi Service.

The **shutdown** command is not blocked if there are active gRPC sessions. Shutting down gRPC will terminate all active gRPC sessions.

The **no** form of this command starts the gRPC server.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>grpc>tcp-keepalive shutdown)

Full Context configure system grpc tcp-keepalive shutdown

Description This command stops the TCP keepalives from being sent to all gRPC clients.

The **no** form of this command restarts the sending of TCP keepalives to all gRPC clients.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>snmp>streaming shutdown)

Full Context configure system snmp streaming shutdown

Description This command administratively disables proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes.

The **no** form of the command administratively re-enables SNMP request/response bundling and TCP-based transport mechanism.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>snmp shutdown)

Full Context configure system snmp shutdown

Description This command administratively disables SNMP agent operations. System management can then only be performed using the command line interface (CLI). Shutting down SNMP does not remove or change configuration parameters other than the administrative state. This command does not prevent the agent from sending SNMP notifications to any configured SNMP trap destinations. SNMP trap destinations are configured under the **config>log>snmp-trap-group** context.

This command is automatically invoked in the event of a reboot when the processing of the configuration file fails to complete or when an SNMP persistent index file fails while the **bof persist on** command is enabled.

The **no** form of the command administratively enables SNMP which is the default state.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>tls>cert-profile shutdown)

Full Context configure system security tls cert-profile shutdown

Description This command disables the certificate profile. When the certificate profile is disabled, it will not be sent to the TLS server.

The **no** form of the command enables the certificate profile and allows it to be sent to the TLS server.

Default shutdown

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>system>security>tls>client-tls-profile shutdown)
[Tree] (config>system>security>tls>server-tls-profile shutdown)

Full Context configure system security tls client-tls-profile shutdown
configure system security tls server-tls-profile shutdown

Description This command administratively enables or disables the TLS profile. If the TLS profile is shut down, the TLS operational status will be down. Therefore, if the TLS profile is shut down, any application using TLS should not attempt to send any PDUs.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>bgp shutdown)
[Tree] (config>router>bgp>group shutdown)
[Tree] (config>router>bgp>group>neighbor shutdown)
[Tree] (config>router>bgp>monitor shutdown)
[Tree] (config>router>bgp>segment-routing shutdown)
[Tree] (config>bmp shutdown)
[Tree] (config>bmp>station shutdown)
[Tree] (config>bmp>station>connection>tcp-keepalive shutdown)
[Tree] (config>router>bgp>monitor shutdown)
[Tree] (config>router>bgp>group>monitor shutdown)
[Tree] (config>router>bgp>group>neighbor>monitor shutdown)
[Tree] (config>service>vprn>bgp>monitor shutdown)
[Tree] (config>service>vprn>bgp>group>monitor shutdown)
[Tree] (config>service>vprn>bgp>group>neighbor>monitor shutdown)

Full Context configure bmp shutdown
configure bmp station connection tcp-keepalive shutdown
configure bmp station shutdown
configure router bgp group monitor shutdown
configure router bgp group neighbor monitor shutdown
configure router bgp group neighbor shutdown
configure router bgp group shutdown
configure router bgp monitor shutdown
configure router bgp segment-routing shutdown
configure router bgp shutdown
configure service vprn bgp group monitor shutdown
configure service vprn bgp group neighbor monitor shutdown
configure service vprn bgp monitor shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables an entity.

Unlike other commands and parameters where the default state is not indicated in the configuration file, the **shutdown** and **no shutdown** states are always indicated in system generated configuration files.

Default administrative states for services and service entities are described in Special Cases.

The **no** form of this command places an entity in an administratively enabled state.

Platforms All

Special Cases **BGP Global —** The BGP protocol is created in the **no shutdown** state.

BGP Group — BGP groups are created in the **no shutdown** state.

BGP Neighbor — BGP neighbors/peers are created in the **no shutdown** state.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>isis shutdown)
[Tree] (config>router>isis>igp-shortcut shutdown)
[Tree] (config>router>isis>interface shutdown)
[Tree] (config>router>isis>if>level shutdown)
[Tree] (config>router>isis>level>bier shutdown)
[Tree] (config>router>isis>segment-routing shutdown)
[Tree] (config>router>isis>segm-rtng>mapping-server shutdown)

Full Context configure router isis interface level shutdown
configure router isis igp-shortcut shutdown
configure router isis interface shutdown
configure router isis level bier shutdown
configure router isis segment-routing mapping-server shutdown
configure router isis segment-routing shutdown
configure router isis shutdown

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables an entity.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default shutdown

Platforms All

Special Cases

IS-IS IGP-Shortcut — In the **config>router>isis>igp-shortcut** context, the command enables or disables IGP shortcuts in the IGP instance.

IS-IS Interface — In the **config>router>isis>interface** context, the command disables the IS-IS interface. By default, the IS-IS interface is enabled, **no shutdown**.

IS-IS Interface and Level — In the **config>router>isis>interface** *ip-int-name*>**level** context, the command disables the IS-IS interface for the level. By default, the IS-IS interface at the level is enabled, **no shutdown**.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>isis>flex-algos shutdown)

Full Context configure router isis flexible-algorithms shutdown

Description This command enables IS-IS flexible algorithms. If it is enabled with the **no shutdown** command the router starts supporting the flexible algorithms IGP LSDB extensions. Flexible algorithm IGP LSDB extensions are by default not enabled.

The **no** form of this command enables the router to support flexible algorithms.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>ospf>flex-algos shutdown)

Full Context configure router ospf flexible-algorithms shutdown

Description This command enables OSPFv2 flexible algorithms. If **no shutdown** is configured, the router enables support for the flexible algorithms IGP LSDB extensions. Flexible algorithm IGP LSDB extensions are disabled by default.

The **no** form of this command enables the router to support flexible algorithms.

Default shutdown

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>ospf shutdown)
[Tree] (config>router>ospf shutdown)
[Tree] (config>router>ospf>area>bier shutdown)
[Tree] (config>router>ospf>area>virtual-link shutdown)
[Tree] (config>router>ospf>igp-shortcut shutdown)
[Tree] (config>router>ospf>segm-rtng shutdown)
[Tree] (config>router>ospf>segm-rtng>mapping-server shutdown)
[Tree] (config>router>ospf3 shutdown)
[Tree] (config>router>ospf3>area>interface shutdown)
[Tree] (config>router>ospf3>area>virtual-link shutdown)

Full Context configure router ospf area bier shutdown
configure router ospf area virtual-link shutdown
configure router ospf igp-shortcut shutdown
configure router ospf segment-routing mapping-server shutdown
configure router ospf segment-routing shutdown
configure router ospf shutdown
configure router ospf3 area interface shutdown
configure router ospf3 area virtual-link shutdown
configure router ospf3 shutdown

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within.

Many objects must be shut down before they may be deleted. Many entities must be explicitly enabled using the **no shutdown** command.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

The **no** form of this command puts an entity into the administratively enabled state.

Platforms All

Special Cases **OSPF Interface —** When an IP interface is configured as an OSPF interface, OSPF on the interface is in the **no shutdown** state by default.

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>rip shutdown)
[Tree] (config>router>rip>group shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>rip>group>neighbor shutdown)
[Tree] (config>router>ripng shutdown)
[Tree] (config>router>ripng>group shutdown)
[Tree] (config>router>ripng>group>neighbor shutdown)

Full Context

configure router rip group neighbor shutdown
configure router rip group shutdown
configure router rip shutdown
configure router ripng group neighbor shutdown
configure router ripng group shutdown
configure router ripng shutdown

Description

This command administratively disables an entity. Downing an entity does not change, reset or remove any configuration settings or statistics. Many objects must be shutdown before they may be deleted.

The **shutdown** command administratively downs an entity. Administratively downing an entity changes the operational state of the entity to down and the operational state of any entities contained within the administratively down entity.

Unlike other commands and parameters where the default state will not be indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

The **no** form of the command puts an entity into the administratively enabled state.

Platforms

All

Special Cases

RIP Global — In the **config>router>rip** context, the **shutdown** command administratively enables/disables the RIP protocol instance. If RIP is globally shutdown, then all RIP group and neighbor interfaces transition to the operationally down state. Routes learned from a neighbor that is shutdown are immediately removed from the RIP database and route table manager (RTM). A RIP protocol instance is administratively enabled by default.

RIP Group — In the **config>router>rip>group** *group-name* context, the **shutdown** command administratively enables/disables the RIP group. If a RIP group is shutdown, all member neighbor interfaces transition to the operationally down state. Routes learned from a neighbor that is shutdown are immediately removed from the RIP database and route table manager (RTM). A RIP group is administratively enabled by default.

RIP Neighbor — In the **config>router>rip>group** *group-name*>**neighbor** *ip-int-name* context, the **shutdown** command administratively enables/disables the RIP neighbor interface. If a RIP neighbor is shutdown, the neighbor interface transitions to the operationally down state. Routes learned from a neighbor that is shutdown are immediately removed from the RIP database and route table manager (RTM). A RIP neighbor interface is administratively enabled by default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>segment-routing>maintenance-policy shutdown)

Full Context configure router segment-routing maintenance-policy shutdown

Description This command deactivates all segment routing policies and removes the associated entries from the forwarding plane of the router.

The **no** form of this command enables all segment routing policies so that they can be revalidated and reinstalled as necessary.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>segment-routing>sr-policies>egress-statistics shutdown)
[Tree] (config>router>segment-routing>sr-policies>ingress-statistics shutdown)

Full Context configure router segment-routing sr-policies egress-statistics shutdown
configure router segment-routing sr-policies ingress-statistics shutdown

Description This command administratively disables the collection of egress or ingress statistics for all segment routing policies.

The **no** form of this command administratively enables the collection of egress or ingress statistics for all segment routing policies.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>segment-routing>sr-policies shutdown)

Full Context configure router segment-routing sr-policies shutdown

Description This command deactivates all segment routing policies and removes the associated entries from the forwarding plane of the router.

It is necessary to execute this shutdown if you want to make a change to the reserved-label-block reference.

The **no** form of this command enables all segment routing policies so that they can be revalidated and reinstalled as necessary.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy>segment-list shutdown)

Full Context configure router segment-routing sr-policies static-policy segment-list shutdown

Description This command deactivates a segment-list. If this is done on an active policy with more than one segment list, then traffic forwarded by the policy will be diverted to the remaining segment-lists.

The **no** form of this command enables the segment list so that it can be validated and installed as necessary.

Default shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy shutdown)

Full Context configure router segment-routing sr-policies static-policy shutdown

Description This command deactivates the associated static policy and causes another policy for the same (color, endpoint) combination to be promoted as the active path, assuming there is another valid policy.

It is necessary to execute this shutdown if you want to make critical configuration changes to the static policy.

The **no** form of this command enables the static policy so that it can be validated and installed as necessary.

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>lease-split shutdown)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>lease-split shutdown)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>relay>lease-split shutdown)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>lease-split shutdown)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay lease-split shutdown
configure service ies subscriber-interface ipv6 dhcp6 relay lease-split shutdown
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay lease-split shutdown
configure service vprn subscriber-interface ipv6 dhcp6 relay lease-split shutdown

Description This command administratively disables DHCPv6 lease split on the interface.

The **no** form of this command administratively enables lease split.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>port>ethernet>dot1x>per-host-authentication shutdown)

Full Context configure port ethernet dot1x per-host-authentication shutdown

Description This command administratively configures per-host authentication on the port.

The **no** form of this command administratively enables per-host authentication on the port.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>port>ethernet>dot1x shutdown)

Full Context configure port ethernet dot1x shutdown

Description This command administratively configures the 802.1x functionality (consisting of packet extraction and processing on the CPM) on the port.

The **no** form of this command administratively enables the 802.1x functionality on the port.

Default no shutdown

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>sfm shutdown)

Full Context configure sfm shutdown

Description This command administratively disables the SFM.

The **no** form of this command administratively enables the SFM.

Default no shutdown

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-2s, 7750 SR-7/12/12e, 7750 SR-7s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>segment-routing>srv6>locator shutdown)
[Tree] (config>router>isis>srv6 shutdown)

Full Context configure router isis segment-routing-v6 shutdown
configure router segment-routing segment-routing-v6 locator shutdown

Description This command administratively disables the SRv6 context in a ISIS instance or a SRv6 locator.

The **no** form of this command enables the SRv6 context in a ISIS instance or a SRv6 locator.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>bgp>egress-peer-engineering shutdown)

Full Context configure router bgp egress-peer-engineering shutdown

Description This command administratively enables or disables BGP-EPE. If enabled, peer node SIDs and peer adjacency SIDs are advertised in BGP-LS.

The **no** form of this command places the entity into an administratively enabled state and prevents peer node SIDs and peer adjacency SIDs from being advertised in BGP-LS.

Default no shutdown

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>bgp>group>egress-engineering shutdown)

Full Context configure router bgp group egress-engineering shutdown

Description This command administratively enables or disable egress engineering on a BGP neighbor or group of neighbors.

If this command is enabled along with the **egress-peer-engineering** command in BGP, SIDs in the form of MPLS labels are allocated for the segments toward the neighbor and to all links (adjacencies). These adjacencies are then advertised in BGP LS.

The **no** form of this command places the entity into an administratively enabled state.

Default no shutdown

Platforms All

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>sis shutdown)

Full Context configure subscriber-mgmt subscriber-interface-statistics shutdown

Description This command disables the collection of aggregate subscriber interface statistics.

The **no** form of this command enables subscriber interface statistics collection.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>subscr-mgmt>gis shutdown)

Full Context configure subscriber-mgmt group-interface-statistics shutdown

Description This command disables the collection of aggregate group interface statistics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command enables group interface statistics collection.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>test-oam>link-meas>template shutdown)

Full Context configure test-oam link-measurement measurement-template shutdown

Description This command administratively enables and disables the measurement template. The **measurement-template** can be referenced even if it is disabled. The template must be administratively enabled to transmit probes on any associated IP interface. The template configuration can be modified even if it is administratively enabled. The template can be administratively disabled even if interfaces are actively registered with the template. When the template configuration is modified, all registered IP interfaces start from the initial state and enter a first reporting scenario. This is true even if the template is administratively disabled and enabled, and no configuration changes are made.

The **no** form of this command disables the measurement template.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

shutdown

Syntax [**no**] **shutdown**

Context **[Tree]** (config>router>if>if-attr>delay>dyn>twamp>ipv4 shutdown)
[Tree] (config>router>if>if-attr>delay>dyn>twamp>ipv6 shutdown)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv4 shutdown
configure router interface if-attribute delay dynamic twamp-light ipv6 shutdown

Description This command enables and disables the TWAMP Light IPv4 or IPv6 protocol. Only one protocol, IPv4 or IPv6, can be enabled at any time. Attempting to enable both protocols is rejected.

The **no** form of this command administratively disables the IPv4 or IPv6 protocol.

Default shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.226 sid

sid

Syntax **sid label** *value*

Context **[Tree]** (config>router>isis>segm-rtng>adjacency-set sid)
[Tree] (config>router>ospf>segm-rtng>adjacency-set sid)

Full Context configure router isis segment-routing adjacency-set sid
configure router ospf segment-routing adjacency-set sid

Description This command allows a static SID value to be assigned to an adjacency set in IS-IS or OSPF segment routing.

The **label** option specifies the value is assigned to an MPLS label.

The **no** form of this command removes the adjacency SID.

Parameters **label** *value* — Specifies the value of adjacency SID label.

Values 18432 to 524287 | 1048575 (FP4 only)

Platforms All

23.227 sid-action

sid-action

Syntax **sid-action** *action*
no sid-action

Context **[Tree]** (config>router>p2mp-sr-tree>replication-segment sid-action)

Full Context configure router p2mp-sr-tree replication-segment sid-action

Description This command configures the SID action to take for the replication segment of the P2MP SR tree.

The **no** form of this command removes the SID action.

Default no sid-action

Parameters *action* — Specifies the name of the SID action.

Values **push** — Specifies that an outgoing SID list is pushed and forwarded on to the corresponding programmed outgoing interfaces.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pop — Specifies that on the leaf node the incoming SID is popped on the underlay packet forwarded to the host.

swap — Specifies, if an incoming SID is configured, that the SID is swapped with an outgoing SID or SID list and forwarded to the corresponding OIF.

Platforms All

23.228 sid-allocation

sid-allocation

Syntax **sid-allocation** {**sequential** | **random**}
no sid-allocation

Context **[Tree]** (config>subscr-mgmt>ppp-policy sid-allocation)

Full Context configure subscriber-mgmt ppp-policy sid-allocation

Description This command configures the method for allocating the PPPoE session ID.

For both **sequential** and **random** options, the session ID range is 1 to 8191.

The **no** form of this command reverts to the default.

Default sid-allocation sequential

Parameters **sequential** — Specifies for PPPoE sessions with the same client MAC address and active on the same SAP, to allocate the session ID in sequential order starting with ID = 1.

random — Specifies for PPPoE sessions with the same client MAC address and active on the same SAP, to allocate a unique session ID in random order.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.229 sid-map

sid-map

Syntax **sid-map node-sid** {**index** *value* [**range** *value*]} **prefix** {{*ip-addressImask*} | {*ip-address*} {*netmask*}} [**set-flags** {**s**}] [**level** {**1** | **2** | **1/2**}] [**clear-n-flag**]
no sid-map node-sid index *value*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>isis>segm-rtng>mapping-server sid-map)

Full Context configure router isis segment-routing mapping-server sid-map

Description This command configures the Segment Routing mapping server database in IS-IS.

The user enters the node SID index for one or a range of prefixes by specifying the first index value and optionally a range value can be entered. The default value for the range option is 1. Only the first prefix in a consecutive range of prefixes must be entered. The user can enter the first prefix with a mask lower than 32 and the SID or label binding TLV is advertised, but the routers will not resolve these prefix SIDs and will generate a trap.

By setting the S-flag, the user can indicate to the IS-IS routers in the rest of the network that the flooding scope of the SID or label binding TLV is the entire domain. In that case, a router receiving the TLV advertisement should leak it between ISIS levels. If leaked from level 2 to level 1, the D-flag must be set and once set the TLV cannot be leaked back into level 2. Otherwise, the S-flag is clear by default and the TLV must not be leaked by routers that receive the mapping server advertisement.

Note that the SR OS does not leak this TLV between IS-IS instances and does not support the multi-topology SID/Label Binding TLV format.

In addition, the user can specify the mapping server own flooding scope for the generated SID or label binding TLV using the **level** option. This option allows the user to narrow the flooding scope configured under the router IS-IS level-capability for a one or more SID or label binding TLVs if required. The default flooding scope of the mapping server is Layer 1 or Layer 2, which can be narrowed by the value configured under the router IS-IS level-capability.

The A-flag and M-flag are not supported by the mapping server feature. The mapping client ignores the flags.

Each time a prefix or a range of prefixes is configured in the SR mapping database in any routing instance, the router issues for this prefix or range of prefixes, a prefix-SID sub-TLV within a ISIS SID or label binding TLV in that instance. The flooding scope of the TLV from the mapping server is determined as explained above. No further check of the reachability of that prefix in the mapping server route table is performed. Additionally, no check is performed if the SID index is a duplicate of an existing prefix in the local IGP instance database or if the SID index is out of range with the local SRGB.

The **no** form of this command deletes the range of node SIDs beginning with the specified index value.

Parameters *index* — Specifies the node SID index for the IS-IS prefix which will be advertised in a SID/Label Binding TLV.

Values 0 to 4294967295

Default none

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

value — Specifies the node SID range for the IS-IS prefix which will be advertised in a SID/Label Binding TLV.

Values 0 to 65535

Default none

ip-address/mask — Specifies the IP address and mask.

Values *ip-address:* **a.b.c.d.** (host bits must be 0)
mask: **0 to 32**

ip-address netmask — Specifies the IP address netmask.

Values **a.b.c.d.** (network bits all 1 and host bits all 0)

set-flags — Specifies the flooding scope of the SID/Label binding TLV.

Default **S-flag clear**
The TLV is not leaked by routers receiving the mapping server advertisement

level {1 | 2| 1/2} — Configures the mapping server own flooding scope for the generated SID/Label binding TLV.

Default 1/2

clear-n-flag — Specifies whether the node-sid flag (N-flag) should be cleared in a SID Label Binding TLV.

Platforms All

sid-map

Syntax **sid-map node-sid index** *index-value* [**range** *range-value*] **prefix** *ip-addressImask* [*netmask*]
sid-map node-sid index *index-value* [**range** *range-value*] **prefix** *ip-addressImask* [*netmask*] **scope** {**area** *area-id* | **as**}
no sid-map node-sid index *index-value*

Context **[Tree]** (config>router>ospf>segm-rtng>mapping-server sid-map)

Full Context configure router ospf segment-routing mapping-server sid-map

Description This command configures the Segment Routing mapping server database in OSPF.

The user enters the node SID index for one or a range of prefixes by specifying the first index value and optionally a range value. The default value for the range option is 1. Only the first prefix in a consecutive range of prefixes must be entered. If the user enters the first prefix with a mask lower than 32, the OSPF Extended Prefix Range TLV is advertised but a router which receives it will not resolve SID and instead originates a trap.

The user specifies the mapping server own flooding scope for the generated OSPF Extended Prefix Range TLV using the scope option. There is no default value. If the scope is a specific area, then the TLV is flooded only in that area.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An ABR that propagates an intra-area OSPF Extended Prefix Range TLV flooded by the mapping server in that area into other areas, sets the inter-area flag (IA-flag). The ABR also propagates the TLV if received with the inter-area flag set from other ABR nodes but only from the backbone to leaf areas and not vice-versa. However, if the exact same TLV is advertised as an intra-area TLV in a leaf area, the ABR will not flood the inter-area TLV into that leaf area.

Note: SR OS does not leak this TLV between OSPF instances.

Each time a prefix or a range of prefixes is configured in the SR mapping database in any routing instance, the router issues for this prefix, or range of prefixes, a prefix-SID sub-TLV within a OSPF Extended Prefix Range TLV in that instance. The flooding scope of the TLV from the mapping server is determined as previously explained. No further check of the reachability of that prefix in the mapping server route table is performed and no check if the SID index is duplicate with some existing prefix in the local IGP instance database or if the SID index is out of range with the local SRGB.

The **no** form of this command deletes the range of node SIDs beginning with the specified index value.

Default no prefix-sid-range

Parameters **index** *index-value* — Specifies the index.

Values 0 to 4294967295

range *range-value* — Specifies the range.

Values 1 to 65535

prefix *ip-address/mask* — Specifies the IP address in dotted decimal notation.

Values ip-address/mask:

- ip-address a.b.c.d (host bits must be 0)

mask: 0 to 132

netmask — Specifies the netmask.

Values netmask — a.b.c.d (network bits all 1 and host bits all 0)

area *area-id* — Configures the mapping server own flooding scope for the generated OSPF Extended Prefix Range TLV.

Values ip-address | 0 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.230 sid-protection

sid-protection

Syntax [**no**] **sid-protection**

Context **[Tree]** (config>router>isis>interface sid-protection)

Full Context configure router isis interface sid-protection

Description This command enables or disables adjacency SID protection by LFA and remote LFA.

While LFA and remote LFA Fast-Reroute (FRR) protection is enabled for all node SIDs and local adjacency SIDs when the user enables the **loopfree-alternates** option in IS-IS or OSPF at the LER and LSR, there are applications where the user wants traffic to never divert from the strict hop computed by CSPF for a SR-TE LSP. In that case, the user can disable protection for all adjacency SIDs formed over a given network IP interface using this command.

The protection state of an adjacency SID is advertised in the B-FLAG of the IS-IS or OSPF Adjacency SID sub-TLV.

Default sid-protection

Platforms All

sid-protection

Syntax [**no**] **sid-protection**

Context **[Tree]** (config>router>ospf>area>interface sid-protection)

Full Context configure router ospf area interface sid-protection

Description This command enables or disables adjacency SID protection by LFA and remote LFA.

LFA and remote LFA Fast-Reroute (FRR) protection is enabled for all node SIDs and local adjacency SIDs when the user enables the **loopfree-alternate** option in IS-IS or OSPF at the LER and LSR. However, may be applications where the user never wants traffic to divert from the strict hop computed by CSPF for an SR-TE LSP. In this case, the user can disable protection for all adjacency SIDs formed over a particular network IP interface using this command.

The protection state of an adjacency SID is advertised in the B-FLAG of the IS-IS or OSPF Adjacency SID sub-TLV.

Default sid-protection

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.231 signal-label

signal-label

Syntax **signal-label** *value*
no signal-label

Context **[Tree]** (config>port>sonet-sdh>path signal-label)

Full Context configure port sonet-sdh path signal-label

Description This command sets the C2 byte value. The purpose of this byte is to communicate the payload type being encapsulated by SONET framing.

This command is supported on TDM satellite.

Default signal-label 0xcf

Parameters *value* — Specifies the C2 byte value, expressed as a decimal integer or a value in hex format.

Values 1 to 254 or 0x01 to 0xfe

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.232 signal-mode

signal-mode

Syntax **signal-mode** {**cas**}
no signal-mode

Context **[Tree]** (config>port>tdm>ds1 signal-mode)
[Tree] (config>port>tdm>e1 signal-mode)

Full Context configure port tdm ds1 signal-mode
configure port tdm e1 signal-mode

Description This command activates the signal mode on the channel. When enabled, it uses routing information to direct the payload of voice or data to its destination.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no signal-mode

Parameters **cas** — Specifies channel associated signaling.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

23.233 signaled-vc-type-override

signaled-vc-type-override

Syntax **signaled-vc-type-override** *atm-vcc*
no signaled-vc-type-override

Context **[Tree]** (config>service>apipe signaled-vc-type-override)

Full Context configure service apipe signaled-vc-type-override

Description This command overrides the pseudowire type signaled to type 0x0009 N:1 VCC cell within an Apipe VLL service of vc-type atm-cell. Normally, this service vc-type signals a pseudowire of type 0x0003 ATM Transparent Cell.

This command is not allowed in an Apipe VLL of vc-type value atm-cell if a configured ATM SAP is not using a connection profile. Conversely, if the signaling override command is enabled, only an ATM SAP with a connection profile assigned will be allowed.

The **override** command is not allowed on Apipe VLL service of vc-type value other than atm-cell. It is also not allowed on a VLL service with the vc-switching option enabled since signaling of the PW FEC in a Multi-Segment PW (MS-PW) is controlled by the T-PE nodes. Therefore, for this feature to be used on a MS-PW, it is required to configure an Apipe service of vc-type atm-cell at the T-PE nodes with the signaled-vc-type-override enabled, and to configure a Apipe VLL service of vc-type atm-vcc at the S-PE node with the vc-switching option enabled.

The **no** form of this command returns the Apipe VLL service to signal its default pseudowire type.

Parameters *atm-vcc* — Specifies the pseudowire type to be signaled in the pseudowire establishment.

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.234 signaling

signaling

Syntax **signaling** *signaling*

Context **[Tree]** (config>service>epipe>spoke-sdp-fec signaling)

Full Context configure service epipe spoke-sdp-fec signaling

Description This command enables a user to configure this router as the active or passive T-PE for signaling this MS-PW, or to automatically select whether this T-PE is active or passive based on the prefix. In an active role, this endpoint initiates MS-PW signaling without waiting for a T-LDP label mapping message to arrive from the far end T-PE. In a passive role, it will wait for the initial label mapping message from the far end before sending a label mapping for this end of the PW. In auto mode, if the SAII has the greater prefix value, then the router will initiate MS-PW signaling without waiting for a label mapping message from the far end. However, if the TAII has the greater value prefix, then the router will assume that the far end T-PE will initiate MS-PW signaling and will wait for that label mapping message before responding with a T-LDP label mapping message for the MS-PW in the reverse direction.

The **no** form of this command means that the router T-PE automatically selects the which router will initiate MS-PW signaling based on the prefix values configured in the SAII and TAII of the spoke SDP, as previously described.

Default signaling auto

Parameters *signaling* — Configures this router as the active T-PE for signaling this MS-PW.

Values auto, master

Platforms All

signaling

Syntax **signaling** {**off** | **tldp** | **bgp**}

Context **[Tree]** (config>service>sdp signaling)

Full Context configure service sdp signaling

Description This command specifies the signaling protocol used to obtain the ingress and egress pseudowire labels in frames transmitted and received on the SDP. When signaling is *off* then labels are manually configured when the SDP is bound to a service. The signaling value can only be changed while the administrative status of the SDP is down. Additionally, the signaling can only be changed on an SDP if that SDP is not in use by BGP-AD or BGP-VPLS. BGP signaling can only be enabled if that SDP does not already have pseudowires signaled over it.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: If the **tldp** option is selected as the mechanism for exchanging service labels over an MPLS or GRE SDP and the T-LDP session is automatically established, an explicit T-LDP session that is subsequently configured takes precedence over the automatic T-LDP session. However, if the explicit, manually-configured session is then removed, the system does not revert to the automatic session and the automatic session is also deleted. To address this, recreate the T-LDP session by disabling and re-enabling the SDP using the **shutdown** and **no shutdown** commands.

The **no** form of this command is not applicable. To modify the signaling configuration, the SDP must be administratively shut down and then the signaling parameter can be modified and re-enabled.

Default signaling tldp

Parameters **off** — Ingress and egress signal auto-labeling is not enabled. If this parameter is selected, then each service using the specified SDP must manually configure VPN labels. This configuration is independent of the SDP's transport type, GRE, MPLS (RSVP or LDP).

tldp — Ingress and egress pseudowire signaling using T-LDP is enabled. Default value used when BGP AD automatically instantiates the SDP.

bgp — Ingress and egress pseudowire signaling using BGP is enabled. Default value used when BGP VPLS automatically instantiates the SDP.

Platforms All

23.235 significant-change

significant-change

Syntax **significant-change** *delta*
no significant-change

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr significant-change)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record significant-change

Description This command configures the significant change required to generate the record.

Parameters *delta* — Specifies the delta change (significant change) that is required for the custom record to be generated.

Values 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

significant-change

Syntax **significant-change** *delta*
no significant-change

Context **[Tree]** (config>app-assure>rad-acct-plcy significant-change)

Full Context configure application-assurance radius-accounting-policy significant-change

Description This command configures the significant change required to generate the record.

The **no** form of this command reverts to the default.

Default no significant-change

Parameters *delta* — Specifies the delta change (significant change) that is required for the charging-group counts to be included in the RADIUS Accounting VSAs.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

significant-change

Syntax **significant-change** *delta*
no significant-change

Context **[Tree]** (config>log>acct-policy>cr significant-change)

Full Context configure log accounting-policy custom-record significant-change

Description This command configures the significant change required to generate the record. The custom record is only generated when the change in the reference counters equals or exceeds the configured (non-zero) significant change value. Only the reference counters for which there are corresponding counters configured under the related queues and policers are used for the significant change comparison. For reference queues and policers, the change applies to the sum of all configured reference queue and policer counters. When no reference counters are configured or **significant-change** is zero, the significant change reporting is not active.

Default significant-change 0

Parameters *delta* — Specifies the delta change (significant change) that is required for the custom record to be written to the XML file.

Values 0 to 4294967295 (For custom-record-aa-sub only values 0 or 1 are supported.)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.236 single-fiber

single-fiber

Syntax [**no**] **single-fiber**

Context **[Tree]** (config>port>ethernet single-fiber)
[Tree] (config>port>sonet-sdh single-fiber)

Full Context configure port ethernet single-fiber
configure port sonet-sdh single-fiber

Description This command enables packet gathering and redirection of IP packets from a single fiber (RX) port of the Ethernet or SONET/SDH interface and redistributes packets to other interfaces through either static routes or policy-based forwarding.

This parameter can be applied in conjunction with the strip-label command. If they are applied together, the port must have the single-fiber option configured before it can be associated with an interface that is configured with the strip-label option.

Once a port is configured with single-fiber, traffic will no longer be transmitted out of that port. This command can be used in conjunction with strip-label.

Default no single-fiber

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.237 single-mac

single-mac

Syntax [**no**] **single-mac**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>static-host-mgmt>mac-learning-options single-mac)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host-mgmt>mac-learning-options single-mac)

Full Context configure service ies subscriber-interface group-interface sap static-host-mgmt mac-learning-options single-mac
configure service vprn subscriber-interface group-interface sap static-host-mgmt mac-learning-options single-mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls how the SAP learns the IPv6 static host MAC address. Enabling this command indicates that this particular SAP only has one subscriber and only has one MAC address for all hosts. With this parameter enabled, the subscriber's NS and RS source MAC address is used to automatically populate the subscriber MAC address. To allow this auto-populate behavior, the subscriber's NS and RS source IP must be of type link local address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.238 single-sfm-overload

single-sfm-overload

Syntax **single-sfm-overload** [**holdoff-time** *holdoff-time*]
no single-sfm-overload

Context **[Tree]** (config>service>vprn single-sfm-overload)

Full Context configure service vprn single-sfm-overload

Description This command configures OSPF, OSPFv3 and IS-IS to set overload when the router has fewer than the full set of SFMs functioning, which reduces forwarding capacity. Setting overload enables a router to still participate in exchanging routing information, but routes all traffic away from it.

The conditions to set overload are as follows:

- 7950 XRS-20, 7750 SR-12/SR-7, and 7450 ESS-12/ESS-7 platforms: if an SF/CPMs fails, the protocol will set the overload
- 7950-40 XRS and 7750 SR-12e platforms: if two SFMs fail (a connected pair on the XRS-40) the protocol will set the overload

The **no** form of this command configures the router to not set overload if an SFM fails.

Default no single-sfm-overload

Parameters *holdoff-time* — Specifies the delay between detecting SFM failures and setting overload.

Values 1 to 600 seconds

Default 0 seconds

Platforms 7450 ESS, 7750 SR, 7750 SR-14s, 7750 SR-2s, 7750 SR-7s, 7750 SR-a, 7750 SR-e, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

single-sfm-overload

Syntax **single-sfm-overload** [**holdoff-time** *holdoff-time*]
no single-sfm-overload

Context **[Tree]** (config>router single-sfm-overload)

Full Context configure router single-sfm-overload

Description This command configures OSPF, OSPFv3 and IS-IS to set overload when the router has fewer than the full set of SFMs functioning, which reduces forwarding capacity. Setting overload enables a router to still participate in exchanging routing information, but routes all traffic away from it.

The conditions to set overload are as follows:

- 7750 SR-12/SR-7 and 7450 ESS-12/ESS-7 platforms: protocol sets overload if one of the SF/CPMs fails
- 7750 SR-12e and 7950 XRS platforms: protocol sets overload if two SFMs fail (two SFMs belonging to different SFM pairs on the XRS-40)

The **no** form of this command configures the router to not set overload if an SFM fails.

Default no single-sfm-overload

Parameters *holdoff-time* — Specifies the delay between detecting SFM failures and setting overload.

Values 1 to 600 seconds

Default 0 seconds

Platforms 7450 ESS, 7750 SR, 7750 SR-14s, 7750 SR-2s, 7750 SR-7s, 7750 SR-a, 7750 SR-e, 7950 XRS, VSR

23.239 single-sub-parameters

single-sub-parameters

Syntax **single-sub-parameters**

Context **[Tree]** (config>subscr-mgmt>msap-policy>sub-sla-mgmt single-sub-parameters)

Full Context configure subscriber-mgmt msap-policy sub-sla-mgmt single-sub-parameters

Description Commands in this context configure single subscriber MSAP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

single-sub-parameters

Syntax **single-sub-parameters**

Context **[Tree]** (config>service>ies>if>sap>sub-sla-mgmt single-sub-parameters)
[Tree] (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt single-sub-parameters)
[Tree] (config>service>vpls>sap>sub-sla-mgmt single-sub-parameters)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt single-sub-parameters)

Full Context configure service ies interface sap sub-sla-mgmt single-sub-parameters
configure service ies subscriber-interface group-interface sap sub-sla-mgmt single-sub-parameters
configure service vpls sap sub-sla-mgmt single-sub-parameters
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt single-sub-parameters

Description Commands in this context configure single subscriber SAP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.240 sip

sip

Syntax [**no**] **sip**

Context **[Tree]** (config>service>nat>nat-policy>alg sip)
[Tree] (config>service>nat>firewall-policy>alg sip)
[Tree] (config>service>nat>up-nat-policy>alg sip)

Full Context configure service nat firewall-policy alg sip
configure service nat nat-policy alg sip
configure service nat up-nat-policy alg sip

Description This command enables SIP ALG.

The **no** form of the command disables SIP ALG.

Default no sip

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy alg sip
- configure service nat nat-policy alg sip

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service nat firewall-policy alg sip

sip

Syntax **sip** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no sip

Context **[Tree]** (config>service>nat>nat-policy>timeouts sip)
[Tree] (config>service>nat>firewall-policy>timeouts sip)
[Tree] (config>service>nat>up-nat-policy>timeouts sip)

Full Context configure service nat firewall-policy timeouts sip
configure service nat nat-policy timeouts sip
configure service nat up-nat-policy timeouts sip

Description This command configures the SIP inactive media timeout.

Default sip min 2

Parameters *hours* — Specifies the SIP inactive media timeout, in hours.

Values 1 to 2

minutes — Specifies the SIP inactive media timeout, in minutes.

Values 1 to 59

seconds — Specifies the SIP inactive media timeout, in seconds.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy timeouts sip
- configure service nat nat-policy timeouts sip

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts sip

23.241 site

site

Syntax **site** *name* [**create**]
no site *name*

Context **[Tree]** (config>service>vpls site)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls site

Description This command configures a VPLS site.

The no form of this command removes the name from the configuration.

Parameters *name* — Specifies a site name up to 32 characters in length.

create — This keyword is mandatory while creating a VPLS site.

Platforms All

site

Syntax **site** *name* [**create**]
no site name

Context **[Tree]** (config>service>epipe site)

Full Context configure service epipe site

Description This command configures a Epipe site.

The **no** form of this command removes the name from the configuration.

Parameters *name* — Specifies a site name up to 32 characters in length.

create — This keyword is mandatory while creating a Epipe service.

Platforms All

23.242 site-activation-timer

site-activation-timer

Syntax **site-activation-timer** *seconds*
no site-activation-timer

Context **[Tree]** (config>redundancy>bgp-mh site-activation-timer)

Full Context configure redundancy bgp-mh site-activation-timer

Description This command defines the amount of time the service manager will keep the local sites in standby status, waiting for BGP updates from remote PEs before running the DF election algorithm to decide whether the site should be unblocked. The timer is started when one of the following event occurs only if the site is operationally up:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- Manual site activation using “no shutdown” at site-id level or at member object(s) level (for example, SAP(s) or PW(s)
- Site activation after a failure

The **no** form of this command sets the value to 2.

Default no site-activation-timer

Parameters *seconds* — Specifies the timer, in seconds.

Values 1 to 100

site-activation-timer

Syntax **site-activation-timer** *seconds*
no site-activation-timer

Context **[Tree]** (config>service>vpls>site site-activation-timer)

Full Context configure service vpls site site-activation-timer

Description This command configures the time-period the system keeps the local sites in standby status, waiting for BGP updates from remote PEs before running the DF (designated-forwarder) election algorithm to decide whether the site should be unblocked. This timer if terminated if an update is received for which the remote PE has transitioned from DF to non-DF.

The no form of this command removes the value from the configuration.

Default site-activation-timer 2

Parameters *seconds* — Specifies the site activation timer in seconds.

Values 0 to 100

Platforms All

site-activation-timer

Syntax **site-activation-timer** *seconds*
no site-activation-timer

Context **[Tree]** (config>service>epipe>site site-activation-timer)

Full Context configure service epipe site site-activation-timer

Description This command configures the time-period the system keeps the local sites in standby status, waiting for BGP updates from remote PEs before running the DF (designated-forwarder) election algorithm to decide whether the site should be unblocked. This timer is terminated if an update is received for which the remote PE has transitioned from DF to non-DF.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the value from the configuration.

Default site-activation-timer 2

Parameters *seconds* — Specifies the site activation timer in seconds.

Values 0 to 100

Platforms All

site-activation-timer

Syntax **site-activation-timer** *seconds*
no site-activation-timer

Context **[Tree]** (config>redundancy>bgp-multi-homing site-activation-timer)

Full Context configure redundancy bgp-multi-homing site-activation-timer

Description This command defines the amount of time the service manager will keep the local sites in standby status, waiting for BGP updates from remote PEs before running the DF election algorithm to decide whether the site should be unblocked. The timer is started when one of the following events occurs if the site is operationally up:

- Manual site activation using the **no shutdown** command at site-id level or at member object(s) level (SAP(s) or PW(s))
- Site activation after a failure

Default no site-activation-timer

Parameters *seconds* — Specifies the standby status in seconds.

Values 0 to 100

Default 2

Platforms All

23.243 site-id

site-id

Syntax **site-id** *value*
no site-id

Context **[Tree]** (config>service>vpls>site site-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls site site-id

Description This command configures the identifier for the site in this service.

Parameters *value* — Specifies the site identifier.

Values 1 to 65535

Platforms All

site-id

Syntax **site-id** *value*
no site-id

Context **[Tree]** (config>service>epipe>site site-id)

Full Context configure service epipe site site-id

Description This command configures the identifier for the site in this service. It must match between services but it is local to the service.

Parameters *value* — Specifies the site identifier.

Values 1 to 65535

Platforms All

23.244 site-min-down-timer

site-min-down-timer

Syntax **site-min-down-timer** *seconds*
no site-min-down-timer

Context **[Tree]** (config>redundancy>bgp-multi-homing site-min-down-timer)

Full Context configure redundancy bgp-multi-homing site-min-down-timer

Description This command configures the BGP multi-homing site minimum down time. When this value is set and the site goes operationally down, it remains operationally down for at least the length of time configured by this timer, regardless of whether other state changes might cause the site to go operationally up. This timer is restarted every time the site transitions from operationally up to down.

This timer is optimized in the following circumstances:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- If the site goes down on the DF but there are no BGP multi-homing peers with the same site in an up state, this timer is not used.
- If the site goes down on the DF but there are no active BGP multi-homing peers, this timer is not used.
- If this timer is active and a BGP multihoming update is received from the DF indicating its site is down, this timer is immediately terminated and the BGP multihoming algorithm is triggered to determine whether this PE should become the DF.

The **no** form of this command removes the value from the configuration.

Default no site-min-down-timer

Parameters *seconds* — Specifies the time, in seconds, that a BGP multi-homing site remains operationally down after a transition from up to down.

Values 1 to 100

Platforms All

site-min-down-timer

Syntax **site-min-down-timer** *min-down-time*
no site-min-down-timer

Context **[Tree]** (config>service>vpls>site site-min-down-timer)

Full Context configure service vpls site site-min-down-timer

Description This command configures the BGP multi-homing site minimum down time. When set to a non-zero value, if the site goes operationally down it will remain operationally down for at least the length of time configured for the **site-min-down-timer**, regardless of whether other state changes would have caused it to go operationally up. This timer is restarted every time that the site transitions from up to down. Setting this parameter to zero allows the minimum down timer to be disabled for this service.

The above operation is optimized in the following circumstances:

- If the site goes down on the designated forwarder but there are no BGP multi-homing peers with the same site in an operationally up state, then the **site-min-down-timer** is not started and is not used.
- If the site goes down on the designated forwarder but there are no active BGP multi-homing peers, then the **site-min-down-timer** is not started and is not used.
- If the s**ite-min-down-timer** is active and a BGP multi-homing update is received from the designated forwarder indicating its site has gone down, the **site-min-down-timer** is immediately terminated and this PE becomes the designated forwarder if the BGP multi-homing algorithm determines it should be the designated forwarder.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default Taken from the value of **site-min-down-timer** configured for Multi-Chassis BGP multi-homing under the **config>redundancy>bgp-multi-homing** context.

Parameters *min-down-time* — Specifies the time, in seconds, that a BGP multi-homing site remains operationally down after a transition from up to down.

Values 0 to 100 seconds

Platforms All

site-min-down-timer

Syntax **site-min-down-timer** *min-down-time*
no site-min-down-timer

Context **[Tree]** (config>service>epipe>site site-min-down-timer)

Full Context configure service epipe site site-min-down-timer

Description This command configures the BGP multi-homing site minimum down time. When set to a non-zero value, if the site goes operationally down it will remain operationally down for at least the length of time configured for the **site-min-down-timer**, regardless of whether other state changes would have caused it to go operationally up. This timer is restarted every time that the site transitions from up to down. Setting this parameter to zero allows the minimum down timer to be disabled for this service.

The preceding operation is optimized in the following circumstances:

- If the site goes down on the designated forwarder but there are no BGP multi-homing peers with the same site in an operationally up state, then the **site-min-down-timer** is not started and is not used.
- If the site goes down on the designated forwarder but there are no active BGP multi-homing peers, then the s**ite-min-down-timer** is not started and is not used.
- If the **site-min-down-timer** is active and a BGP multi-homing update is received from the designated forwarder indicating its site has gone down, the **site-min-down-timer** is immediately terminated and this PE becomes the designated forwarder if the BGP multi-homing algorithm determines it should be the designated forwarder.

The **no** form of this command reverts to default value.

Default Taken from the value of **site-min-down-timer** configured for Multi-Chassis BGP multi-homing under the **config>redundancy>bgp-multi-homing** context.

Parameters *min-down-time* — Specifies the time, in seconds, that a BGP multi-homing site remains operationally down after a transition from up to down.

Values 0 to 100

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.245 site-preference

site-preference

Syntax **site-preference** *preference-value*
no site-preference

Context **[Tree]** (config>service>epipe>site site-preference)

Full Context configure service epipe site site-preference

Description This command defines the value to advertise in the VPLS preference field of the BGP VPWS and BGP Multi-homing NLRI extended community. This value can be changed without having to shutdown the site itself. The site-preference is only applicable to VPWS services.

When not configured, the default is zero, indicating that the VPLS preference is not in use.

Default no site-preference, value=0

Parameters *preference-value* — Specifies the preference value to advertise in the NLRI L2 extended community for this site.

Values 1 to 65535

primary — Sets the site-preference to 65535.

backup — Sets the site-preference to 1.

Platforms All

23.246 size

size

Syntax **size** *cache-size*

Context **[Tree]** (config>app-assure>group>dns-ip-cache>ip-cache size)

Full Context configure application-assurance group dns-ip-cache ip-cache size

Description This command configures the maximum number of entries in the cache.

Default size 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *cache-size* — Specifies the maximum number of IP addresses that can be stored in the cache.

Values 10 to 32000

Default 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

size

Syntax **size** *url-list-size*

Context **[Tree]** (config>app-assure>group>url-list size)

Full Context configure application-assurance group url-list size

Description This command specifies the size of the URL list that can be filtered. The size can be set to either standard or extended. Configuring the specified url-list as extended provides support for filtering on a larger number of URLs.

Default size standard

Parameters *url-list-size* — Specifies the size of the AA url-list for URL filtering.

Values standard, extended

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

size

Syntax **size** *octets*
no size

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy size)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy size)

Full Context configure saa test type-multi-line lsp-ping sr-policy size
configure saa test type-multi-line lsp-trace sr-policy size

Description This command configures the MPLS echo request packet size.

The **no** form of this command reverts to the default value.

Default size 1

Parameters *octets* — Specifies the size in octets. The request payload is padded with zeros to the specified size.

Values 1 to 9786

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

size

Syntax **size** *octets*
no size

Context **[Tree]** (config>test-oam>icmp>ping-template size)

Full Context configure test-oam icmp ping-template size

Description This command configures the size of the Data field (in other words, padding) of the outgoing ICMP echo packet. Minimum packet sizes should be used to test connectivity. Larger packet size should only be used if there is a requirement to spot-check large packet size issues on a very limited number of tests and should not be used for normal connectivity testing. Packet sizes should never be configured to require fragmentation anywhere along the path. Exceeding these recommendations will negatively affect the scale and performance of icmp ping check testing.

The **no** form of this command reverts to the default value.

Default size 56

Parameters *octets* — Specifies the size of the ICMP echo ping padding field, in octets.

Values 12 to 9786

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.247 size-limit

size-limit

Syntax **size-limit** *limit-value*
no size-limit

Context **[Tree]** (config>call-trace>location size-limit)

Full Context configure call-trace location size-limit

Description This command limits the total size of call-trace files on the specified compact flash card.

The **no** form of this command removes the size restriction.

Default size-limit 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *limit-value* — Specifies the total size of call-trace files on the specified compact flash card, in Mbytes.

Values 1 to 65536

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

size-limit

Syntax **size-limit** *limit-value*

Context **[Tree]** (config>call-trace>trace-profile size-limit)

Full Context configure call-trace trace-profile size-limit

Description This command specifies a maximum of how big a trace may grow before it is stopped.

Default size-limit 10

Parameters *limit-value* — Specifies the maximum data volume generated by a single call trace job to the output in megabytes. After reaching the limit the call trace job for a given host is automatically terminated.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.248 skip-gtp-ipv4-alloc

skip-gtp-ipv4-alloc

Syntax [**no**] **skip-gtp-ipv4-alloc**

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn skip-gtp-ipv4-alloc)

Full Context configure subscriber-mgmt gtp apn-policy apn skip-gtp-ipv4-alloc

Description This command enables the ability to skip IPv4 address assignment using a GTP session setup response when PCO "allocation via NAS" is not present in a GTP session creation request. Without this configuration, IPv4 address allocation is done using GTP session setup response, even in absence of the PCO "allocation via NAS" in a GTP session setup request.

The **no** form of this command reverts to IPv4 address allocation using GTP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.249 skip-ttl-decrement

skip-ttl-decrement

Syntax [**no**] **skip-ttl-decrement**

Context **[Tree]** (config>filter>gre-tun-tmp>ipv4 skip-ttl-decrement)

Full Context configure filter gre-tunnel-template ipv4 skip-ttl-decrement

Description This command enables an option to not decrement the TTL of the IP packet matching the IPv4/IPv6 filter, when it is encapsulated into the GRE tunnel header.

The **no** form of this command disables this option (default). This results in the matching of IP packet's TTL field to be decremented before it is encapsulated in the GRE tunnel header.

Platforms All

23.250 sla-profile

sla-profile

Syntax [**no**] **sla-profile**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute sla-profile)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute sla-profile

Description This command specifies that SLA profile attributes should be included into RADIUS accounting messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sla-profile

Syntax **sla-profile** *sla-profile-name*
no sla-profile

Context **[Tree]** (config>service>ies>if>sap>static-host sla-profile)
[Tree] (config>service>vpls>sap>static-host sla-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host sla-profile)
[Tree] (config>service>vprn>if>sap>static-host sla-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host sla-profile)

Full Context configure service ies interface sap static-host sla-profile
configure service ies subscriber-interface group-interface sap static-host sla-profile
configure service vpls sap static-host sla-profile
configure service vprn interface sap static-host sla-profile
configure service vprn subscriber-interface group-interface sap static-host sla-profile

Description This command specifies an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

The **no** form of this command reverts to the default.

Parameters *sla-profile-name* — Specifies the SLA profile name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sla-profile

Syntax **sla-profile** *sla-profile-name* [**create**]
no sla-profile *sla-profile-name*

Context **[Tree]** (config>subscr-mgmt sla-profile)

Full Context configure subscriber-mgmt sla-profile

Description This command configures an SLA profile mapping. Hosts associated with a subscriber are subdivided into Service Level Agreement (SLA) profiles. For each subscriber host an SLA profile can be specified. For a subscriber host, the SLA profile determines:

- The QoS-policies to use
  - The classification
  - The queues
  - The queue mapping
- The IP filters to use

The SLA profile also has the attribute host-limits which limits the total number of hosts (belonging to the same subscriber) on a certain SAP that can be using this SLA profile.

The **no** form of this command reverts to the default.

Parameters *sla-profile-name* — Specifies the name of the SLA profile.

create — Keyword used to create the SLA profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.251 sla-profile-map

sla-profile-map

Syntax **sla-profile-map**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol sla-profile-map)

Full Context configure subscriber-mgmt sub-ident-policy sla-profile-map

Description Commands in this context configure SLA profile mapping parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sla-profile-map

Syntax **sla-profile-map**

Context **[Tree]** (config>subscr-mgmt>sub-prof sla-profile-map)

Full Context configure subscriber-mgmt sub-profile sla-profile-map

Description Commands in this context configure SLA profile mapping.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.252 sla-profile-string

sla-profile-string

Syntax **sla-profile-string** *sla-profile-string*
no sla-profile-string

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings sla-profile-string)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings sla-profile-string)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings sla-profile-string
configure subscriber-mgmt local-user-db ppp host identification-strings sla-profile-string

Description This command specifies the SLA profile string which is encoded in the identification strings.

The **no** form of this command returns to the default.

Parameters *sla-profile-string* — Specifies the SLA profile string, up to 16 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sla-profile-string

Syntax **sla-profile-string** *string*
no sla-profile-string

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile sla-profile-string)

Full Context configure subscriber-mgmt vrgw brg brg-profile sla-profile-string

Description This command configures the SLA profile string which will be used as a default for SLA-profile lookup. This string can be overridden during BRG or host authentication.

The **no** form of the command removes the string from the configuration.

Default no sla-profile-string

Parameters *string* — Specifies the string to use to look up the subscriber profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.253 slaac

slaac

Syntax **slaac**

Context **[Tree]** (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client slaac)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client slaac)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client slaac
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client slaac

Description This command configures SLAAC for the DHCPv6 client.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.254 slaac-prefix

slaac-prefix

Syntax **slaac-prefix** *ipv6-address*
no slaac-prefix

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query slaac-prefix)

Full Context configure subscriber-mgmt wlan-gw ue-query slaac-prefix

Description This command enables matching on UEs with the specified SLAAC prefix.

The **no** form of this command disables matching on the SLAAC prefix.

Default no slaac-prefix

Parameters *ipv6-address* — Specifies the SLAAC prefix.

Values	
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.255 sleep

sleep

Syntax **sleep** [*seconds*]

Context **[Tree]** (global sleep)

Full Context global sleep

Description This command causes the console session to pause operation (sleep) for 1 second (default) or for the specified number of seconds.

Default sleep 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the number of seconds for the console session to sleep, expressed as a decimal integer.

Values 1 to 100

Default 1

23.256 slice-size

slice-size

Syntax **slice-size** *slice-size*
no slice-size

Context **[Tree]** (config>mirror>mirror-dest slice-size)

Full Context configure mirror mirror-dest slice-size

Description This command enables mirrored frame truncation and specifies the maximum size, in bytes, of a mirrored frame that can be transmitted to the mirror destination.

This command enables mirroring larger frames than the destination packet decode equipment can handle. It also allows conservation of mirroring resources by limiting the size of the packet stream through the router and the core network.

When defined, the mirror **slice-size** creates a threshold that truncates a mirrored frame to a specific size. For example, if the value of 256 bytes is defined, a frame larger than 256 bytes will only have the first 256 bytes transmitted to the mirror destination. The original frame is not affected by the truncation. The mirrored frame size may increase if encapsulation information is added during transmission through the network core or out the mirror destination SAP to the packet/protocol decode equipment.

The actual capability of the router to transmit a sliced or non-sliced frame is also dictated by the mirror destination SDP **path-mtu** or the mirror destination SAP physical MTU. Packets that require a larger MTU than the mirroring destination supports are discarded if the defined **slice-size** does not truncate the packet to an acceptable size.

Notes:

- When configuring IP mirroring, packet slice is rejected as an incorrect option as it will cause IP packets to be rejected by the next hop with an IP header verification error.
- Slice-size is not supported by CEM encap-types or IP-mirroring.

The **no** form of this command disables mirrored packet truncation.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *slice-size* — Specifies the number of bytes to which mirrored frames are truncated, expressed as a decimal integer.

Values 128 to 9216

Platforms All

23.257 slm

slm

Syntax **slm** [**test-id** *test-id*] [**create**]
no slm

Context **[Tree]** (config>oam-pm>session>ethernet slm)

Full Context configure oam-pm session ethernet slm

Description This command defines the test ID to be assigned to the synthetic loss test and creates the container to allow the individual test parameters to be configured.

The **no** form of this command removes the SLM test function from the PM Session.

Parameters *test-id* — Specifies the value to be placed in the 4-byte test ID field of an ETH-SLM PDU.

Values 0 to 2147483647

create — Creates the test.

Platforms All

slm

Syntax **slm**

Context **[Tree]** (config>eth-cfm slm)

Full Context configure eth-cfm slm

Description This is the container that provides the global configuration parameters for ITU-T Synthetic Loss Measurement (ETH-SL).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.258 slope-policy

slope-policy

Syntax **slope-policy** *name*
no slope-policy

Context **[Tree]** (config>port>access>egress>channel>pool slope-policy)
[Tree] (config>port>access>egress>pool slope-policy)
[Tree] (config>port>access>ingress>pool slope-policy)
[Tree] (config>port>network>egress>pool slope-policy)

Full Context configure port access egress channel pool slope-policy
configure port access egress pool slope-policy
configure port access ingress pool slope-policy
configure port network egress pool slope-policy

Description This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The policy is defined in the **config>qos>slope-policy** context.

Default slope-policy default

Parameters *name* — Specifies the policy name, a string up to 32 characters.

Platforms All

slope-policy

Syntax **slope-policy** *slope-policy-name*
no slope-policy

Context **[Tree]** (config>card>fp>egress>wred-queue-control slope-policy)

Full Context configure card fp egress wred-queue-control slope-policy

Description This command configures WRED slopes within the WRED mega-pool. The WRED slopes in the WRED mega-pool are used when WRED queues are requesting buffers from the mega-pool while they are over their CBS threshold. Once over the CBS threshold, the WRED queue stops receiving buffers from the CBS reserve in the mega-pool and starts competing for buffers in the shared portion of the mega-pool. If the packet resulting in the buffer request is inplus-profile, the packet will be associated with the highplus-slope. In-profile packets are associated with the high slope. Out-of-profile packets are associated with the low slope. Exceed-profile packets are associated with the exceed slope. While the queue is within its CBS threshold, the slopes are ignored.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Within the defined slope-policy, each slope is enabled or disabled (no shutdown or shutdown) and each slope's geometry is defined as percentages of shared portion depth. If a slope is shutdown, the related traffic uses the minimum of the queue MBS and egress WRED megapool size as a drop tail.

The slope-policy also defines the time average factor (TAF) value that is used to determine how the pool's weighted average depth is calculated. The higher the factor, the slower the average depth tracks the actual pool depth.

The **no** form of this command reverts to the default slope policy to the WRED mega-pool.

Default slope-policy default

Parameters *slope-policy-name* — Specifies which slope policy the system should apply to the WRED mega-pool. When slope-policy is not executed, the WRED mega-pool will use the default slope policy. The defined slope policy must already exist or the command will fail. 32 characters maximum.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

slope-policy

Syntax **slope-policy** *name*
no slope-policy

Context **[Tree]** (config>card>fp>ingress>network>pool slope-policy)

Full Context configure card fp ingress network pool slope-policy

Description This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The policy is defined in the **config>qos>slope-policy** context.

Default slope-policy default

Parameters *name* — Specifies the policy name, a string up to 32 characters.

Platforms All

slope-policy

Syntax **slope-policy** *slope-policy-name*
no slope-policy

Context **[Tree]** (config>isa>aa-grp>qos>egress>from-subscriber>pool slope-policy)
[Tree] (config>isa>aa-grp>qos>egress>to-subscriber>pool slope-policy)

Full Context configure isa application-assurance-group qos egress from-subscriber pool slope-policy
configure isa application-assurance-group qos egress to-subscriber pool slope-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The slope policy is defined in the **config**>**qos**>**slope-policy** context.

Parameters *slope-policy-name* — Specifies the name of the slope policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

slope-policy

Syntax **slope-policy** *policy-name*
no slope-policy

Context **[Tree]** (config>qos>hs-pool-policy>mid-tier>mid-pool slope-policy)
[Tree] (config>qos>hs-pool-policy>root-tier>root-pool slope-policy)

Full Context configure qos hs-pool-policy mid-tier mid-pool slope-policy
configure qos hs-pool-policy root-tier root-pool slope-policy

Description This command specifies the slope policy to be used to define the high, low, and exceed slopes within the pool. The slope (high, low, or exceed) used on the egress queue for the packet that generated the buffer request is also used in the mid-pool from the applied slope policy. The pool's current allocation amount is applied to the appropriate slope to derive the buffer rejection probability. The probability value is compared to a randomly-generated number. If the probability decision generates a rejection decision or the buffer pool has no remaining free buffers, the buffer request fails and the arriving packet is discarded. Otherwise, a buffer is allocated as long as the port-class and root-tier buffer pools also honor the buffer request.

The **no** form of the command restores the default slope policy to the associated pool.

Default slope-policy _tmnx_hs_default

Parameters *policy-name* — Specifies the slope policy associated with this pool, up to 32 characters.

Platforms 7750 SR-7/12/12e

slope-policy

Syntax **slope-policy** *policy-name*
no slope-policy

Context **[Tree]** (config>qos>hs-port-pool-policy>alt-port-class-pools>class-pool slope-policy)
[Tree] (config>qos>hs-port-pool-policy>std-port-class-pools>class-pool slope-policy)

Full Context configure qos hs-port-pool-policy alt-port-class-pools class-pool slope-policy
configure qos hs-port-pool-policy std-port-class-pools class-pool slope-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the slope policy that is used to define the high, low, and exceed slopes within the port-class pool. The slope used on the egress queue for the packet that generated the buffer request is also used in the class-pool. The pool's current allocation amount is applied to the appropriate slope to derive the buffer rejection probability. The probability value is compared to a randomly generated number. If the probability decision generates a rejection or the buffer pool has no remaining free buffers, the buffer request fails and the arriving packet is discarded. Otherwise, a buffer is allocated as long as the mid-tier and root-tier buffer pools also honor the buffer request.

The **no** form of the command restores the default slope policy to the associated class-pool.

Default slope-policy _tmnx_hs_default

Parameters *policy-name* — Specifies the policy name, up to 32 characters. This parameter is required when executing the **slope-policy** command and must refer to an existing slope policy within the system. If a slope policy with the specified name does not exist, the **slope-policy** command fails without modifying the slope behavior on the pool. A non-existent slope-policy error is generated. After a slope policy is associated with any HSQ queue or buffer pool, the policy cannot be deleted.

Platforms 7750 SR-7/12/12e

slope-policy

Syntax **slope-policy** *name* [**create**]
no slope-policy *name*

Context **[Tree]** (config>qos slope-policy)

Full Context configure qos slope-policy

Description Commands in this context configure a QoS slope policy.

Default slope-policy "default"

Parameters *name* — The name of the slope policy.

Values Valid names consist of any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Platforms All

slope-policy

Syntax **slope-policy** *src-name dst-name* [**overwrite**]

Context **[Tree]** (config>qos>copy slope-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos copy slope-policy

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

The **copy** command is a configuration-level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.

Parameters **slope-policy** — Indicates that the source policy ID and the destination policy ID are slope policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination policy will be overwritten with the contents of the source policy. If **overwrite** is not specified, an error will occur if the destination policy ID exists.

```
ALA-7>config>qos# copy slope-policy default sp1
MINOR: CLI Destination "sp1" exists - use {overwrite}.
ALA-7>config>qos#overwrite
```

Platforms All

23.259 slow-psc-timer

slow-psc-timer

Syntax **slow-psc-timer** *interval*
no slow-psc-timer

Context **[Tree]** (config>router>mpls>mpls-tp>protection-template slow-psc-timer)

Full Context configure router mpls mpls-tp protection-template slow-psc-timer

Description This command configures the slow timer value to be used for protection switching coordination (PSC) packets for MPLS-TP linear protection (RFC 6378).

Default slow-psc-timer 5

Parameters *interval* — Specifies the slow timer interval in seconds.

Values 5 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.260 slow-queue-threshold

slow-queue-threshold

Syntax **slow-queue-threshold** *kilobits-per-second*
no slow-queue-threshold

Context **[Tree]** (config>card>virt-sched-adj slow-queue-threshold)

Full Context configure card virtual-scheduler-adjustment slow-queue-threshold

Description This command overrides the system default rate threshold where policers and queues are placed in the “slow” queue category. Slow rate policers and queues use a different minimum rate calculation interval time than fast rate queues. The rate is determined based on the previous calculated offered rate for the policer or queue.

The default slow policer or queue rate is 1 Mb/s. The fast rate is derived by multiplying the slow rate by a factor of 1.5 resulting in a default fast rate of 1.5 Mb/s. The slow-queue-threshold command uses a “Kilobit-Per-Second” value to modify the default slow queue rate threshold and indirectly changes the fast queue rate threshold.

The **no** form of this command restores the default slow queue and fast rate thresholds.

Default no slow-queue-threshold

Parameters *kilobits-per-second* — Specifies that the kilobit-per-second parameter is required and is used to modify the default slow rate threshold. Defining a value of 0 forces all policers and queues to be treated as fast rate. Defining a value of 1000 (1 Mb/s) returns the threshold to the default value and is equivalent to executing **no slow-queue-threshold**.

The fast rate threshold is derived by multiplying the new slow rate threshold by a factor of 1.5.

Values 0 to 1000000 kb/s

Default 1000 kb/s

Platforms All

23.261 sm-tti

sm-tti

Syntax **sm-tti**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>otu sm-tti)

Full Context configure port otu sm-tti

Description Commands in this context configure section monitoring trail trace identifier parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.262 snap-oui

snap-oui

Syntax **snap-oui** {**zero** | **non-zero**}
no snap-oui

Context [Tree] (config>qos>sap-ingress>mac-criteria>entry>match snap-oui)

Full Context configure qos sap-ingress mac-criteria entry match snap-oui

Description Configures an IEEE 802.3 LLC SNAP Ethernet frame OUI zero or non-zero value to be used as a service ingress QoS policy match criterion.

The **no** form of this command removes the criterion from the match criteria.

Default no snap-oui

Parameters **zero** — Specifies to match packets with the 3-byte OUI field in the SNAP-ID set to zero.

non-zero — Specifies to match packets with the 3-byte OUI field in the SNAP-ID not set to zero.

Platforms All

snap-oui

Syntax **snap-oui** {**zero** | **non-zero**}
no snap-oui

Context [Tree] (config>filter>mac-filter>entry>match snap-oui)

Full Context configure filter mac-filter entry match snap-oui

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame OUI zero or non-zero value to be used as a MAC filter match criterion.

The **no** form of the command removes the criterion from the match criteria.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no snap-oui

Parameters **zero** — Specifies to match packets with the three-byte OUI field in the SNAP-ID set to zero.

non-zero — Specifies to match packets with the three-byte OUI field in the SNAP-ID not set to zero.

Platforms All

snap-oui

Syntax **snap-oui** {**zero** | **non-zero**}
no snap-oui

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match snap-oui)

Full Context configure system security management-access-filter mac-filter entry match snap-oui

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame OUI zero or non-zero value to be used as a MAC filter match criterion.

The **no** form of this command removes the criterion from the match criteria.

Default no snap-oui

Parameters **zero** — Specifies to match packets with the three-byte OUI field in the SNAP-ID set to zero.

non-zero — Specifies to match packets with the three-byte OUI field in the SNAP-ID not set to zero.

Platforms All

23.263 snap-pid

snap-pid

Syntax **snap-pid** *snap-pid*
no snap-pid

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match snap-pid)

Full Context configure qos sap-ingress mac-criteria entry match snap-pid

Description Configures an IEEE 802.3 LLC SNAP Ethernet frame PID value to be used as a service ingress QoS policy match criterion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This is a 2-byte protocol id that is part of the IEEE 802.3 LLC SNAP Ethernet Frame that follows the 3-byte OUI field.

The snap-pid field, etype field, ssap, and dsap fields are mutually exclusive and cannot be part of the same match criteria.

The **snap-pid** match criteria is independent of the OUI field within the SNAP header. Two packets with different 3-byte OUI fields, but the same PID field, will both match the same policy entry based on a snap-pid match criteria.

The **no** form of this command removes the snap-pid value as the match criteria.

Default no snap-pid

Parameters *snap-pid* — The 2-byte snap-pid value to be used as a match criterion in hexadecimal.

Values 0x0000 to 0xFFFF

Platforms All

snap-pid

Syntax **snap-pid** *snap-pid*
no snap-pid

Context **[Tree]** (config>filter>mac-filter>entry>match snap-pid)

Full Context configure filter mac-filter entry match snap-pid

Description Configures an IEEE 802.3 LLC SNAP Ethernet Frame PID value to be used as a MAC filter match criterion.

This is a two-byte protocol id that is part of the IEEE 802.3 LLC SNAP Ethernet Frame that follows the three-byte OUI field.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria.

The snap-pid match criterion is independent of the OUI field within the SNAP header. Two packets with different three-byte OUI fields but the same PID field will both match the same filter entry based on a snap-pid match criteria.

The **no** form of the command removes the snap-pid value as the match criteria.

Default no snap-pid

Parameters *snap-pid* — Specifies the two-byte snap-pid value to be used as a match criterion. The value can be expressed in decimal integer or hexadecimal format.

Values 0 to 65535 or 0x0000 to 0xFFFF

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

snap-pid

Syntax **snap-pid** *snap-pid*
no snap-pid

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match snap-pid)

Full Context configure system security management-access-filter mac-filter entry match snap-pid

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame PID value to be used as a MAC filter match criterion.

This is a two-byte protocol id that is part of the IEEE 802.3 LLC SNAP Ethernet Frame that follows the three-byte OUI field.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide* for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

Note: The snap-pid match criterion is independent of the OUI field within the SNAP header. Two packets with different three-byte OUI fields but the same PID field will both match the same filter entry based on a snap-pid match criteria.

The **no** form of this command removes the snap-pid value as the match criteria.

Default no snap-pid

Parameters *pid-value* — Specifies the two-byte snap-pid value to be used as a match criterion in hexadecimal.

Values 0x0000 to 0xFFFF

Platforms All

23.264 snmp

snmp

Syntax **snmp**

Context **[Tree]** (config>service>vprn snmp)

Full Context configure service vprn snmp

Description Commands in this context configure SNMP parameters for this VPRN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

snmp

Syntax **snmp**

Context **[Tree]** (config>system>security>user snmp)

Full Context configure system security user snmp

Description This command creates the context to configure SNMP group membership for a specific user and defines encryption and authentication parameters.

All SNMPv3 users must be configured with the commands available in this CLI node.

The OS always uses the configured SNMPv3 user name as the security user name.

Platforms All

snmp

Syntax **snmp**

Context **[Tree]** (config>system snmp)
[Tree] (config>system>security snmp)

Full Context configure system security snmp
configure system snmp

Description This command creates the context to configure SNMPv1, SNMPv2, and SNMPv3 parameters**.**

Platforms All

23.265 snmp-trap-group

snmp-trap-group

Syntax **snmp-trap-group** *log-id* | *log-name* [**name** *log-name*]
no snmp-trap-group *log-id* | *log-name*

Context **[Tree]** (config>service>vprn>log snmp-trap-group)

Full Context configure service vprn log snmp-trap-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a specific *log-id*.

A group specifies the types of SNMP traps and specifies the log ID that will receive the group of SNMP traps. The user must configure a trap group before SNMP traps can be sent.

To suppress the generation of all alarms and traps, see the **event-control** command. To suppress alarms and traps that are sent to this log-id, see the **filter** command. After alarms and traps are generated, they can be directed to one or more SNMP trap groups. Log events that can be forwarded as SNMP traps are always defined on the main event source.

The **no** form of this command deletes the SNMP trap group.

Default There are no default SNMP trap groups.

Parameters *log-id* | *log-name* — Specifies the log ID or name (up to 32 characters).

Values *log-id*: 1 to 100

name *log-name* — Specifies an optional log name of a log configured in the **log-id** context, up to 32 characters, that can be used to refer to the log after it is created. Alarms and traps cannot be sent to the trap receivers until a valid *log-id* exists.

Platforms All

snmp-trap-group

Syntax **snmp-trap-group** *log-id* | *log-name* [**name** *log-name*]
no snmp-trap-group *log-id* | *log-name*

Context **[Tree]** (config>log snmp-trap-group)

Full Context configure log snmp-trap-group

Description This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a specified *log-id*.

A group specifies the types of SNMP traps and the log ID which that will receive the SNMP trap group. The user must configure a trap to send SNMP traps.

To suppress the generation of all alarms and traps, see the **event-control** command. To suppress alarms and traps that are sent to this log ID, see the filter command. When alarms and traps are generated, they can be directed to one or more SNMP trap groups. Log events that can be forwarded as SNMP traps are always defined at the main event source.

The **no** form of this command deletes the SNMP trap group.

Parameters *log-id* | *log-name* — Specifies the log ID or log name (up to 32 characters).

Values *log-id*: 1 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name *log-name* — Specifies an optional log name of a log configured in the **log-id** context, up to 32 characters, that can be used to refer to the log after it is created. Alarms and traps cannot be sent to the trap receivers until a valid *log-id* exists.

Platforms All

23.266 snoop

snoop

Syntax [**no**] **snoop**

Context **[Tree]** (config>service>vpls>sap>dhcp snoop)
[Tree] (config>service>vpls>spoke-sdp>dhcp snoop)
[Tree] (config>service>vpls>mesh-sdp>dhcp snoop)
[Tree] (config>service>vprn>if>dhcp>option snoop)
[Tree] (config>service>vprn>nw-if>dhcp snoop)

Full Context configure service vpls mesh-sdp dhcp snoop
configure service vpls sap dhcp snoop
configure service vpls spoke-sdp dhcp snoop
configure service vprn interface dhcp option snoop
configure service vprn nw-if dhcp snoop

Description This command enables snooping of DHCP or DHCP6 messages on the SAP or SDP. Enabling DHCP or DHCP6 snooping on interfaces (SAPs and SDP bindings) is required where DHCP or DHCP6 messages important to lease state table population are received, or where Option 82 information is to be inserted. This includes interfaces that are in the path to receive messages from either DHCP or DHCP6 servers or from subscribers.

The **no** form of this command disables DHCP or DHCP6 snooping on the specified SAP or SDP binding.

Default no snoop

Platforms All

23.267 snooping

snooping

Syntax [**no**] **snooping**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 snooping)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 snooping)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 snooping
configure service vprn subscriber-interface group-interface ipv6 dhcp6 snooping

Description This command enables the group-interface to snoop DHCPv6 relay messages exchange between the subscriber host and the DHCPv6 server. A successful DHCPv6 address assignment triggers ESM DHCPv6 host creation and a release of the lease triggers host deletion. This feature is for ESMv6 applications where a Layer 3 aggregation network is upstream from the BNG.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.268 sntp

sntp

Syntax [**no**] **sntp**

Context [Tree] (config>system>time sntp)

Full Context configure system time sntp

Description This command creates the context to edit the Simple Network Time Protocol (SNTP).

SNTP can be configured in either broadcast or unicast client mode. SNTP is a compact, client-only version of the NTP. SNTP can only receive the time from SNTP/NTP servers. It cannot be used to provide time services to other systems.

The system clock is automatically adjusted at system initialization time or when the protocol first starts up.

When the time differential between the SNTP/NTP server and the system is more than 2.5 seconds, the time on the system is gradually adjusted.

SNTP is created in an administratively enabled state (**no shutdown**).

The **no** form of the command removes the SNTP instance and configuration. SNTP does not need to be administratively disabled when removing the SNTP instance and configuration.

Default sntp

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.269 socket

socket

Syntax **socket** [**neighbor** *ip-address* | **group** *name*]
no socket

Context **[Tree]** (debug>router>bgp socket)

Full Context debug router bgp socket

Description This command logs all TCP socket events to the debug log.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

23.270 soft-preemption

soft-preemption

Syntax [**no**] **soft-preemption**

Context **[Tree]** (config>router>mpls>lsp soft-preemption)
[Tree] (config>router>mpls>lsp-template soft-preemption)

Full Context configure router mpls lsp soft-preemption
configure router mpls lsp-template soft-preemption

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables soft preemption for LSPs of type **p2mp-lsp** and LSP templates of type **p2mp**. The soft preemption bit is set to 1 if the following conditions are met; otherwise, the bit is set to 0.

- soft preemption is enabled, and
- the P2MP LSP is adaptive, has non-zero bandwidth, and is computed using the local CSPF method

The **no** form of the command disables soft preemption on the P2MP LSP and P2MP LSP template.

Note: Soft preemption is always enabled for P2P LSPs and P2P LSP templates and cannot be disabled.

Default no soft-preemption

Platforms All

23.271 soft-quota-exhausted

soft-quota-exhausted

Syntax [**no**] **soft-quota-exhausted**

Context **[Tree]** (config>aaa>isa-radius-policy>acct-update-triggers soft-quota-exhausted)
[Tree] (config>subscr-mgmt>wlan-gw>ue-query soft-quota-exhausted)

Full Context configure aaa isa-radius-policy acct-update-triggers soft-quota-exhausted
configure subscriber-mgmt wlan-gw ue-query soft-quota-exhausted

Description This command sends an interim update message when a soft volume quota is reached.

Default soft-quota-exhausted

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.272 soft-quota-exhausted-filter

soft-quota-exhausted-filter

Syntax **soft-quota-exhausted-filter** *dsm-ip-filter-name*
no soft-quota-exhausted-filter

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm soft-quota-exhausted-filter)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm soft-quota-exhausted-filter)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt soft-quota-exhausted-filter
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt soft-quota-exhausted-filter

Description This command applies a filter when a soft volume quota is reached. The filter replaces the currently applied filter (which can be preconfigured using the **vlan-range ip-filter** command or be set using RADIUS authentication/ CoA message) for the UE upon quota exhaustion. If the quota is extended using a RADIUS CoA message, the filter is automatically reverted. Configuration changes apply only to new DSM UEs and not to existing UEs.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.273 software-repository

software-repository

Syntax **software-repository** *repository-name*
no software-repository

Context **[Tree]** (config>system>satellite>eth-sat software-repository)
[Tree] (config>system>satellite>tdm-sat software-repository)

Full Context configure system satellite eth-sat software-repository
configure system satellite tdm-sat software-repository

Description This command binds the specified software repository to the associated satellite. The software repository is used to locate and serve the correct software image to the satellite at boot time.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured software repository is only used when the satellite boots. Changing the software repository for an active satellite does not have an effect until the next time a satellite boots.

A satellite cannot be booted if there is no software repository defined for it.

The **no** form of the command removes the software repository.

Default no software-repository

Parameters *repository-name* — Specifies a string, up to 32 characters, that uniquely identifies the software repository.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure system satellite eth-sat software-repository

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure system satellite tdm-sat software-repository

software-repository

Syntax **software-repository** *repository-name* [**create**]
no software-repository *repository-name*

Context **[Tree]** (config>system software-repository)

Full Context configure system software-repository

Description This command creates or deletes an instance of a software repository. The instance is identified by a repository name.

A software repository is used to obtain files to upgrade software on certain subsystems of the router (for example, Ethernet satellites).

Up to three locations can be specified within a software repository for the router to access files in the repository. The router will first attempt to access the file at the primary location. If the primary location is not configured or the files are not found at the primary location, then the router will attempt to access the files at the secondary location. If the secondary location is not configured or the files are not found at the secondary location, then the router will attempt to access the files at the tertiary location. If the tertiary location is not configured or the files are not found at the tertiary location, then the software repository access will fail.

The **no** form of the command removes the software repository.

Parameters *repository-name* — Specifies a string, up to 32 characters, that uniquely identifies the software repository.

create — Specifies the keyword required when the software-repository context is first created. Once the context is created, it can be accessed without the **create** keyword.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.274 solicit-delay

solicit-delay

Syntax **solicit-delay** *delay*
no solicit-delay

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection solicit-delay)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>advertise-selection solicit-delay)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection solicit-delay)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection solicit-delay
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection solicit-delay
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection solicit-delay

Description This command configures the default time to delay DHCPv6 Solicit messages. The delay is applied to all DHCPv6 Solicit messages for which no per DHCPv6 server or per client MAC delay or preference option value is configured.

The **no** form of this command removes the delay timeout.

Parameters *delay* — Specifies the default amount of time to delay DHCPv6 Solicit messages, in deciseconds.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

solicit-delay

Syntax **solicit-delay** *delay*
no solicit-delay

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection>client-mac solicit-delay)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>advertise-selection>client-mac solicit-delay)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree]
(config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection>client-mac solicit-delay)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac solicit-delay
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac solicit-delay
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection client-mac solicit-delay

Description This command configures the time to delay DHCPv6 Solicit messages with an odd or even source MAC address.

The **no** form of this command removes the delay timeout.

Parameters *delay* — Specifies the time to delay DHCPv6 Solicit messages with an odd or even source MAC address, in deciseconds.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

solicit-delay

Syntax **solicit-delay** *delay*
no solicit-delay

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection>server solicit-delay)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>advertise-selection>server solicit-delay)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>advertise-selection>server solicit-delay)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server solicit-delay
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server solicit-delay
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection server solicit-delay

Description This command configures the time to delay DHCPv6 Solicit messages relayed to the server.

The **no** form of this command removes the delay timeout.

Parameters *delay* — Specifies the time to delay DHCPv6 Solicit messages that are relayed to the server, in deciseconds.

Values 1 to 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.275 solicited-release

solicited-release

Syntax [**no**] **solicited-release**

Context **[Tree]** (config>service>vprn>dhcp6>server>lease-hold-time-for solicited-release)
[Tree] (config>router>dhcp6>server>lease-hold-time-for solicited-release)
[Tree] (config>service>vprn>dhcp>server>lease-hold-time-for solicited-release)
[Tree] (config>router>dhcp>server>lease-hold-time-for solicited-release)

Full Context configure router dhcp local-dhcp-server lease-hold-time-for solicited-release
configure router dhcp6 local-dhcp-server lease-hold-time-for solicited-release
configure service vprn dhcp local-dhcp-server lease-hold-time-for solicited-release
configure service vprn dhcp6 local-dhcp-server lease-hold-time-for solicited-release

Description This command enables the server to hold up a lease even in case of solicited release; for example, when the server receives a normal DHCP release message.

The **no** form of this command disables the ability of the server to hold up a lease when a solicited release is received.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.276 sonet-sdh

sonet-sdh

Syntax **sonet-sdh**

Context **[Tree]** (config>port sonet-sdh)

Full Context configure port sonet-sdh

Description This command enables access to the context to configure SONET/SDH ports. This context can only be used when configuring an OC-3 and OC-12 SONET/SDH ports on an appropriate MDA.

This command also enables access to the context to configure SONET/SDH parameters for an Ethernet port in WAN PHY (xgig wan) mode.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The 10 Gigabit Ethernet LAN port also has SONET/SDH characteristics. However, these characteristics are predetermined and not configurable.

This command is supported by TDM satellite.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.277 source

source

Syntax [**no**] **source** *ipv6-address*

Context **[Tree]** (config>subscr-mgmt>igmp-policy>static>group source)
[Tree] (config>subscr-mgmt>igmp-policy source)
[Tree] (config>subscr-mgmt>mld-policy>static>group source)

Full Context configure subscriber-mgmt igmp-policy source
configure subscriber-mgmt igmp-policy static group source
configure subscriber-mgmt mld-policy static group source

Description This command adds or removes a static multicast source.

The **no** form of this command reverts to the default.

Parameters *grp-ipv6-address* — Specifies the IPv6 address.

Values ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D
- multicast group IPv6 address

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source

Syntax [**no**] **source** *ip-address*
[**no**] **source** *src-ipv6-address*

Context **[Tree]** (config>service>vpls>sap>igmp-snooping>static>group source)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping>static>group source)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping>static>group source)
[Tree] (config>service>vpls>sap>mld-snooping>static>group source)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping>static>group source)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>mesh-sdp>mld-snooping>static>group source)

Full Context
configure service vpls mesh-sdp igmp-snooping static group source
configure service vpls mesh-sdp mld-snooping static group source
configure service vpls sap igmp-snooping static group source
configure service vpls sap mld-snooping static group source
configure service vpls spoke-sdp igmp-snooping static group source
configure service vpls spoke-sdp mld-snooping static group source

Description
This command specifies a IPv4 or IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the sources that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The **source** command in combination with the group is used to create a specific (S,G) static group entry.

Static (s,g) entries cannot be entered when a starg is already created.

Use the **no** form of this command to remove the source from the configuration.

Parameters
ip-address — Specifies the IPv4 unicast address

src-ipv6-address — Specifies the IPv6 unicast address.

Platforms
All

source

Syntax
source *ip-address*
no source

Context
[Tree] (config>service>ies>if>sap>ip-tunnel source)
[Tree] (config>service>vprn>if>sap>ip-tunnel source)

Full Context
configure service ies interface sap ip-tunnel source
configure service vprn interface sap ip-tunnel source

Description
This command configures the source IPv4 or IPv6 address to use for an IP tunnel. This configuration applies to the outer IP header of the encapsulated packets. The IPv4 or IPv6 address must belong to the one of the IP subnets associated with the public SAP interface of the tunnel-group. The **source** address, **remote-ip** address and **backup-remote-ip** address of a tunnel must all belong to the same address family (IPv4 or IPv6). When the source address contains an IPv6 address it must be a global unicast address.

The **no** form of this command deletes the source address from the tunnel configuration. The tunnel must be administratively shutdown before issuing the **no source** command.

Default
no source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies an IPv4 address or an IPv6 address.

Values

ipv4-address	a.b.c.d	
ipv6-address		x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
	x	[0..FFFF]H
	d	[0..255]D

Platforms All

source

Syntax [**no**] **source** *ip-address*

Context **[Tree]** (config>service>vprn>igmp>ssm-translate>grp-range source)

Full Context configure service vprn igmp ssm-translate grp-range source

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

Platforms All

source

Syntax **source** *ip-address*

Context **[Tree]** (config>service>vprn>igmp>if>static>group source)

Full Context configure service vprn igmp interface static group source

Description This command specifies an IPv4 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group is to receive multicast traffic from, and from the sources that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The **source** command in combination with the group is used to create a specific (S,G) static group entry.

Use the **no** form of this command to remove the source from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the IPv4 unicast address.

Platforms All

source

Syntax [**no**] **source** *src-ipv6-address*

Context **[Tree]** (config>service>vprn>mld>if>static>group source)

Full Context configure service vprn mld interface static group source

Description This command specifies an IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the sources that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The **source** command, in combination with the group, is used to create a specific (S,G) static group entry.

The **no** form of this command removes the source from the configuration.

Parameters *src-ipv6-address* — Specifies the IPv6 unicast address.

Platforms All

source

Syntax [**no**] **source** *ip-address*

Context **[Tree]** (config>service>vprn>mld>ssm-translate>grp-range source)

Full Context configure service vprn mld ssm-translate grp-range source

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

Platforms All

source

Syntax [**no**] **source** *unicast-ip-prefix/mask*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>msdp source)

Full Context configure service vprn msdp source

Description This command limits the number of active source messages the router accepts from sources in the specified address range.

If the prefix and mask provided is already a configured then this command only provides the context to configure the parameters pertaining to this active source-message filter.

If the prefix and mask provided is not already a configured, then the source node instance must be created and the context to configure the parameters pertaining to this node should be provided. In this case, the $ prompt to indicate that a new entity (source) is being created should be used.

The source active msdp messages are not rate limited based on the source address range.

The **no** form of this message removes the source active rate limiter for this source address range.

Parameters *unicast-ip-prefix* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ip-prefix/mask: ip-prefix a.b.c.d (host bits must be 0)

mask — Specifies the subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values 0 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

Platforms All

source

Syntax [**no**] **source** *ip-address* [*l**mask*]
[**no**] **source any**

Context [Tree] (config>service>vprn>mvpn>pt>selective>multistream-spmsi>group source)
[Tree] (config>service>vprn>mvpn>pt>selective>umh-rm>group source)

Full Context configure service vprn mvpn provider-tunnel selective multistream-spmsi group source
configure service vprn mvpn provider-tunnel selective umh-rate-monitoring group source

Description This command creates source prefixes for specific groups that map to the multicast stream.

The **no** form removes the source prefix.

Parameters *ip-address/mask* — Specifies the IP address of the group.

Values

ipv4-prefix	a.b.c.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	ipv4-prefix-length	[0..32]
ipv6-prefix		x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
	x	[0..FFFF]H
	d	[0..255]D
	ipv6-prefix-length	[0..128]

Platforms All

source

Syntax **source** *source-type*
source *source-type* **level** *level*
no source *source-type*

Context **[Tree]** (config>app-assure>group>anl source)

Full Context configure application-assurance group access-network-location source

Description This command configures location sources for the dynamic experience management. The location source types are, for example, 3G and congestion point.

Default source mobile-3g

Parameters *source-type* — Specifies the location or access technology.

Values **access-point** — Provides Dynamic Experience Management (DEM) for the WLGW access point.

Note: The access points do not need to support the Nokia CEA function.

level — Specifies which congestion point within the specified source-type to monitor for congestion.

Values **MAC+VLAN** — WLGW access point (MAC) and radio (VLAN).

Note: The access points do not need to support the Nokia CEA function.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

source

Syntax [**no**] **source** *ip-address*

Context **[Tree]** (config>router>igmp>if>ssm-translate>grp-range source)
[Tree] (config>router>igmp>ssm-translate>grp-range source)

Full Context configure router igmp interface ssm-translate grp-range source
configure router igmp ssm-translate grp-range source

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

Platforms All

source

Syntax [**no**] **source** *ip-address*

Context **[Tree]** (config>router>igmp>if>static>group source)

Full Context configure router igmp interface static group source

Description This command specifies a IPv4 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The **source** command in combination with the group is used to create a specific (S,G) static group entry.

The **no** form of the command removes the source from the configuration.

Parameters *ip-address* — Specifies the IPv4 unicast address.

Platforms All

source

Syntax [**no**] **source** *ip-address*

Context **[Tree]** (config>router>igmp>tunnel-interface>static>group source)

Full Context configure router igmp tunnel-interface static group source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies a IPv4 unicast address of a multicast source. The source command is mutually exclusive with the specification of individual sources for the same group. The source command in combination with the group is used to create a specific (S,G) group entry in a static group join on a tunnel interface associated with a P2MP RSVP LSP.

The **no** form of the command removes the source from the configuration.

Parameters *ip-address* — Specifies the IPv4 unicast address.

Platforms All

source

Syntax [**no**] **source** *src-ipv6-address*

Context **[Tree]** (config>router>mld>if>static>group source)

Full Context configure router mld interface static group source

Description This command specifies an IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The **source** command, in combination with the group, is used to create a specific (S,G) static group entry.

The **no** form of this command removes the source from the configuration.

Parameters *src-ipv6-address* — Specifies the IPv6 unicast address.

Platforms All

source

Syntax [**no**] **source** *ipv6-address*

Context **[Tree]** (config>router>mld>ssm-translate>grp-range source)
[Tree] (config>router>mld>if>ssm-translate>grp-range source)

Full Context configure router mld interface ssm-translate grp-range source
configure router mld ssm-translate grp-range source

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

The **no** form of this command removes the IPv6 address form the group range configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-address* — Specifies the IPv6 address that will be sending data.

Platforms All

source

Syntax [**no**] **source** *ip-prefix/mask*

Context **[Tree]** (config>router>msdp source)

Full Context configure router msdp source

Description This command limits the number of active source messages the router accepts from sources in the specified address range.

If the prefix and mask provided is already a configured then this command only provides the context to configure the parameters pertaining to this active source-message filter.

If the prefix and mask provided is not already a configured, then the source node instance must be created and the context to configure the parameters pertaining to this node should be provided. In this case, the $ prompt to indicate that a new entity (source) is being created should be used.

The source active **config>router msdp** messages are not rate limited based on the source address range.

The **no** form of this message removes the source active rate limiter for this source address range.

Parameters *ip-prefix* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ip-prefix/mask: ip-prefix a.b.c.d (host bits must be 0)

mask — Specifies the subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values 0 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

Platforms All

source

Syntax **source mep** *mep-id* **domain** *md-index* **association** *ma-index*
source mep *mep-id* **domain-name** *admin-name* **association-name** *admin-name*
no source

Context **[Tree]** (config>oam-pm>session>ethernet source)

Full Context configure oam-pm session ethernet source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the source launch point identification Y.1731 parameters that are used by the individual tests within the session. If an MEP matching the configuration does not exist, the session is allowed to become active, however the frames sent frames and received as seen under the **show >oam-pm>statistics>session** *session-name* command is zero. The preferred reference to the MEP launch point is by *admin-name*. Therefore, the syntax **source mep** *mep-id* **domain-name** *admin-name* **association-name** *admin-name* should be used.

The **no** form of this command removes this session parameter.

Parameters *mep-id* — Specifies the maintenance association end point identifier of the launch point.

Values 1 to 8191

md-index — Specifies the maintenance domain (MD) index value of the launch point. The **domain-name** *admin-name* parameter is preferred for specifying the domain information.

Values 1 to 4294967295

ma-index — Specifies the maintenance association (MA) index value of the launch point. The **association-name** *ma-name* parameter is preferred for specifying the association information.

Values 1 to 4294967295

admin-name — Specifies the name reference for the maintenance domain (MD), or the association (MA) *admin-name* value of the launch point, up to 64 characters.

Platforms All

source

Syntax **source** *ip-address*
no source

Context **[Tree]** (config>oam-pm>session>ip source)

Full Context configure oam-pm session ip source

Description This command defines the source IP address that the session controller (launch point) uses for the test. The source address must be a local resident IP address in the context; otherwise, the response packets are processed by the TWAMP Light application. Only source addresses configured as part of TWAMP tests can process the reflected TWAMP packets from the session reflector.

The **no** form of this command removes the source address parameters.

Parameters **source** — Indicates the launch point.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address — Specifies the source IP address that the session controller (launch point) uses for the test.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

source

Syntax **source** {**line-ref** | **internal-clock**}

Context **[Tree]** (config>system>sync-if-timing>bits>output source)

Full Context configure system sync-if-timing bits output source

Description This command configures the values used to identify the source of the BITS (Building Integrated Timing Supply) output. This is either the signal recovered directly from ref1, ref2 or ptp, or it is the output of the node's central clock. The directly recovered signal would be used when the BITS output signal is feeding into an external standalone timing distribution device (BITS/SASE). The specific directly recovered signal used is the best of the available signals based of the QL and/or the ref-order. The central clock output would be used when no BITS/SASE device is present and the BITS output signal is used to monitor the quality of the recovered clock within the system.

Default source line-ref

Parameters **line-ref** — Specifies that the BITS output timing is selected from one of the input references, without any filtering.

internal-clock — Specifies that the BITS output timing is driven from the system timing.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

source

Syntax **source** *ip-address*
no source

Context **[Tree]** (config>router>if>if-attr>delay>dyn>twamp>ipv4 source)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv4 source

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the unicast IPv4 address used as the source of the TWAMP Light test packet. When this command is not configured, the primary IPv4 address, or the reference IPv4 address in the case of unnumbered interfaces, is used as the source. This command can be used when the IPv4 primary address or reference interface is not the desired source address for the packet.

Changes are allowed without administratively disabling the IPv4 protocol.

The **no** form of this command removes the specified address, which causes the source address to be auto-learned.

Default no source

Parameters *ip-address* — Specifies TWAMP Light IPv4 source address.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

source

Syntax **source** *ipv6-address*
no source

Context **[Tree]** (config>router>if>if-attr>delay>dyn>twamp>ipv6 source)

Full Context configure router interface if-attribute delay dynamic twamp-light ipv6 source

Description This command configures the IPv6 address used as the source of the TWAMP Light test packet. When this command is not configured, no source address is present and an error is raised to prevent the transmission of the test packet.

The IPv6 protocol can be enabled even without addressing. However, the test will not transmit packets. The link local address must be in the form fe80::/64 in accordance with RFC 4291, *IP Version 6 Addressing Architecture*.

The **no** form of this command removes the specified address.

Default no source

Parameters *ipv6-address* — Specifies the TWAMP Light IPv6 source address.

Values

ipv6-address:	x:x:x:x:x:x:x:x
	x - [0 to FFFF]H
	unicast and link local IPv6 address only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.278 source-address

source-address

Syntax **source-address** *ipv6-address*
no source-address

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6-relay source-address)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>relay source-address)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay source-address)
[Tree] (config>service>vprn>if>ipv6>dhcp6-relay source-address)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay source-address)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay source-address)

Full Context configure service ies interface ipv6 dhcp6-relay source-address
configure service ies subscriber-interface group-interface ipv6 dhcp6 relay source-address
configure service ies subscriber-interface ipv6 dhcp6 relay source-address
configure service vprn interface ipv6 dhcp6-relay source-address
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay source-address
configure service vprn subscriber-interface ipv6 dhcp6 relay source-address

Description This command configures the source IPv6 address of the DHCPv6 relay messages.

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the source IPv6 address of the DHCPv6 relay messages.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay source-address
- configure service ies subscriber-interface ipv6 dhcp6 relay source-address
- configure service ies subscriber-interface group-interface ipv6 dhcp6 relay source-address
- configure service vprn subscriber-interface ipv6 dhcp6 relay source-address

All

- configure service ies interface ipv6 dhcp6-relay source-address
- configure service vprn interface ipv6 dhcp6-relay source-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>aaa>l2tp-acct-plcy>radius-acct-server source-address)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server source-address

Description This command configures the source address of the RADIUS messages.

The **no** form of this command reverts to the default value.

Parameters *ip-address* — Specifies the source address to be used for NAT RADIUS accounting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>system>management-interface>remote-management source-address)

Full Context configure system management-interface remote-management source-address

Description This command configures the address local to this device that NISH uses to connect to this node.

If this command is also configured for a specific manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command causes the system to select the source address based on the selected routing instance of the manager.

Parameters *ip-address* — Specifies the IP address that NISH managers use to connect to the node.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>system>management-interface>remote-management>manager source-address)

Full Context configure system management-interface remote-management manager source-address

Description This command configures the address local to this device that this NISH manager uses to connect to this node.

This command takes precedence over the command configured in the global context (**config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command causes the source address to be inherited from the global context (**config**>**system**>**management-interface**>**remote-management**).

Parameters *ip-address* — Specifies the IP address that NISH managers use to connect to the node.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

Platforms All

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server source-address)
[Tree] (config>subscr-mgmt>acct-plcy>server source-address)

Full Context configure subscriber-mgmt radius-accounting-policy radius-accounting-server source-address
configure subscriber-mgmt authentication-policy radius-authentication-server source-address

Description This command configures the source address of the RADIUS packet.

The system IP address must be configured in order for the RADIUS client to work. See Configuring a System Interface in the Router Configuration Guide.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: The system IP address must only be configured if the source-address is not specified. When the **no source-address** command is executed, the source address is determined at the moment the request is sent. This address is also used in the nas-ip-address attribute: over there it is set to the system IP address if **no source-address** was given.

The **no** form of this command reverts to the default value.

Default System IP address

Parameters *ip-address* — Specifies the IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source-address

Syntax **source-address** *ip-address* [**allow-connections**]
no source-address

Context **[Tree]** (config>aaa>diam>node source-address)

Full Context configure aaa diameter node source-address

Description This command configures IPv4 source address that the SR OS node will use for its peering connection.

The **no** form of this command removes the IP address from the configuration.

Parameters *ip-address* — Specifies IP prefix for the IP match criterion in dotted decimal notation

Values 0.0.0.0 **to** 255.255.255.255

allow-connections — Specifies to accept peering connections on the configured source IPv4 address. The peer initiating the connection can only be an inter-chassis peer.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>redundancy>multi-chassis>peer source-address)

Full Context configure redundancy multi-chassis peer source-address

Description This command specifies the source address used to communicate with the multi-chassis peer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the source address used to communicate with the multi-chassis peer.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>aaa>radius-srv-plcy>servers source-address)

Full Context configure aaa radius-server-policy servers source-address

Description This command configures the source address of the RADIUS packet. The system IP address must be configured in order for the RADIUS client to work. See Configuring a System Interface in the 7750 SR OS Configuration Guide.

Note: The system IP address must only be configured if the source-address is not specified. When the no source-address command is executed, the source address is determined at the moment the request is sent. This address is also used in the *nas-ip-address* attribute: over there it is set to the system IP address if no source-address was given.

The **no** form of this command reverts to the default value.

Parameters *ip-address* — Specifies the source address of RADIUS packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source-address

Syntax **source-address**

Context **[Tree]** (config>service>vprn source-address)

Full Context configure service vprn source-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context specify the source address and application that should be used in all unsolicited packets.

Platforms All

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>router>ldp>lsp-bfd source-address)

Full Context configure router ldp lsp-bfd source-address

Description This command configures the source address of periodic LSP ping packets and BFD control packets for LSP BFD sessions that are associated with LDP prefixes in the prefix list. The system IP address is used by default. If the system IP address is not routable from the far-end node of the BFD session, then an alternate routable IP address that is local to the source node should be used.

Default no source-address

Parameters *ip-address* — Specifies a routable IPv4 or IPv6 address that is local to the node.

Values *ipv4-address* — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — 0 to FFFF in hexadecimal
d — 0 to 255 in decimal

Default system IP address

Platforms All

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>app-assure>rad-acct-plcy>server source-address)

Full Context configure application-assurance radius-accounting-policy radius-accounting-server source-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the source address of the RADIUS packet. The system IP address must be configured in order for the RADIUS client to work. See “Configuring a System Interface” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*. The system IP address must only be configured if the source-address is not specified. When the **no source-address** command is executed, the source address is determined at the moment the request is sent. This address is also used in the nas-ip-address attribute: over there it is set to the system IP address if no source address was given.

The **no** form of this command reverts to the default value, where the source address is the system IP address.

Default no source-address

Parameters *ip-address* — The IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>service>ipfix>export-policy>collector source-address)

Full Context configure service ipfix ipfix-export-policy collector source-address

Description This command configures the source address from which UDP streams containing IPFIX flow records will be sourced.

Default no source-address

Parameters *ip-address* — Source IPv4 address from which UDP streams are sent.

Platforms All

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>filter>gre-tun-tmp>ipv4 source-address)

Full Context configure filter gre-tunnel-template ipv4 source-address

Description This command defines the source IPv4 address to be used in the GRE IP header used to encapsulate the matching IPv4/IPv6 packet. This IP address can be configured as any value and is not validated against a local IP address. The **source-address** command must be configured for the template to be valid.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the source IP address configuration from the associated GRE tunnel template.

Parameters *ip-address* — Specifies the IPv4 address (in dotted decimal notation) to be used as the source address.

Platforms All

source-address

Syntax **source-address** [*ip-address*]
no source-address

Context **[Tree]** (config>filter>redirect-policy>dest>ping-test source-address)

Full Context configure filter redirect-policy destination ping-test source-address

Description This command configures the source address to use in the IP packet of the ping test for this destination.

Default no source-address

Parameters *ip-address* — The source address of the IP packet. This can be IPv4 only for an IPv4 destination and IPv6 only for an IPv6 destination.

Values

ipv4-address:	a.b.c.d.
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms All

source-address

Syntax **source-address**

Context **[Tree]** (config>system>security source-address)

Full Context configure system security source-address

Description This command specifies the IP source address that is used in all unsolicited packets sent by the application.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This configuration applies to packets transmitted in-band (for example, a network port on an IOM) and does not apply to packets transmitted out-of-band on the management interface on the CPM ethernet port. Packets transmitted using the CPM ethernet port use the address of the CPM ethernet port as the IP source address in the packet.

When a source address is specified for the **ptp** application, the port-based 1588 hardware timestamping assist function will be applied to PTP packets matching the IPv4 address of the router interface used to ingress the SR/ESS or IP address specified in this command. If the IP address is removed, then the port-based 1588 hardware timestamping assist function will only be applied to PTP packets matching the IPv4 address of the router interface.

Platforms All

source-address

Syntax **source-address** *ip-address*

Context **[Tree]** (config>system>security>dot1x>radius-plcy source-address)

Full Context configure system security dot1x radius-plcy source-address

Description This command configures the NAS IP address to be sent in the RADIUS packet.

The **no** form of this command reverts to the default value.

Parameters *ip-address* — Specifies the IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255

Platforms All

source-address

Syntax **source-address** *ip-address*
source-address prefix-list *prefix-list-name*
no source-address

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from source-address)

Full Context configure router policy-options policy-statement entry from source-address

Description This command specifies the source address that is embedded in the join or prune packet as a filter criterion.

The **no** form of this command removes the criterion from the configuration.

This command specifies a multicast data source address as a match criterion for this entry.

Default no source-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the IP prefix for the IP match criterion in dotted decimal notation.

Values ipv4-address:
- a.b.c.d

ipv6-address:
- x:x:x:x:x:x:x:x
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

prefix-list-name — The prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

source-address

Syntax **source-address** *ip-address*
no source-address

Context **[Tree]** (config>aaa>diam-peer-plcy source-address)

Full Context configure aaa diameter-peer-policy source-address

Description This command configures the IPv4 source address that the SR OS node uses for the peering policy.

The **no** form of this command removes the IP address from the configuration.

Parameters *ip-address* — Specifies the IP prefix for the IP match criterion in dotted decimal notation

Values 0.0.0.0 to 255.255.255.255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source-address

Syntax **source-address** *ipv6-address*
no source-address

Context **[Tree]** (config>router>segment-routing>srv6 source-address)

Full Context configure router segment-routing segment-routing-v6 source-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the global default source IPv6 address used in the SA field of the outer IPv6 header of the SRv6 encapsulated packet. This value is inherited in the BGP and service contexts by default, but can be overwritten in each context. A maximum of 16 address values can be configured in all contexts in the system.

There is no default value for this command. A default source IPv6 address must be configured in this context or in the BGP or service context. The system does not check if the entered address is a valid local address.

The **no** form of this command removes the source IPv6 address from the configuration.

Parameters *ipv6-address* — Specifies the source IPv6 address of the SRv6.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

source-address

Syntax **source-address** *ipv6-address*
no source-address

Context **[Tree]** (config>router>bgp>srv6 source-address)

Full Context configure router bgp segment-routing-v6 source-address

Description This command configures the source IPv6 address for SRv6.

This command overrides the source IPv6 address for all address families in the base router instance. By default, BGP uses the value from the top level configuration under **config**>**router**>**segment-routing**>**segment-routing-v6**.

The **no** form of this command removes the source IPv6 address from the configuration.

Default no source-address

Parameters *ipv6-address* — Specifies the source IPv6 address of the SRv6.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

source-address

Syntax **source-address** *ipv6-address*
no source-address

Context **[Tree]** (config>service>vprn>bgp-ipvpn>srv6 source-address)
[Tree] (config>service>epipe>bgp-evpn>srv6 source-address)

Full Context configure service epipe bgp-evpn segment-routing-v6 source-address
configure service vprn bgp-ipvpn segment-routing-v6 source-address

Description This command configures the source IPv6 address used in the instance for SRv6 packets.

The **no** form of this command removes the source IPv6 address from the configuration.

Default no source-address

Parameters *ipv6-address* — Specifies the source IPv6 address of the SRv6.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.279 source-address-range

source-address-range

Syntax **source-address-range** *start-ip-address*
no source-address-range

Context **[Tree]** (config>aaa>isa-radius-plcy>servers source-address-range)

Full Context configure aaa isa-radius-policy servers source-address-range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the first IP address in the range of IPv4 addresses that are assigned to a BB-ISA in a given NAT group for NAT RADIUS accounting. The IP addresses are unique within the NAT group and are used to bind the RADIUS client instantiated on each BB-ISA card. The number of IPv4 addresses allocated is equal to the number of BB-ISAs in a NAT group that are enabled for NAT RADIUS accounting. Although only the first IPv4 address is explicitly configured with this command, each internally allocated IPv4 address associated with the BB-ISA card can be seen in the routing table (via show commands) as /32 with protocol designation 'NAT'.

Default no source-address-range

Parameters *start-ip-address* — The starting IP address of the IP address range.

Values 0.0.0.0 - 255.255.255.255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

source-address-range

Syntax [**no**] **source-address-range start** *ip-address* **end** *ip-address*

Context **[Tree]** (config>service>vprn>wlan-gw>gtp>source-ranges source-address-range)

Full Context configure service vprn wlan-gw gtp source-ranges source-address-range

Description This command configures a range of IP addresses used by ISA MDA's as source address in GTP messages.

The **no** form of this command removes the IP address ranges.

Parameters **start** *ip-address* — Specifies the start of the source IP address range.

Values ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0..255]D

end *ip-address* — Specifies the end of the source IP address range.

Values ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0..255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.280 source-bmac

source-bmac

Syntax **source-bmac** *ieee-address*
no source-bmac

Context **[Tree]** (config>service>pbb source-bmac)

Full Context configure service pbb source-bmac

Description This command configures the source B-VPLS MAC address to use with PBB and provisions a chassis level source B-MAC.

Parameters *ieee-address* — The MAC address assigned to the B-MAC. The value should be input in either a xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format.

Platforms All

source-bmac

Syntax **source-bmac** *ieee-address*

Context **[Tree]** (config>service>vpls>pbb source-bmac)

Full Context configure service vpls pbb source-bmac

Description This command configures the base source B-MAC for the B-VPLS. The first 32 bits must be the same with what is configured in the MC-LAG peer. If not configured here, it will inherit the chassis level B-MAC configured under the new PBB object added in the previous section. If the **use-sap-bmac** command is on, the value of the last 16 bits (lsb) of the source B-MAC must be part of the **reserved-source-bmac-lsb** configured at chassis level, under service PBB component. If that is not the case, the command will fail.

Platforms All

23.281 source-bmac-lsb

source-bmac-lsb

Syntax **source-bmac-lsb** *MAC-Lsb* [**es-bmac-table-size** *size*]
no source-bmac-lsb

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>system>bgp-evpn>eth-seg source-bmac-lsb)

Full Context configure service system bgp-evpn ethernet-segment source-bmac-lsb

Description This command configures the least significant two bytes of the B-MAC used as the source B-MAC for packets generated from the Ethernet-Segment in PBB-EVPN.

When the multi-homing mode is **all-active**, this value and the first high order four bytes must match on all the PEs that are part of the same Ethernet-Segment.

The **es-bmac-table-size** parameter modifies the default value (8) for the maximum number of virtual bmacs that can be associated to the Ethernet-Segment, that is, the es-bmacs. When the **source-bmac-lsb** is configured, the associated **es-bmac-table-size** is reserved out of the total FDB. The es-bmac will consume a separate B-MAC per B-VPLS that is linked to an Ethernet-Segment.

Parameters *MAC-Lsb* — Specifies the two least significant bytes of the es-bmac.

Values 1 to 65535, or xx-xx or xx:xx

size — Specifies the reserved space in the FDB for a specified es-bmac. By default the system reserves 8 entries for a specified Ethernet-Segment B-MAC.

Values 1 to 511999

Default 8

Platforms All

source-bmac-lsb

Syntax **source-bmac-lsb** *mac-lsb* **control-pw-vc-id** *vc-id*
no source-bmac-lsb

Context [Tree] (config>service>sdp source-bmac-lsb)

Full Context configure service sdp source-bmac-lsb

Description This command defines the 16 least significant bits (lsb) which, when combined with the 32 most significant bits of the PBB **source-bmac**, are used as the virtual backbone MAC associated with this SDP. The virtual backbone MAC is used as the source backbone MAC for traffic received on a PBB EPIPE spoke-SDP with **use-sdp-bmac** configured (that is, a redundant pseudowire) and forwarded into the B-VPLS domain.

The control-pw-vc-id defines VC identifier of the spoke-SDP relating to the control pseudowire whose status is to be used to determine whether SPBM advertises this virtual backbone MAC. This is a mandatory parameter when the **source-bmac-lsb** is added or changed. The spoke SDP must have the parameter **use-sdp-bmac** for the control pseudowire to be active.

Default no source-bmac-lsb

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *mac-lsb* — Specifies the 16 least significant bits of the virtual backbone MAC associated with this SDP.

Values 1 to 65535 or xx-xx or xx:xx

control-pw-vc-id *vc-id* — Specifies the VC identifier of the control pseudowire.

Values 1 to 4294967295

Platforms All

23.282 source-class

source-class

Syntax **source-class** *source-index*
no source-class [*source-index*]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect source-class)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel source-class)
[Tree] (config>service>vprn>static-route-entry>next-hop source-class)

Full Context configure service vprn static-route-entry indirect source-class
configure service vprn static-route-entry ipsec-tunnel source-class
configure service vprn static-route-entry next-hop source-class

Description This command configures the policy accounting source-class index to be used when incrementing accounting statistic for traffic matching the associated static route.

If source route policy accounting is enabled and a source-class index is configured, traffic with a source IP address matches the associated static route, the source accounting statistics for the specified class will be incremented.

The **no** form of this command removes the associated destination-class from the associated static route nexthop.

Default no source-class

Parameters *source-index* — Specifies an integer value for the accounting source class index.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

source-class

Syntax **source-class** *source-index*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no source-class [*source-index*]

Context **[Tree]** (config>router>static-route-entry>indirect source-class)
[Tree] (config>router>static-route-entry>next-hop source-class)

Full Context configure router static-route-entry indirect source-class
configure router static-route-entry next-hop source-class

Description This command configures the policy accounting source-class index to be used when incrementing accounting statistic for traffic matching the associated static route.

If source route policy accounting is enabled and a source-class index is configured, traffic with a source IP address matches the associated static route, the source accounting statistics for the specified class will be incremented.

The **no** form of this command removes the associated destination-class from the associated static route nexthop.

Default no source-class

Parameters *source-index* — Specifies an integer value for the accounting source class index.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

source-class

Syntax **source-class** *index* [*index*]
source-class {*index* | **all**}

Context **[Tree]** (config>router>policy-acct-template source-class)

Full Context configure router policy-acct-template source-class

Description This command configures a source class index.

The **no** form of this command deletes the specified source class index.

Parameters *index* — Specifies the index value.

Values 1 to 255

all — Deletes all the source class indices.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

source-class

Syntax **source-class** [*value*]
no source-class

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>policy-options>policy-statement>entry>action source-class)
[Tree] (config>router>policy-options>policy-statement>default-action source-class)

Full Context configure router policy-options policy-statement default-action source-class
configure router policy-options policy-statement entry action source-class

Description This command specifies the policy accounting source class index to associate with matched routes.

Parameters *value* — Specifies the default operational source-class for this policy statement.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

23.283 source-destination-prefix

source-destination-prefix

Syntax [**no**] **source-destination-prefix**

Context [Tree] (config>cflowd>collector>aggregation source-destination-prefix)

Full Context configure cflowd collector aggregation source-destination-prefix

Description This command configures cflowd aggregation based on source and destination prefixes.

The **no** form of this command removes this type of aggregation from the collector configuration.

Platforms All

23.284 source-ip

source-ip

Syntax **source-ip** *ip-address*
no source-ip

Context [Tree] (config>subscr-mgmt>shcv-policy>vpls source-ip)

Full Context configure subscriber-mgmt shcv-policy vpls source-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the IPv4 address to be used as source address for connectivity verification in a VPLS service.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the IPv4 address to be used as source address for connectivity verification in a VPLS service.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

source-ip

Syntax **source-ip** *ipv6-address*
no source-ip

Context **[Tree]** (config>service>vprn>sub-if>wlan-gw>pool-manager>dhcp6-client source-ip)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager>dhcp6-client source-ip)

Full Context configure service ies subscriber-interface wlan-gw pool-manager dhcpv6-client source-ip
configure service vprn subscriber-interface wlan-gw pool-manager dhcpv6-client source-ip

Description This command specifies the source-ip to be used by the DHCPv6 client.

The **no** form of this command removes the specific source-ip. In this case the DHCPv6 client will fall back to the IP address configured on the outgoing interface.

Parameters *ipv6-address* — Specifies the IPv6 address, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.285 source-ip-address-ranges

source-ip-address-ranges

Syntax **source-ip-address-ranges**

Context **[Tree]** (config>service>vprn>wlan-gw>gtp source-ip-address-ranges)

Full Context configure service vprn wlan-gw gtp source-ip-address-ranges

Description Commands in this context configure IP addresses used by the ISA MDA's as source address in GTP messages

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.286 source-ip-origin

source-ip-origin

Syntax **source-ip-origin** {**interface** | **vrrp**}
no source-ip-origin

Context **[Tree]** (config>subscr-mgmt>shcv-policy>layer-3 source-ip-origin)

Full Context configure subscriber-mgmt shcv-policy layer-3 source-ip-origin

Description This command selects the source IP address to be used for SHCV messages.

The **no** form of this command reverts to the default.

Parameters **interface** — Specifies to use the interface IP as the source address of SHCV.

vrrp — Specifies to use the VRRP configured IP as the source address of SHCV.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.287 source-mac

source-mac

Syntax **source-mac** *ieee-address*
no source-mac

Context **[Tree]** (config>subscr-mgmt>shcv-policy>vpls source-mac)

Full Context configure subscriber-mgmt shcv-policy vpls source-mac

Description Specifies the MAC address to be used as source address for connectivity verification in a VPLS service.

The **no** form of this command reverts to the default.

Parameters *ieee-address* — Specifies the 48-bit MAC address in the xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx format.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.288 source-override

source-override

Syntax **source-override** *ip-address* [**create**]
no source-override *ip-address*

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>channel source-override)

Full Context configure mcast-management multicast-info-policy bundle channel source-override

Description This command defines a multicast channel parameter override context for a specific multicast sender within the channel range. The specified sender's IP address must be the same IP type, IPv4 or IPv6, as defined in the **channel** command.

The **no** form of this command removes the specified sender override context from the channel range.

Parameters *ip-address* — Specifies either an IPv4 or IPv6 address and must be the same IP type as the containing **channel** command range.

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

create — The **create** keyword is required if creating a new source override when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified source override IP address already exists.

Platforms All

23.289 source-port

source-port

Syntax **source-port** *port-num*
no source-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>video source-port)

Full Context configure mcast-management multicast-info-policy bundle video source-port

Description This command configures the source port for upstream RET requests. The **source-port** *port-num* value is the only configuration parameter in the bundle "default" context.

The **no** form of the command removes the value from the configuration.

Parameters *port-num* — Specifies the source port in the received RTP multicast stream.

Values 1024 to 65535

source-port

Syntax **source-port** *port-id*
no source-port

Context [Tree] (config>system>sync-if-timing>ref1 source-port)
[Tree] (config>system>sync-if-timing>ref2 source-port)

Full Context configure system sync-if-timing ref1 source-port
configure system sync-if-timing ref2 source-port

Description This command configures the source port for timing reference **ref1** or **ref2**. If the port is unavailable or the link is down, then the reference sources are re-evaluated according to the reference order configured in the **ref-order** command.

In addition to physical port on the 7750 SR, T1 or E1 channels on a channelized OC3/OC12/STM1/STM4 Circuit Emulation Service port can be specified if they are using adaptive timing.

There are restrictions on the source-port location for **ref1** and **ref2** based on platform. Refer to the description of the **ref1** command for details.

Default no source-port

Parameters *port-id* — Identifies the physical port in the *slot/mda/port*, **esat**-*id*/*slot*/*port*, or **pxc**-*id*.*sub-port* format.

Values *slot*/*mda*/*port* [.*channel*]

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

source-port

Syntax **source-port** *port*
source-port grpc
no source-port

Context [Tree] (config>system>management-interface>remote-management source-port)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system management-interface remote-management source-port

Description This command configures the TCP port local to this device that NISH uses to send packets to this node.

If this command is also configured for a specific manager in the **config**>**system**>**management-interface**>**remote-management**>**manager** context, that configuration takes precedence.

The **no** form of this command causes the system to select the default gRPC port, 57400.

Default source-port grpc

Parameters *port* — Specifies the TCP source port.

Values 1 to 65535

grpc — Keyword that specifies the default gRPC protocol port as the source port.

Platforms All

source-port

Syntax **source-port** *port*
source-port grpc
no source-port

Context **[Tree]** (config>system>management-interface>remote-management>manager source-port)

Full Context configure system management-interface remote-management manager source-port

Description This command configures the TCP port local to this device that this NISH manager uses to send packets to this node.

This command takes precedence over the same command configured in the global context (**config**>**system**>**management-interface**>**remote-management**).

The **no** form of this command causes the source port to be inherited from the global context (**config**>**system**>**management-interface**>**remote-management**).

Parameters *port* — Specifies the TCP source port.

Values 1 to 65535

Default 57400

grpc — Keyword that specifies the default gRPC protocol port as the source port.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.290 source-prefix

source-prefix

Syntax [**no**] **source-prefix**

Context **[Tree]** (config>cflowd>collector>aggregation source-prefix)

Full Context configure cflowd collector aggregation source-prefix

Description This command configures cflowd aggregation based on source prefix information.

The **no** form of this command removes this type of aggregation from the collector configuration.

Platforms All

23.291 source-prefix-list

source-prefix-list

Syntax **source-prefix-list** *prefix-list-name*
no source-prefix-list

Context **[Tree]** (config>service>vprn>nat>inside source-prefix-list)
[Tree] (config>router>nat>inside source-prefix-list)

Full Context configure router nat inside source-prefix-list
configure service vprn nat inside source-prefix-list

Description This command references the **nat-prefix-list** that contains source IP addresses on the inside (private side).

The source IP addresses on the inside must be known in advance in a **dnat-only** instance. This is required so the corresponding routes can be installed in the routing table and thus the downstream traffic is properly routed towards the MS-ISAs where the original translation was performed (and state is kept).

In the **dnat-only** case, it is mandatory that the inside (private side) and the outside (public side) are in separated VPRNs.

Default none

Parameters *prefix-list-name* — Specifies the name, up to 32 characters in length, of the NAT prefix list that contains the source IP addresses (original IP addresses).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.292 source-udp-port

source-udp-port

Syntax **source-udp-port** *udp-port-number*
no source-udp-port

Context **[Tree]** (config>oam-pm>session>ip source-udp-port)

Full Context configure oam-pm session ip source-udp-port

Description This command should only be used if a TWAMP Client is used to establish a TCP connection and communicate the test parameters to a TWAMP Server over TWAMP TCP Control and the test is launched from OAM-PM (Session-Sender). This command should not be used when the reflection point is a TWAMP Light reflector that does not require TCP TWAMP Control. When this command is included, the source UDP range is restricted. When this command is omitted, the source UDP port is dynamically allocated by the system.

The **no** form of this command removes the source UDP port setting when the default allocation is used.

Parameters *udp-port-number* — Specifies the UDP source port.

Values 64374 to 64383

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.293 source-vtep-security

source-vtep-security

Syntax [**no**] **source-vtep-security**

Context **[Tree]** (config>service>vpls>vxlan source-vtep-security)

Full Context configure service vpls vxlan source-vtep-security

Description This command enables the outer IP Source Address lookup of incoming VXLAN packets, and discards those coming from untrusted VTEPs. The list of trusted VTEPs is shown in the **show service vxlan** command. Specifically, it shows the existing learned EVPN VTEPs (always trusted), and the statically configured VTEPs in any service (Epipe and VPLS).

The command is supported in VXLAN instances with static egress VTEPs or VXLAN instances with EVPN created VTEPs.

The **no** version of this command disables the outer IP source address lookup.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no source-vtep-security

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.294 sp-reverse-route

sp-reverse-route

Syntax **sp-reverse-route** [**ignore-default-route**]
no sp-reverse-route

Context **[Tree]** (config>ipsec>tnl-temp sp-reverse-route)

Full Context configure ipsec tunnel-template sp-reverse-route

Description This command enables the system to automatically create a reverse route based on dynamic LAN-to-LAN tunnel's TSi in private service.

If **ignore-default-route** is specified, the system ignores any full range traffic selector when creating a reverse route. Otherwise, the system refuses to create a CHILD_SA if any full range traffic selector is included in TSi.

The **no** form of this command disables sp-reverse-route.

Default no sp-reverse-route

Parameters **ignore-default-route** — Specifies to ignore any full range traffic selector in TSi.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.295 space

space

Syntax [**no**] **space**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment>command-completion space)

Full Context configure system management-interface cli md-cli environment command-completion space

Description This command enables completion on the space character.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default space

Platforms All

23.296 spb

spb

Syntax **spb** [*isis-instance*] [**fid** *fid*] [**create**]
no spb

Context **[Tree]** (config>service>vpls spb)
[Tree] (config>service>vpls>sap spb)
[Tree] (config>service>vpls>spoke-sdp spb)

Full Context configure service vpls sap spb
configure service vpls spb
configure service vpls spoke-sdp spb

Description This command enables Shortest Path Bridging (SPB) on a B-VPLS instance. SPB uses IS-IS that supports multiple instances, therefore an instance must be specified. The declaration of SPB in this context is the control configuration for the SPB. This is an SPB management interface and it manages the configuration for IS-IS. Various parameters that define this SPB instance are configured under this SPB instance. Several of the parameters are shared with other B-VPLS service instances using SPB.

SPB enables an instance of IS-IS protocol with the **no shutdown** command. Alternatively, the IS-IS protocol instance under SPB is disabled with the **shutdown** command in the **config>service>vpls b-vpls>spb** context.

A Forwarding Identifier (FID) is optionally specified which is an abstraction of the BVID used for forwarding in SPB. When no FID is configured the control VPLS is advertised with FID value 1. When a FID value is specified, the control VPLS is advertised and associated with the FID value specified. The default algorithm for any FID declared or implicit is low-path-id. When a FID is specified, the ect-algorithm can be specified for the FID and changed only when there are no VPLS, SAPs or SDP bindings associated with the FID. The FID for a control instance cannot be changed after it is created. To change a FID the SPB component would have to be shutdown, deleted and re-created with a new FID.

Note: SPB operates with disable-learning, disable aging and discard-unknown. The state of these commands is ignored when SPB is configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no spb

Parameters *isis-instance* — Specifies the instance ID for an SPB IS-IS instance.

Values 1024 to 2047 (4 available)

Default 1024

FID — Specifies the FID value.

Values 1 to 4095

Default 1

Platforms All

23.297 spbm-control-vpls

spbm-control-vpls

Syntax **spbm-control-vpls** *service-id* **fid** *fid*
no spbm-control-vpls

Context **[Tree]** (config>service>vpls>b-vpls spbm-control-vpls)

Full Context configure service vpls b-vpls spbm-control-vpls

Description This command associates a user B-VPLS with a particular control B-VPLS and a FID. The ECT algorithm and the behavior of unicast and multicast come from the association to the FID.

A Forwarding Identifier (FID) is specified which is an abstraction of the BVID used for forwarding in SPB. The ect-algorithm is associated with the FID and can be changed only when there are no VPLS, SAPs or SDP bindings associated with the FID. The FID must be independent from the FID assigned to other services.

Parameters *service-id* — The B-VPLS service identifier.

Values 1 to 2147483647 | *svc-name*: 64 characters max

fid — The forwarding identifier.

Values 1 to 4095

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.298 spe-address

spe-address

Syntax **spe-address** *global-id:prefix*
no spe-address

Context **[Tree]** (config>service>pw-routing spe-address)

Full Context configure service pw-routing spe-address

Description This command configures a single S-PE Address for the node to be used for dynamic MS-PWs. This value is used for the pseudowire switching point TLV used in LDP signaling, and is the value used by pseudowire status signaling to indicate the PE that originates a pseudowire status message. Configuration of this parameter is mandatory to enable dynamic MS-PW support on a node.

If the S-PE Address is not configured, spoke-sdps that use dynamic MS-PWs and pw-routing local-prefixes cannot be configured on a T-PE. Furthermore, the node will send a label release for any label mappings received for FEC129 AII type 2.

The S-PE Address cannot be changed unless the dynamic ms-pw configuration is removed. Furthermore, changing the S-PE Address will also result in all dynamic MS-PWs for which this node is an S-PE being released. It is recommended that the S-PE Address should be configured for the life of an MS-PW configuration after reboot of the router.

The **no** form of this command removes the configured S-PE Address.

Default no spe-address

Parameters *global-id* — Specifies a 4-octet value that is unique to the service provider. For example, the global ID can contain the 2-octet or 4-octet value of the provider's Autonomous System Number (ASN).

Values

<global-id:prefix>:	<global-id>:{<prefix>| <ipaddress>}
global-id	1 to 4294967295
prefix	1 to 4294967295
ipaddress	a.b.c.d

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.299 speed

speed

Syntax **speed** {**10** | **100** | **1000** | **10000** | **25000** | **40000** | **50000** | **100000**}

Context **[Tree]** (config>port>ethernet speed)

Full Context configure port ethernet speed

Description For ports that support multiple speeds, this command configures the port speed to be used. This applies to the following:

- fast Ethernet when autonegotiate is disabled
- 10/100/1000 Ethernet when autonegotiate is disabled
- 10/1G ports supporting 10G SFP+ or 1G SFP
- 40/100G ports supporting QSFP28s on non-connector-based MDAs

If the port is configured to autonegotiate this parameter is ignored. Speed cannot be configured for ports that are part of a Link Aggregation Group (LAG).

Default dependent on port type

Parameters **10** — Sets the link to 10 Mb/s speed.

100 — Sets the link to 100 Mb/s speed.

1000 — Sets the link to 1000 Mb/s speed.

10000 — Sets the link to 10000 Mb/s speed.

25000 — Sets the link to 25000 Mb/s speed.

40000 — Sets the link to 40000 Mb/s speed.

50000 — Sets the link to 50000 Mb/s speed.

100000 — Sets the link to 100000 Mb/s speed.

Platforms All

speed

Syntax **speed** {**oc3** | **oc12**}
no speed

Context **[Tree]** (config>port>sonet-sdh speed)

Full Context configure port sonet-sdh speed

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the speed of a SONET/SDH port as either OC3 or OC12. The framer for this MDA operates in groups of four. Changing the port speed for a port requires resetting the framer and causes a slight disruption on all four ports. The first framer controls ports 1,2,3,4, the second framer controls ports 5,6,7,8 and so on.

To change the port speed on a SONET/SDH port, the port must be administratively shut down and all channels must be removed. When the port speed is changed, the default channel configuration is recreated.

The **no** form of this command reverts back to default.

This command is supported on TDM satellite.

Default speed oc12

Parameters **oc3** — Sets the speed of the port to OC-3.

oc12 — Sets the speed of the port to OC-12.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

speed

Syntax **speed** {**56** | **64**}

Context **[Tree]** (config>port>tdm>ds1>channel-group speed)
[Tree] (config>port>tdm>e1>channel-group speed)

Full Context configure port tdm ds1 channel-group speed
configure port tdm e1 channel-group speed

Description This command sets the speed of the DS-0 channels used in the associated channel-group.

Default speed 64

Parameters **56** — Specifies that 56k byte (7-bits per byte) encoding will be used for the associated DS-0 channels. This channel speed value is only supported on the m4-chds3-as and m12-chds3-as MDAs and on DS-1 channels (ESF and SF framing) and not on E-1 (G.704) channels.

64 — Specifies that 64k byte (8-bits per byte) encoding will be used for the associated DS-0 channels.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

speed

Syntax **speed** *speed*

Context **[Tree]** (bof speed)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context bof speed

Description This command configures the speed for the CPM management Ethernet port when autonegotiation is disabled in the running configuration and the Boot Option File (BOF).

If the port is configured to autonegotiate, this parameter is ignored.

Available speed options are dependent on the specific CPM variant in the system.

Default speed 100

Parameters *speed* — Sets the link speed, in Mb/s.

Values 10, 100, 1000

Platforms All

23.300 spf

spf

Syntax [**no**] **spf** [*level-number*] [*system-id*]

Context **[Tree]** (debug>router>isis spf)

Full Context debug router isis spf

Description This command enables debugging for IS-IS SFP.

The **no** form of the command disables debugging.

Parameters *system-id* — When specified, only the specified system-id is debugged. A 6-octet system identifier (xxxx.xxxx.xxxx).

level-number — Specifies the interface level (1, 2, or 1 and 2).

Platforms All

spf

Syntax **spf** [**type**] [*dest-addr*]
no spf

Context **[Tree]** (debug>router>ospf spf)
[Tree] (debug>router>ospf3 spf)

Full Context debug router ospf spf
debug router ospf3 spf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables debugging for OSPF SPF. Information regarding overall SPF start and stop times will be shown. To see detailed information regarding the SPF calculation of a given route, the route must be specified as an optional argument.

Parameters *type* — Specifies the area to debug.

Values intra-area, inter-area, external

dest-addr — Specifies the destination IP address to debug.

Platforms All

23.301 spf-wait

spf-wait

Syntax **spf-wait** *spf-wait* [**spf-initial-wait** *spf-initial-wait*] [**spf-second-wait** *spf-second-wait*]
no spf-wait

Context **[Tree]** (config>service>vpls>b-vpls>spb>timers spf-wait)

Full Context configure service vpls b-vpls spb timers spf-wait

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second and subsequent SPF calculations after a topology change occurs can be controlled with this command.

Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the *spf-wait* value. The SPF interval will stay at *spf-wait* value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to *spf-initial-wait*.

Default no spf-wait

Parameters *spf-wait* — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

Values 10 to 120000

Default 10000

spf-initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change.

Values 10 to 100000

Default 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spf-second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation.

Values 10 to 100000

Default 1000

spf-wait

Syntax **spf-wait** *spf-wait* [**spf-initial-wait** *spf-initial-wait*] [**spf-second-wait** *spf-second-wait*]
no spf-wait

Context **[Tree]** (config>service>vpls>spb>timers spf-wait)

Full Context configure service vpls spb timers spf-wait

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second and subsequent SPF calculations after a topology change occurs can be controlled with this command.

Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, and so on, until it reaches the *spf-wait* value. The SPF interval will stay at *spf-wait* value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to *spf-initial-wait*.

Note: The IS-IS timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default spf-wait 10000 spf-initial-wait 1000 spf-second-wait 1000

Parameters *spf-wait* — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

Values 10 to 120000

Default 10000

initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change

Values 10 to 100000

Default 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation

Values 10 to 100000

Default 1000

Platforms All

spf-wait

Syntax **spf-wait** *spf-wait* [**spf-initial-wait** *initial-wait*] [**spf-second-wait** *second-wait*]
no spf-wait

Context **[Tree]** (config>service>vprn>isis>timers spf-wait)

Full Context configure service vprn isis timers spf-wait

Description This command defines the maximum interval, in milliseconds, between two consecutive SPF calculations. Timers that determine when to initiate the first, second and subsequent SPF calculations after a topology change occurs can be controlled with this command.

Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the **spf-second-wait** interval. For example, if the **spf-second-wait** interval is 1000, then the next SPF will run after 2000 milliseconds, and the next SPF after that will run after 4000 milliseconds, and so on, until it reaches the *spf-wait* value. The SPF interval will stay at the *spf-wait* value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to the SPF *initial-wait* value.

Note: The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Parameters *spf-wait* — Specifies the maximum interval, in milliseconds, between two consecutive SPF calculations.

Values 10 to 120000

Default 10000

initial-wait — Specifies the initial SPF calculation delay, in milliseconds, after a topology change.

Values 10 to 100000

Default 1000

second-wait — Specifies the hold time, in milliseconds, between the first and second SPF calculation.

Values 10 to 100000

Default 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

spf-wait

Syntax **spf-wait** *max-spf-wait* [**spf-initial-wait** *spf-initial-wait*] [**spf-second-wait** *spf-second-wait*]
no spf-wait

Context **[Tree]** (config>service>vprn>ospf>timers spf-wait)
[Tree] (config>service>vprn>ospf3>timers spf-wait)

Full Context configure service vprn ospf timers spf-wait
configure service vprn ospf3 timers spf-wait

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second, and subsequent SPF calculations after a topology change occurs can be controlled with this command.

Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, and so on, until it reaches the **spf-wait** value. The SPF interval will stay at the **spf-wait** value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to *spf-initial-wait*.

Use the **no** form of this command to return to the default.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is ≥ 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Parameters *max-spf-wait* — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

Values 10 to 120000

Default 10000

spf-initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change.

Values 10 to 100000

Default 1000

spf-second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation.

Values 10 to 100000

Default 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

spf-wait

Syntax **spf-wait** *max-wait* [**initial-wait** *initial-wait*] [**second-wait** *second-wait*]
no spf-wait

Context **[Tree]** (config>router>bgp>optimal-route-reflection spf-wait)

Full Context configure router bgp optimal-route-reflection spf-wait

Description This command controls the interval between consecutive SPF calculations performed by the TE DB in support of BGP optimal route reflection. The time parameters of this command implement an exponential back-off algorithm.

The **no** form of this command causes a return to default values.

Default no spf-wait

Parameters *max-wait* — Specifies the maximum interval in seconds between two consecutive SPF calculations.

Values 1 to 600

Default 60

initial-wait *initial-wait* — Specifies the initial SPF calculation delay in seconds after a topology change.

Values 1 to 300

Default 5

second-wait *second-wait* — Specifies the delay in seconds between the first and second SPF calculation.

Values 1 to 300

Default 15

Platforms All

spf-wait

Syntax **spf-wait** *spf-wait* [**spf-initial-wait** *initial-wait*] [**spf-second-wait** *second-wait*]]
no spf-wait

Context **[Tree]** (config>router>isis>timers spf-wait)

Full Context configure router isis timers spf-wait

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second and subsequent SPF calculations after a topology change occurs can be controlled with this command.

Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the *spf-wait* value. The SPF interval will stay at *spf-wait* value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to *spf-initial-wait*.

Note: The timer granularity is 100 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default spf-wait 10000 spf-initial-wait 1000 spf-second-wait 1000

Parameters *spf-wait* — Specifies the maximum interval, in milliseconds, between two consecutive SPF calculations.

Values 10 to 120000

initial-wait — Specifies the initial SPF calculation delay, in milliseconds, after a topology change.

Values 10 to 100000

second-wait — Specifies the hold time, in milliseconds, between the first and second SPF calculation.

Values 10 to 100000

Platforms All

spf-wait

Syntax **spf-wait** *max-spf-wait* [**spf-initial-wait** *spf-initial-wait* [**spf-second-wait** *spf-second-wait*]]
no spf-wait

Context **[Tree]** (config>router>ospf>timers spf-wait)
[Tree] (config>router>ospf3>timers spf-wait)

Full Context configure router ospf timers spf-wait
configure router ospf3 timers spf-wait

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second, and subsequent SPF calculations after a topology change occurs can be controlled with this command. Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, and so on, until it reaches the **spf-wait** value. The SPF interval will stay at the **spf-wait** value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to *spf-initial-wait*.

The timer must be entered in increments of 100 milliseconds. Values entered that do not match this requirement will be rejected.

Use the **no** form of this command to return to the default.

Note: The timer granularity is 10 ms if the value is less than 500 ms, and 100 ms if the value is greater than or equal to 500 ms. Timer values are rounded down to the nearest granularity, for example a configured value of 550 ms is internally rounded down to 500 ms.

Default spf-wait 10000

Parameters *max-spf-wait* — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

Values 10 to 120000

Default 10000

spf-initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change.

Values 10 to 100000

Default 1000

spf-second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation.

Values 10 to 100000

Default 1000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.302 spi

spi

Syntax **spi** *spi*
no spi

Context **[Tree]** (config>ipsec>static-sa spi)

Full Context configure ipsec static-sa spi

Description This command configures the SPI key value for an IPsec manual SA.

This command specifies the SPI (Security Parameter Index) used to lookup the instruction to verify and decrypt the incoming IPsec packets when the value of the **direction** command is **inbound**.

The SPI value specifies the SPI that will be used in the encoding of the outgoing packets when the when the value of the **direction** command is **outbound**. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.

If **no spi** is selected, then this static SA cannot be used.

The **no** form of this command reverts to the default value.

Default no spi

Parameters *spi* — Specifies the security parameter index for this SA.

Values 256 to 16383

Platforms All

23.303 spi-load-balancing

spi-load-balancing

Syntax [**no**] **spi-load-balancing**

Context **[Tree]** (config>service>vpls>load-balancing>config>service>template>vpls-template>load-balancing spi-load-balancing)

Full Context configure service vpls load-balancing config service template vpls-template load-balancing spi-load-balancing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables use of the SPI in hashing for ESP/AH encrypted IPv4/v6 traffic. This is a per interface setting.

The **no** form disables the SPI function.

Default no spi-load-balancing

spi-load-balancing

Syntax [**no**] **spi-load-balancing**

Context **[Tree]** (config>service>ies>if>load-balancing spi-load-balancing)

Full Context configure service ies interface load-balancing spi-load-balancing

Description This command enables use of the SPI in hashing for ESP/AH encrypted IPv4/v6 traffic. This is a per interface setting.

The **no** form disables the SPI function.

Default no spi-load-balancing

Platforms All

spi-load-balancing

Syntax [**no**] **spi-load-balancing**

Context **[Tree]** (config>service>vprn>nw-if>load-balancing spi-load-balancing)

Full Context configure service vprn network-interface load-balancing spi-load-balancing

Description This command enables use of the SPI in hashing for ESP/AH encrypted IPv4/v6 traffic. This is a per interface setting.

The **no** form disables the SPI function.

Default no spi-load-balancing

Platforms All

spi-load-balancing

Syntax [**no**] **spi-load-balancing**

Context **[Tree]** (config>router>if>load-balancing spi-load-balancing)

Full Context configure router interface load-balancing spi-load-balancing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables use of the SPI in hashing for ESP/AH encrypted IPv4/v6 traffic. This is a per interface setting.

The **no** form disables the SPI function.

Default no spi-load-balancing

Platforms All

23.304 spi-sharing-group-id

spi-sharing-group-id

Syntax **spi-sharing-group-id** *group-id*
no spi-sharing-group-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings spi-sharing-group-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings spi-sharing-group-id)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings spi-sharing-group-id
configure subscriber-mgmt local-user-db ppp host identification-strings spi-sharing-group-id

Description This command configures the SLA Profile Instance (SPI) sharing group identifier for an IPoE or PPPoE session. It overrides the default SPI sharing method (**def-instance-sharing**) configured in the SLA profile.

When an spi-sharing-group-id is configured, the IPoE or PPPoE session shares the SLA Profile Instance with other IPoE or PPPoE sessions from the same subscriber that: have the same SLA profile associated, are active on the same SAP, and have the same group identifier.

Configuring an **spi-sharing-group-id** *group-id* for an IPoE host, when the IPoE session is disabled on the group interface, results in a setup failure.

The **no** form of this command returns the SPI sharing group identifier to its default.

Parameters *group-id* — Specifies the SPI group identifier.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.305 spi-sharing-id

spi-sharing-id

Syntax [**no**] **spi-sharing-id**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute spi-sharing-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute spi-sharing-id

Description This command enables RADIUS accounting messages to include the Alc-SPI-Sharing-Id RADIUS attribute. Together with the SLA profile name, this attribute provides details on the applicable SPI or queuing instance for this accounting session.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.306 split-horizon

split-horizon

Syntax **split-horizon**
no split-horizon

Context **[Tree]** (config>service>vprn>bgp split-horizon)
[Tree] (config>service>vprn>bgp>group split-horizon)
[Tree] (config>service>vprn>bgp>group>neighbor split-horizon)

Full Context configure service vprn bgp group neighbor split-horizon
configure service vprn bgp group split-horizon
configure service vprn bgp split-horizon

Description This command enables the use of split-horizon. When applied globally, to a group, or a specific peer, split-horizon prevents routes from being reflected back to a peer that sends the best route. It applies to routes of all address families and to any type of sending peer; confed-EBGP, EBGP and IBGP.

The configuration default is **no split-horizon**, meaning that no effort is taken to prevent a best route from being reflected back to the sending peer.

Caution: Use of the **split-horizon** command may have a detrimental impact on peer and route scaling and therefore operators are encouraged to use it only when absolutely needed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables split horizon command which allows the lower level to inherit the setting from an upper level.

Default no split-horizon

Platforms All

split-horizon

Syntax **split-horizon** {**enable** | **disable**}
no split-horizon

Context **[Tree]** (config>service>vprn>rip split-horizon)
[Tree] (config>service>vprn>rip>group split-horizon)
[Tree] (config>service>vprn>rip>group>neighbor split-horizon)
[Tree] (config>service>vprn>ripng split-horizon)
[Tree] (config>service>vprn>ripng>group split-horizon)
[Tree] (config>service>vprn>ripng>group>neighbor split-horizon)

Full Context configure service vprn rip group neighbor split-horizon
configure service vprn rip group split-horizon
configure service vprn rip split-horizon
configure service vprn ripng group neighbor split-horizon
configure service vprn ripng group split-horizon
configure service vprn ripng split-horizon

Description This command enables the use of split-horizon. RIP uses split horizon with poison reverse to protect from such problems as “counting to infinity”. Split horizon with poison reverse means that routes learned from a neighbor through a given interface are advertised in updates out of the same interface but with a metric of 16 (infinity).

The **no** form of this command disables the **split-horizon** command, which allows the lower level to inherit the setting from an upper level.

Default split-horizon enable

Parameters **enable** — Enables split horizon and poison reverse.

disable — Enables split horizon without poison reverse. This allows the routes to be readvertised on interfaces other than the interface that learned the route, with the advertised metric equaling an increment of the metric-in value.This configuration parameter can be set at three levels: global level (applies to all groups and neighbor interfaces), group level (applies to all neighbor interfaces in the group) or neighbor level (only applies to the specified neighbor interface). The most specific value is used. In particular, if no value is set (**no split-horizon**), the lower level inherits the setting from the less-specific level.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

split-horizon

Syntax [**no**] **split-horizon**

Context **[Tree]** (config>router>bgp split-horizon)
[Tree] (config>router>bgp>group split-horizon)
[Tree] (config>router>bgp>group>neighbor split-horizon)

Full Context configure router bgp group neighbor split-horizon
configure router bgp group split-horizon
configure router bgp split-horizon

Description This command enables the use of split-horizon. Split-horizon prevents routes from being reflected back to a peer that sends the best route. It applies to routes of all address families and to any type of sending peer; confed-EBGP, EBGP and IBGP.

The configuration default is **no split-horizon**, meaning that no effort is taken to prevent a best route from being reflected back to the sending peer.

Default no split-horizon

Platforms All

split-horizon

Syntax **split-horizon** {**enable** | **disable**}
no split-horizon

Context **[Tree]** (config>router>rip split-horizon)
[Tree] (config>router>rip>group split-horizon)
[Tree] (config>router>rip>group>neighbor split-horizon)
[Tree] (config>router>ripng split-horizon)
[Tree] (config>router>ripng>group split-horizon)
[Tree] (config>router>ripng>group>neighbor split-horizon)

Full Context configure router rip group neighbor split-horizon
configure router rip group split-horizon
configure router rip split-horizon
configure router ripng group neighbor split-horizon
configure router ripng group split-horizon
configure router ripng split-horizon

Description This command enables the use of split-horizon.

RIP uses split-horizon with poison-reverse to protect from such problems as “counting to infinity”. Split-horizon with poison reverse means that routes learned from a neighbor through a given interface are advertised in updates out of the same interface but with a metric of 16 (infinity).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **split-horizon disable** command enables split horizon without poison reverse. This allows the routes to be re-advertised on interfaces other than the interface that learned the route, with the advertised metric equaling an increment of the metric-in value.

This configuration parameter can be set at three levels: global level (applies to all groups and neighbor interfaces), group level (applies to all neighbor interfaces in the group) or neighbor level (only applies to the specified neighbor interface). The most specific value is used. In particular if no value is set (**no split-horizon**), the setting from the less specific level is inherited by the lower level.

The **no** form of the command disables split horizon command which allows the lower level to inherit the setting from an upper level.

Default enabled

Parameters **enable** — Specifies enable split horizon and poison reverse.

disable — Specifies disable split horizon allowing routes to be re-advertised on the same interface on which they were learned with the advertised metric incremented by the **metric-in** value.

Platforms All

23.307 split-horizon-group

split-horizon-group

Syntax **split-horizon-group** [*group-name*] [**residential-group**] [**create**]

Context **[Tree]** (config>service>vpls split-horizon-group)

Full Context configure service vpls split-horizon-group

Description This command creates a new split horizon group for the VPLS instance. Traffic arriving on a SAP or spoke-SDP within this split horizon group will not be copied to other SAPs or spoke-SDPs in the same split horizon group.

A split horizon group must be created before SAPs and spoke-SDPs can be assigned to the group.

The split horizon group is defined within the context of a single VPLS. The same group-name can be re-used in different VPLS instances.

Up to 30 split horizon groups can be defined per VPLS instance. Half are supported in i-VPLS.

The **no** form of this command removes the group name from the configuration.

Default A split horizon group is by default not created as a residential-group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-name* — Specifies the name of the split horizon group to which the SDP belongs

residential-group — Defines a split horizon group as a residential split horizon group (RSHG). Doing so entails that:

a) SAPs which are members of this Residential Split Horizon Group will have:

- Double-pass queuing at ingress as default setting (can be disabled)
- STP disabled (cannot be enabled)
- ARP reply agent enabled per default (can be disabled)
- MAC pinning enabled per default (can be disabled)
- Downstream broadcast packets are discarded thus also blocking the unknown, flooded traffic
- Downstream multicast packets are allowed when IGMP snooping is enabled

b) Spoke SDPs which are members of this Residential Split Horizon Group will have:

- Downstream multicast traffic supported
- Double-pass queuing is not applicable
- STP is disabled (can be enabled)
- ARP reply agent is not applicable (dhcp-lease-states are not supported on spoke-SDPs)
- MAC pinning enabled per default (can be disabled)

Platforms All

split-horizon-group

Syntax **split-horizon-group** *group-name*

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only split-horizon-group)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters split-horizon-group

Description This command specifies the name of the split horizon group to which the MSAP belongs.

Parameters *group-name* — Specifies the split horizon group name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

split-horizon-group

Syntax **split-horizon-group** *name*
no split-horizon-group

Context **[Tree]** (config>service>vpls>bgp-evpn>mpls split-horizon-group)

Full Context configure service vpls bgp-evpn mpls split-horizon-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the user to configure an explicit split-horizon-group for all BGP-EVPN MPLS destinations that can be shared by other SAPs and/or spoke SDPs. The use of explicit split-horizon-groups for EVPN-MPLS and spoke SDPs allows the integration of VPLS and EVPN-MPLS networks.

If the **split-horizon-group** command for **bgp-evpn>mpls>** is not used, the default split-horizon-group (that contains all the EVPN destinations) is still used, but it is not possible to refer to it on SAPs/spoke SDPs. User-configured split-horizon-groups can be configured within the service context. The same group-name can be associated to SAPs, spoke SDPs, pw-templates, pw-template-bindings and EVPN-MPLS destinations. The configuration of **bgp-evpn>mpls> split-horizon-group** will only be allowed if **bgp-evpn>mpls** is shutdown; no changes are allowed when bgp-evpn>mpls is **no shutdown**.

When the SAPs and/or spoke SDPs (manual or BGP-AD-discovered) are configured within the same **split-horizon-group** as the EVPN-MPLS endpoints, MAC addresses will still be learned on them but they will not be advertised in BGP-EVPN. If provider-tunnel is enabled in the bgp-evpn service, the SAPs and SDP bindings that share the same split-horizon-group of the EVPN-MPLS provider-tunnel will be brought operationally down if the point-to-multipoint tunnel is operationally up.

Default no split-horizon-group

Parameters *name* — Specifies the split-horizon-group name.

Platforms All

split-horizon-group

Syntax **split-horizon-group** *group-name*
no split-horizon-group

Context **[Tree]** (config>service>vpls>site split-horizon-group)

Full Context configure service vpls site split-horizon-group

Description This command configures the value of split-horizon group associated with this site.

The **no** form of this command reverts the default.

Default no split-horizon-group

Parameters *group-name* — Specifies a split-horizon group name

Platforms All

split-horizon-group

Syntax **split-horizon-group** *group-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no split-horizon-group

Context [Tree] (config>service>pw-template split-horizon-group)

Full Context configure service pw-template split-horizon-group

Description This command creates a new split horizon group (SGH).

Comparing a “residential” SGH and a “regular” SHG is that a residential SHG:

- Has different defaults for the SAP or SDP that belong to this group (ARP reply agent enabled (SAP only), MAC pinning enabled). These can be disabled in the configuration.
- Does not allow enabling spanning tree (STP) on a SAP. It is allowed on an SDP.
- Does not allow for downstream broadcast (broadcast/unknown unicast) on a SAP. It is allowed on an SDP.
- On a SAP, downstream multicast is only allowed when IGMP is enabled (for which an MFIB state exists; only IP multicast); on a SDP, downstream mcast is allowed.

When the feature was initially introduced, residential SHGs were also using ingress shared queuing by default to increase SAP scaling.

A residential SAP (SAP that belongs to a RSHG) is used to scale the number of SAPs in a single VPLS instance. The limit depends on the hardware used and is higher for residential SAPs (where there is no need for egress multicast replication on residential SAPs) than for regular SAPs. Therefore, residential SAPs are useful in residential aggregation environments (for example, triple play networks) with a VLAN/subscriber model.

The **no** form of the command removes the group name from the configuration.

Parameters *group-name* — Specifies the name of the split horizon group to which the SDP belongs.

residential-group — Defines a split horizon group as a residential split horizon group (RSHG). Doing so entails that:

- SAPs which are members of this Residential Split Horizon Group will have:
  - Double-pass queuing at ingress as default setting (can be disabled)
  - STP disabled (cannot be enabled)
  - ARP reply agent enabled per default (can be disabled)
  - MAC pinning enabled per default (can be disabled)
  - Downstream Broadcast packets are discarded thus also blocking the unknown, flooded traffic
  - Downstream Multicast packets are allowed when IGMP snooping is enabled
- Spoke SDPs which are members of this Residential Split Horizon Group will have:
  - Downstream multicast traffic supported
  - Double-pass queuing is not applicable
  - STP is disabled (can be enabled)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- ARP reply agent is not applicable on the 7750 SR and 7450 ESS (dhcp-lease-states are not supported on spoke SDPs)
- MAC pinning enabled per default (can be disabled)

Platforms All

23.308 spoke-sdp

spoke-sdp

Syntax **spoke-sdp** *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**]
no spoke-sdp *sdp-id*[**:***vc-id*]

Context **[Tree]** (config>service>vpls spoke-sdp)

Full Context configure service vpls spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a VPLS service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. When removed, no packets are forwarded to the far-end router.

Default No *sdp-id* is bound to a service.

Special Cases **VPLS —** Several SDPs can be bound to a VPLS service. Each SDP must use unique *vc-ids*. An error message is generated if two SDP bindings with identical *vc-ids* terminate on the same router. Split horizon groups can only be created in the scope of a VPLS service.

Parameters *sdp-id* — Specifies the SDP identifier

Values 1 to 32767

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vc-id — Specifies the virtual circuit identifier

Values 1 to 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. Changing the binding's VC type causes the binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

The VC type value for Ethernet is 0x0005.

The VC type value for an Ethernet VLAN is 0x0004.

Values ether, vlan

ether — Defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings.

The VLAN VC-type inserts one dot1q tag within each encapsulated Ethernet packet transmitted to the far end and strips one dotQ tag, if a tag is present, from traffic received on the pseudowire.

The system expects a symmetrical configuration with its peer, specifically it expects to remove the same number of VLAN tags from received traffic as it adds to transmitted traffic. As some of the related configuration parameters are local and not communicated in the signaling plane, an asymmetrical behavior cannot always be detected and so cannot be blocked. Consequently, protocol extractions will not necessarily function for asymmetrical configurations as they would with a symmetrical configurations resulting in an unexpected operation.

group-name — Specifies the name of the split horizon group to which the SDP belongs

endpoint — Specifies the service endpoint to which this SDP bind is attached. The service ID of the SDP binding must match the service ID of the service endpoint.

no endpoint — Removes the association of a spoke SDP with an explicit endpoint name

root-leaf-tag — Specifies a tagging spoke SDP under an E-Tree VPLS. When a tag SDP binding is required, it is created with a root-leaf-tag flag. Only VLAN tag SDP bindings are supported. The VLAN type must be set to VC VLAN type. The root-leaf-tag parameter indicates this SDP binding is a tag SDP that will use a default VID tag of 1 for root and 2 for leaf. The SDP binding tags egress E-Tree traffic with root and leaf VIDs as appropriate. Root and leaf VIDs are only significant between peering VPLS but the values must be consistent on each end. On ingress a tag SDP binding removes the VID tag on the interface between VPLS in the same E-Tree service. The tag SDP receives root tagged traffic and marks the traffic with a root indication internally. This option is not available on BGP EVPN-enabled E-Tree services.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

leaf-ac — Specifies an access (AC) spoke SDP binding under a E-Tree VPLS as a leaf access (AC) SDP. The default E-Tree SDP binding type is a root-ac if *leaf-ac* or *root-leaf-tag* is not specified at SDP creation. This option is only available when the VPLS is designated as an E-Tree VPLS. BGP EVPN-enabled E-Tree VPLS services support the **leaf-ac** option.

Platforms All

spoke-sdp

Syntax **spoke-sdp** *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**] **endpoint** *endpoint* **root-leaf-tag**
spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**] **endpoint** *endpoint* **leaf-ac**
spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**] [**no-endpoint**]
spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**] **endpoint** *endpoint*
spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**] [**no-endpoint**] **leaf-ac**
spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] [**create**] [**no-endpoint**] **root-leaf-tag**
no spoke-sdp *sdp-id*[**:***vc-id*]

Context **[Tree]** (config>service>vpls spoke-sdp)

Full Context configure service vpls spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP).

A spoke SDP is treated like the equivalent of a traditional bridge port where flooded traffic received on the spoke SDP is replicated on all other ports (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a VPLS service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end 7450 ESS or 7750 SR devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Special Cases **VPLS —** Several SDPs can be bound to a VPLS service. Each SDP must use unique *vc-ids*. An error message is generated if two SDP bindings with identical *vc-ids* terminate on the same router. Split horizon groups can only be created in the scope of a VPLS service.

Parameters *sdp-id* — Specifies the SDP identifier.

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier.

Values 1 to 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the binding's VC type causes the binding to signal the new VC type to the far end when signaling is enabled.

VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

The VC type value for Ethernet is 0x0005.

The VC type value for an Ethernet VLAN is 0x0004.

Values ether, vlan

ether — Defines the VC type as Ethernet. The **ethernet**, **vlan,** and **vpls** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke SDP binding (hex 5).

vlan — Defines the VC type as VLAN. The **ethernet**, **vlan,** and **vpls** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. The VLAN VC-type requires at least one dot1Q tag within each encapsulated Ethernet packet transmitted to the far end.

group-name — Specifies the name of the split horizon group to which the SDP belongs.

root-leaf-tag — Specifies a SAP as a root leaf tag SDP. This option is only available when the VPLS is designated as an E-Tree VPLS.

leaf-tag-vid — Specifies to replace the outer SDP ID for leaf traffic. The leaf tag VID is only significant between peering VPLS but the values must be consistent on each end.

leaf-ac — Specifies a SDP as a leaf access (AC) SDP. The default E-Tree SAP type is root AC if **leaf-ac** (or **root-leaf-tag**) is not specified at SDP creation. This option is only available when the VPLS is designated as an E-Tree VPLS.

create — Keyword used to create the spoke SDP. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id* [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name*] **endpoint** [**no-endpoint**] [**root-leaf-tag** | **leaf-ac**]
no spoke-sdp *sdp-id:vc-id*

Context **[Tree]** (config>service>vpls spoke-sdp)

Full Context configure service vpls spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP). A spoke-SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke-SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a VPLS service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the sdp-id does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. After it is removed, no packets are forwarded to the far-end router.

Parameters *sdp-id* — Specifies the SDP identifier

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier

Values 1 to 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

The VC type value for Ethernet is 0x0005.

The VC type value for an Ethernet VLAN is 0x0004.

Values ether, vlan

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ether — Defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke-SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke-SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke-SDP bindings. The VLAN VC-type inserts one dot1q tag within each encapsulated Ethernet packet transmitted to the far end and strips one dotQ tag, if a tag is present, from traffic received on the pseudowire.

Note: The system expects a symmetrical configuration with its peer, specifically it expects to remove the same number of VLAN tags from received traffic as it adds to transmitted traffic. As some of the related configuration parameters are local and not communicated in the signaling plane, an asymmetrical behavior cannot always be detected and so cannot be blocked. Consequently, protocol extractions will not necessarily function for asymmetrical configurations as they would with a symmetrical configurations resulting in an unexpected operation.

group-name — Specifies the name of the split horizon group to which the SDP belongs.

endpoint — Specifies the service endpoint to which this SDP bind is attached. The service ID of the SDP binding must match the service ID of the service endpoint.

no endpoint — Removes the association of a spoke-SDP with an explicit endpoint name.

root-leaf-tag — Specifies a tagging spoke-SDP under an E-Tree VPLS. When a tag SDP binding is required, it is created with a root-leaf-tag flag. Only VLAN tag SDP bindings are supported. The VLAN type must be set to VC VLAN type. The root-leaf-tag parameter indicates this SDP binding is a tag SDP that will use a default VID tag of 1 for root and 2 for leaf. The SDP binding tags egress E-Tree traffic with root and leaf VIDs as appropriate. Root and leaf VIDs are only significant between peering VPLS but the values must be consistent on each end. On ingress a tag SDP binding removes the VID tag on the interface between VPLS in the same E-Tree service. The tag SDP receives root tagged traffic and marks the traffic with a root indication internally. This option is not available on BGP EVPN-enabled E-Tree services.

leaf-ac — Specifies an access (AC) spoke-SDP binding under a E-Tree VPLS as a leaf access (AC) SDP. The default E-Tree SDP binding type is a root-ac if *leaf-ac* or *root-leaf-tag* is not specified at SDP creation. This option is only available when the VPLS is designated as an E-Tree VPLS. BGP EVPN-enabled E-Tree VPLS services support the **leaf-ac** option.

Platforms All

spoke-sdp

Syntax **spoke-sdp** *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**split-horizon-group** *group-name***]** **endpoint** [**no-endpoint**] [**root-leaf-tag** | **leaf-ac**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no spoke-sdp *sdp-id*[:*vc-id*]

Context [Tree] (config>service>vpls spoke-sdp)

Full Context configure service vpls spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP). A spoke-SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke-SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a VPLS service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No *sdp-id* is bound to a service.

Special Cases **VPLS —** Several SDPs can be bound to a VPLS service. Each SDP must use unique *vc-ids*. An error message is generated if two SDP bindings with identical *vc-ids* terminate on the same router. Split horizon groups can only be created in the scope of a VPLS service.

Parameters *sdp-id* — Specifies the SDP identifier

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier

Values 1 to 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

The VC type value for Ethernet is 0x0005.

The VC type value for an Ethernet VLAN is 0x0004.

Values ether, vlan

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ether — Defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke-SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke-SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke-SDP bindings. The VLAN VC-type inserts one dot1q tag within each encapsulated Ethernet packet transmitted to the far end and strips one dotQ tag, if a tag is present, from traffic received on the pseudowire.

Note: The system expects a symmetrical configuration with its peer, specifically it expects to remove the same number of VLAN tags from received traffic as it adds to transmitted traffic. As some of the related configuration parameters are local and not communicated in the signaling plane, an asymmetrical behavior cannot always be detected and so cannot be blocked. Consequently, protocol extractions will not necessarily function for asymmetrical configurations as they would with a symmetrical configurations resulting in an unexpected operation.

group-name — Specifies the name of the split horizon group to which the SDP belongs

endpoint — Specifies the service endpoint to which this SDP bind is attached. The service ID of the SDP binding must match the service ID of the service endpoint.

no endpoint — Removes the association of a spoke-SDP with an explicit endpoint name

root-leaf-tag — Specifies a tagging spoke-SDP under an E-Tree VPLS. When a tag SDP binding is required, it is created with a root-leaf-tag flag. Only VLAN tag SDP bindings are supported. The VLAN type must be set to VC VLAN type. The root-leaf-tag parameter indicates this SDP binding is a tag SDP that will use a default VID tag of 1 for root and 2 for leaf. The SDP binding tags egress E-Tree traffic with root and leaf VIDs as appropriate. Root and leaf VIDs are only significant between peering VPLS but the values must be consistent on each end. On ingress a tag SDP binding removes the VID tag on the interface between VPLS in the same E-Tree service. The tag SDP receives root tagged traffic and marks the traffic with a root indication internally. This option is not available on BGP EVPN-enabled E-Tree services.

leaf-ac — Specifies an access (AC) spoke-SDP binding under a E-Tree VPLS as a leaf access (AC) SDP. The default E-Tree SDP binding type is a root-ac if *leaf-ac* or *root-leaf-tag* is not specified at SDP creation. This option is only available when the VPLS is designated as an E-Tree VPLS. BGP EVPN-enabled E-Tree VPLS services support the **leaf-ac** option.

Platforms All

spoke-sdp

Syntax [**no**] **spoke-sdp** *sdp-id*

Context **[Tree]** (config>service>vprn spoke-sdp)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP).

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a VPRN service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end 7750 SR devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Special Cases **VPRN —** Several SDPs can be bound to a VPRN service. Each SDP must be destined to a different 7750 SR OS. If two *sdp-id* bindings terminate on the same 7750 SR, an error occurs and the second SDP binding is rejected.

Parameters *sdp-id* — Specifies the SDP identifier. Allowed values are integers in the range of 1 and 17407 for existing SDPs.

vc-id — Specifies the virtual circuit identifier.

Values 1 to 4294967295

Platforms All

spoke-sdp

Syntax **spoke-sdp** *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **ipipe**}] [**create**]
no spoke-sdp *sdp-id*[**:***vc-id*]

Context **[Tree]** (config>service>ies>if spoke-sdp)
[Tree] (config>service>ies>redundant-interface spoke-sdp)
[Tree] (config>service>vprn>if spoke-sdp)
[Tree] (config>service>vprn>red-if spoke-sdp)

Full Context configure service ies interface spoke-sdp
configure service ies redundant-interface spoke-sdp
configure service vprn interface spoke-sdp
configure service vprn redundant-interface spoke-sdp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command binds a service to an existing Service Distribution Point (SDP).

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with an IES service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

Class-based forwarding is not supported on a spoke SDP used for termination on an IES or VPRN services. All packets are forwarded over the default LSP.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router. The spoke SDP must be shut down first before it can be deleted from the configuration.

Default no spoke-sdp

Special Cases **IES —** At most, only one *sdp-id* can be bound to an IES service.

Parameters *sdp-id* — Specifies the SDP identifier. Allowed values are integers in the range of 1 and 17407 for existing SDPs.

vc-id — Specifies the virtual circuit identifier.

Values 1 to 4294967295

vc-type — Specifies the encapsulation and pseudowire type for the spoke SDP.

Values ether: specifies Ethernet pseudowire as the type of virtual circuit (VC) associated with the SDP binding

ipipe: specifies Ipipe pseudowire as the type of virtual circuit (VC) associated with the SDP binding

Default ether

create — Keyword used to create the spoke SDP. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp
- configure service ies redundant-interface spoke-sdp

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies interface spoke-sdp
- configure service vprn interface spoke-sdp

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id*
no spoke-sdp

Context **[Tree]** (config>service>vpls>site spoke-sdp)

Full Context configure service vpls site spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP).

The **no** form of this command removes the parameter from the configuration.

Parameters *sdp-id* — Specifies the SDP identifier

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier.

Values 1 to 429496729

Platforms All

spoke-sdp

Syntax **spoke-sdp** *sdp-id*[**:***vc-id*] [**no-endpoint**]
spoke-sdp *sdp-id*[:*vc-id*] **endpoint** *endpoint-name* [**icb**]
no spoke-sdp *sdp-id*[**:***vc-id*]

Context **[Tree]** (config>service>apipe spoke-sdp)
[Tree] (config>service>cpipe spoke-sdp)
[Tree] (config>service>fpipe spoke-sdp)
[Tree] (config>service>ipipe spoke-sdp)

Full Context configure service apipe spoke-sdp
configure service cpipe spoke-sdp
configure service fpipe spoke-sdp
configure service ipipe spoke-sdp

Description This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end SR/ESS devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No *sdp-id* is bound to a service.

Parameters *sdp-id* — The SDP identifier.

Values 1 to 32767

vc-id — The virtual circuit identifier.

Values 1 to 4294967295

no-endpoint — Adds or removes a spoke SDP association.

endpoint-name — Specifies the name of the service endpoint.

icb — Configures the spoke SDP as an inter-chassis backup SDP binding.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp
- configure service fpipe spoke-sdp

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp

All

- configure service ipipe spoke-sdp

spoke-sdp

Syntax **spoke-sdp** *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**create**] [**no-endpoint**]
spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**create**] **endpoint** *endpoint-name* [**icb**]
no spoke-sdp *sdp-id*[**:***vc-id*]

Context **[Tree]** (config>service>epipe spoke-sdp)

Full Context configure service epipe spoke-sdp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with an Epipe, VPLS, VPRN, VPRN service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

This command can also be used to associate a GRE tunnel carrying Ethernet payload with an Epipe and terminate it on a PW port referenced within the same Epipe service. The spoke SDP represents a L2oGRE tunnel with SDP delivery type set to **eth-gre-bridged**. With this configuration, the **vc-id** is unused since there is no multiplexing of Ethernet payload within the same tunnel. The **vc-id** value is included only to maintain the expected spoke SDP structure within an EPIPE service. For L2oGRE tunnels, the **vc-id** can be set to any arbitrary value within its configurable range.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No *sdp-id* is bound to a service.

Special Cases **Epipe —** At most, only one *sdp-id* can be bound to an Epipe service. Since an Epipe is a point-to-point service, it can have, at most, two end points. The two end points can be one SAP and one SDP or two SAPs. Vc-switching VLLs are an exception. If the VLL is a “vc-switching” VLL, then the two endpoints must both be SDPs.

L2TPv3 SDP types are only supported on Epipe services and not other xpipe services.

Parameters *sdp-id* — The SDP identifier.

Values 1 to 17407

vc-id — The virtual circuit identifier. The VC-ID is not used with L2TPv3 SDPs or L2oGRE tunnels, however it must be configured.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled.

VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

The VC type value for Ethernet is 0x0005.

The VC type value for an Ethernet VLAN is 0x0004.

Values ethernet

ether — Defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke SDP binding.

vlan — Defines the VC type as VLAN. The top VLAN tag, if a VLAN tag is present, is stripped from traffic received on the pseudowire, and a VLAN tag is inserted when forwarding into the pseudowire. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings.

The VLAN VC-type requires at least one dot1q tag within each encapsulated Ethernet packet transmitted to the far end.

Note: The system expects a symmetrical configuration with its peer, specifically it expects to remove the same number of VLAN tags from received traffic as it adds to transmitted traffic. As some of the related configuration parameters are local and not communicated in the signaling plane, an asymmetrical behavior cannot always be detected and so cannot be blocked. Consequently, protocol extractions will not necessarily function for asymmetrical configurations as they would with a symmetrical configurations resulting in an unexpected operation.

no-endpoint — Removes the association of a spoke SDP with an explicit endpoint name.

endpoint-name — Specifies the name of the service endpoint.

icb — Specifies the spoke SDP as an inter-chassis backup SDP binding.

Platforms All

spoke-sdp

Syntax [**no**] **spoke-sdp** *spoke-id*

Context **[Tree]** (config>service>vpls>mac-move>primary-ports spoke-sdp)
[Tree] (config>service>vpls>mac-move>secondary-ports spoke-sdp)

Full Context configure service vpls mac-move primary-ports spoke-sdp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mac-move secondary-ports spoke-sdp

Description This command declares a specified spoke-SDP as a primary (or secondary) VPLS port.

Parameters *spoke-id* — Specifies the SDP ID to configure as the primary VPLS port

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier

Values 1 to 4294967295

Platforms All

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id* [**create**]
no spoke-sdp *sdp-id:vc-id*

Context **[Tree]** (config>service>ies>aarp-interface spoke-sdp)

Full Context configure service ies aarp-interface spoke-sdp

Description This command binds a service to an existing SDP. A spoke SDP is treated like the equivalent of a traditional bridge port where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default no spoke-sdp

Parameters *sdp-id* — Specifies the SDP identifier.

Values 1 to 17407

vc-id — Specifies the virtual circuit identifier. The VC-ID is not used with L2TPv3 SDPs, however it must be configured.

Values 1 to 4294967295

create — Keyword used to create the spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id* [**create**]
no spoke-sdp *sdp-id:vc-id*

Context **[Tree]** (config>service>vprn>aarp-interface spoke-sdp)

Full Context configure service vprn aarp-interface spoke-sdp

Description This command binds a service to an existing SDP. A spoke SDP is treated like the equivalent of a traditional bridge port where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default no spoke-sdp

Parameters *sdp-id* — — Specifies the SDP identifier.

Values 1 to 17407

vc-id — The virtual circuit identifier. The VC-ID is not used with L2TPv3 SDPs, however it must be configured.

Values 1 to 4294967295

create — Keyword used to create the spoke SDP.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id* [**create**] [**no-endpoint**]
spoke-sdp *sdp-id:vc-id* [**create**] **endpoint** *name* [**icb**]
no sdp *sdp-id:vc-id*

Context **[Tree]** (config>mirror>mirror-dest spoke-sdp)
[Tree] (config>mirror>mirror-dest>remote-source spoke-sdp)

Full Context configure mirror mirror-dest remote-source spoke-sdp
configure mirror mirror-dest spoke-sdp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command binds an existing (mirror) service distribution path (SDP) to the mirror destination service ID.

Spoke SDPs are used to send and receive mirrored traffic between mirror source and destination routers in a remote mirroring solution. A spoke SDP configured in the remote-source context (**remote-src>spoke-sdp**) is used on the destination router. A spoke SDP configured in the mirror service context (**mirror-dest>spoke-sdp**) is used on the source router.

The destination node should be configured with **remote-src>spoke-sdp** entries when using L2TPv3, MPLS-TP or LDP IPv6 LSP SDPs in the remote mirroring solution. For all other types of SDPs, r**emote-source>far-end** entries should be used.

Spoke SDPs are not applicable when routable LI encapsulation is employed (mirror-dest>encap).

A mirror destination service that is configured for a destination router must not be configured as for a source router.

The **no** form of this command removes the SDP binding from the mirror destination service.

Default An SDP ID is bound to a mirror destination service ID. If no SDP is bound to the service, the mirror destination will be local and cannot be sent to another router over the core network.

Parameters *sdp-id:vc-id* — Specifies a locally unique SDP identification (ID) number. The SDP ID must exist. If the SDP ID does not exist, an error will occur and the command will not execute.

For mirror services, the *vc-id* defaults to the *service-id*. However, there are scenarios where the *vc-id* is being used by another service. In this case, the SDP binding cannot be created. So, to avoid this, the mirror service SDP bindings now accepts *vc-ids*.

Values 1 to 17407

no-endpoint — Removes the association of a SAP or a SDP with an explicit endpoint name.

name — Specifies the name of the endpoint associated with the SAP.

icb — Indicates that the SDP is of type Inter-Chassis Backup (ICB). This is a special pseudowire used for MC-LAG and pseudowire redundancy application.

An explicitly named endpoint can have a maximum of one SAP and one ICB. Once a SAP is added to the endpoint, only one more object of type ICB SDP is allowed. The ICB SDP cannot be added to the endpoint if the SAP is not part of a MC-LAG instance. This means that all other SAP types cannot exist on the same endpoint as an ICB SDP since non Ethernet SAP cannot be part of a MC-LAG instance. Conversely, a SAP which is not part of a MC-LAG instance cannot be added to an endpoint which already has an ICB SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

An explicitly named endpoint, which does not have a SAP object, can have a maximum of four SDPs, which can include any of the following: a single primary SDP, one or many secondary SDPs with precedence, and a single ICB SDP.

Default Null. The user should explicitly configure this option at create time. The user can remove the ICB type simply by retyping the SDP configuration without the **icb** keyword.

Platforms All

spoke-sdp

Syntax **spoke-sdp** *sdp-id:vc-id* [**create**]
no spoke-sdp *sdp-id:vc-id*

Context **[Tree]** (config>service>vprn>ip-mirror-interface spoke-sdp)

Full Context configure service vprn ip-mirror-interface spoke-sdp

Description This command binds a service to an existing SDP.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with the VPRN service. SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router. The spoke SDP must be shut down before it can be deleted from the configuration.

Parameters *sdp-id* — Specifies SDP identifier.

Values 1 to 32767

vc-id — Specifies the virtual circuit identifier.

Values 1 to 4294967295

create — Keyword used to create an IP mirror interface.

Platforms All

23.309 spoke-sdp-fec

spoke-sdp-fec

Syntax **spoke-sdp-fec**
spoke-sdp-fec *spoke-sdp-fec-id* [**fec** *fec-type*] [**aii-type** *aii-type*] [**create**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spoke-sdp-fec *spoke-sdp-fec-id* **no-endpoint**
spoke-sdp-fec *spoke-sdp-fec-id* [**fec** *fec-type*] [**aii-type** *aii-type*] [**create**] **endpoint** *name* [**icb**]

Context **[Tree]** (config>service>epipe spoke-sdp-fec)

Full Context configure service epipe spoke-sdp-fec

Description This command binds a service to an existing Service Distribution Point (SDP), using a dynamic MS-PW.

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

When using dynamic MS-PWs, the particular SDP to bind-to is automatically selected based on the Target Attachment Individual Identifier (TAII) and the path to use, specified under spoke SDP FEC. The selected SDP will terminate on the first hop S-PE of the MS-PW. Therefore, an SDP must already be defined in the config>service>sdp context that reaches the first hop router of the MS-PW. The router will in order to associate an SDP with a service. If an SDP to that is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

It differs from the spoke-sdp command in that the spoke-sdp command creates a spoke SDP binding that uses a pseudowire with the PW ID FEC. However, the spoke-sdp-fec command enables pseudowires with other FEC types to be used. Only the Generalized ID FEC (FEC129) may be specified using this command.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Parameters *spoke-sdp-fec-id* — An unsigned integer value identifying the spoke SDP.

Values 1 to 4294967295

fec-type — An unsigned integer value for the type of the FEC used by the MS-PW.

Values 129 to 130

aii-type — An unsigned integer value for the Attachment Individual Identifier (AII) type used to identify the MS-PW endpoints.

Values 1 to 2

endpoint-name — Specifies the name of the service endpoint.

no endpoint — Adds or removes a spoke SDP association.

icb — Configures the spoke SDP as an inter-chassis backup SDP binding.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.310 spt-switchover-threshold

spt-switchover-threshold

Syntax **spt-switchover-threshold** {*grp-ip-address/mask* | *grp-ip-address netmask*} *spt-threshold*
spt-switchover-threshold *grp-ipv6-addr/prefix-length spt-threshold*
no spt-switchover-threshold {*grp-ip-address/mask* | *grp-ip-address netmask*}
no spt-switchover-threshold *grp-ipv6-addr/prefix-length*

Context **[Tree]** (config>service>vprn>pim spt-switchover-threshold)

Full Context configure service vprn pim spt-switchover-threshold

Description This command configures a shortest path tree (SPT tree) switchover threshold for a group prefix.

Parameters *grp-ip-address* — Specifies the multicast group address.

grp-ipv6-address — Specifies the multicast group address.

prefix-length — Specifies the address prefix length.

Values

grp-ipv6-address	: x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x [0 to FFFF]H d [0 to 255]D
prefix-length	[1 to 128]

mask — Defines the mask of the multicast-ip-address.

Values 4 to 32

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

spt-threshold — Specifies the configured threshold in kilobits per second (kb/s) for the group to which this (S,G) belongs. For a group G configured with a threshold, switchover to SPT for an (S,G) is attempted only if the (S,G)'s rate exceeds this configured threshold.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spt-switchover-threshold

Syntax **spt-switchover-threshold** {*grp-ipv4-prefix*|*ipv4-prefix-length* | *grp-ipv4-prefix netmask* | *grp-ipv6-prefix*|*ipv6-prefix-length*} *spt-threshold*
no spt-switchover-threshold {*grp-ipv4-prefix*|*ipv4-prefix-length* | *grp-ipv4-prefix netmask* | *grp-ipv6-prefix*|*ipv6-prefix-length*}

Context **[Tree]** (config>router>pim spt-switchover-threshold)

Full Context configure router pim spt-switchover-threshold

Description This command configures shortest path (SPT) tree switchover thresholds for group prefixes.

PIM-SM routers with directly connected routers receive multicast traffic initially on a shared tree rooted at the Rendezvous Point (RP). Once the traffic arrives on the shared tree and the source of the traffic is known, a switchover to the SPT tree rooted at the source is attempted.

For a group that falls in the range of a prefix configured in the table, the corresponding threshold value determines when the router should switch over from the shared tree to the source specific tree. The switchover is attempted only if the traffic rate on the shared tree for the group exceeds the configured threshold.

In the absence of any matching prefix in the table, the default behavior is to switchover when the first packet is seen. In the presence of multiple prefixes matching a given group, the most specific entry is used.

The **no** form of this command removes the parameters from the PIM configuration.

Parameters *grp-ipv4-prefix* — Specifies the group IPv4 multicast address in dotted decimal notation.

Values a.b.c.d

ipv4-prefix-length — Specifies the length of the IPv4 prefix.

Values 4 to 32

netmask — Specifies the netmask associated with the IPv4 prefix, expressed in dotted decimal notation. Network bits must be 1, and host bits must be 0.

Values a.b.c.d

grp-ipv6-prefix — Specifies the group IPv6 multicast address in hexadecimal notation.

Values xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
xx — 0 to FF (hex)

ipv6-prefix-length — Specifies the length of the IPv6 prefix.

Values 8 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spt-threshold — Specifies the configured threshold in kilobits per second (kb/s) for a group prefix. A switchover is attempted only if the traffic rate on the shared tree for the group exceeds this configured threshold. When the **infinity** keyword is specified, no switchover will occur at any time, regardless of the traffic level is detected.

Values 1 to 4294967294, infinity

Platforms All

23.311 squelch

squelch

Syntax [**no**] **squelch**

Context **[Tree]** (config>system>sync-if-timing>bits>output squelch)

Full Context configure system sync-if-timing bits output squelch

Description This command configures the behavior of the BITSout port when there is no valid reference selected. When enabled with no valid reference, no signal is sent out the port. When disabled with no valid reference, an AIS signal is presented along with the QL-DNU/TL-DUS SSM code if the signal format supports SSM.

Default no squelch

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.312 squelch-ingress-ctag-levels

squelch-ingress-ctag-levels

Syntax **squelch-ingress-ctag-levels** [*md-level* [*md-level*]]
no squelch-ingress-ctag-levels

Context **[Tree]** (config>service>epipe>sap>eth-cfm squelch-ingress-ctag-levels)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm squelch-ingress-ctag-levels)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm squelch-ingress-ctag-levels)
[Tree] (config>service>vpls>sap>eth-cfm squelch-ingress-ctag-levels)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm squelch-ingress-ctag-levels)

Full Context configure service epipe sap eth-cfm squelch-ingress-ctag-levels
configure service epipe spoke-sdp eth-cfm squelch-ingress-ctag-levels

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp eth-cfm squelch-ingress-ctag-levels
configure service vpls sap eth-cfm squelch-ingress-ctag-levels
configure service vpls spoke-sdp eth-cfm squelch-ingress-ctag-levels

Description This command defines the levels of the ETH-CFM packets that are silently discarded on ingress into the SAP or SDP binding from the wire that matches the service delineation of the SAP or SDP binding plus an additional VLAN, up to a maximum tag length of two tags. All ETH-CFM packets inbound to the SAP or SDP binding that match the configured levels are dropped without regard for any other ETH-CFM criteria. No statistical information or drop count is available for any ETH-CFM packet that is silently discarded by this option. The list of levels must be a complete contiguous list from 0 up to the highest level to be dropped. The command must be retyped in complete form to modify a previous configuration, if the operator does not want to delete it first. Entering the command without any valid level information removes the command from the configuration and disables the feature.

The **no** form of this command removes the silent discarding of previously matching ETH-CFM PDUs.

Default no squelch-ingress-ctag-levels

Parameters *md-level* — Identifies the level

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.313 squelch-ingress-levels

squelch-ingress-levels

Syntax **squelch-ingress-levels** [*md-level* [*md-level*]]
no squelch-ingress-levels

Context **[Tree]** (config>service>ies>if>sap>eth-cfm squelch-ingress-levels)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm squelch-ingress-levels)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm squelch-ingress-levels)
[Tree] (config>service>epipe>sap>eth-cfm squelch-ingress-levels)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm squelch-ingress-levels)
[Tree] (config>service>vpls>sap>eth-cfm squelch-ingress-levels)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm squelch-ingress-levels)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm squelch-ingress-levels)
[Tree] (config>service>ipipe>sap>eth-cfm squelch-ingress-levels)
[Tree] (config>service>template>vpls-sap-template>eth-cfm squelch-ingress-levels)
[Tree] (config>service>vprn>if>sap>eth-cfm squelch-ingress-levels)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm squelch-ingress-levels)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm squelch-ingress-levels)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context
configure service epipe sap eth-cfm squelch-ingress-levels
configure service epipe spoke-sdp eth-cfm squelch-ingress-levels
configure service ies interface sap eth-cfm squelch-ingress-levels
configure service ies interface spoke-sdp eth-cfm squelch-ingress-levels
configure service ies subscriber-interface group-interface sap eth-cfm squelch-ingress-levels
configure service ipipe sap eth-cfm squelch-ingress-levels
configure service template vpls-sap-template eth-cfm squelch-ingress-levels
configure service vpls mesh-sdp eth-cfm squelch-ingress-levels
configure service vpls sap eth-cfm squelch-ingress-levels
configure service vpls spoke-sdp eth-cfm squelch-ingress-levels
configure service vprn interface sap eth-cfm squelch-ingress-levels
configure service vprn interface spoke-sdp eth-cfm squelch-ingress-levels
configure service vprn subscriber-interface group-interface sap eth-cfm squelch-ingress-levels

Description
This command defines the levels of the ETH-CFM packets that are silently discarded on ingress into the SAP or SDP binding from the wire that matches the service delineation of the SAP or SDP binding. All ETH-CFM packets inbound to the SAP or SDP binding that match the configured levels are dropped without regard for any other ETH-CFM criteria. No statistical information or drop count is available for any ETH-CFM packet that is silently discarded by this option. The operator must configure a complete contiguous list of md-levels up to the highest level that are to be dropped. The command must be retyped in complete form to modify a previous configuration, if the operator does not want to delete it first. Entering the command with no associated md-level information is equivalent to the **no** version of the command.

The **no** form of this command removes the silent discarding of previously matching ETH-CFM PDUs.

Default
no squelch-ingress-levels

Parameters
md-level — Identifies the level

Values 0 to 7

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm squelch-ingress-levels
- configure service ies subscriber-interface group-interface sap eth-cfm squelch-ingress-levels

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ipipe sap eth-cfm squelch-ingress-levels
- configure service epipe sap eth-cfm squelch-ingress-levels
- configure service vpls spoke-sdp eth-cfm squelch-ingress-levels
- configure service template vpls-sap-template eth-cfm squelch-ingress-levels
- configure service vpls mesh-sdp eth-cfm squelch-ingress-levels
- configure service ies interface spoke-sdp eth-cfm squelch-ingress-levels

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vpls sap eth-cfm squelch-ingress-levels
- configure service ies interface sap eth-cfm squelch-ingress-levels
- configure service vprn interface spoke-sdp eth-cfm squelch-ingress-levels
- configure service vprn interface sap eth-cfm squelch-ingress-levels
- configure service epipe spoke-sdp eth-cfm squelch-ingress-levels

23.314 sr-isis

sr-isis

Syntax [**no**] **sr-isis**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-isis)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-isis)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-isis)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter sr-isis)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter sr-isis
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter sr-isis
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter sr-isis
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-isis

Description This command selects the Segment Routing (SR) tunnel type programed by an IS-IS instance in TTM.

When the **sr-isis** value (or **sr-ospf**) is enabled, an SR tunnel to the BGP next hop is selected in the TTM from the lowest-numbered IS-IS (OSPF) instance.

The **no** form of this command disables the SR-ISIS setting for the auto-bind tunnel.

Default no sr-isis

Platforms All

sr-isis

Syntax [**no**] **sr-isis**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter sr-isis)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter sr-isis

Description This command enables the use of SR-ISIS sourced tunnel entries in the TTM to resolve the associated static route next hop.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no sr-isis

Platforms All

sr-isis

Syntax [**no**] **sr-isis**

Context **[Tree]** (config>service>sdp sr-isis)

Full Context configure service sdp sr-isis

Description This command configures an MPLS SDP of LSP type ISIS Segment Routing. The SDP of LSP type sr-isis can be used with the far-end option. The signaling protocol for the service labels for an SDP using an SR tunnel can be configured to static (off), T-LDP (tldp), or BGP (bgp).

Platforms All

sr-isis

Syntax [**no**] **sr-isis**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter sr-isis)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter sr-isis)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter sr-isis
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter sr-isis

Description This command selects the Segment Routing (SR) tunnel type programmed by an IS-IS instance in TTM for next-hop resolution of BGP routes and labeled routes. This option allows BGP to use the segment- routing tunnel in the tunnel table submitted by the lowest preference IS-IS instance or, in case of a tie, the lowest numbered IS-IS instance.

Platforms All

23.315 sr-label-index

sr-label-index

Syntax **sr-label-index** {*value* | *param-name*} [**prefer-igp**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no sr-label-index

Context [Tree] (config>router>policy-options>policy-statement>entry>action sr-label-index)
[Tree] (config>router>policy-options>policy-statement>default-action sr-label-index)

Full Context configure router policy-options policy-statement default-action sr-label-index
configure router policy-options policy-statement entry action sr-label-index

Description This command associates a BGP segment-routing label index value with all /32 BGP labeled IPv4 routes matching the entry or policy **default-action**.

Note: Avoid using this action in a policy entry that matches more than one /32 label-ipv4 route, otherwise SID conflicts are created.

The **sr-label-index** action only takes effect in BGP peer import policies (and only on received /32 label-ipv4 routes) and in route-table-import policies associated with the label-ipv4 RIB.

The **prefer-igp** applies only in a route-table-import policy. If **prefer-igp** is specified and BGP segment-routing uses **prefix-sid-range global**, then BGP tries, as a first priority, to use the IGP segment routing label index for the IGP route matched by the **route-table-import** policy. If the IGP route does not have an SID index, or **prefer-igp** is not configured or **prefix-sid-range** is not **global**, BGP tries to use the label index value specified by this command.

When this action occurs in a policy applied as a peer-import policy, it can add a prefix SID attribute to a received /32 label-ipv4 route that was not sent with this attribute, or it can replace the received prefix SID attribute with a new one.

If this command specifies an index value that causes a SID conflict with another BGP route, then all conflicting BGP routes are re-advertised with label values based on dynamic allocation rather than SID-based allocation.

If this command specifies an index value that causes a SID conflict with an IGP route, the BGP route is re-advertised with a label value based on dynamic allocation rather than an SID-based allocation.

The **no** form of this command causes matched BGP routes to be advertised without any new or changed prefix SID attributes.

Default no sr-label-index

Parameters *value* — Specifies the BGP segment routing label index to associate with the matched route or routes.

Values 0 to 52487

param-name — Specifies the **type** parameter variable name, up to 32 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefer-igp — A keyword that is applicable only in **route-table-import** policies, to instruct BGP to borrow the SID index from the IGP route if it has an SID index and the **prefix-sid-range** is **global**.

Platforms All

23.316 sr-labels

sr-labels

Syntax **sr-labels start** *start-value* **end** *end-value*
no sr-labels

Context **[Tree]** (config>router>mpls-labels sr-labels)

Full Context configure router mpls-labels sr-labels

Description This command configures the range of the Segment Routing Global Block (SRGB). It is a label block which is used for assigning labels to segment routing prefix SIDs originated by this router. This range is carved from the system dynamic label range and is not instantiated by default.

This is a reserved label and once configured it cannot be used by other protocols such as RSVP, LDP, and BGP to assign a label dynamically.

Default no sr-labels

Parameters *start-value* — Specifies the start label value in the SRGB

Values 18432 to 524287 within dynamic label range | 1048575 (FP4 only)

end-value — Specifies the end label value in the SRGB

Values 18432 to 524287 within dynamic label range | 1048575 (FP4 only)

Platforms All

23.317 sr-maintenance-policy

sr-maintenance-policy

Syntax **sr-maintenance-policy** *maintenance-policy-name*
no sr-maintenance-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>policy-options>policy-statement>entry>action sr-maintenance-policy)
[Tree] (config>router>policy-options>policy-statement>default-action sr-maintenance-policy)

Full Context configure router policy-options policy-statement default-action sr-maintenance-policy
configure router policy-options policy-statement entry action sr-maintenance-policy

Description This command applies a named segment routing maintenance policy to the matching routes. It is only used for SR policy routes. The named policy must exist under the **config**>**router**>**segment-routing** context.

The **no** form of this command removes the specified maintenance policy.

Parameters *maintenance-policy-name* — Specifies the name of the maintenance policy, up to 32 characters and cannot start with a space or underscore.

Platforms All

23.318 sr-mpls

sr-mpls

Syntax **sr-mpls**

Context [Tree] (config>router>segment-routing sr-mpls)

Full Context configure router segment-routing sr-mpls

Description Commands in this context configure the SR MPLS properties.

Platforms All

23.319 sr-ospf

sr-ospf

Syntax [**no**] **sr-ospf**

Context [Tree] (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter sr-ospf

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter sr-ospf
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter sr-ospf
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-ospf

Description This command selects the Segment Routing (SR) tunnel type programed by an OSPF instance in TTM.

When the **sr-ospf** (or **sr-isis**) value is enabled, an SR tunnel to the BGP next hop is selected in the TTM from the lowest-numbered IS-IS (OSPF) instance.

The **no** form of this command disables the SR-OSPF setting for the auto-bind tunnel.

Default no sr-ospf

Platforms All

sr-ospf

Syntax [**no**] **sr-ospf**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter sr-ospf)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter sr-ospf

Description This command enables the use of SR-OSPF sourced tunnel entries in the TTM to resolve the associated static route next hop.

Default no sr-ospf

Platforms All

sr-ospf

Syntax [**no**] **sr-ospf**

Context **[Tree]** (config>service>sdp sr-ospf)

Full Context configure service sdp sr-ospf

Description This command configures an MPLS SDP of LSP type OSPF Segment Routing. The SDP of LSP type sr-ospf can be used with the far-end option. The signaling protocol for the service labels for an SDP using an SR tunnel can be configured to static (off), T-LDP (tldp), or BGP (bgp).

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sr-ospf

Syntax [**no**] **sr-ospf**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter sr-ospf)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter sr-ospf)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter sr-ospf
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter sr-ospf

Description This command selects the Segment Routing (SR) tunnel type programmed by an OSPF instance in TTM for next-hop resolution of BGP routes and labeled routes. This option allows BGP to use the segment routing tunnel in the tunnel table submitted by the lowest preference OSPF instance or, in case of a tie, the lowest numbered OSPF instance.

The **no** form of this command disables the use of SR-OSPF tunneling for next-hop resolution.

Platforms All

23.320 sr-ospf3

sr-ospf3

Syntax [**no**] **sr-ospf3**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf3)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf3)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf3)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter sr-ospf3)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter sr-ospf3
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter sr-ospf3
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter sr-ospf3
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-ospf3

Description This command selects the Segment Routing (SR) tunnel type programed by an OSPFv3 instance in TTM.

When the **sr-ospf3** (or **sr-isis**) command is enabled, an SR tunnel to the BGP next hop is selected in the TTM from the lowest-numbered IS-IS (OSPFv3) instance.

The **no** form of this command disables the OSPFv3 setting for the auto-bind tunnel.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no sr-ospf3

Platforms All

sr-ospf3

Syntax [**no**] **sr-ospf3**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter sr-ospf3)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter sr-ospf3)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter sr-ospf3
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter sr-ospf3

Description This command selects the IPv6 segment routing tunnel type programmed by an OSPFv3 instance in the TTMv6 for next-hop resolution of BGP routes and labeled routes. This option allows BGP to use the segment routing tunnel in the tunnel table submitted by the lowest preference OSPFv3 instance or, in case of a tie, the lowest-numbered OSPFv3 instance.

The **no** form of this command disables the use of SR-OSPF3 for next-hop resolution.

Default no sr-ospf3

Platforms All

23.321 sr-policies

sr-policies

Syntax **sr-policies**

Context **[Tree]** (config>router>segment-routing sr-policies)

Full Context configure router segment-routing sr-policies

Description This command creates the context to configure segment routing policies. A segment routing policy specifies traffic to be matched by the policy and actions to take on the matched traffic by applying the instructions encoded in one or more segment lists.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.322 sr-policy

sr-policy

Syntax [**no**] **sr-policy**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-policy)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-policy)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-policy)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter sr-policy)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter sr-policy
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter sr-policy
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter sr-policy
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-policy

Description This command selects the tunnel type for the SR policy.

The **sr-policy** value instructs BGP to search for an SR policy with a non-null endpoint and color value that matches the BGP next hop and color extended community value of the EVPN route.

The **no** form of this command disables the SR policy setting for the auto-bind tunnel.

Default no sr-policy

Platforms All

sr-policy

Syntax **sr-policy**
sr-policy color *color-id* **endpoint** *ip-address*

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping sr-policy)
[Tree] (config>saa>test>type-multi-line>lsp-trace sr-policy)

Full Context configure saa test type-multi-line lsp-ping sr-policy
configure saa test type-multi-line lsp-trace sr-policy

Description This command configures the SR policy target FEC.

Note: The **sr-policy** target FEC type is supported under the OAM context and under **type-multi-line node** in the SAA context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **color** *color* — Specifies the color ID.

Values 0 to 4294967295

endpoint *ip-address* — Specifies the endpoint address.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

sr-policy

Syntax [**no**] **sr-policy**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter sr-policy)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter sr-policy)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter sr-policy
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter sr-policy

Description This command enables the use of segment routing (SR) policies to resolve the BGP next hop of certain BGP routes (depending on the context). The SR policies that are considered are statically configured in the local router or learned by BGP routes (AFI 1/SAFI 73). For a BGP route to be resolved by an SR policy, the highest numbered color-extended community attached to BGP route must match the color of the SR policy. Next hop resolution of VPN IP routes by SR policies is not supported.

The **no** form of this command disables the use of SR policies to resolve the BGP next hop of a BGP route.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.323 sr-policy-import

sr-policy-import

Syntax [**no**] **sr-policy-import**

Context **[Tree]** (config>router>bgp sr-policy-import)

Full Context configure router bgp sr-policy-import

Description This command instructs BGP to import all statically-configured non-local segment routing policies from the segment routing DB into the BGP RIB so that they can be advertised, as originated routes, towards BGP peers supporting the **sr-policy-ipv4** address family.

The **no** form of this command instructs BGP to not import any statically defined segment routing policies into BGP.

Default no sr-policy-import

Platforms All

23.324 sr-te

sr-te

Syntax [**no**] **sr-te**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-te)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-te)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter sr-te)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter sr-te)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter sr-te
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter sr-te
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter sr-te
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter sr-te

Description This command selects the Segment Routing (SR) Traffic Engineered (SR-TE) LSP programmed in TTM.

The **sr-te** value instructs the system to search for the best metric SR-TE LSP to the address of the BGP next hop. The LSP metric is provided by MPLS in the tunnel table. In the case of multiple SR-TE LSPs with the same lowest metric, BGP selects the LSP with the lowest tunnel ID.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the SR-TE LSP setting for the auto-bind tunnel.

Default no sr-te

Platforms All

sr-te

Syntax [**no**] **sr-te**

Context **[Tree]** (config>router>mpls>pce-initiated-lsp sr-te)

Full Context configure router mpls pce-initiated-lsp sr-te

Description This command enables support for SR-TE PCE-initiated LSPs.

The **no** form of this command removes SR-TE PCE-initiated LSP support. All PCE-initiated SR-TE LSPs are deleted.

Platforms All

sr-te

Syntax **sr-te** *value*
no sr-te

Context **[Tree]** (config>router>mpls>tunnel-table-pref sr-te)

Full Context configure router mpls tunnel-table-pref sr-te

Description This command configures the tunnel table preference for an SR-TE LSP tunnel type away from its default value.

The tunnel table preference applies to the next-hop resolution of BGP routes of the following families: EVPN, IPv4, IPv6, VPN-IPv4, VPN-IPv6, label-IPv4, and label-IPv6 in the tunnel table.

This feature does not apply to a VPRN, VPLS, or VLL service with explicit binding to an SDP that enabled the **mixed-lsp-mode** option. The tunnel preference in such an SDP is fixed and is controlled by the service manager. The configuration of the tunnel table preference parameter does not modify the behavior of such an SDP and the services that bind to it.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

The **no** form of this command reverts to the default value.

Default sr-te 8

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the tunnel table preference value for SR-TE LSP.

Values 1 to 255

Default 8

Platforms All

sr-te

Syntax [**no**] **sr-te**

Context **[Tree]** (config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter sr-te)

Full Context configure router static-route-entry indirect tunnel-next-hop resolution-filter sr-te

Description The sr-te value instructs the code to search for the set of lowest metric SR-TE LSPs to the address of the indirect next-hop. The LSP metric is provided by MPLS in the tunnel table. The static route treats a set of SR-TE LSPs with the same lowest metric as an ECMP set. The user has the option of configuring a list of SR-TE LSP names to be used exclusively instead of searching in the tunnel table. In that case, all LSPs must have the same LSP metric in order for the static route to use them as an ECMP set. Otherwise, only the LSPs with the lowest common metric value are selected.

Default no sr-te

Platforms All

sr-te

Syntax [**no**] **sr-te**

Context **[Tree]** (config>router>bgp>next-hop-resolution>shortcut-tunn>family>resolution-filter sr-te)
[Tree] (config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter sr-te)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter sr-te
configure router bgp next-hop-resolution shortcut-tunnel family resolution-filter sr-te

Description This command selects the Segment Routing (SR) tunnel type programmed by a traffic engineered (TE) instance in TTM for next-hop resolution. In the case of multiple SR-TE tunnels with the same lowest metric, BGP selects the tunnel with the lowest tunnel ID.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sr-te

Syntax [**no**] **sr-te**

Context **[Tree]** (config>router>isis>igp-shortcut>tunnel-next-hop>family sr-te)

Full Context configure router isis igp-shortcut tunnel-next-hop family sr-te

Description This command selects the SR-TE tunnel type in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

sr-te

Syntax [**no**] **sr-te**

Context **[Tree]** (config>router>ospf>igp-shortcut>tunnel-next-hop>family sr-te)
[Tree] (config>router>ospf3>igp-shortcut>tunnel-next-hop>family sr-te)

Full Context configure router ospf igp-shortcut tunnel-next-hop family sr-te
configure router ospf3 igp-shortcut tunnel-next-hop family sr-te

Description This command selects the SR-TE tunnel type in the resolution of the IP prefix or SR tunnel family using IGP shortcuts.

sr-te

Syntax **sr-te** {**legacy** | **application-specific-link-attributes**}
no sr-te

Context **[Tree]** (config>router>ospf>traffic-engineering-options sr-te)

Full Context configure router ospf traffic-engineering-options sr-te

Description This command configures the advertisement of TE attributes of each link on a per-application basis. Two applications are supported in SR OS: RSVP-TE and SR-TE. Although the **legacy** mode of advertising TE attributes is supported, additional configurations are possible.

The **no** form of this command deletes the context.

Default no sr-te

Parameters **legacy** — Advertises the TE attributes for MPLS-enabled SR links using TE Opaque LSAs.

Note: Do not configure the **legacy** mode if the network has both RSVP-TE and SR-TE attributes and the links are not congruent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

application-specific-link-attributes — Advertises TE information for MPLS-enabled SR links using the new Application Specific Link Attributes (ASLA) TLVs.

Platforms All

23.325 sr-te-lsp

sr-te-lsp

Syntax [**no**] **sr-te-lsp** *lsp-name*

Context **[Tree]** (config>service>sdp sr-te-lsp)

Full Context configure service sdp sr-te-lsp

Description This command configures an MPLS SDP of LSP type SR-TE.

The user can specify up to 16 SR-TE LSP names. The destination address of all LSPs must match that of the SDP far-end option. Service data packets are sprayed over the set of LSPs in the SDP using the same procedures as for tunnel selection in ECMP. Each SR-TE LSP can, however, have up to 32 next-hops at the ingress LER when the first segment is a node SID-based SR tunnel. Thus, the service data packet is forwarded over one of a maximum of 16x32 next-hops.

The **tunnel-far-end** option is not supported. In addition, the **mixed-lsp-mode** option does not support the **sr-te** tunnel type.

The signaling protocol for the service labels for an SDP using a SR-TE LSP can be configured to static (**off**), T-LDP (**tldp**), or BGP (**bgp**).

Platforms All

23.326 sr-te-resignal

sr-te-resignal

Syntax **sr-te-resignal**

Context **[Tree]** (config>router>mpls sr-te-resignal)

Full Context configure router mpls sr-te-resignal

Description Commands in this context configure the re-optimization parameters of SR-TE LSPs.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.327 src-access-list

src-access-list

Syntax **src-access-list** *list-name*
no src-access-list *list-name*

Context **[Tree]** (config>system>security>snmp src-access-list)

Full Context configure system security snmp src-access-list

Description This command is used to identify a list of source IP addresses that can be used to validate SNMPv1 and SNMPv2c requests once the list is associated with one or more SNMPv1 and SNMPv2c communities.

An src-address-list referenced by one or more **community** instances is used to verify the source IP addresses of an SNMP request using the **community** regardless of which VPRN/VRF interface (or “Base” interface) the request arrived on. For example, if an SNMP request arrives on an interface in vprn 100 but the request is referencing a **community**, then the source IP address in the packet would be validated against the src-address-list configured for the **community**. This occurs regardless of whether the request is destined to a VPRN interface address and the VPRN has SNMP access enabled, or the request is destined to the base system address via GRT leaking. If the request message’s source IP address does not match the *ip-address* of any of the **src-host**s contained in the list, then the request is discarded and logged as an SNMP authentication failure.

Using src-access-list validation can have an impact on the time it takes for an SR OS node to reply to an SNMP request. It is recommended to keep the lists short, including only the addresses that are needed, and to place SNMP managers that send the highest volume of requests, such as the NSP NFM-P, at the top of the list.

A maximum of 16 source access lists can be configured. Each source access lists can contain a maximum of 16 source hosts.

The **no** form of this command removes the named src-access-list. You cannot remove an **src-access-list** that is referenced by one or more **community** instances.

Parameters *list-name* — Configures the name or key of the **src-access-list**. The *list-name* parameter must begin with a letter (a-z or A-Z).

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.328 src-gsn

src-gsn

Syntax **src-gsn** *ip address*
src-gsn ip-prefix-list *ip-prefix-list-name*
no src-gsn

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>imsi-apn-fltr>entry src-gsn)

Full Context configure application-assurance group gtp gtp-filter imsi-apn-filter entry src-gsn

Description This command configures a matching condition for the GSN IP address. The IP address value is checked only against the source IP address of the GTP packets that contain an APN IE or an IMSI IE.

Parameters *ip address* — Specifies a valid unicast address associated with the IMSI-APN filter entry.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D
	prefix-length [1..128]

ip-prefix-list-name — Specifies an IP address prefix list for the source IP address match criteria, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.329 src-host

src-host

Syntax **src-host** *host-name* **address** *ip-address*
no src-host *host-name*

Context **[Tree]** (config>system>security>snmp>src-access-list src-host)

Full Context configure system security snmp src-access-list src-host

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to configure a source IP address entry that can be used to validate SNMPv1 and SNMPv2c requests.

The **no** form of this command removes the specified entry.

Parameters *host-name* — Configures the name of the **src-host** entry.

ip-address — Configures an allowed source address for SNMP requests. This can be an IPv4 or IPv6 address.

Values ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

Platforms All

23.330 src-ip

src-ip

Syntax **src-ip** {*ip-address/mask* | *ip-address netmask*}
src-ip {*ipv6-address* | *prefix-length*}
no src-ip

Context **[Tree]** (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match src-ip)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match src-ip)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match src-ip
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match src-ip

Description This command configures the source IP match condition.

The **no** form of this command reverts to the default.

Parameters *ipv6-address* — Specifies the IPv6 address (applies only to the 7750 SR).

Values

ipv6-address	x:x:x:x:x:x:x:x (where x is [0 to FFFF]H)
	x:x:x:x:x:x:d.d.d.d (where d is [0 to 255]D)

prefix-length — Specifies the prefix length (applies only to the 7750 SR).

Values 1 to 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address/mask — Specifies the IPv4 address and mask.

Values ip-address a.b.c.d
mask 0 to 32

netmask — Specifies the mask, expressed as a dotted quad.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

src-ip

Syntax **src-ip** *ip-address*
no src-ip

Context **[Tree]** (config>redundancy>mc>peer>mc>l3-ring>connectivity-verify src-ip)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring connectivity-verify src-ip

Description This command specifies the source IP address used in ring-node connectivity verification of this ring node.

The **no** form of this command reverts to the default.

Parameters *ip-address* — Specifies the source IP address used in ring-node connectivity verification of this ring node.

src-ip

Syntax **src-ip** *ip-address*
no src-ip

Context **[Tree]** (config>redundancy>mc>peer>mcr>node>cv src-ip)

Full Context configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify src-ip

Description This command specifies the source IP address used in the ring-node connectivity verification of this ring node.

Default no src-ip

Parameters *ip-address* — Specifies the source IP address.

Values a.b.c.d (no multicast address)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-ip

Syntax **src-ip** {**eq** | **neq**} *ip-address*
src-ip {**eq** | **neq**} **ip-prefix-list** *ip-prefix-list-name*
no src-ip

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match src-ip)

Full Context configure application-assurance group policy app-qos-policy entry match src-ip

Description This command specifies a source TCP/UDP address to use as match criteria.

Default no src-ip

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified address or prefix.

neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D
	prefix-length [1..128]

ip-prefix-list-name — Specifies an IP prefix list name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

src-ip

Syntax **src-ip** *ip-address*
src-ip ip-prefix-list *ip-prefix-list-name*
no src-ip

Context **[Tree]** (config>app-assure>group>sess-fltr>entry>match src-ip)

Full Context configure application-assurance group session-filter entry match src-ip

Description This command specifies a source TCP/UDP address to use as match criteria.

Default no src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies a valid unicast address.

Values

ipv4-address	a.b.c.d[/mask]
	mask - [1..32]
ipv6-address	x:x:x:x:x:x:x:x/prefix-length
	x:x:x:x:x:x:d.d.d.d
	x - [0..FFFF]H
	d - [0..255]D
	prefix-length [1..128]

ip-prefix-list-name — Specifies an IP prefix list name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

src-ip

Syntax **src-ip** {**eq** | **neq**} *ip-address*
no src-ip

Context **[Tree]** (debug>app-assure>group>traffic-capture>match src-ip)

Full Context debug application-assurance group traffic-capture match src-ip

Description This command configures debugging on a source IP address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

src-ip

Syntax **src-ip** {ip-address/mask | *ip-address ipv4-address-mask*}

Context **[Tree]** (config>li>li-filter>li-ip-filter>entry>match src-ip)

Full Context configure li li-filter li-ip-filter entry match src-ip

Description This command configures source IP address LI filter match criterion.

The **no** form of this command removes any configured source IP. The match criterion is ignored.

Parameters *ip-address* — Specifies an address specified as dotted quad.

Values a.b.c.d

mask — Specifies eight 16-bit hexadecimal pieces representing bit match criteria.

Values 1 to 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-address-mask — Any mask expressed in dotted quad notation.

Values 0.0.0.0 to 255.255.255.255

Platforms All

src-ip

Syntax **src-ip** {ipv6-address/prefix-length | *ipv6-address ipv6-address-mask*}
no src-ip

Context **[Tree]** (config>li>li-filter>li-ipv6-filter>entry>match src-ip)

Full Context configure li li-filter li-ipv6-filter entry match src-ip

Description This command configures source IPv6 address LI filter match criterion.

The **no** form of this command removes any configured source IPv6 address. The match criterion is ignored.

Parameters *ipv6-address* — Specifies an IPv6 address entered as:.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

prefix-length — Specifies a length.

Values 1 to 128

ipv6-address-mask — Specifies an IPv6 address mask expressed as:

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

src-ip

Syntax **src-ip** {*ip-address/mask* | *ip-address* [*ipv4-address-mask*] | **ip-prefix-list** *prefix-list-name*}
no src-ip

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry>match src-ip)
[Tree] (config>qos>sap-egress>ip-criteria>entry>match src-ip)

Full Context configure qos sap-egress ip-criteria entry match src-ip
configure qos sap-ingress ip-criteria entry match src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a source IPv4 address range to be used as an SAP QoS policy match criterion.

To match on the source IPv4 or IPv6 address, specify the address and its associated mask, e.g. 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used for IPv4.

The **no** form of this command removes the source IPv4 or IPv6 address match criterion.

Default no src-ip

Parameters *ip-address* — Specifies the source IPv4 address specified in dotted decimal notation.

Values ip-address: a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

prefix-list-name — Specifies the IPv4 prefix list name, a string of up to 32 printable ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

src-ip

Syntax **src-ip** {*ipv6-address/prefix-length* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *ipv6-prefix-list-name*}
no src-ip

Context **[Tree]** (config>qos>sap-ingress>ipv6-criteria>entry>match src-ip)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry>match src-ip)

Full Context configure qos sap-egress ipv6-criteria entry match src-ip
configure qos sap-ingress ipv6-criteria entry match src-ip

Description This command configures a source IPv6 address range to be used as an SAP QoS policy match criterion.

To match on the source IPv6 address, specify the address and its associated mask, for example, 2001:db8:1000::/64.

The **no** form of this command removes the source IPv6 address match criterion.

Default no src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-address* — Specifies the IPv6 address for the IP match criterion in hexadecimal digits.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

prefix-length — Specifies the IPv6 prefix length for the IPv6 address expressed as a decimal integer.

Values 1 to 128

ipv6-address-mask — Specifies the IPv6 address mask.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

ipv6-prefix-list-name — Specifies the IPv6 prefix list name, a string of up to 32 printable ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Platforms All

src-ip

Syntax **src-ip** {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *ip-prefix-list-name*}
src-ip {*ipv6-address/mask* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *ipv6-prefix-list-name*}
no src-ip

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry>match src-ip)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry>match src-ip)
[Tree] (config>qos>network>egress>ip-criteria>entry>match src-ip)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match src-ip)

Full Context configure qos network egress ip-criteria entry match src-ip
configure qos network egress ipv6-criteria entry match src-ip
configure qos network ingress ip-criteria entry match src-ip
configure qos network ingress ipv6-criteria entry match src-ip

Description This command configures a source IPv4 or IPv6 address range to be used as a network QoS policy match criterion.

To match on the source IPv4 or IPv6 address, specify the address and its associated mask, for example, when specifying an IPv4 address, 10.1.0.0/16 or 10.1.0.0 255.255.0.0 can be used.

The **no** form of this command removes the source IPv4 or IPv6 address match criterion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the source IPv4 address specified in dotted decimal notation.

Values ip-address: a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

ip-prefix-list-name — Specifies an IPv4 prefix list which contains IPv4 address prefixes to be matched. IP prefix lists are only supported at a network ingress.

Values A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

ipv6-address — Specifies the IPv6 prefix for the IP match criterion in hex digits.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

mask — Specifies the length of the ipv6-address expressed as a decimal integer.

Values 1 to 128

ipv6-address-mask — Specifies the eight 16-bit hexadecimal pieces representing bit match criteria.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

ipv6-prefix-list-name — Specifies an IPv6 prefix list which contains IPv6 address prefixes to be matched. IPv6 prefix lists are only supported at a network ingress.

Values A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

src-ip

Syntax **IPv4:**

src-ip {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}

IPv6:

src-ip {*ipv6-address/prefix-length* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *prefix-list-name*}

no src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>ip-exception>entry>match src-ip)
[Tree] (config>filter>ipv6-filter>entry>match src-ip)
[Tree] (config>filter>ipv6-exception>entry>match src-ip)
[Tree] (config>filter>ipv6-filter>entry>match src-ip)

Full Context configure filter ip-exception entry match src-ip
configure filter ipv6-exception entry match src-ip
configure filter ipv6-filter entry match src-ip

Description This command configures a source IPv4 or IPv6 address range to be used as an IP filter or IP exception match criterion.

To match on the source IPv4 or IPv6 address, specify the address and its associated mask, for example, 10.1.0.0/16 for IPv4. The conventional notation of 10.1.0.0 255.255.0.0 may also be used for IPv4.

The **no** form of the command removes the source IP address match criterion.

Default no src-ip

Parameters *ip-address* — Specifies the destination IPv4 address specified in dotted decimal notation.

Values a.b.c.d

mask — Specifies the length in bits of the subnet mask.

Values 1 to 32

ipv4-address-mask — Specifies the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

ip-prefix-list or **ipv6-prefix-list** *prefix-list-name* — Specifies to use a list of IP prefixes referred to by prefix-list-name, which is a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

ipv6-address — Specifies an IPv6 prefix for the IP match criterion in hex digits.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

prefix-length — Specifies whether a the IPv6 prefix length for the specified *ipv6-address* expressed as a decimal integer.

Values 1 to 128

ipv6-address-mask — Specifies eight 16-bit hexadecimal pieces representing bit match criteria.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0..FFFF]H
d: [0..255]D

Platforms All

- configure filter ipv6-filter entry match src-ip

VSR

- configure filter ip-exception entry match src-ip
- configure filter ipv6-exception entry match src-ip

src-ip

Syntax **src-ip** *ip-prefix*[/*mask*] [*netmask*]
src-ip ip-prefix-list *ip-prefix-list-name*
no src-ip

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry src-ip)

Full Context configure system security management-access-filter ip-filter entry src-ip

Description This command configures a source IP address range or an IP prefix list to be used as a management access filter match criterion.

The **no** form of this command removes the source IP address match criterion.

Default no src-ip

Parameters *ip-prefix* — Specifies the IP prefix for the IP match criterion in dotted decimal notation.

mask — Specifies the subnet mask length expressed as a decimal integer.

Values 1 **to** 32 (mask length), 0.0.0.0 **to** 255.255.255.255 (dotted decimal)

netmask — Specifies the dotted quad equivalent of the mask length.

Values 0.0.0.0 to 255.255.255.255

ip-prefix-list-name — Specifies the IP prefix list used as a match criterion for the source IP address. It is a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

src-ip

Syntax **src-ip** *ipv6-address/prefix-length*
src-ip ipv6-prefix-list *ipv6-prefix-list-name*
no src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry src-ip)

Full Context configure system security management-access-filter ipv6-filter entry src-ip

Description This command configures a source IPv6 address range or an IPv6 prefix list to be used as a management access filter match criterion. This command only applies to the 7750 SR and 7950 XRS.

The **no** form of this command removes the source IPv6 address match criterion.

Default no src-ip

Parameters *ipv6-address/prefix-length* — Specifies the IPv6 address for the IPv6 match criterion in dotted decimal notation. An IPv6 IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:0:217A.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D
prefix-length	1 to 128

ipv6-prefix-list-name — Specifies the IPv6 prefix list used a match criterion for the source IP address. It is a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms All

src-ip

Syntax **src-ip** [*ipv6-address*/*prefix-length* | **ip-prefix-list** *prefix-list-name*]
no src-ip

Context [Tree] (cfg>sys>sec>cpm>ip-filter>entry>match src-ip)

Full Context configure system security cpm-filter ip-filter entry match src-ip

Description This command specifies the IP address to match the source IP address of the packet.

To match on the source IP address, specify the address and its associated mask, such as 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

The **no** form of this command removes the source IP address match criterion.

Default no src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ipv6-address/prefix-length* — Specifies the IP address for the match criterion in dotted decimal notation. An IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:0:217A.

Values

ipv4-address	a.b.c.d (host bits must be 0)
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 characters maximum, mandatory for link local addresses
prefix-length	1 to 128

ip-prefix-list — Creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

src-ip

Syntax **src-ip** [*ip-address*/*mask* | **ipv6-prefix-list** *ipv6-prefix-list-name*]
no src-ip

Context **[Tree]** (cfg>sys>sec>cpm>ipv6-filter>entry>match src-ip)

Full Context configure system security cpm-filter ipv6-filter entry match src-ip

Description This command specifies the IPv6 address to match the source IPv6 address of the packet.

To match on the source IP address, specify the address and its associated mask, such as 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

The **no** form of this command removes the source IP address match criterion.

This command only applies to the 7750 SR and 7950 XRS.

Default no src-ip

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address/mask* — Specifies the IP address for the match criterion in dotted decimal notation. An IP address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address can be left out, so that 2001:db8::0:217A is the same as 2001:db8:0:0:0:0:0:217A.

Values

ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 characters maximum, mandatory for link local addresses
mask:	Specifies eight 16-bit hexadecimal pieces representing bit match criteria.
	Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

ipv6-prefix-list — Creates a list of IPv6 prefixes for match criteria in IPv6 ACL and CPM filter policies.

ipv6-prefix-list-name — Specifies a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.331 src-ip-address

src-ip-address

Syntax **src-ip-address** *ip-address*
no src-ip-address

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy src-ip-address)
[Tree] (config>saa>test>type-multi-line>lsp-trace>sr-policy src-ip-address)

Full Context configure saa test type-multi-line lsp-ping sr-policy src-ip-address
configure saa test type-multi-line lsp-trace sr-policy src-ip-address

Description This command configures the source IP address. This option is used when an OAM packet must be generated from a different address than the node's system interface address. For example, when the OAM packet is sent over an LDP LSP and the LDP LSR-ID of the corresponding LDP session to the next hop is set to an address other than the system interface address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the configuration.

Parameters *ip-address* — Specifies the source IP address.

Values
ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0 to FFFF]H
d - [0 to 255]D

Platforms All

23.332 src-ipv4-address

src-ipv4-address

Syntax **src-ipv4-address** *a.b.c.d*
no src-ipv4-address

Context **[Tree]** (config>test-oam>build-packet>header>ipv4 src-ipv4-address)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv4 src-ipv4-address)

Full Context configure test-oam build-packet header ipv4 src-ipv4-address
debug oam build-packet packet field-override header ipv4 src-ipv4-address

Description This command defines the source IPv4 address to be used in the IPv4 header.

The **no** form of this command removes the source IPv4 address.

Default src-ipv4-address 0.0.0.0

Parameters *a.b.c.d* — Specifies the IPv4 source address to be used in the IPv4 header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.333 src-ipv6-address

src-ipv6-address

Syntax **src-ipv6-address** *ipv6-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no src-ipv6-address

Context [Tree] (config>test-oam>build-packet>header>ipv6 src-ipv6-address)
[Tree] (debug>oam>build-packet>packet>field-override>header>ipv6 src-ipv6-address)

Full Context configure test-oam build-packet header ipv6 src-ipv6-address
debug oam build-packet packet field-override header ipv6 src-ipv6-address

Description This command defines the source IPv6 address to be used in the IPv6 header.

The **no** form of the removes the source IPv6 address.

Parameters *ipv6-address* — Specifies the IPv6 source address to be used in the IPv6 header.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
x:	0 to FFFF]H
d:	[0 to 255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.334 src-mac

src-mac

Syntax **src-mac** *ieee-address*
no src-mac

Context [Tree] (config>redundancy>mc>peer>mc>l3-ring>connectivity-verify src-mac)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring connectivity-verify src-mac

Description This command specifies the source MAC address used for the Ring-Node Connectivity Verification of this ring node.

If all zeros are specified, then the MAC address of the system management processor (CPM) is used.

The **no** form of this command reverts to the default.

Parameters *ieee-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-mac

Syntax **src-mac** *ieee-address*
no src-mac

Context **[Tree]** (config>redundancy>mc>peer>mcr>node>cv src-mac)

Full Context configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify src-mac

Description This command specifies the source MAC address used for the Ring-Node Connectivity Verification of this ring node.

A value of all zeros (000000000000 H (0:0:0:0:0:0)) specifies that the MAC address of the system management processor (CPM) is used.

Default no src-mac

Parameters *ieee-address* — Specifies the source MAC address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Platforms All

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context **[Tree]** (config>li>li-filter>li-mac-filter>entry>match src-mac)

Full Context configure li li-filter li-mac-filter entry match src-mac

Description This command configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of this command removes the source mac as the match criteria.

Parameters *ieee-address* — Specifies the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — Specifies a 48-bit mask that can be configured using:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default **0xFFFFFFFFFFFF** (exact match)

Values 0x00000000000000 to 0xFFFFFFFFFFFF

Platforms All

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match src-mac)

Full Context configure qos sap-ingress mac-criteria entry match src-mac

Description This command configures a source MAC address or range to be used as a service ingress QoS policy match criterion.

The **no** form of this command removes the source mac as the match criteria.

Default no src-mac

Parameters *ieee-address* — Enter the 48-bit IEEE MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — This 48-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure all packets with a source MAC OUI value of 00-03-FA to be subject to a match condition, the entry should be specified as: 003FA000000 0xFFFFFF000000

Values 0x00000000000000 to 0xFFFFFFFFFFFF (hex)

Default 0xFFFFFFFFFFFF (hex) (exact match)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context **[Tree]** (config>filter>ip-filter>entry>match src-mac)
[Tree] (config>filter>ipv6-filter>entry>match src-mac)
[Tree] (config>filter>mac-filter>entry>match src-mac)

Full Context configure filter ip-filter entry match src-mac
configure filter ipv6-filter entry match src-mac
configure filter mac-filter entry match src-mac

Description Configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of the command removes the source mac as the match criteria.

Default no src-mac

Parameters *ieee-address* — Specifies the 48-bit IEEE MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit; both upper and lower case are supported.

ieee-address-mask — Specifies the 48-bit mask to match a range of MAC address values.

To configure so that all packets with a source MAC OUI value of 00:03:FA are subject to a match condition then the entry should be specified as: 00:03:FA:00:00:00 FF:FF:FF:00:00:00

Default ff:ff:ff:ff:ff:ff (exact match)

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is an hexadecimal digit; both upper and lower case are supported.

Platforms All

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match src-mac)

Full Context configure system security management-access-filter mac-filter entry match src-mac

Description This command configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of this command removes the source mac as the match criteria.

Default no src-mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ieee-address* — Specifies the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — Specifies a 48-bit mask that can be configured using the formats listed in Table 131:

Table 131 **ieee-address-mask Formats**

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default 0xFFFFFFFFFFFF (exact match)

Values 0x00000000000000 to 0xFFFFFFFFFFFF

Platforms All

23.335 src-mac-address

src-mac-address

Syntax **src-mac-address** *ieee-address*
no src-mac-address

Context **[Tree]** (config>test-oam>build-packet>header>ethernet src-mac-address)
[Tree] (debug>oam>build-packet>packet>field-override>header>ethernet src-mac-address)

Full Context configure test-oam build-packet header ethernet src-mac-address
debug oam build-packet packet field-override header ethernet src-mac-address

Description This command defines the source MAC address for the Ethernet header.

The **no** form of this command deletes the configured MAC address.

Default no override

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ieee-address* — Specifies the source Ethernet MAC address to be used in the Ethernet header. Specifies the 48-bit MAC address.

Values xx:xx:xx:xx:xx:xx

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.336 src-port

src-port

Syntax **src-port** {**lt** | **gt** | **eq**} *src-port-number*
src-port range *start end*
no src-port

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match src-port)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match src-port)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match src-port)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match src-port)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match src-port
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match src-port
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match src-port
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match src-port

Description This command configures the source port match condition.

The **no** form of this command reverts to the default.

Parameters **lt | gt | eq** — Specifies the operators.

src-port-number — Specifies the source port number as a decimal hex or binary.

Values 0 to 65535

dst-port-number — Specifies the destination port number as a decimal hex or binary.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-port

Syntax **src-port** {**eq** | **neq**} *port-num*
src-port {**eq** | **neq**} **port-list** *port-list-name*
src-port {**eq** | **neq**} **range** *start-port-num end-port-num*
no src-port

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match src-port)

Full Context configure application-assurance group policy app-qos-policy entry match src-port

Description This command specifies a source IP port, source port list, or source range to use as match criteria.

The **no** form of this command removes the parameters from the configuration.

Default no src-port

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified port.

neq — Specifies that a successful match occurs when the flow does not match the specified port.

port-num — Specifies the source port number.

Values 0 to 65535

start-port-num end-port-num — Specifies the start or end source port number.

Values 0 to 65535

port-list-name — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

src-port

Syntax **src-port** {**eq** | **gt** | **lt**} *port-num*
src-port port-list *port-list-name*
src-port range *start-port-num end-port-num*
no src-port

Context **[Tree]** (config>app-assure>group>sess-fltr>entry>match src-port)

Full Context configure application-assurance group session-filter entry match src-port

Description This command specifies a source IP port, source port list, or source range to use as match criteria.

The **no** form of this command removes the parameters from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no src-port

Parameters **eq** — Specifies that a successful match occurs when the flow matches the specified port.

gt — Specifies all port numbers greater than the port-number match.

lt — Specifies all port numbers less than the port-number match.

port-num — Specifies the source port number.

Values 0 to 65535

start-port-num end-port-num — Specifies the start or end source port number.

Values 0 to 65535

port-list-name — Specifies a named port-list, up to 32 characters, containing a set of ports or ranges of ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

src-port

Syntax **src-port** {**eq** | **neq**} *port-num*
no src-port

Context **[Tree]** (debug>app-assure>group>traffic-capture>match src-port)

Full Context debug application-assurance group traffic-capture match src-port

Description This command configures debugging on a source port.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

src-port

Syntax **src-port** {**lt** | **gt** | **eq**} *src-port-number*
src-port range *src-port-number src-port-number*
no src-port

Context **[Tree]** (config>li>li-filter>li-ip-filter>entry>match src-port)
[Tree] (config>li>li-filter>li-ipv6-filter>entry>match src-port)

Full Context configure li li-filter li-ip-filter entry match src-port
configure li li-filter li-ipv6-filter entry match src-port

Description This command configures a source TCP or UDP port number or port range for an IP LI filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (second, third, and so on) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of this command removes the source port match criterion.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **lt** — Specifies all port numbers less than *src-port-number* match.

gt — Specifies all port numbers greater than *src-port-number* match.

eq — Specifies that *src-port-number* must be an exact match.

src-port-number — Specifies the source port number to be used as a match criteria expressed as a decimal integer.

Values [0..65535]D
[0x0..0xFFFF]H
[0b0..0b1111111111111111]B

Platforms All

src-port

Syntax **src-port** {**lt** | **gt** | **eq**} *src-port-number*
src-port range *start end*
no src-port

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry>match src-port)
[Tree] (config>qos>sap-egress>ip-criteria>entry>match src-port)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry>match src-port)
[Tree] (config>qos>sap-egress>ipv6-criteria>entry>match src-port)

Full Context configure qos sap-egress ip-criteria entry match src-port
configure qos sap-egress ipv6-criteria entry match src-port
configure qos sap-ingress ip-criteria entry match src-port
configure qos sap-ingress ipv6-criteria entry match src-port

Description This command configures a source TCP or UDP port number or port range for a SAP QoS policy match criterion.

The **no** form of this command removes the source port match criterion.

Default no src-port

Parameters **{lt | gt | eq}** *src-port-number* — The TCP or UDP port numbers to match, specified as less than (**lt**), greater than (**gt**), or equal to (**eq**) to the source port value, specified as a decimal integer.

Values 1 to 65535 (decimal)

range *start end* — The range of TCP or UDP port values to match, specified as between the *start* and *end* source port values inclusive.

Values 1 to 65535 (decimal)

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-port

Syntax **src-port** {**lt** | **gt** | **eq**} *src-port-number*
src-port port-list *port-list-name*
src-port range *start end*
no src-port

Context **[Tree]** (config>qos>network>ingress>ip-criteria>entry>match src-port)
[Tree] (config>qos>network>ingress>ipv6-criteria>entry>match src-port)
[Tree] (config>qos>network>egress>ip-criteria>entry>match src-port)
[Tree] (config>qos>network>egress>ipv6-criteria>entry>match src-port)

Full Context configure qos network egress ip-criteria entry match src-port
configure qos network egress ipv6-criteria entry match src-port
configure qos network ingress ip-criteria entry match src-port
configure qos network ingress ipv6-criteria entry match src-port

Description This command configures a source TCP or UDP port number, port range, or a port list for a network QoS policy match criterion.

The **no** form of this command removes the source port match criterion.

Default no src-port

Parameters **lt** — Keyword used to specify TCP or UDP port numbers to match that are less than the source port value.

gt — Keyword used to specify TCP or UDP port numbers to match that are greater than the source port value.

eq — Keyword used to specify TCP or UDP port numbers to match that are equal to the source port value.

src-port-number — The source port value, specified as a decimal integer.

Values 1 to 65535

port-list-name — Specifies a port list name, up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

start — Specifies the starting range of TCP or UDP source port values to match.

Values 1 to 65535

end — Specifies the end range of TCP or UDP source port values to match.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-port

Syntax **src-port** {**lt** | **gt** | **eq**} *src-port-number*
src-port port-list *port-list-name*
src-port range *src-port-number src-port-number*
no src-port

Context **[Tree]** (config>filter>ip-exception>entry>match src-port)
[Tree] (config>filter>ip-filter>entry>match src-port)
[Tree] (config>filter>ipv6-exception>entry>match src-port)
[Tree] (config>filter>ipv6-filter>entry>match src-port)

Full Context configure filter ip-exception entry match src-port
configure filter ip-filter entry match src-port
configure filter ipv6-exception entry match src-port
configure filter ipv6-filter entry match src-port

Description This command configures a source TCP, UDP, or SCTP port number, port range, or port match list for an IP filter or IP exception match criterion. An entry containing Layer 4 non-zero match criteria will not match non-initial (2nd, 3rd, and so on) fragments of a fragmented packet since only the first fragment contains the Layer 4 information. Similarly an entry containing "**src-port eq** 0" match criterion, may match non-initial fragments when the source port value is not present in a packet fragment and other match criteria are also met.

The **no** form of the command removes the source port match criterion.

Default no src-port

Parameters **lt | gt | eq** — Specifies the operator to use relative to *src-port-number* for specifying the port number match criteria.

lt specifies that all port numbers less than *src-port-number* match.

gt specifies that all port numbers greater than *src-port-number* match.

eq specifies that *src-port-number* must be an exact match.

src-port-number — Specifies the source port number to be used as a match criteria expressed as a decimal integer, and in hexadecimal or binary format. Below shows decimal integer only.

Values 0 to 65535

port-list-name — Specifies to use a list of ports referred to by *port-list-name*, which is a string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

src-port-number src-port-number — Specifies inclusive port range between two src-port-number values.

Platforms All

- configure filter ip-filter entry match src-port
- configure filter ipv6-filter entry match src-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

VSR

- configure filter ipv6-exception entry match src-port
- configure filter ip-exception entry match src-port

src-port

Syntax **src-port** {*port-id* | **cpm** | **lag** *lag-id*}
no src-port

Context **[Tree]** (config>system>security>mgmt-access-filter>ip-filter>entry src-port)
[Tree] (config>system>security>mgmt-access-filter>ipv6-filter>entry src-port)

Full Context configure system security management-access-filter ip-filter entry src-port
configure system security management-access-filter ipv6-filter entry src-port

Description This command restricts ingress management traffic to either the CPM/CCM Ethernet port or any other logical port (for example LAG) on the device.

When the source interface is configured, only management traffic arriving on those ports satisfy the match criteria.

The **no** form of this command reverts to the default value.

Default no src-port

Parameters *port-id* — Specifies the port ID in formats shown below.

Values

slot/*mda*/*port*[.*channel*]		
bundle-id	**bundle**-*type*-*slot*/*mda*.*bundle-num*	
	bundle	keyword
	type	**ima**, **fr**, or **ppp**
	bundle-num	1 to 336
bpgrp-id	**bpgrp**-*type*-*bpgrp-num*	
	bpgrp	keyword
	type	**ima** or **ppp**
	bpgrp-num	1 to 2000
aps-id	**aps**-*group-id*[.*channel*]	
	aps	keyword
	group-id	1 to 128
ccag-id	**ccag**-*id*. *path-id*[*cc-type*]	
	ccag	keyword
	id	1 to 8
	path-id	**a**, **b**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cc-type **.sap-net**, **.net-sap**

cpm — Matches any traffic received on any Ethernet port.

lag-id — Specifies the LAG identifier.

Values 1 to 800

Platforms All

src-port

Syntax **src-port** *tcp/udp port-number* [*mask*]
scr-port port-list *port-list-name*
scr-port range *tcp/udp port-number tcp/udp port-number*
no scr-port

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match src-port)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match src-port)

Full Context configure system security cpm-filter ip-filter entry match src-port
configure system security cpm-filter ipv6-filter entry match src-port

Description This command specifies the TCP/UDP port to match the source port of the packet.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

Default no src-port

Parameters *tcp/udp port-number* — Specifies the source port number to be used as a match criteria expressed as a decimal integer.

Values 0 to 65535

port-list-name — Specifies the port list name to be used as a match criteria for the destination port.

mask — Specifies the 16 bit mask to be applied when matching the destination port.

Values [0x0000..0xFFFF] | [0..65535] | [0b0000000000000000..0b1111111111111111]

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.337 src-prefix

src-prefix

Syntax **src-prefix** *ip-address/mask* [*ip-address/mask*]
no src-prefix *ip-address/mask*

Context **[Tree]** (config>service>vprn>mvpn>red-source-list src-prefix)

Full Context configure service vprn mvpn red-source-list src-prefix

Description This command configures multicast source IPv4 prefixes for preferred source selection. Single or multi-line inputs are allowed.

The **no** form of this command deletes specified prefix from the list.

Default No prefixes are specified.

Parameters *ip-address/mask* — IPv4 address prefix with mask. Up to 8 maximum.

Platforms All

src-prefix

Syntax **src-prefix** *ipv6-ip-address/prefix-length* [*ipv6-address/prefix-length*]
no *ipv6-ip-address/prefix-length*

Context **[Tree]** (config>service>vprn>mvpn>red-source-list>ipv6 src-prefix)

Full Context configure service vprn mvpn red-source-list ipv6 src-prefix

Description This command configures multicast source IPv6 prefixes for preferred source selection. Single or multi-line inputs are allowed.

The **no** form of this command deletes specified prefix from the list

Default No prefixes are specified.

Parameters *ipv6-ip-address/mask* — IPv6 address prefix with prefix-length. Up to 8 maximum.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.338 src-route-option

src-route-option

Syntax **src-route-option** {**true** | **false**}
no source-route-option

Context **[Tree]** (config>filter>ip-filter>entry>match src-route-option)

Full Context configure filter ip-filter entry match src-route-option

Description This command enables source route option match conditions. When enabled, this filter should match if a (strict or loose) source route option is present/not present at any location within the IP header, as per the value of this object. The **no** form of the command removes the criterion from the match entry.

Default no src-route-option

Parameters **true** — Enables source route option match conditions.

false — Disables source route option match conditions.

Platforms All

23.339 src-tcp-port

src-tcp-port

Syntax **src-tcp-port** *tcp-port*
no src-tcp-port

Context **[Tree]** (config>test-oam>build-packet>header>tcp src-tcp-port)

Full Context configure test-oam build-packet header tcp src-tcp-port

Description This command defines the source TCP port to be used in the test TCP header.

The **no** form of this command reverts to the default.

Default src-tcp-port 0

Parameters *tcp-port* — Specifies the source TCP port to be used in the test TCP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-tcp-port

Syntax **src-tcp-port** *tcp-port*
no src-tcp-port

Context **[Tree]** (debug>oam>build-packet>packet>field-override>header>tcp src-tcp-port)

Full Context debug oam build-packet packet field-override header tcp src-tcp-port

Description This command defines the source TCP port to be used in the TCP header.

The **no** form of this command reverts to the default.

Default no override

Parameters *tcp-port* — Specifies the source TCP port to be used in the test TCP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.340 src-udp-port

src-udp-port

Syntax **src-udp-port** *udp-port*
no src-udp-port

Context **[Tree]** (config>test-oam>build-packet>header>udp src-udp-port)

Full Context configure test-oam build-packet header udp src-udp-port

Description This command defines the source UDP port to be used in the test UDP header.

The **no** form of this command reverts to the default.

Default src-udp-port 0

Parameters *udp-port* — Specifies the source UDP port to be used in the test UDP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

src-udp-port

Syntax **src-udp-port** *udp-port*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no src-udp-port

Context [Tree] (debug>oam>build-packet>packet>field-override>header>udp src-udp-port)

Full Context debug oam build-packet packet field-override header udp src-udp-port

Description This command defines the source UDP port to be used in the UDP header.

The **no** form of this command reverts to the default.

Default no override

Parameters *udp-port* — Specifies the source UDP port to be used in the UDP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.341 srefresh

srefresh

Syntax **srefresh** [**detail**]
no srefresh

Context [Tree] (debug>router>gmpls>packet srefresh)

Full Context debug router gmpls packet srefresh

Description This command enables debugging for GMPLS Srefresh packets.

The **no** form of the command disables debugging for GMPLS Srefresh packets.

Parameters **detail** — Keyword to produce debug output in greater detail.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

srefresh

Syntax **srefresh** [**detail**]
no srefresh

Context [Tree] (debug>router>rsvp>packet srefresh)

Full Context debug router rsvp packet srefresh

Description This command debugs srefresh packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about srefresh packets.

Platforms All

23.342 srh-mode

srh-mode

Syntax **srh-mode** *srh-mode*
no srh-mode

Context **[Tree]** (config>router>segment-routing>srv6>inst>loc>func>end srh-mode)
[Tree] (config>router>segment-routing>srv6>inst>loc>func>end-x srh-mode)

Full Context configure router segment-routing segment-routing-v6 base-routing-instance locator function end srh-mode
configure router segment-routing segment-routing-v6 base-routing-instance locator function end-x srh-mode

Description This command configures the SRH penultimate or ultimate popping mode for the SID.

The **no** form of this command reverts to the default value.

Default srh-mode psp

Parameters *srh-mode* — Specifies the SRH mode for the SID.

Values psp — penultimate segment pop of the SRH
usp — ultimate segment pop of the SRH

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.343 srlb

srlb

Syntax **srlb** *reserved-label-block-name*
no srlb

Context **[Tree]** (config>router>ospf>segm-rtng srlb)
[Tree] (config>router>isis>segm-rtng srlb)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router isis segment-routing srlb
configure router ospf segment-routing srlb

Description This command specifies the reserved label block to use for the Segment Routing Local Block (SRLB) for the specified IS-IS or OSPF instance. The named reserved label block must already have been configured under **config**>**router**>**mpls**>**mpls-labels**.

The **no** form of this command removes an SRLB.

Parameters *reserved-label-block-name* — Specifies the name of the reserved label block, up to 64 characters.

Platforms All

23.344 srlg

srlg

Syntax [**no**] **srlg**

Context **[Tree]** (config>router>mpls>lsp>secondary srlg)

Full Context configure router mpls lsp secondary srlg

Description This command enables the use of the SRLG constraint in the computation of a secondary path for an LSP at the head-end LER. The command is configurable for both RSVP-TE and SR-TE LSPs.

When SRLG is enabled, CSPF includes the SRLG constraint in the computation of the secondary LSP path if **path-computation-method local-cspf** is configured on the LSP. CSPF returns the list of SRLG groups along with the ERO during primary path CSPF computation. At a subsequent establishment of a secondary path with the SRLG constraint, the MPLS task again queries CSPF by providing the list of SRLG group numbers to be avoided. CSPF prunes all links with interfaces that belong to the same SRLGs as the interfaces included in the ERO of the primary path. If CSPF finds a path, the secondary path is set up. If a path is not found, MPLS keeps retrying the requests to CSPF.

An SRLG enabled secondary or standby path of the LSP configured with a value of the **path-computation-method** command other than **local-cspf** remains operationally down with a failure code of srlgPrimaryCspfDisabled(25).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When an LSP is administratively enabled, the SRLG-enabled secondary path is not tried if the first attempt to bring up the primary path is in progress. The SRLG enabled secondary path is kept down temporarily with failure code srlgPrimaryPathDown(26). After this first attempt, MPLS begins setting up the SRLG-enabled standby paths. If primary path computation fails or primary path was not configured, MPLS requests CSPF to compute the secondary path using an empty primary SRLG list. The SRLG *disjoint* state field shows *True* in this scenario.

If the primary path is re-optimized, has undergone MBB, or has come back up after being down, the MPLS task check determines if any SRLG secondary paths should be re-signaled. If MPLS finds that a secondary path is no longer SRLG disjointed, and therefore becomes ineligible, MPLS puts it on a delayed MBB immediately after the expiry of the retry timer. If MBB fails at the first try, the secondary path is torn down and the path is put on retry if not active. If the secondary path is active, then it is only torn down and resignaled when the primary path is activated. The secondary path can remain active even when ineligible while the revert timer to activate the primary path is still running.

If the primary goes down while active, the LSP uses the path of an eligible SRLG secondary path if it is up. If all secondary eligible SRLG paths are down, MPLS uses a non-SRLG secondary path, if configured and up. While the LSP is using a non-SRLG secondary path, if an eligible SRLG secondary path comes back up, MPLS switches the path of the LSP to the eligible SRLG secondary path. As soon as a path for the primary is successfully computed by CSPF, MPLS schedules the delay retry MBB for the secondary path using the new SRLG list.

If the primary path goes down while inactive, for example it is waiting for the revert timer to expire, MPLS resets the SRLG list of the primary to empty and changes the state of all secondary paths, including the currently active one, to the Disjointed state. A delay retry MBB is still performed but results in no change to the active secondary path.

A secondary path that becomes ineligible as a result of an update to the SRLG membership list of the primary path has the ineligibility status removed on any of the following events:

- a successful delay retry MBB of the secondary SRLG path that makes it eligible again
- the secondary path goes down. MPLS puts the standby on retry at the expiry of the retry timer. If successful, it becomes eligible. If not successful after the retry-timer expires or the number of retries reached the number configured under the **retry-limit** parameter, it is left down.

Once the primary path of the LSP is set up and is operationally up, any subsequent changes to the SRLG group membership of an interface that the primary path is using is not considered until the next opportunity the primary path is re-signaled. The primary path may be re-signaled due to a failure or to a make-before-break operation. Make-before-break occurs as a result of a global revertive operation, a timer based or manual re-optimization of the LSP path, or an operator change to any of the path constraints.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Once an SRLG secondary path is set up and is operationally up, any subsequent changes to the SRLG group membership of an interface the secondary path is using is not considered until the next opportunity when the secondary path is re-signaled. The secondary path is re-signaled due to a failure, to a re-signaling of the primary path, or to a make before break operation. Make-before-break occurs as a result of a timer based or manual re-optimization of the secondary path, or an operator change to any of the path constraints of the secondary path, except for enabling or disabling the **srlg** command itself. Enabling or disabling the **srlg** command on an active secondary or on an active or inactive secondary standby path causes the path to be torn down and re-signaled.

In addition, the user-configured **include** or **exclude** admin group statements for a secondary path are also checked together with the SRLG constraints by CSPF.

The following behavior of the feature is specific to the SR-TE LSP.

- An SRLG-enabled SR-TE LSP secondary path with SID label hops remains operational with failure code srlgPathWithSidHops(59).
- An SR-TE LSP uses IGP advertised link SRLG information in the TE database. It does not support the use of SRLG information in the static user SRLG database (**configure router mpls srlg-database**).
- Delay Retry MBB for making a non-disjointed path a disjointed one is not supported with an SR-TE LSP. Instead, the system performs a break-before-make (that is, teardown and retry) operation. If a non-disjointed path is the active path of the LSP, that path is torn down and retried after the router switches to another path (for example, after **revert-timer** expires). If the non-disjointed path is not an active path, it is torn down and retried immediately.

The **no** form of this command reverts to the default value.

Default no srlg

Platforms All

23.345 srlg-database

srlg-database

Syntax [**no**] **srlg-database**

Context **[Tree]** (config>router>mpls srlg-database)

Full Context configure router mpls srlg-database

Description Commands in this context configure the link members of SRLG groups for the entire network at any node that needs to signal LSP paths (for example, a head-end node).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the entire SRLG database. CSPF assumes all interfaces have no SRLG membership association if the database was not disabled with the command **config>router>mpls>user-srlg-db disable**.

Platforms All

23.346 srlg-enable

srlg-enable

Syntax [**no**] **srlg-enable**

Context **[Tree]** (config>router>route-next-hop-policy>template srlg-enable)

Full Context configure router route-next-hop-policy template srlg-enable

Description This command configures the SRLG constraint into the route next-hop policy template.

When this command is applied to a prefix, the LFA SPF will attempt to select an LFA next-hop, among the computed ones, which uses an outgoing interface that does not participate in any of the SLRGs of the outgoing interface used by the primary next-hop.

The SRLG criterion is applied before running the LFA next-hop selection algorithm.

The **no** form deletes the SRLG constraint from the route next-hop policy template.

Default no srlg-enable

Platforms All

23.347 srlg-frr

srlg-frr

Syntax **srlg-frr** [**strict**]
no srlg-frr

Context **[Tree]** (config>router>mpls srlg-frr)

Full Context configure router mpls srlg-frr

Description This command enables the use of the SRLG constraint in the computation of FRR bypass or detour to be associated with any primary LSP path on this system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When this option is enabled, CSPF includes the SRLG constraint in the computation of a FRR detour or bypass for protecting the primary LSP path.

CSPF prunes all links with interfaces that belong to the same SRLG as the interface that is being protected, that is, the outgoing interface at the PLR the primary path is using. If one or more paths are found, the MPLS task will select one based on best cost and will signal the bypass/detour. If not found and the user has included the **strict** option, the bypass/detour is not setup and the MPLS task will keep retrying the request to CSPF. Otherwise, if a path exists that meets the other TE constraints, other than the SRLG one, the bypass/detour is setup.

A bypass or a detour LSP path is not intended to be SRLG disjoint from the entire primary path. Only the SRLGs of the outgoing interface at the PLR that the primary path is using are avoided.

When the MPLS task is searching for an SRLG bypass tunnel to associate with the primary path of the protected LSP, it will first check if any configured manual bypass LSP with CSPF enabled satisfies the SRLG constraints. The search skips any non-CSPF manual bypass LSP because there is no ERO returned to check the SRLG constraint. If no path is found, the task will check if an existing dynamic bypass LSP satisfies the SRLG and other primary path constraints. If not found, it will make a request to CSPF.

Once the primary path of the LSP is configured and is operationally up, subsequent changes to the SRLG group membership of an interface the primary path is using are not considered by the MPLS task at the PLR for bypass/detour association until the next opportunity the bypass LSP path or the primary path is resignaled. The path may be resignaled due to a failure or a Make-Before-Break (MBB) operation. MBB occurs as a result of a global revertive operation, a timer based or manual re-optimization of the bypass LSP or LSP primary path, or a user update of the primary path constraints.

Once the bypass or detour path is set up and is operationally up, subsequent changes to the SRLG group membership of an interface the bypass/detour path is using are not considered by the MPLS task at the PLR until the next opportunity when the association with the primary LSP path is rechecked. The association is rechecked if the bypass path is re-optimized using the timer or manual resignal MBB. Detour paths cannot be re-optimized separately from the primary path.

Enabling or disabling **srlg-frr** command only takes effect when the LSP primary path or the bypass path is resignaled. The user can either wait for the resignal timer to expire or cause the paths to be resignaled immediately by executing, at the ingress LER, the manual resignal command for the LSP primary path or for the bypass LSP path.

A MPLS interface can belong to a maximum of 64 SRLG groups. The SRLG groups are configured using the **config>router>if-attribute>srlg-group** command. The SRLG groups that an RSVP interface belong to are configured using the **srlg-group** command in the **config>router>mpls>interface** context.

The **no** form of this command reverts to the default value.

Default no srlg-frr

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **strict** — Specifies the name of the SRLG group within a virtual router instance.

Values no srlg-frr (default) srlg-frr (non-strict) srlg-frr **strict** (strict)

Platforms All

23.348 srlg-group

srlg-group

Syntax [**no**] **srlg-group** *group-name* [*group-name*]
no srlg-group

Context **[Tree]** (config>router>if>if-attribute srlg-group)
[Tree] (config>service>ies>if>if-attribute srlg-group)
[Tree] (config>service>vprn>if>if-attribute srlg-group)
[Tree] (config>router>mpls>if srlg-group)

Full Context configure router interface if-attribute srlg-group
configure router mpls interface srlg-group
configure service ies interface if-attribute srlg-group
configure service vprn interface if-attribute srlg-group

Description This command configures the SRLG membership of an interface. The user can apply SRLGs to an IES, VPRN, network IP, or MPLS interface.

An interface can belong to up to 64 SRLG groups. However, each single operation of the **srlg-group** command allows a maximum of five (5) groups to be specified at a time. Once an SRLG group is bound to one or more interface, its value cannot be changed until all bindings are removed.

The configured SRLG membership is applied in all levels/areas the interface is participating in. The same interface cannot have different memberships in different levels/areas.

Only the SRLGs bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the **traffic-engineering** option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

The **no** form of this command deletes one or more of the SRLG memberships of an interface. The user can also delete all memberships of an interface by not specifying a group name.

Parameters *group-name* — Specifies the name of the group, up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain. Each single operation of the **srlg-group** command allows a maximum of 5 groups to be specified at a time.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

srlg-group

Syntax **srlg-group** *group-name* **value** *group-value* [**penalty-weight** *penalty-weight*]
no srlg-group *group-name*

Context **[Tree]** (config>router>if-attribute srlg-group)

Full Context configure router if-attribute srlg-group

Description This command defines a Shared Risk Link Group (SRLG) which can be associated with an IP or MPLS interface.

SRLG is used to tag IP or MPLS interfaces which share a specific fate with the same identifier. For example, an SRLG group identifier could represent all links which use separate fibers but are carried in the same fiber conduit. If the conduit is accidentally cut, all the fiber links are cut which means all interfaces using these fiber links will fail.

The user first configures locally on each router the name and identifier of each SRLG group. A maximum of 1024 SRLGs can be configured per system.

The user then configures the SRLG membership of an interface. The user can apply SRLGs to an IES, VPRN, network IP, or MPLS interface. A maximum of 64 SRLGs can be applied to a given interface.

When SRLGs are applied to MPLS interfaces, CSPF at an LER will exclude the SRLGs of interfaces used by the LSP primary path when computing the path of the secondary path. CSPF at an LER or LSR will also exclude the SRLGs of the outgoing interface of the primary LSP path in the computation of the path of the FRR backup LSP. This provides path disjointness between the primary path and the secondary path or FRR backup path of an LSP.

When SRLGs applied to IES, VPRN, or network IP interfaces, they are evaluated in the route next-hop selection by adding the **srlg-enable** option in a route next-hop policy template applied to an interface or a set of prefixes. For instance, the user can enable the SRLG constraint to select a LFA next-hop for a prefix which avoids all interfaces that share fate with the primary next-hop.

The following provisioning rules are applied to SRLG configuration. The system will reject the creation of a SRLG if it re-uses the same name but with a different group value than an existing group. The system will also reject the creation of an SRLG if it re-uses the same group value but with a different name than an existing group.

Only the SRLGs bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the **traffic-engineering** option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

A user may specify a penalty weight (**penalty-weight**) associated with an SRLG. This controls the likelihood of paths with links sharing SRLG values with a primary path being used by a bypass or detour LSP. The higher the penalty weight, the less desirable it is to use the link with a given SRLG.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *group-name* — Specifies the name of the group, up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain.

group-value — Specifies the integer value associated with the group. The association of group name and value should be unique within an IP/MPLS domain.

Values 0 to 4294967295

penalty-weight — Specifies the integer value of the penalty weight that is assigned to the SRLG group

Values 0 to 65535

Default 0

Platforms All

23.349 srrp

srrp

Syntax **srrp** *srrp-id* [**create**]
no srrp *srrp-id*

Context **[Tree]** (config>service>ies>sub-if>grp-if srrp)
[Tree] (config>service>vprn>sub-if>grp-if srrp)

Full Context configure service ies subscriber-interface group-interface srrp
configure service vprn subscriber-interface group-interface srrp

Description This command creates a Subscriber Router Redundancy Protocol (SRRP) instance on a group IP interface. An SRRP instance manages all subscriber subnets within the group interfaces subscriber IP interface or other subscriber IP interfaces that are associated through a wholesale/retail relationship. Only one unique SRRP instance can be configured per group interface.

The **no** form of this command removes an SRRP instance from a group IP interface. Once removed, the group interface ignores ARP requests for the SRRP gateway IP addresses that may exist on subscriber subnets associated with the group IP interface. Then the group interface stops routing using the redundant IP interface associated with the group IP interface and will stop routing with the SRRP gateway MAC address. Ingress packets destined to the SRRP gateway MAC will also be silently discarded. This is the same behavior as a group IP interface that is disabled (shutdown).

The **no** form of this command removes the SRRP ID from the configuration.

Default no srrp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *srrp-id* — Specifies a 32 bit instance ID that must be unique to the system. The instance ID must also match the instance ID used by the remote router that is participating in the same SRRP context. SRRP is intended to perform a function similar to VRRP where adjacent IP hosts within local subnets use a default gateway to access IP hosts on other subnets.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

srrp

Syntax [**no**] **srrp**

Context **[Tree]** (debug>router srrp)

Full Context debug router srrp

Description This command enables debugging for SRRP packets.

The **no** form of this command disables debugging.

Platforms All

srrp

Syntax [**no**] **srrp**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync srrp)

Full Context configure redundancy multi-chassis peer sync srrp

Description This command specifies whether subscriber routed redundancy protocol (SRRP) information should be synchronized with the multi-chassis peer.

Default no srrp

Platforms All

srrp

Syntax **srrp**

Context **[Tree]** (config>redundancy srrp)

Full Context configure redundancy srrp

Description Commands in this context configure system parameters for BNG CUPS inter-UPF resiliency.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.350 srrp-enabled-routing

srrp-enabled-routing

Syntax **srrp-enabled-routing** [**hold-time** *hold-time*]
no srrp-enabled-routing

Context **[Tree]** (config>service>ies>sub-if>grp-if srrp-enabled-routing)
[Tree] (config>service>vprn>sub-if>grp-if srrp-enabled-routing)

Full Context configure service ies subscriber-interface group-interface srrp-enabled-routing
configure service vprn subscriber-interface group-interface srrp-enabled-routing

Description This command configures SRRP-enabled routing.

The **no** form of this command reverts to the default.

Parameters **hold-time** *hold-time* — Specifies the hold time, in deci-seconds.

Values 1 to 50

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.351 srrp-instance

srrp-instance

Syntax [**no**] **srrp-instance** *srrp-id*

Context **[Tree]** (config>redundancy>mc>peer>mc>l3-ring srrp-instance)

Full Context configure redundancy multi-chassis peer multi-chassis l3-ring srrp-instance

Description This command configures an SRRP instance for Layer 3 ring.

The **no** form of this command reverts to the default.

Parameters *srrp-id* — Specifies the SRRP ID of this SRRP instance.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.352 srv6

srv6

Syntax **srv6** {**origination**| **termination}**
no srv6

Context **[Tree]** (config>fwd-path-ext>fpe srv6)

Full Context configure fwd-path-ext fpe srv6

Description This command configures if the SRv6 FPE application type is used for the origination or termination of SRv6 tunnels.

The origination or termination of SRv6 on services requires the configuration of a dedicated SRv6 FPE and cannot share the same FPE. A single FPE can be configured for SRv6 origination. One or more FPEs can be configured for SRv6 termination, where a termination SRv6 FPE is assigned one or more configured locators. Transit SRv6 routers do not need SRv6 FPEs.

The **no** form of this command disables SRv6 on an FPE.

Parameters **origination** — Keyword used to specify the origination FPE application type.

termination — Keyword used to specify the termination FPE application type.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.353 srv6-instance

srv6-instance

Syntax **srv6-instance** *id* **default-locator** *name*
no srv6-instance

Context **[Tree]** (config>service>vprn>bgp-ipvpn>srv6 srv6-instance)

Full Context configure service vprn bgp-ipvpn segment-routing-v6 srv6-instance

Description This command configures an SRv6 instance.

The **no** form of this command removes the SRv6 instance from the BGP IP-VPN control plane for the service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *id* — Specifies the SRv6 instance ID that exist in the service and is associated to a IP-VPN control plane.

Values 1, 2

default-locator — Keyword that refers to the locator that exists in the service SRv6 instance and is used as the default locator for the service.

name — Specifies a default locator name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.354 ssap

ssap

Syntax **ssap** *ssap-value* [*ssap-mask*]
no ssap

Context **[Tree]** (config>qos>sap-ingress>mac-criteria>entry>match ssap)

Full Context configure qos sap-ingress mac-criteria entry match ssap

Description This command configures an Ethernet 802.2 LLC SSAP value or range for an ingress SAP QoS policy match criterion.

This is a 1-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap, and dsap fields are mutually exclusive and cannot be part of the same match criteria.

The **no** form of this command removes the ssap match criterion.

Default no ssap

Parameters *ssap-value* — The 8-bit ssap match criteria value in hex.

Values 0x00 to 0xFF (hex)

ssap-mask — This is optional and can be used when specifying a range of ssap values to use as the match criteria.

This 8-bit mask can be configured using the following formats:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Values 0x00 to 0xFF

Platforms All

ssap

Syntax **ssap** *ssap-value* [*ssap-mask*]
no ssap

Context **[Tree]** (config>filter>mac-filter>entry>match ssap)

Full Context configure filter mac-filter entry match ssap

Description This command configures an Ethernet 802.2 LLC SSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria.

The **no** form of the command removes the ssap match criterion.

Default no ssap

Parameters *ssap-value* — Specifies the 8-bit ssap match criteria value in decimal, hexadecimal or binary.

Values 0 to 255

ssap-mask — Specifies an optional parameter that may be used when specifying a range of ssap values to use as the match criteria.

This 8 bit mask and the ssap value can be configured as described in Table 132.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 132 **8-bit Mask Syntax**

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Values 0 to 255

Platforms All

ssap

Syntax **ssap** *ssap-value* [*ssap-mask*]
no ssap

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match ssap)

Full Context configure system security management-access-filter mac-filter entry match ssap

Description This command configures an Ethernet 802.2 LLC SSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide* for information about MAC Match Criteria Exclusivity Rules fields that are exclusive based on the frame format.

The **no** form of this command removes the SSAP match criterion.

Default no ssap

Parameters *ssap-value* — Specifies the 8-bit SSAP match criteria value in hex.

Values 0x00 to 0xFF

ssap-mask — Specifies a range of SSAP values to use as the match criteria.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.355 ssh

ssh

Syntax **ssh** *host* [**-l** *username*] [**-v** *ssh-version*] [{**router** *router-instance* | **service-name** *service-name*}] [**re-exchange-min** *minutes*] [**re-exchange-mbyte** *megabytes*]

Context **[Tree]** (global ssh)

Full Context global ssh

Description This command initiates a client SSH session with the remote host and is independent from the administrative or operational state of the SSH server. However, to be the target of an SSH session, the SSH server must be operational. This command also allows the user to initiate a SSH session, with a key re-exchange, based on maximum megabytes or minutes, whichever occurs first. If the re-exchange options are not set, the default behavior will not perform a key re-exchange.

Quitting SSH while in the process of authentication is accomplished by either executing a ctrl-c or "~." (tilde and dot), assuming the “~” is the default escape character for SSH session.

Parameters *host* — Specifies the remote host for the SSH session.

Values

host: *user@hostname* - [up to 255 characters]	
user	up to 32 characters
hostname	[*dns-name* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[*-interface*]
	x:x:x:x:x:x:d.d.d.d[*-interface*]
	x - [0 to FFFF]H
	d - [0 to 255]D
	interface: up to 32 characters, mandatory for link local addresses
dns-name	up to128 characters

username — Specifies the user name to use when opening the SSH session, up to 32 characters.

router-instance — Specifies the router name or service ID.

Values

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

router-instance: *router-name* or *vprn-svc-id*

router-name	“Base”, “management”, “vpls-management”
vprn-svc-id	1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

minutes — Specifies the time interval after which the SSH client will initiate the key-re-exchange.

Values 1 to 1440 minutes

megabytes — Specifies the number of megabytes, on a SSH session, after which the SSH client will initiate the key re-exchange.

Values 1 to 64000 megabytes

ssh

Syntax **ssh**

Context **[Tree]** (config>system>login-control ssh)
[Tree] (config>system>security ssh)

Full Context configure system login-control ssh
configure system security ssh

Description Commands in this context configure the SSH parameters.

Platforms All

23.356 ssh-max-sessions

ssh-max-sessions

Syntax **ssh-max-sessions** *number-of-sessions*
no ssh-max-sessions

Context **[Tree]** (config>system>security>cli-session-group ssh-max-sessions)
[Tree] (config>system>security>profile ssh-max-sessions)

Full Context configure system security cli-session-group ssh-max-sessions
configure system security profile ssh-max-sessions

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to limit the number of SSH-based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.

The **no** form of this command disables the command and the profile/group limit is not applied on the number of sessions.

Default no ssh-max-sessions

Parameters *number-of-sessions* — Specifies the maximum number of allowed SSH-based CLI sessions.

Values 0 to 50

Platforms All

23.357 ssh-reply

ssh-reply

Syntax [**no**] **ssh-reply**

Context **[Tree]** (config>service>ies>if>vrrp ssh-reply)

Full Context configure service ies interface vrrp ssh-reply

Description This command enables the non-owner master to reply to SSH Requests directed at the virtual router instances IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Proper login and CLI command authentication is still enforced.

When ssh-reply is not enabled, SSH packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to SSH regardless of the ssh-reply configuration.

The ssh-reply command is only available in non-owner vrrp virtual-router-id nodal context. If the ssh-reply command is not executed, SSH packets to the virtual router instance IP addresses is silently discarded.

The **no** form of this command restores the default operation of discarding all SSH packets destined to the non-owner virtual router instance IP addresses.

Default no ssh-reply

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ssh-reply

Syntax [**no**] **ssh-reply**

Context **[Tree]** (config>service>vprn>if>vrrp ssh-reply)

Full Context configure service vprn interface vrrp ssh-reply

Description This command enables the non-owner master to reply to SSH Requests directed at the virtual router instance's IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Proper login and CLI command authentication is still enforced.

When ssh-reply is not enabled, SSH packets to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers never respond to SSH regardless of the ssh-reply configuration.

The ssh-reply command is only available in non-owner **vrrp** *virtual-router-id* nodal context. If the ssh-reply command is not executed, SSH packets to the virtual router instance IP addresses is silently discarded.

The **no** form of this command restores the default operation of discarding all SSH packets destined to the non-owner virtual router instance IP addresses.

Default no ssh-reply

Platforms All

ssh-reply

Syntax [**no**] **ssh-reply**

Context **[Tree]** (config>router>if>vrrp ssh-reply)

Full Context configure router interface vrrp ssh-reply

Description This command enables the non-owner master to reply to SSH requests directed at the virtual router instance IP addresses. This command is only applicable to IPv4.

Non-owner virtual router instances are limited by the VRRP specifications to responding to ARP requests destined to the virtual router IP addresses and routing IP packets not addressed to the virtual router IP addresses.

This limitation can be disregarded for certain applications. Ping, Telnet and SSH can be individually enabled or disabled on a per-virtual-router-instance basis.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **ssh-reply** command enables the non-owner master to reply to SSH requests directed at the virtual router instances IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Correct login and CLI command authentication is still enforced.

When **ssh-reply** is not enabled, SSH requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to SSH requests regardless of the **ssh-reply** setting.

The **ssh-reply** command is only available in non-owner **vrrp** nodal context.

By default, SSH requests to the virtual router instance IP addresses are silently discarded.

The **no** form of the command discards all SSH request messages destined to the non-owner virtual router instance IP addresses.

Default no ssh-reply — SSH requests to the virtual router instance IP addresses are discarded.

Platforms All

23.358 ssm

ssm

Syntax **ssm**

Context **[Tree]** (config>port>ethernet ssm)

Full Context configure port ethernet ssm

Description This command enables the Ethernet Synchronization Messaging Channel (ESMC) for the Ethernet port. ESMC carries the Synchronization Status Message (SSM) code representing the quality level of the source of frequency of the central clock of the node.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.359 ssm-assert-compatible-mode

ssm-assert-compatible-mode

Syntax **ssm-assert-compatible-mode** [**enable** | **disable**]

Context **[Tree]** (config>service>vprn>pim ssm-assert-compatible-mode)

Full Context configure service vprn pim ssm-assert-compatible-mode

Description This command specifies whether SSM assert is enabled in compatibility mode for this PIM protocol instance. When enabled, for SSM groups, PIM will consider the SPT bit to be implicitly set to compute the value of CouldAssert (S,G,I) as defined in RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. When disabled, for SSM groups, PIM will not assume the SPT bit to be set. The SPT bit is set by Update_SPTbit(S,G,iif) macro defined in RFC 4601.

Default ssm-assert-compatible-mode disable

Parameters **enable** — enables SSM assert in compatibility mode for this PIM protocol instance

disable — disabled SSM assert in compatibility mode for this PIM protocol instance

Platforms All

23.360 ssm-bit

ssm-bit

Syntax **ssm-bit** *sa-bit*

Context **[Tree]** (config>system>sync-if-timing>bits ssm-bit)

Full Context configure system sync-if-timing bits ssm-bit

Description This command configures which sa-bit to use for conveying SSM information when the interface-type is E1.

Default ssm-bit 8

Parameters *sa-bit* — Specifies the sa-bit value.

Values 4 to 8

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.361 ssm-default-range-disable

ssm-default-range-disable

Syntax **ssm-default-range-disable ipv4**

Context **[Tree]** (config>service>vprn>pim ssm-default-range-disable)

Full Context configure service vprn pim ssm-default-range-disable

Description This command specifies whether to disable the use of default range (232/8) for SSM so that it can be used by ASM to process (*,G). When enabled, the use of default range is disabled for SSM and it can be used by ASM. When disabled, the SSM default range is enabled.

Default ssm-default-range-disable

Platforms All

23.362 ssm-groups

ssm-groups

Syntax [**no**] **ssm-groups**

Context **[Tree]** (config>service>vprn ssm-groups)

Full Context configure service vprn ssm-groups

Description This command enables access to the context to enable a source-specific multicast (SSM) configuration instance.

ssm-groups

Syntax [**no**] **ssm-groups**

Context **[Tree]** (config>router>pim ssm-groups)

Full Context configure router pim ssm-groups

Description Commands in this context enable an ssm-group configuration instance.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.363 ssm-translate

ssm-translate

Syntax **ssm-translate**

Context **[Tree]** (config>service>vprn>igmp ssm-translate)
[Tree] (config>service>vprn>igmp>if ssm-translate)

Full Context configure service vprn igmp interface ssm-translate
configure service vprn igmp ssm-translate

Description Commands in this context configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the **starg** command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

Platforms All

ssm-translate

Syntax **ssm-translate**

Context **[Tree]** (config>service>vprn>mld ssm-translate)

Full Context configure service vprn mld ssm-translate

Description Commands in this context configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

Platforms All

ssm-translate

Syntax **ssm-translate**

Context **[Tree]** (config>router>igmp ssm-translate)
[Tree] (config>router>igmp>if ssm-translate)

Full Context configure router igmp interface ssm-translate
configure router igmp ssm-translate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

Platforms All

ssm-translate

Syntax **ssm-translate**

Context **[Tree]** (config>router>mld ssm-translate)
[Tree] (config>router>mld>if ssm-translate)

Full Context configure router mld interface ssm-translate
configure router mld ssm-translate

Description Commands in this context configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

Platforms All

23.364 stable-pool-sizing

stable-pool-sizing

Syntax [**no**] **stable-pool-sizing**

Context **[Tree]** (config>card>fp stable-pool-sizing)

Full Context configure card fp stable-pool-sizing

Description This command provides a stable buffer pool allocation environment for all default port buffer pools on a forwarding plane. This stable environment is provided at the expense of optimal buffer allocation between the various port buffer pools. Normally, port pools are sized according to a ports relative bandwidth with other ports and the ability of a port to use pool buffers. As an example, on a forwarding plane with two potential MDAs and only one equipped, the normal behavior is to provide all available default pool buffers to the ports on the currently equipped MDA. If a second MDA is equipped in the future, buffers are freed from the existing MDA and provided to the ports on the new MDA. Stable pool sizing alters this

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

behavior by reserving buffers for both MDAs whether they are equipped or not thus preventing a resizing event when an MDA is equipped. In addition, existing ports on a module always receive their maximum bandwidth share of buffers independent on any sub-rate condition that may currently exist. This provides a stable amount of buffers to other ports on the module independent of link or configuration events that may occur on the port.

Stable pool sizing preserves the ability to modify the effective bandwidth used to determine a port's relative share of the available buffers through the use of the ing-percentage-of-rate and egr-percentage-of-rate commands under the port configuration. Changing the values associated with these commands will cause a reevaluation of buffer distribution and thus a possible resizing of pools on each port within the module. These commands have no effect on ports associated with other modules on the forwarding plane.

Stable pool sizing may be enabled or disabled at any time on a forwarding plane. The system will dynamically change the pool sizes according to the stable pool sizing state.

When a port connector breakout is configured, its ports is included in the stable pool sizing calculation. Consequently, adding or removing a port connector breakout to or from the configuration will cause the buffer pool allocation to be recalculated even when stable pool sizing is enabled.

The **no** form of this command disables stable pool sizing on a forwarding plane. Existing buffer pools are resized according to normal pool sizing behavior.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.365 stack

stack

Syntax **stack** [**ipv4**] [**ipv6-slaac**]
no stack

Context **[Tree]** (config>subscr-mgmt>pppoe-client-policy stack)

Full Context configure subscriber-mgmt pppoe-client-policy stack

Description This command defines which NCP session is started in the PPPoE client and how addresses are retrieved within that NCP session.

Default stack ipv4

Parameters **ipv4** — Indicates that IPCP should be started and used to retrieve an IPv4 address.

ipv6-slaac — Indicates that IPv6CP should be started and that SLAAC is used to retrieve an IPv6 prefix.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.366 stack-capability-signaling

stack-capability-signaling

Syntax [**no**] **stack-capability-signaling**

Context **[Tree]** (config>service>ipipe stack-capability-signaling)

Full Context configure service ipipe stack-capability-signaling

Description This command enables stack-capability signaling in the initial label mapping message of the Ipipe PW to indicate that IPv6 is supported.

When enabled, the 7750 SR includes the stack-capability TLV with the IPv6 stack bit set according to the **ce-address-discovery ipv6** keyword, and also checks the value of the stack-capability TLV received from the far end.

This command must be blocked if no **ce-address-discovery** is specified, or the **ipv6** keyword is not included with the **ce-address-discovery** command.

This command if only applicable to the Ipipe service and must be blocked for all other services.

This command has no effect if both SAPs on the Ipipe service are local to the node.

Default no stack-capability-signaling

Platforms All

23.367 stale-routes-time

stale-routes-time

Syntax [**no**] **stale-routes-time** *time*

Context **[Tree]** (config>service>vprn>bgp>graceful-restart stale-routes-time)
[Tree] (config>service>vprn>bgp>group>graceful-restart stale-routes-time)
[Tree] (config>service>vprn>bgp>group>neighbor>graceful-restart stale-routes-time)

Full Context configure service vprn bgp graceful-restart stale-routes-time
configure service vprn bgp group graceful-restart stale-routes-time
configure service vprn bgp group neighbor graceful-restart stale-routes-time

Description This command configures the time period to keep stale routes before the END-OF-RIB message is received from the restarting router.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default 360 seconds

Parameters *time* — 1 to 3600 seconds

Platforms All

stale-routes-time

Syntax **stale-routes-time** *time*
no stale-routes-time

Context **[Tree]** (config>router>bgp>graceful-restart stale-routes-time)
[Tree] (config>router>bgp>group>graceful-restart stale-routes-time)
[Tree] (config>router>bgp>group>neighbor>graceful-restart stale-routes-time)

Full Context configure router bgp graceful-restart stale-routes-time
configure router bgp group graceful-restart stale-routes-time
configure router bgp group neighbor graceful-restart stale-routes-time

Description This command configures the maximum amount of time in seconds that stale routes should be maintained after a graceful restart is initiated.

The **no** form of this command resets the stale routes time back to the default of 360 seconds.

Default no stale-routes-time

Parameters *time* — Specifies the amount of time that stale routes should be maintained after a graceful restart is initiated.

Values 1 to 3600 seconds

Platforms All

23.368 stale-time

stale-time

Syntax **stale-time** *seconds*
no stale-time

Context **[Tree]** (config>service>ies>ipv6 stale-time)
[Tree] (config>service>ies>if>ipv6 stale-time)
[Tree] (config>service>vprn>ipv6 stale-time)
[Tree] (config>service>vprn>if>ipv6 stale-time)

Full Context configure service ies interface ipv6 stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies ipv6 stale-time
configure service vprn interface ipv6 stale-time
configure service vprn ipv6 stale-time

Description This command configures the time a neighbor discovery cache entry can remain stale before being removed.

The **no** form of this command removes the stale-time value.

Default no stale-time

Parameters *seconds* — The allowed stale time (in seconds) before a neighbor discovery cache entry is removed.

Values 60 to 65535

Platforms All

stale-time

Syntax **stale-time** *seconds*
no stale-time

Context **[Tree]** (config>router>ipv6 stale-time)

Full Context configure router ipv6 stale-time

Description This command configures the time a neighbor discovery cache entry can remain stale before being removed.

The **no** form of this command removes the stale-time value.

Default stale-time 14400

Parameters *seconds* — Specifies the allowed stale time (in seconds) before a neighbor discovery cache entry is removed.

Values 60 to 65535

Platforms All

stale-time

Syntax **stale-time** *seconds*
no stale-time

Context **[Tree]** (config>router>origin-validation>rpki-session stale-time)

Full Context configure router origin-validation rpki-session stale-time

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the maximum length of time that prefix origin validation records learned from the cache server remain usable after the RPKI-Router session goes down. The default stale-time is 3600 seconds (1 hour). When the timer expires all remaining stale entries associated with the session are deleted.

Default no stale-time

Parameters *seconds* — Specifies a time, in seconds.

Values 60 to 3600

Platforms All

stale-time

Syntax **stale-time** *seconds*
no stale-time

Context **[Tree]** (config>router>if>ipv6 stale-time)

Full Context configure router interface ipv6 stale-time

Description This command configures the time a neighbor discovery cache entry can remain stale before being removed.

The **no** form of this command removes the stale-time value.

Default no stale-time

Parameters *seconds* — The allowed stale time (in seconds) before a neighbor discovery cache entry is removed.

Values 60 to 65535

Platforms All

23.369 standard-multi-instance

standard-multi-instance

Syntax [**no**] **standard-multi-instance**

Context **[Tree]** (config>service>vprn>isis standard-multi-instance)

Full Context configure service vprn isis standard-multi-instance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables IS-IS multi-instance (MI) as described in draft-ginsberg-isis-mi-bis-01. Multiple instances allow instance-specific adjacencies to be formed that support multiple network topologies on the same physical interfaces. Each instance has an LSDB, and each PDU contains a TLV identifying the instance and the topology to which the PDU belongs. A single topology is supported in each instance, so the instance-specific topology identifier (ITID) is set to 0 and cannot be changed.

The **standard-multi-instance** (based on draft-ginsberg-isis-mi-bis-01) and **iid-tlv-enable** (based on draft-ietf-isis-mi-02) commands cannot be configured in the same instance, because the MAC addresses and PDUs from the two standards are incompatible.

The **no** form of this command removes the **standard-multi-instance** configuration.

Default no standard-multi-instance

Platforms All

standard-multi-instance

Syntax [**no**] **standard-multi-instance**

Context **[Tree]** (config>router>isis standard-multi-instance)

Full Context configure router isis standard-multi-instance

Description This command enables IS-IS multi-instance (MI) as described in *draft-ginsberg-isis-mi-bis-01*. Multiple instances allow instance-specific adjacencies to be formed that support multiple network topologies on the same physical interfaces. Each instance has an LSDB, and each PDU contains a TLV identifying the instance and the topology to which the PDU belongs. A single topology is supported in each instance, so the instance-specific topology identifier (ITID) is set to 0 and cannot be changed.

The **standard-multi-instance** (based on *draft-ginsberg-isis-mi-bis-01*) and **iid-tlv-enable** (based on *draft-ietf-isis-mi-02*) commands cannot be configured in the same instance, because the MAC addresses and PDUs from the two standards are incompatible.

The **no** form of this command removes the **standard-multi-instance** configuration.

Default no standard-multi-instance

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.370 standby

standby

Syntax [**no**] **standby**

Context **[Tree]** (config>router>mpls>lsp>secondary standby)

Full Context configure router mpls lsp secondary standby

Description The secondary path LSP is normally signaled once the primary path LSP fails. The **standby** keyword ensures that the secondary path LSP is signaled and maintained indefinitely in a hot standby state. Standby paths are selected in preference to non-standby secondary paths. When multiple standby secondary paths exist, then the path-preference is used to determine the order in which the paths are selected. If multiple standby secondary paths have the same, lowest, path-preference value then the system will select the path with the lowest up-time. When the primary path is re-established then the traffic is switched back to the primary path LSP.

The **no** form of this command specifies that the secondary LSP is signaled when the primary path LSP fails.

Platforms All

23.371 standby-forwarding

standby-forwarding

Syntax [**no**] **standby-forwarding**

Context **[Tree]** (config>service>ies>if>ipv6>vrrp standby-forwarding)

Full Context configure service ies interface ipv6 vrrp standby-forwarding

Description This command allows the forwarding of packets by a standby router.

The **no** form of this command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router’s real MAC address.

Default no standby-forwarding

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

standby-forwarding

Syntax [**no**] **standby-forwarding**

Context **[Tree]** (config>service>ies>if>vrrp standby-forwarding)

Full Context configure service ies interface vrrp standby-forwarding

Description This command allows the forwarding of packets by a standby router.

The **no** form of this command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router's real MAC address.

Default no standby-forwarding

Platforms All

standby-forwarding

Syntax [**no**] **standby-forwarding**

Context **[Tree]** (config>service>vprn>if>vrrp standby-forwarding)
[Tree] (config>service>vprn>if>ipv6>vrrp standby-forwarding)

Full Context configure service vprn interface ipv6 vrrp standby-forwarding
configure service vprn interface vrrp standby-forwarding

Description This command allows the forwarding of packets by a standby router.

The **no** form of this command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router's real MAC address.

Default no standby-forwarding

Platforms All

standby-forwarding

Syntax [**no**] **standby-forwarding**

Context **[Tree]** (config>router>if>vrrp standby-forwarding)
[Tree] (config>router>if>ipv6>vrrp standby-forwarding)

Full Context configure router interface ipv6 vrrp standby-forwarding
configure router interface vrrp standby-forwarding

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies whether this VRRP instance allows forwarding packets to a standby router. When disabled, a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router's real MAC address. When enabled, a standby router should forward all traffic.

Default no standby-forwarding

Platforms All

23.372 standby-ip-lifetime

standby-ip-lifetime

Syntax **standby-ip-lifetime** [**days** *days*] [**hrs** *hrs*] [**min** *min*] [**sec** *sec*]
standby-ip-lifetime [*seconds*]
standby-ip-lifetime

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile>dhcp-pool standby-ip-lifetime)

Full Context configure subscriber-mgmt vrgw brg brg-profile dhcp-pool standby-ip-lifetime

Description This command defines how long these addresses are kept aside when standby addresses are signaled to the pool. During this time these addresses can only be used by devices explicitly requesting the IP (for example, datatrigger or DHCP renew/rebind). When the timer expires the addresses will again become available for dynamic allocation.

Default standby-ip-lifetime hrs 6

Parameters *days* — Specifies the standby IP lifetime in days.

Values 1 to 3650

hrs — Specifies the standby IP lifetime in hours.

Values 1 to 23

min — Specifies the standby IP lifetime in minutes.

Values 1 to 59

sec — Specifies the standby IP lifetime in seconds.

Values 1 to 59

seconds — Specifies the lifetime of the standby IP addresses

Values 300 to 315446399

seconds — Specifies the lifetime in seconds.

Values 300 to 315446399

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.373 standby-mep-shutdown

standby-mep-shutdown

Syntax [**no**] **standby-mep-shutdown**

Context **[Tree]** (config>eth-cfm>redundancy>mc-lag standby-mep-shutdown)

Full Context configure eth-cfm redundancy mc-lag standby-mep-shutdown

Description This system wide command enables MEPs to track the state of MC-LAG. This allows MEPs on the standby MC-LAG to act administratively down.

The **no** form of command disables the MEP tracking.

Default no standby-mep-shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.374 standby-signaling

standby-signaling

Syntax **standby-signaling** {**lacp** | **power-off**}
no standby-signaling

Context **[Tree]** (config>lag standby-signaling)

Full Context configure lag standby-signaling

Description This command specifies how the state of a member port is signaled to the remote side when the status corresponding to this member port has the **standby** value.

Default standby-signaling lacp

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.375 standby-signaling-master

standby-signaling-master

Syntax [**no**] **standby-signaling-master**

Context **[Tree]** (config>service>epipe>endpoint standby-signaling-master)
[Tree] (config>service>ipipe>endpoint standby-signaling-master)

Full Context configure service epipe endpoint standby-signaling-master
configure service ipipe endpoint standby-signaling-master

Description When this command is enabled, the pseudowire standby bit (value 0x00000020) is sent to T-LDP peer for each spoke SDP of the endpoint that is selected as a standby.

This command is mutually exclusive with a VLL mate SAP created on a mc-lag/mc-aps or ICB. It is also mutually exclusive with vc-switching.

Default standby-signaling-master

Platforms All

23.376 standby-signaling-slave

standby-signaling-slave

Syntax [**no**] **standby-signaling-slave**

Context **[Tree]** (config>service>epipe>spoke-sdp-fec standby-signaling-slave)

Full Context configure service epipe spoke-sdp-fec standby-signaling-slave

Description This command enables standby-signaling-slave for an Epipe.

Platforms All

standby-signaling-slave

Syntax [**no**] **standby-signaling-slave**

Context **[Tree]** (config>service>epipe>endpoint standby-signaling-slave)
[Tree] (config>service>epipe>spoke-sdp standby-signaling-slave)

Full Context configure service epipe endpoint standby-signaling-slave

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service epipe spoke-sdp standby-signaling-slave

Description When this command is enabled, the node will block the transmit forwarding direction of a spoke SDP based on the pseudowire standby bit received from a T-LDP peer.

This command is present at the endpoint level as well as the spoke SDP level. If the spoke SDP is part of an explicit-endpoint, it will not be possible to change this setting at the spoke SDP level. An existing spoke SDP can be made part of the explicit endpoint only if the settings do not conflict. A newly created spoke SDP, which is part of a specific explicit-endpoint, will inherit this setting from the endpoint configuration.

This command is mutually exclusive with an endpoint that is part of an mc-lag, mc-aps or an ICB.

If the command is disabled, the node assumes the existing independent mode of behavior for the forwarding on the spoke SDP.

Default no standby-signaling-slave

Platforms All

23.377 starg

starg

Syntax [**no**] **starg**

Context **[Tree]** (config>subscr-mgmt>igmp-policy>static>group starg)
[Tree] (config>subscr-mgmt>igmp-policy starg)
[Tree] (config>subscr-mgmt>mld-policy>static>group starg)

Full Context configure subscriber-mgmt igmp-policy starg
configure subscriber-mgmt igmp-policy static group starg
configure subscriber-mgmt mld-policy static group starg

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

The **no** form of this command removes the starg entry from the configuration.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

starg

Syntax [**no**] **starg**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap>igmp-snooping>static>group starg)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping>static>group starg)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping>static>group starg)
[Tree] (config>service>vpls>sap>mld-snooping>static>group starg)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping>static>group starg)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping>static>group starg)

Full Context configure service vpls mesh-sdp igmp-snooping static group starg
configure service vpls mesh-sdp mld-snooping static group starg
configure service vpls sap igmp-snooping static group starg
configure service vpls sap mld-snooping static group starg
configure service vpls spoke-sdp igmp-snooping static group starg
configure service vpls spoke-sdp mld-snooping static group starg

Description This command adds a static (*,g) entry to allow multicast traffic for the corresponding multicast group from any source. This command can only be enabled if no existing source addresses for this group are specified.

The **no** form of this command removes the starg entry from the configuration.

Default no starg

Platforms All

starg

Syntax **starg**

Context [Tree] (config>service>vprn>igmp>if>static>group starg)

Full Context configure service vprn igmp interface static group starg

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the **no** form of this command to remove the starg entry from the configuration.

Platforms All

starg

Syntax [**no**] **starg**

Context [Tree] (config>service>vprn>mld>if>static>group starg)

Full Context configure service vprn mld interface static group starg

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Use the **no** form of this command to remove the **starg** entry from the configuration.

Platforms All

starg

Syntax [**no**] **starg**

Context **[Tree]** (config>router>igmp>if>static>group starg)

Full Context configure router igmp interface static group starg

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the **no** form of the command to remove the (*,G) entry from the configuration.

Platforms All

starg

Syntax [**no**] **starg**

Context **[Tree]** (config>router>igmp>tunnel-interface>static>group starg)

Full Context configure router igmp tunnel-interface static group starg

Description This command adds a static (*,G) group entry in a static group join on a tunnel interface associated with a P2MP RSVP LSP.

This command can only be enabled if no existing source addresses for this group are specified.

The **no** form of the command removes the (*,G) entry from the configuration.

Platforms All

starg

Syntax [**no**] **starg**

Context **[Tree]** (config>router>mld>if>static>group starg)

Full Context configure router mld interface static group starg

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the starg entry from the configuration.

Platforms All

23.378 start

start

Syntax **start** {**immediate** | **on-new-session**}

Context **[Tree]** (debug>app-assure>group>traffic-capture>record start)

Full Context debug application-assurance group traffic-capture record start

Description This command records limit conditions.

Parameters **immediate** — Start recording immediately for new or existing flows or sessions.

on-new-session — Only start recording record for new flows or sessions.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

start

Syntax **start** *start-week start-day start-month hours-minutes*

Context **[Tree]** (config>system>time>dst-zone start)

Full Context configure system time dst-zone start

Description This command configures start of summer time settings.

Default start first sunday january 00:00

Parameters *start-week* — Specifies the starting week of the month when the summer time takes effect.

Values first, second, third, fourth, last

Default first

start-day — Specifies the starting day of the week when the summer time takes effect.

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

Default sunday

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

start-month — Specifies the starting month of the year when the summer time takes effect.

Values january, february, march, april, may, june, july, august, september, october, november, december

Default january

hours-minutes — Specifies the time at which the summer time takes effect, in hh:mm format.

Values hours: 00 to 23
minutes: 00 to 59

Default 00:00

Platforms All

23.379 start-avg

start-avg

Syntax **start-avg** *percent*
no start-avg

Context **[Tree]** (config>qos>slope-policy>exceed-slope start-avg)
[Tree] (config>qos>slope-policy>highplus-slope start-avg)
[Tree] (config>qos>slope-policy>high-slope start-avg)
[Tree] (config>qos>slope-policy>low-slope start-avg)

Full Context configure qos slope-policy exceed-slope start-avg
configure qos slope-policy high-slope start-avg
configure qos slope-policy highplus-slope start-avg
configure qos slope-policy low-slope start-avg

Description This command sets the exceed, low, high, or highplus Random Early Detection (RED) slope position for the shared buffer average utilization value where the packet discard probability starts to increase above zero. The percent parameter is expressed as a percentage of the shared buffer size.

The **no** form of this command restores the start-avg value to the default setting. If the max-avg setting is smaller than the default, an error will occur and the start-avg setting will not be changed to the default.

Default start-avg 85 - Highplus slope default is 85% buffer utilization before discard probability starts to increase above zero.

start-avg 70 — High slope default is 70% buffer utilization before discard probability starts to increase above zero.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

start-avg 50 — Low slope default is 50% buffer utilization before discard probability starts to increase above zero.

start-avg 30 — Exceed slope default is 30% buffer utilization before discard probability starts to increase above zero.

Parameters *percent* — The percentage of the shared buffer space for the buffer pool at which point the drop probability starts to increase above zero. The value entered must be less than or equal to the current setting of **max-avg**. If the entered value is greater than the current value of **max-avg**, an error will occur and no change will take place.

Values 0 to 100

Platforms All

23.380 start-entry

start-entry

Syntax **start-entry** *entry-id* **count** *count*
no start-entry

Context **[Tree]** (config>li>li-filter-block-reservation>li-reserved-block start-entry)

Full Context configure li li-filter-block-reservation li-reserved-block start-entry

Description This command defines a block of reserved filter entries that are used to insert LI filter entries into a normal filter.

The **no** form of this command removes the entry ID and count from the configuration.

Parameters *entry-id* — Specifies an entry identification to start a block of reserved filter entries.

Values 1 to 65536

count — Specifies the number of entries in the block.

Values 1 to 8192

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.381 start-label

start-label

Syntax **start-label** *start-value* **end-label** *end-value*
no start-label

Context **[Tree]** (config>router>mpls-labels>reserved-label-block start-label)

Full Context configure router mpls-labels reserved-label-block start-label

Description This command configures start and end labels for a reserved label block. This command must be configured for a reserved label block to be created.

Default start-label 0, end-label 0

Parameters *start-value* — Specifies a starting value.

Values 18432 to 524287 within dynamic label range | 1048575 (FP4 only)

end-value — Specifies an ending value.

Values 18432 to 524287 within dynamic label range | 1048575 (FP4 only)

Platforms All

23.382 startup-wait-time

startup-wait-time

Syntax **startup-wait-time** [**min** *minutes*] [**sec** *seconds*] [**hrs** *hours*]
no startup-wait-time [**min** *minutes*] [**sec** *seconds*]

Context **[Tree]** (config>router>dhcp>server>failover startup-wait-time)
[Tree] (config>router>dhcp>server>pool>failover startup-wait-time)
[Tree] (config>router>dhcp6>server>failover startup-wait-time)
[Tree] (config>router>dhcp6>server>pool>failover startup-wait-time)

Full Context configure router dhcp local-dhcp-server failover startup-wait-time
configure router dhcp server pool failover startup-wait-time
configure router dhcp6 local-dhcp-server failover startup-wait-time
configure router dhcp6 server pool failover startup-wait-time

Description This command enables the startup wait time during which each peer waits after the initialization process before assuming the active role for the prefix designated as local or access-driven. This is to avoid transient issues during the initialization process.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **startup-wait-time** should be configured to an interval in which, after boot, both nodes can set up an MCS TCP link and start MCS. The timer is restarted each time the server downloads a lease from the MCS database and stops when the last state record from the peer is synchronized. The next state is (PRE-)NORMAL, unless the timer times out or is forced to stop via the tools command (**tools>perform>router>dhcp** or **dhcp6>local-dhcp-server** *server-name*>**pool**/**failover**>**abort-startup-wait**), in which case the local DHCP server transitions immediately to the COMMUNICATIONS-INTERRUPTED state.

Default startup-wait-time min 2

Parameters *minutes* — Specifies the startup wait time, in minutes.

Values 1 to 59

seconds — Specifies the startup wait time, in seconds.

Values 1 to 59

hours — Specifies the startup wait time, in hours.

Values 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.383 stat-mode

stat-mode

Syntax **stat-mode** *stat-mode*
no stat mode

Context **[Tree]** (config>subscr-mgmt>sla-prof>ingress>qos>policer stat-mode)
[Tree] (config>subscr-mgmt>sla-prof>ingress>qos>queue stat-mode)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>policer stat-mode)
[Tree] (config>subscr-mgmt>sla-prof>egress>qos>queue stat-mode)

Full Context configure subscriber-mgmt sla-profile egress qos policer stat-mode
configure subscriber-mgmt sla-profile egress qos queue stat-mode
configure subscriber-mgmt sla-profile ingress qos policer stat-mode
configure subscriber-mgmt sla-profile ingress qos queue stat-mode

Description This command is used to configure the forwarding plane octet and packet counters of a policer or queue to count packets of a specific type or state. For example separate counters for IPv4/IPv6 or separate counters for offered high and low priority policed traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For policers, this command overrides the policer stat-mode configuration as defined in the sap-ingress or sap-egress qos policy. For details on sap-ingress and sap-egress policer stat-mode, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*. For use in Enhanced Subscriber Management (ESM) context only, an additional stat-mode enables separate counters for IPv4 and IPv6 packets.

When a policer's stat-mode is changed while the sla profile is in use, any previous counter values are lost and any new counters are set to zero.

For queues, this command sets the stat-mode. Queue stat-mode is only available for use in Enhanced Subscriber Management (ESM) context to enable separate IPv4/IPv6 counters.

A queue's stat-mode cannot be changed while the SLA profile is in use.

The **no** form of this command reverts to the default.

Default For policers, the default is no stat-mode override. The sap-ingress or sap-egress stat-mode is used instead.

For queues, the default is to count in-/out-of-profile octets and packets.

Parameters *stat-mode* — Specifies the stat mode for the policer.

For ingress and egress qos queue stat-mode overrides.

For ingress and egress qos policer stat-mode overrides, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for details on the **sap-ingress** and **sap-egress policer stat-mode** parameters.

For use in Enhanced Subscriber Management (ESM) context only:

Values no-stats, minimal, offered-profile-no-cir, offered-priority-no-cir, offered-profile-cir, offered-priority-cir, offered-total-cir, offered-limited-profile-cir, offered-profile-capped-cir, offered-limited-capped-cir, v4-v6 (count IPv4 and IPv6 forwarded/dropped octets and packets separately)

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt sla-profile egress qos queue stat-mode
- configure subscriber-mgmt sla-profile ingress qos queue stat-mode

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt sla-profile ingress qos policer stat-mode
- configure subscriber-mgmt sla-profile egress qos policer stat-mode

stat-mode

Syntax **stat-mode** *stat-mode*
no stat mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>card>fp>ingress>access>qgrp>policer-over>plcr stat-mode)
[Tree] (config>card>fp>ingress>network>qgrp>policer-over>plcr stat-mode)

Full Context configure card fp ingress access queue-group policer-override policer stat-mode
configure card fp ingress network queue-group policer-override policer stat-mode

Description This command configures the forwarding plane counters that allow offered, output and discard accounting to occur for the policer. An ingress policer has multiple types of offered packets (explicit in-profile, explicit out-of-profile, high priority or low priority) and each of these offered types is interacting with the policer's metering and profiling functions resulting in colored output packets (green, yellow and red). Due to the large number of policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly profiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported which prevents any packet accounting, the use of the policer's **parent** command requires at the policer's **stat-mode** to be set at least to the **minimal** setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated. Once a policer has been made a child to a parent policer, the **stat-mode** cannot be changed to **no-stats** unless the policer parenting is first removed.

Each time the policer's **stat-mode** is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. You can view the total/allocated/free stats by using the **tools dump resource-usage** command. If insufficient counters exist to implement a mode on any policer instance, the **stat-mode** change will fail and the previous mode will continue unaffected for all instances of the policer.

The default **stat-mode** when a policer is created within the policy is **minimal**.

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the **stat-mode** override command will fail. The previous **stat-mode** setting active for the policer will continue to be used by the policer.

The **no** form of this command attempts to return the policer's stat-mode setting to minimal. The command will fail if insufficient policer counter resources exist to implement minimal where the QoS policer is currently applied and has a forwarding class mapping.

Parameters
- See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for details on the policer stat-mode parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

stat-mode

Syntax **stat-mode** *stat-mode*
no stat-mode

Context **[Tree]** (config>service>apipe>sap>egress>policer-over>plcr stat-mode)
[Tree] (config>service>apipe>sap>ingress>policer-over>plcr stat-mode)
[Tree] (config>service>cpipe>sap>egress>policer-over>plcr stat-mode)
[Tree] (config>service>cpipe>sap>ingress>policer-over>plcr stat-mode)
[Tree] (config>service>epipe>sap>egress>policer-over>plcr stat-mode)
[Tree] (config>service>epipe>sap>ingress>policer-over>plcr stat-mode)
[Tree] (config>service>fpipe>sap>egress>policer-over>plcr stat-mode)
[Tree] (config>service>fpipe>sap>ingress>policer-over>plcr stat-mode)
[Tree] (config>service>ipipe>sap>egress>policer-over>plcr stat-mode)
[Tree] (config>service>ipipe>sap>ingress>policer-over>plcr stat-mode)

Full Context configure service apipe sap egress policer-override policer stat-mode
configure service apipe sap ingress policer-override policer stat-mode
configure service cpipe sap egress policer-override policer stat-mode
configure service cpipe sap ingress policer-override policer stat-mode
configure service epipe sap egress policer-override policer stat-mode
configure service epipe sap ingress policer-override policer stat-mode
configure service fpipe sap egress policer-override policer stat-mode
configure service fpipe sap ingress policer-override policer stat-mode
configure service ipipe sap egress policer-override policer stat-mode
configure service ipipe sap ingress policer-override policer stat-mode

Description The SAP QoS policy's **policer stat-mode** command is used to configure the forwarding plane counters that allow offered, output, and discard accounting to occur for the policer. A policer has multiple types of offered packets (for example, soft in-profile and out-of-profile from ingress and hard in-profile and out-of-profile due to egress profile overrides) and each of these offered types is interacting with the policers metering and profiling functions resulting in colored output packets (green, yellow, and red). Due to the potentially large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly re-profiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and indicates how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported that prevents any packet accounting, the use of the policer's parent command requires that the policer's **stat-mode** to be set at least to the minimal setting so that offered statistics are available for the policer's Fair Information Rate (FIR) to be calculated.

Each time the policer's stat mode is changed, any previous counter values are lost and any new counters are set to zero.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. The total/allocated/free statistics can be viewed by using the **tools dump resource-usage card** *slot-num* **fp** *fp-number* command. If insufficient counters exist to implement a mode on any policer instance, the stat-mode change will fail and the previous mode will continue unaffected for all instances of the policer.

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on a SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the stat-mode override command will fail. The current active stat mode setting will continue to be used by the policer.

The command will fail if insufficient policer counter resources exist to implement **minimal** where the QoS policer is currently applied and has a forwarding class mapping.

The **no** form of this command attempts to return the policer's stat-mode setting to **minimal**.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for detailed information about the supported parameters for the **policer stat-mode** command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe sap egress policer-override policer stat-mode
- configure service fpipe sap ingress policer-override policer stat-mode
- configure service fpipe sap egress policer-override policer stat-mode
- configure service cpipe sap ingress policer-override policer stat-mode

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure service ipipe sap egress policer-override policer stat-mode
- configure service epipe sap egress policer-override policer stat-mode
- configure service epipe sap ingress policer-override policer stat-mode
- configure service ipipe sap ingress policer-override policer stat-mode

7450 ESS, 7750 SR-7/12/12e, 7750 SR-e, 7950 XRS

- configure service apipe sap egress policer-override policer stat-mode
- configure service apipe sap ingress policer-override policer stat-mode

stat-mode

Syntax **stat-mode** st*at-mode*
no stat-mode

Context **[Tree]** (config>service>vpls>sap>egress>policer-override>plcr stat-mode)
[Tree] (config>service>vpls>sap>ingress>policer-override>plcr stat-mode)

Full Context configure service vpls sap egress policer-override policer stat-mode
configure service vpls sap ingress policer-override policer stat-mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The SAP-egress QoS policy's policer stat-mode command is used to configure the forwarding plane counters that allow offered, output and discard accounting to occur for the policer. A policer has multiple types of offered packets (for example, soft in-profile and out-of-profile from ingress and hard in-profile and out-of-profile due to egress profile overrides) and each of these offered types is interacting with the policers metering and profiling functions resulting in colored output packets (green, yellow and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly re-profiled offered packets. The stat-mode command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a no-stats mode is supported which prevents any packet accounting, the use of the policer's parent command requires that the policer's stat-mode to be set at least to the minimal setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated.

Each time the policer's stat-mode is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. You can view the total/allocated/free stats by using the **tools dump resource-usage card** *slot-num* **fp** *fp-number* command. If insufficient counters exist to implement a mode on any policer instance, the stat-mode change will fail and the previous mode will continue unaffected for all instances of the policer.

The default stat-mode when a policer is created within the policy is minimal.

The stat-mode setting defined for the policer in the QoS policy may be overridden on a SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the stat-mode override command will fail. The previous stat-mode setting active for the policer will continue to be used by the policer.

The **no** form of the command returns the policer's stat-mode setting to minimal.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for detailed information about the **policer stat-mode** command parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

stat-mode

Syntax **stat-mode** st*at-mode*
no stat-mode

Context **[Tree]** (config>service>ies>if>sap>egress>policer-override>plcr stat-mode)
[Tree] (config>service>ies>if>sap>ingress>policer-override>plcr stat-mode)

Full Context configure service ies interface sap egress policer-override policer stat-mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service ies interface sap ingress policer-override policer stat-mode

Description The SAP-egress QoS policy's policer stat-mode command is used to configure the forwarding plane counters that allow offered, output and discard accounting to occur for the policer. A policer has multiple types of offered packets (for example, soft in-profile and out-of-profile from ingress and hard in-profile and out-of-profile due to egress profile overrides) and each of these offered types is interacting with the policers metering and profiling functions resulting in colored output packets (green, yellow and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly re-profiled offered packets. The stat-mode command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a no-stats mode is supported which prevents any packet accounting, the use of the policer's parent command requires that the policer's stat-mode to be set at least to the minimal setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated.

Each time the policer's stat-mode is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. You can view the total/allocated/free stats by using the **tools dump resource-usage card** *slot-num* **fp** *fp-number* command. If insufficient counters exist to implement a mode on any policer instance, the stat-mode change will fail and the previous mode will continue unaffected for all instances of the policer.

The default stat-mode when a policer is created within the policy is minimal.

The stat-mode setting defined for the policer in the QoS policy may be overridden on a SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the stat-mode override command will fail. The previous stat-mode setting active for the policer will continue to be used by the policer.

The **no** form of this command returns the policer's stat-mode setting to minimal.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for detailed information about the **policer stat-mode** command parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

stat-mode

Syntax **stat-mode** st*at-mode*
no stat-mode

Context **[Tree]** (config>service>vprn>if>sap>egress>policer-override>plcr stat-mode)
[Tree] (config>service>vprn>if>sap>ingress>policer-override>plcr stat-mode)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn interface sap egress policer-override policer stat-mode
configure service vprn interface sap ingress policer-override policer stat-mode

Description The SAP-egress QoS policy's policer stat-mode command is used to configure the forwarding plane counters that allow offered, output and discard accounting to occur for the policer. A policer has multiple types of offered packets (for example, soft in-profile and out-of-profile from ingress and hard in-profile and out-of-profile due to egress profile overrides) and each of these offered types is interacting with the policers metering and profiling functions resulting in colored output packets (green, yellow and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly re-profiled offered packets. The stat-mode command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a no-stats mode is supported which prevents any packet accounting, the use of the policer's parent command requires that the policer's stat-mode to be set at least to the minimal setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated.

Each time the policer's stat-mode is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. You can view the total/allocated/free stats by using the **tools dump resource-usage card** *slot-num* **fp** *fp-number* command. If insufficient counters exist to implement a mode on any policer instance, the stat-mode change will fail and the previous mode will continue unaffected for all instances of the policer.

The default stat-mode when a policer is created within the policy is minimal.

The stat-mode setting defined for the policer in the QoS policy may be overridden on a SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the stat-mode override command will fail. The previous stat-mode setting active for the policer will continue to be used by the policer.

The **no** form of this command returns the policer's stat-mode setting to minimal.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide* for detailed information about the **policer stat-mode** command parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

stat-mode

Syntax **stat-mode** {**no-stats** | **minimal** | **offered-profile-no-cir** | **offered-priority-no-cir** | **offered-profile-cir** | **offered-priority-cir** | **offered-total-cir** | **offered-limited-profile-cir** | **offered-profile-capped-cir** | **offered-limited-capped-cir**}
no stat mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>sap-ingress>dyn-policer stat-mode)
[Tree] (config>qos>sap-ingress>policer stat-mode)

Full Context configure qos sap-ingress dynamic-policer stat-mode
configure qos sap-ingress policer stat-mode

Description This command is used to configure the forwarding plane counters that allow offered, forwarded, and dropped accounting to occur for the policer. An ingress policer has multiple types of offered packets (explicit in-profile, explicit out-of-profile, uncolored, high-priority, or low priority) and each of these offered types is interacting with the policer's metering and profiling functions resulting in colored output packets (green, yellow, and red). Due to the large number of policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers, for example, will not be configured with a CIR profiling rate and not all policers will receive explicitly profiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported that prevents any packet accounting, the use of the policer's **parent** command requires that the policer's **stat-mode** be set at least to the **minimal** setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated. When a policer has been made a child to a parent policer, the **stat-mode** cannot be changed to **no-stats** unless the policer parenting is first removed.

Each time the policer's **stat-mode** is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. The total/allocated/free stats can be viewed by using the **tools dump resource-usage card fp** command. If insufficient counters exist to implement a mode on any policer instance, the **stat-mode** change will fail and the previous mode will continue unaffected for all instances of the policer.

The ingress policer stat-modes are described in Table 133.

Table 133 **Ingress Policer Stat Mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
no-stats	0	—	—	—
Minimal	1	Single counter entering policer	Single counter for dropped/forwarded exiting policer	—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 133 **Ingress Policer Stat Mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-profile-no-cir	2	In/out entering policer	In/out entering policer	Intended for when the policer does not change the profile of packets. Includes only in-profile and out-of-profile.
offered-priority-no-cir	2	High/low entering policer	High/low entering policer	Intended for when only packet priority stats are required.
offered-profile-cir	4	In/out/uncolored entering policer	In/out exiting policer	Intended for when the policer can change the profile of packets to in-profile and out-of-profile.
offered-priority-cir	4	High/low entering policer	In/out exiting policer	Intended for when packet priority entering the policer and profile exiting the policer is required.
offered-total-cir	2	Single counter entering policer	In/out exiting policer	—
offered-limited-profile-cir	3	Out/uncolored entering policer	In/out exiting policer	Intended for when the policer can change the profile of packet to in-profile and out-of-profile. The information is limited compared to offered-profile-capped-cir with the benefit of using one less stat resource.
offered-profile-capped-cir	5	In/out/uncolored entering policer	In/out exiting policer	Intended for when the policer has profile-capped configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 133 **Ingress Policer Stat Mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-limited-capped-cir	4	In/uncolored entering policer	In/out exiting policer	Intended for when the policer has profile-capped configured. The information is limited compared to offered-profile-capped-cir with the benefit of using one less stat resource.

The default **stat-mode** when a policer is created within the policy is **minimal**.

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the **stat-mode** override command will fail. The previous **stat-mode** setting active for the policer will continue to be used by the policer.

The **no** form of this command attempts to return the policer's stat-mode setting to minimal. The command will fail if insufficient policer counter resources exist to implement minimal where the QoS policer is currently applied and has a forwarding class mapping.

Parameters **no-stats** — Counter resource allocation: 0

The policer does not have any forwarding plane counters allocated and cannot provide offered, dropped, and forwarded statistics. A policer using no-stats cannot be a child to a parent policer and the policer's parent command will fail.

When **collect-stats** is enabled, no statistics are generated.

minimal — Counter resource allocation: 1

This stat-mode provides the minimal accounting resource usage and counter information, and includes the total offered, dropped and forwarded packet and octet counters for traffic entering (offered) and exiting (dropped/forwarded) the policer.

The default **stat-mode** for a policer is **minimal**. The **minimal** mode allocates 1 forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types (profile or priority) and do not count in-profile or out-of-profile output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate.

This counter mode is useful when only the most basic accounting information is required.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 134.

Table 134 **Ingress Accounting Statistics Collected in minimal stat-mode**

Show Output	Accounting Statistics Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. All	apd	AllPacketsDropped
	aod	AllOctetsDropped
For. All	apf	AllPacketsForwarded
	aof	AllOctetsForwarded

offered-profile-no-cir — Counter resource allocation: 2

This **stat-mode** provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering the policer.

The **offered-profile-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-profile-no-cir** mode is most useful when the policer is receiving only in-profile and out-of-profile premarked (and trusted) packets. It is expected that, in this instance, a CIR rate will not be defined since all packets are already premarked. This mode does not prevent the policer from receiving untrusted (color undefined) traffic nor does it prevent the policer from being configured with a CIR rate.

This mode is intended to be used without profile-capped configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 135.

Table 135 **Ingress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Statistics Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 135 **Ingress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Statistics Collected	
	Field	**Field Description**
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-priority-no-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the packet priority of traffic entering the policer.

The **offered-priority-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-priority-no-cir** mode is most useful when the policer is receiving only untrusted packets and the ingress priority high and priority low classification options are being used without a CIR profiling rate defined. This mode does not prevent the policer from receiving trusted packets that are premarked in-profile or out-of-profile nor does it prevent the policer from being configured with a CIR rate.

This mode is intended to be used without profile-capped configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 136.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 136 **Ingress Accounting Statistics Collected in offered-priority-no-cir stat-mode**

Show Output	Accounting Statistics Collected	
	Field	**Field Description**
Off. HiPrio	hpo	HighPriorityPacketsOffered
	hoo	HighPriorityOctetsOffered
Off. LowPrio	lpo	LowPriorityPacketsOffered
	loo	LowPriorityOctetsOffered
Dro. HiPrio	hpd	HighPriorityPacketsDropped
	hod	HighPriorityOctetsDropped
Dro. LowPrio	lpd	LowPriorityPacketsDropped
	lod	LowPriorityOctetsDropped
For. HiPrio	hpf	HighPriorityPacketsForwarded
	hof	HighPriorityOctetsForwarded
For. LowPrio	lpf	LowPriorityPacketsForwarded
	lof	LowPriorityOctetsForwarded

offered-profile-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed so that the traffic entering the policer comprises hard in/out and uncolored traffic. The offered counters cover traffic explicitly profiled to in-profile, traffic explicitly profiled to out-of-profile, and traffic that has not been explicitly profiled at ingress (uncolored).

The **offered-profile-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-profile-cir** mode is most useful when the policer is receiving trusted out-of-profile and in-profile traffic and is also receiving untrusted packets that are being applied to a defined CIR profiling rate. This mode differs from **offered-limited-profile-cir** mode in that it expects both trusted in-profile and out-of-profile packets while still performing CIR profiling on packets with untrusted markings. If trusted in-profile packets are not being received, the **offered-limited-profile-cir** stat-mode could be used instead, which has the benefit of using a reduced number of stat resources.

This mode is intended to be used without **profile-capped** configured within the policer as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 137.

Table 137 **Ingress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-priority-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the priority of traffic entering the policer and the profile exiting the policer.

The **offered-priority-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-priority-cir** mode is most useful when the policer is receiving only untrusted packets that are being classified as high priority or low priority and are being applied to a defined CIR profiling rate. This mode differs from **offered-profile-cir** mode in that it does not expect trusted in-profile and out-of-profile packets but does not exclude the ability of the policer to receive them.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 138.

Table 138 **Ingress Accounting Statistics Collected in offered-priority-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. HiPrio	hpo	HighPriorityPacketsOffered
	hoo	HighPriorityOctetsOffered
Off. LowPrio	lpo	LowPriorityPacketsOffered
	loo	LowPriorityOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-total-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter.

The **offered-total-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-total-cir** mode is most useful when the policer is not receiving trusted in-profile or out-of-profile traffic and both high- and low-priority classifications are not being used on the untrusted packets and the offered packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile or out-of-profile packets and does not prevent the use of priority high or low classifications on the untrusted packets.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 139.

Table 139 **Ingress Accounting Statistics Collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-profile-cir — Counter resource allocation: 3

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed so that the traffic entering the policer comprises of hard out and uncolored. The offered counters cover traffic explicitly profiled to out-of-profile and traffic that has not been explicitly profiled at ingress (Uncolor). The traffic explicitly profiled to in-profile is counted with the uncolored traffic.

The **offered-limited-profile-cir** mode allocates three forwarding plane offered counters and three traffic manager discard counters.

The **offered-limited-profile-cir** mode is most useful when the policer is receiving trusted out-of-profile (profile out but no profile in) traffic and untrusted packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile packets. If trusted in-profile packets are not being received, the **offered-limited-profile-cir** is preferred over **offered-profile-cir** because it uses a reduced number of stat resources.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 140.

Table 140 **Ingress Accounting Statistics Collected in offered-limited-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-cir — Counter resource allocation: 4

offered-profile-capped-cir — Counter resource allocation: 5

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed so that the traffic entering the policer comprises of hard in/out and uncolored. The offered counters cover traffic explicitly profiled to in-profile, traffic explicitly profiled to out-of-profile, and traffic that has not been explicitly profiled at ingress (Uncolor).

When **offered-profile-capped-cir** is defined, the system creates five offered-output counters in the forwarding plane and five discard counters in the traffic manager.

The **offered-profile-capped-cir** mode is similar to the offered-profile-cir mode except that it includes support for profile in and **soft-in-profile** that may be output as out-of-profile due to enabling **profile-capped** mode on the ingress policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The impact of using **offered-profile-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 141.

Table 141 **Ingress Accounting Statistics Collected in offered-profile-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-capped-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed resulting in the traffic entering the policer comprising of hard in/out and uncolored. The offered counters cover in-profile traffic and traffic that has not been explicitly profiled at ingress (Uncolor). The traffic explicitly profiled to out-of-profile is counted with the uncolored traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When **offered-limited-capped-cir** is defined, the system creates four forwarding plane offered-output counters in the network processor and four discard counters in the traffic manager.

The **offered-limited-capped-cir** mode is similar to the **offered-profile-capped-cir** mode except that it combines **soft in-profile** with **profile in** (InProf) and **profile out** (OutProf) with **soft-out-of-profile** (Uncolor) and eliminates the “offered undefined” statistic. If trusted out-of-profile packets are not being received, the **offered-limited-capped-cir** is preferred over **offered-profile-capped-cir** because it uses a reduced number of stat resources.

This mode is intended to be used with **profile-capped** configured within the policer.

The impact of using **offered-limited-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 142.

Table 142 **Ingress Accounting Statistics Collected in offered-limited-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure qos sap-ingress dynamic-policer stat-mode

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

- configure qos sap-ingress policer stat-mode

stat-mode

Syntax **stat-mode** {**no-stats** | **minimal** | **offered-profile-no-cir** | **offered-profile-cir** | **offered-total-cir** | **offered-limited-capped-cir** | **offered-profile-capped-cir**}
no stat mode

Context **[Tree]** (config>qos>sap-egress>dyn-policer stat-mode)

Full Context configure qos sap-egress dynamic-policer stat-mode

Description The **sap-egress** QoS policy's policer **stat-mode** command is used to configure the forwarding plane counters that allow offered, forwarded, and dropped accounting to occur for the policer. An egress policer has multiple types of offered packets (soft in-profile and out-of-profile from ingress and hard in-profile, out-of-profile, and exceed-profile due to egress profile overrides) and each of these offered types is interacting with the policer's metering and profiling functions resulting in colored output packets (green, yellow, and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers, for example, will not be configured with a CIR profiling rate and not all policers will receive explicitly reprofiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported that prevents any packet accounting, the use of the policer's **parent** command requires that the policer's **stat-mode** be set at least to the **minimal** setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated. When a policer has been made a child to a parent policer, the **stat-mode** cannot be changed to **no-stats** unless the policer parenting is first removed.

Each time the policer's **stat-mode** is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. The total, allocated, and free statistics can be viewed by using the **tools dump resource-usage card fp** command. If insufficient counters exist to implement a mode on any policer instance, the **stat-mode** change will fail and the previous mode will continue unaffected for all instances of the policer.

The egress policer stat-modes are described in Table 143.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 143 **Egress Policer Stat-mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
no-stats	0	—	—	—
minimal	1	Single counter entering policer	Single counter for dropped/forwarded exiting policer	—
offered-profile-no-cir	2	In or out entering policer	In/out entering policer	Intended for when the policer does not change the profile of packets. Includes only in-profile and out-of-profile.
offered-profile-cir	4	In, out, or uncolored (which corresponds to hard in-profile, hard out-of-profile, or soft in- or out-of-profile) entering policer	In/out exiting policer	Intended for when the policer can change the profile of packets to in-profile and out-of-profile.
offered-total-cir	2	Single counter entering policer	In/out exiting policer	—
offered-limited-capped-cir	4	In or out entering policer	In/out exiting policer	Intended for when the policer has **profile-capped** configured. The information is limited compared to **offered-profile-capped-cir** with the benefit of using one less stat resource.
offered-profile-capped-cir	5	In, out, or uncolored (which corresponds to hard in-profile, hard out-of-profile, or soft in- or out-of-profile) entering policer	In/out exiting policer	Intended for when the policer has **profile-capped** configured

When a policer is created within the policy, the default setting for **stat-mode** is **minimal**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the **stat-mode** override command will fail. The previous **stat-mode** setting active for the policer will continue to be used by the policer.

The **no** form of this command attempts to return the policer's **stat-mode** setting to **minimal**. The command will fail if insufficient policer counter resources exist to implement **minimal** where the QoS policer is currently applied and has a forwarding class mapping.

Parameters **no-stats** — Counter resource allocation: 0

The policer does not have any forwarding plane counters allocated and cannot provide offered, discard, and forward statistics. A policer using **no-stats** cannot be a child to a parent policer and the policer's **parent** command will fail.

When **collect-stats** is enabled, no statistics are generated.

minimal — Counter resource allocation: 1

This stat-mode provides the minimal accounting resource usage and counter information, and includes only the total offered, dropped and forwarded packet and octet counters for traffic entering (offered) and exiting (dropped/forwarded) the policer.

The default **stat-mode** for a policer is **minimal**. The **minimal** mode allocates 1 forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types and do not count different profile output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate or using exceed PIR.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 144.

Table 144 **Egress Accounting Statistics Collected in minimal stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. All	apd	AllPacketsDropped
	aod	AllOctetsDropped
For. All	apf	AllPacketsForwarded
	aof	AllOctetsForwarded

offered-profile-no-cir — Counter resource allocation: 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering the policer. inplus-profile traffic is counted with the in-profile counters and exceed-profile traffic is counted with the out-of-profile counters.

The **offered-profile-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-profile-no-cir** mode is most useful when profile-based offered, dropped, and forwarded stats are required from the egress policer, but a CIR or **enable-exceed-pir** is not being used to recolor the soft in-profile and out-of-profile packets. This mode does not prevent the policer from being configured with a CIR rate or using **enable-exceed-pir**.

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 145.

Table 145 **Egress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-cir — Counter resource allocation: 4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is made up of traffic that is inplus-profile, in-profile, out-of-profile, exceed-profile, soft in-profile, and soft out-of-profile. The offered counters cover traffic reclassified to in-profile (which includes traffic reclassified to inplus-profile), traffic reclassified to out-of-profile (which includes traffic reclassified to exceed-profile) and traffic which has not been reclassified at egress (Uncolor). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

The **offered-profile-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-profile-cir** mode is most useful when profile-based offered, dropped and forwarded stats are required from the egress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.

This mode is intended to be used without **profile-capped** or **enable-exceed-pir** configured within the policer as these could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 146.

Table 146 **Egress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 146 **Egress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-total-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

The **offered-total-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-total-cir** mode is most useful when the policer is not receiving trusted in-profile or out-of-profile traffic, and both high- and low- priority classifications are not being used on the untrusted packets, and the offered packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile or out-of-profile packets and does not prevent the use of priority high or low classifications on the untrusted packets.

This mode is intended to be used without **profile-capped** or **enable-exceed-pir** configured within the policer as these could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 147.

Table 147 **Egress Accounting Statistics Collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 147 **Egress Accounting Statistics Collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-capped-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is made up of traffic that is inplus-profile, in-profile, out-of-profile, exceed-profile, soft in-profile, and soft out-of-profile. The offered counters cover in-profile traffic (which includes traffic reclassified to inplus-profile) and out-of-profile traffic (which includes traffic reclassified to exceed-profile). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

offered-limited-capped-cir is defined, the system creates four forwarding plane offered-output counters in the network processor and three discard counters in the traffic manager.

The **offered-limited-capped-cir** mode is similar to the **offered-profile-capped-cir** mode except that it combines **soft in-profile** with **profile in** and **soft-out-of-profile** with **profile out** and eliminates the offered-undefined statistic.

The impact of using **offered-limited-capped-cir** stat-mode while profile-capped mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used and **soft-in-profile** will be treated as offered-in instead of offered-undefined.

This mode is intended to be used with **profile-capped** configured within the policer but without **enable-exceed-pir** configured as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 148.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 148 **Egress Accounting Statistics Collected in offered-limited-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-capped-cir — Counter resource allocation: 5

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is made up of traffic that is inplus-profile, in-profile, out-of-profile, exceed-profile, soft in-profile, and soft out-of-profile. The offered counters cover traffic reclassified to in-profile (which includes traffic reclassified to inplus-profile), traffic reclassified to out-of-profile (which includes traffic reclassified to exceed-profile) and traffic that has not been reclassified at egress (uncolored). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

When **offered-profile-capped-cir** is defined, the system creates five offered-output counters in the forwarding plane and five discard counters in the traffic manager.

The **offered-profile-capped-cir** mode is similar to the **offered-profile-cir** mode except that it includes support for **profile inplus**, **profile in** and **soft-in-profile** that may be output as out-of-profile due to enabling **profile-capped** mode on the ingress policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The impact of using o**ffered-profile-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used and soft-in-profile will be treated as offered-in (hard in-profile) instead of offered-undefined (uncolored).

This mode is intended to be used with **profile-capped** configured within the policer but without **enable-exceed-pir** configured as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 149.

Table 149 **Egress Accounting Statistics Collected in offered-profile-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

stat-mode

Syntax **stat-mode** {**no-stats** | **minimal** | **offered-profile-no-cir** | **offered-profile-cir** |

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

offered-total-cir | **offered-limited-capped-cir** | **offered-profile-capped-cir** | **offered-total-cir-exceed** | **offered-four-profile-no-cir** | **offered-total-cir-four-profile**}

no stat mode

Context **[Tree]** (config>qos>sap-egress>policer stat-mode)

Full Context configure qos sap-egress policer stat-mode

Description The **sap-egress** QoS policy's policer **stat-mode** command is used to configure the forwarding plane counters that allow offered, forwarded, and dropped accounting to occur for the policer. An egress policer has multiple types of offered packets (soft in-profile and out-of-profile from ingress and hard in-profile, out-of-profile, and exceed-profile due to egress profile overrides) and each of these offered types is interacting with the policer's metering and profiling functions resulting in colored output packets (green, yellow, and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers, for example, will not be configured with a CIR profiling rate and not all policers will receive explicitly reprofiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported that prevents any packet accounting, the use of the policer's **parent** command requires that the policer's **stat-mode** be set at least to the **minimal** setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated. When a policer has been made a child to a parent policer, the **stat-mode** cannot be changed to **no-stats** unless the policer parenting is first removed.

Each time the policer's **stat-mode** is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. The total, allocated, and free statistics can be viewed by using the **tools dump resource-usage card fp** command. If insufficient counters exist to implement a mode on any policer instance, the **stat-mode** change will fail and the previous mode will continue unaffected for all instances of the policer.

The egress policer stat-modes are described in Table 150.

Table 150 **Egress Policer Stat-mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
no-stats	0	—	—	—
minimal	1	Single counter entering policer	Single counter for dropped/forwarded exiting policer	—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 150 **Egress Policer Stat-mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-profile-no-cir	2	In or out entering policer	In/out entering policer	Intended for when the policer does not change the profile of packets. Includes only in-profile and out-of-profile.
offered-profile-cir	4	In, out, or uncolored (which corresponds to hard in-profile, hard out-of-profile, or soft in- or out-of-profile) entering policer	In/out exiting policer	Intended for when the policer can change the profile of packets to in-profile and out-of-profile.
offered-total-cir	2	Single counter entering policer	In/out exiting policer	—
offered-limited-capped-cir	4	In or out entering policer	In/out exiting policer	Intended for when the policer has **profile-capped** configured. The information is limited compared to **offered-profile-capped-cir** with the benefit of using one less stat resource.
offered-profile-capped-cir	5	In, out, or uncolored (which corresponds to hard in-profile, hard out-of-profile, or soft in- or out-of-profile) entering policer	In/out exiting policer	Intended for when the policer has **profile-capped** configured

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 150 **Egress Policer Stat-mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-total-cir-exceed	3	Single counter entering policer	In/out/exceed exiting policer	Intended for when the policer is configured with **enable-exceed-pir** to forward packets that exceed its configured PIR or when traffic is reclassified at egress to exceed-profile
offered-four-profile-no-cir	4	Inplus, in, out, or exceed entering policer	Inplus/in/out/ exceed entering policer	Intended to be used when the policer does not change the profile of the packets and traffic is reclassified at egress to inplus and/or exceed-profile
offered-total-cir-four-profile	4	Single counter entering policer	Inplus, in, out, or exceed exiting policer	Intended to be used when the policer can change the profile of the packet and traffic is reclassified at egress to profile inplus

When a policer is created within the policy, the default setting for **stat-mode** is **minimal**.

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the **stat-mode** override command will fail. The previous **stat-mode** setting active for the policer will continue to be used by the policer.

The **no** form of this command attempts to return the policer's **stat-mode** setting to **minimal**. The command will fail if insufficient policer counter resources exist to implement **minimal** where the QoS policer is currently applied and has a forwarding class mapping.

Parameters **no-stats** — Counter resource allocation: 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The policer does not have any forwarding plane counters allocated and cannot provide offered, discard, and forward statistics. A policer using **no-stats** cannot be a child to a parent policer and the policer's **parent** command will fail.

When **collect-stats** is enabled, no statistics are generated.

minimal — Counter resource allocation: 1

This stat-mode provides the minimal accounting resource usage and counter information, and includes only the total offered, dropped and forwarded packet and octet counters for traffic entering (offered) and exiting (dropped/forwarded) the policer.

The default **stat-mode** for a policer is **minimal**. The **minimal** mode allocates 1 forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types and do not count different profile output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate or using exceed PIR.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 151.

Table 151 **Egress Accounting Statistics Collected in minimal stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. All	apd	AllPacketsDropped
	aod	AllOctetsDropped
For. All	apf	AllPacketsForwarded
	aof	AllOctetsForwarded

offered-profile-no-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering the policer. inplus-profile traffic is counted with the in-profile counters and exceed-profile traffic is counted with the out-of-profile counters.

The **offered-profile-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **offered-profile-no-cir** mode is most useful when profile-based offered, dropped, and forwarded stats are required from the egress policer, but a CIR or **enable-exceed-pir** is not being used to recolor the soft in-profile and out-of-profile packets. This mode does not prevent the policer from being configured with a CIR rate or using **enable-exceed-pir**.

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 152.

Table 152 **Egress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is made up of traffic that is inplus-profile, in-profile, out-of-profile, exceed-profile, soft in-profile, and soft out-of-profile. The offered counters cover

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

traffic reclassified to in-profile (which includes traffic reclassified to inplus-profile), traffic reclassified to out-of-profile (which includes traffic reclassified to exceed-profile) and traffic which has not been reclassified at egress (Uncolor). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

The **offered-profile-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-profile-cir** mode is most useful when profile-based offered, dropped and forwarded stats are required from the egress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.

This mode is intended to be used without **profile-capped** or **enable-exceed-pir** configured within the policer as these could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 153.

Table 153 **Egress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

offered-total-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

The **offered-total-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-total-cir** mode is most useful when the policer is not receiving trusted in-profile or out-of-profile traffic, and both high- and low- priority classifications are not being used on the untrusted packets, and the offered packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile or out-of-profile packets and does not prevent the use of priority high or low classifications on the untrusted packets.

This mode is intended to be used without **profile-capped** or **enable-exceed-pir** configured within the policer as these could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 154.

Table 154 **Egress Accounting Statistics Collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-capped-cir — Counter resource allocation: 4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is made up of traffic that is inplus-profile, in-profile, out-of-profile, exceed-profile, soft in-profile, and soft out-of-profile. The offered counters cover in-profile traffic (which includes traffic reclassified to inplus-profile) and out-of-profile traffic (which includes traffic reclassified to exceed-profile). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

offered-limited-capped-cir is defined, the system creates four forwarding plane offered-output counters in the network processor and three discard counters in the traffic manager.

The **offered-limited-capped-cir** mode is similar to the **offered-profile-capped-cir** mode except that it combines **soft in-profile** with **profile in** and **soft-out-of-profile** with **profile out** and eliminates the offered-undefined statistic.

The impact of using **offered-limited-capped-cir** stat-mode while profile-capped mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used and **soft-in-profile** will be treated as offered-in instead of offered-undefined.

This mode is intended to be used with **profile-capped** configured within the policer but without **enable-exceed-pir** configured as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 155.

Table 155 **Egress Accounting Statistics Collected in offered-limited-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 155 **Egress Accounting Statistics Collected in offered-limited-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-capped-cir — Counter resource allocation: 5

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is made up of traffic that is inplus-profile, in-profile, out-of-profile, exceed-profile, soft in-profile, and soft out-of-profile. The offered counters cover traffic reclassified to in-profile (which includes traffic reclassified to inplus-profile), traffic reclassified to out-of-profile (which includes traffic reclassified to exceed-profile) and traffic that has not been reclassified at egress (uncolored). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

When **offered-profile-capped-cir** is defined, the system creates five offered-output counters in the forwarding plane and five discard counters in the traffic manager.

The **offered-profile-capped-cir** mode is similar to the **offered-profile-cir** mode except that it includes support for **profile inplus**, **profile in** and **soft-in-profile** that may be output as out-of-profile due to enabling **profile-capped** mode on the ingress policer.

The impact of using o**ffered-profile-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used and soft-in-profile will be treated as offered-in (hard in-profile) instead of offered-undefined (uncolored).

This mode is intended to be used with **profile-capped** configured within the policer but without **enable-exceed-pir** configured as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 156.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 156 **Egress Accounting Statistics Collected in offered-profile-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-total-cir-exceed — Counter resource allocation: 3

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter. The **offered-total-cir-exceed** mode allocates three forwarding plane offered counters and three traffic manager discard counters.

The **offered-total-cir-exceed** mode is similar to the **offered-total-cir** mode except that it includes support for forwarded and dropped counters for **profile exceed**.

This mode is intended to be used when the policer is configured with **enable-exceed-pir** to forward packets that exceed its configured PIR or when traffic is egress reclassified to profile exceed. The mode gives the forwarded and dropped counters per profile (in, out, exceed). It is also intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer. This stat-mode is not supported for dynamic policers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 157.

Table 157 **Egress Accounting Statistics Collected in offered-total-cir-exceed stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
Dro. ExcProf	xpd	ExceedProfilePktsDropped
	xod	ExceedProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded
For. ExcProf	xpf	ExceedProfilePktsForwarded
	xof	ExceedProfileOctetsForwarded

offered-four-profile-no-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering the policer. Offered, dropped, and forwarded counters are provided for inplus, in, out and exceed-profile traffic.

The **offered-four-profile-no-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-four-profile-no-cir** mode is similar to the **offered-profile-no-cir** mode except that it includes support for offered, dropped, and forwarded counters for both inplus-profile and exceed-profile.

This mode is intended to be used when traffic is egress reclassified to inplus and/or exceed-profile. It is also intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer. This stat-mode is not supported for dynamic policers.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 158.

Table 158 **Egress Accounting Statistics Collected in offered-four-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. ExcProf	xpo	ExceedProfilePacketsOffered
	xoo	ExceedProfileOctetsOffered
Off. InplusProf	ppo	InplusProfilePacketsOffered
	poo	InplusProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
Dro. ExcProf	xpd	ExceedProfilePktsDropped
	xod	ExceedProfileOctetsDropped
Dro. InprofProf	ppd	InplusProfilePktsDropped
	pod	InplusProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded
For. ExcProf	xpf	ExceedProfilePktsForwarded
	xof	ExceedProfileOctetsForwarded

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 158 **Egress Accounting Statistics Collected in offered-four-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. InplusProf	ppf	InplusProfilePktsForwarded
	pof	InplusProfileOctetsForwarded

offered-total-cir-four-profile — Counter resource allocation: 4

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. There is a separate dropped and forwarded counter for inplus, in, out and exceed-profile traffic.

The **offered-total-cir-four-profile** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-total-cir-four-profile** mode is similar to the **offered-total-cir** except that it includes support for forwarded and dropped counters for both **profile inplus** and **profile exceed**.

This mode is intended to be used when traffic is reclassified at egress to inplus-profile. It is also intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer. This stat-mode is not supported for dynamic policers.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 159.

Table 159 **Egress Accounting Statistics Collected in offered-total-cir-four-profile stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 159 **Egress Accounting Statistics Collected in offered-total-cir-four-profile stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Dro. ExcProf	xpd	ExceedProfilePktsDropped
	xod	ExceedProfileOctetsDropped
Dro. InprofProf	ppd	InplusProfilePktsDropped
	pod	InplusProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded
For. ExcProf	xpf	ExceedProfilePktsForwarded
	xof	ExceedProfileOctetsForwarded
For. InplusProf	ppf	InplusProfilePktsForwarded
	pof	InplusProfileOctetsForwarded

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

stat-mode

Syntax **stat-mode** {**no-stats** | **minimal** | **offered-profile-no-cir** | **offered-priority-no-cir** | **offered-profile-cir** | **offered-priority-cir** | **offered-total-cir** | **offered-limited-profile-cir** | **offered-profile-capped-cir** | **offered-limited-capped-cir**}
no stat mode

Context **[Tree]** (config>qos>qgrps>ing>qgrp>policer stat-mode)

Full Context configure qos queue-group-templates ingress queue-group policer stat-mode

Description This command is used to configure the forwarding plane counters that allow offered, forwarded, and dropped accounting to occur for the policer. An ingress policer has multiple types of offered packets (explicit in-profile, explicit out-of-profile, uncolored, high-priority or low-priority) and each of these offered types is interacting with the policer's metering and profiling functions resulting in colored output packets (green, yellow, and red). Due to the large number of policers, it is not economical to allocate counters in the forwarding plane for

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

all possible offered packet types and output conditions. Many policers, for example, will not be configured with a CIR profiling rate and not all policers will receive explicitly profiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported that prevents any packet accounting, the use of the policer's **parent** command requires that the policer's **stat-mode** be set at least to the **minimal** setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated. When a policer has been made a child to a parent policer, the **stat-mode** cannot be changed to **no-stats** unless the policer parenting is first removed.

Each time the policer's **stat-mode** is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. The total/allocated/free stats can be viewed by using the **tools dump resource-usage card fp** command. If insufficient counters exist to implement a mode on any policer instance, the **stat-mode** change will fail and the previous mode will continue unaffected for all instances of the policer.

The stat-modes are described in Table 160.

Table 160 **Stat Mode Descriptions**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
no-stats	0	None	None	—
Minimal	1	Single counter entering policer	Single counter for dropped/forwarded exiting policer	—
offered-profile-no-cir	2	In/out entering policer	In/out entering policer	Intended for when the policer does not change the profile of packets. Includes only in- and out-of-profile.
offered-priority-no-cir	2	High/low entering policer	High/low entering policer	Intended for when only packet priority stats are required.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 160 **Stat Mode Descriptions**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-profile-cir	4	In/out/uncolored entering policer	In/out exiting policer	Intended for when the policer can change the profile of packets to in- and out-of-profile.
offered-priority-cir	4	High/low entering policer	In/out exiting policer	Intended for when packet priority entering the policer and profile exiting the policer is required.
offered-total-cir	2	Single counter entering policer	In/out exiting policer	—
offered-limited-profile-cir	3	Out/uncolored entering policer	In/out exiting policer	Intended for when the policer can change the profile of packet to in- and out-of-profile. The information is limited compared to offered-profile-capped-cir with the benefit of using one less stat resource.
offered-profile-capped-cir	5	In/out/uncolored entering policer	In/out exiting policer	Intended for when the policer has profile-capped configured.
offered-limited-capped-cir	4	In/uncolored entering policer	In/out exiting policer	Intended for when the policer has profile-capped configured. The information is limited compared to offered-profile-capped-cir with the benefit of using one less stat resource.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default **stat-mode** when a policer is created within the policy is **minimal**.

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the **stat-mode** override command will fail. The previous **stat-mode** setting active for the policer will continue to be used by the policer.

The **no** form of this command attempts to return the policer's stat-mode setting to minimal. The command will fail if insufficient policer counter resources exist to implement minimal where the QoS policer is currently applied and has a forwarding class mapping.

Parameters **no-stats** — Counter resource allocation: 0

The policer does not have any forwarding plane counters allocated and cannot provide offered, dropped and forwarded statistics. A policer using no-stats cannot be a child to a parent policer and the policer's parent command will fail.

When **collect-stats** is enabled, no statistics are generated.

minimal — Counter resource allocation: 1

This stat-mode provides the minimal accounting resource usage and counter information, and includes the total offered, dropped and forwarded packet and octet counters for traffic entering (offered) and exiting (dropped/forwarded) the policer.

The default **stat-mode** for a policer is **minimal**. The **minimal** mode allocates 1 forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types (profile or priority) and do not count in-profile or out-of-profile output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate.

This counter mode is useful when only the most basic accounting information is required.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 161.

Table 161 **Ingress Accounting Statistics Collected in minimal stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. All	apd	AllPacketsDropped
	aod	AllOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 161 **Ingress Accounting Statistics Collected in minimal stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. All	apf	AllPacketsForwarded
	aof	AllOctetsForwarded

offered-profile-no-cir — Counter resource allocation: 2

This **stat-mode** provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering the policer.

The **offered-profile-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-profile-no-cir** mode is most useful when the policer is receiving only in-profile and out-of-profile premarked (and trusted) packets. It is expected that, in this instance, a CIR rate will not be defined since all packets are already premarked. This mode does not prevent the policer from receiving untrusted (color undefined) nor does it prevent the policer from being configured with a CIR rate.

This mode is intended to be used without profile-capped configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 162.

Table 162 **Ingress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 162 **Ingress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-priority-no-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the packet priority of traffic entering the policer.

The **offered-priority-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-priority-no-cir** mode is most useful when the policer is receiving only untrusted packets and the ingress priority high and priority low classification options are being used without a CIR profiling rate defined. This mode does not prevent the policer from receiving trusted packets that are premarked in-profile or out-of-profile nor does it prevent the policer from being configured with a CIR rate.

This mode is intended to be used without profile-capped configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 163.

Table 163 **Ingress Accounting Statistics Collected in offered-priority-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. HiPrio	hpo	HighPriorityPacketsOffered
	hoo	HighPriorityOctetsOffered
Off. LowPrio	lpo	LowPriorityPacketsOffered
	loo	LowPriorityOctetsOffered
Dro. HiPrio	hpd	HighPriorityPacketsDropped
	hod	HighPriorityOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 163 **Ingress Accounting Statistics Collected in offered-priority-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Dro. LowPrio	lpd	LowPriorityPacketsDropped
	lod	LowPriorityOctetsDropped
For. HiPrio	hpf	HighPriorityPacketsForwarded
	hof	HighPriorityOctetsForwarded
For. LowPrio	lpf	LowPriorityPacketsForwarded
	lof	LowPriorityOctetsForwarded

offered-profile-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed so that the traffic entering the policer comprises of hard in/out and uncolored. The offered counters cover traffic explicitly profiled to in-profile, traffic explicitly profiled to out-of-profile, and traffic that has not been explicitly profiled at ingress (uncolored).

The **offered-profile-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-profile-cir** mode is most useful when the policer is receiving trusted out-of-profile and in-profile traffic and is also receiving untrusted packets that are being applied to a defined CIR profiling rate. This mode differs from **offered-limited-profile-cir** mode in that it expects both trusted in-profile and out-of-profile packets while still performing CIR profiling on packets with untrusted markings. If trusted in-profile packets are not being received, the **offered-limited-profile-cir** stat-mode could be used instead, which has the benefit of using a reduced number of stat resources.

This mode is intended to be used without **profile-capped** configured within the policer as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 164.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 164 **Ingress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-priority-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the priority of traffic entering the policer and the profile exiting the policer.

The **offered-priority-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-priority-cir** mode is most useful when the policer is receiving only untrusted packets that are being classified as high priority or low priority and are being applied to a defined CIR profiling rate. This mode differs from **offered-profile-cir** mode in that it does not expect trusted in-profile and out-of-profile packets but does not exclude the ability of the policer to receive them.

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 165.

Table 165 **Ingress Accounting Statistics Collected in offered-priority-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. HiPrio	hpo	HighPriorityPacketsOffered
	hoo	HighPriorityOctetsOffered
Off. LowPrio	lpo	LowPriorityPacketsOffered
	loo	LowPriorityOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-total-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter.

The **offered-total-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-total-cir** mode is most useful when the policer is not receiving trusted in-profile or out-of-profile traffic and both high- and low-priority classifications are not being used on the untrusted packets and the offered packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile or out-of-profile packets and does not prevent the use of priority high or low classifications on the untrusted packets.

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 166.

Table 166 **Ingress Accounting Statistics collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-profile-cir — Counter resource allocation: 3

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed so that the traffic entering the policer comprises of hard out and uncolored. The offered counters cover traffic explicitly profiled to out-of-profile and traffic that has not been explicitly profiled at ingress (uncolored). The traffic explicitly profiled to in-profile is counted with the uncolored traffic.

The **offered-limited-profile-cir** mode allocates three forwarding plane offered counters and three traffic manager discard counters.

The **offered-limited-profile-cir** mode is most useful when the policer is receiving trusted out-of-profile (profile out but no profile in) traffic and untrusted packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile packets. If trusted in-profile packets are not being received, the **offered-limited-profile-cir** is preferred over **offered-profile-cir** because it uses a reduced number of stat resources.

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 167.

Table 167 **Ingress Accounting Statistics Collected in offered-limited-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-capped-cir — Counter resource allocation: 5

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed so that the traffic entering the policer comprises of hard in/out and uncolored. The offered counters cover traffic explicitly profiled to in-profile, traffic explicitly profiled to out-of-profile, and traffic that has not been explicitly profiled at ingress (uncolored).

When **offered-profile-capped-cir** is defined, the system creates five offered-output counters in the forwarding plane and five discard counters in the traffic manager.

The **offered-profile-capped-cir** mode is similar to the offered-profile-cir mode except that it includes support for profile in and **soft-in-profile** that may be output as ‘out-of-profile’ due to enabling **profile-capped** mode on the ingress policer.

The impact of using **offered-profile-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 168.

Table 168 **Ingress Accounting Statistics Collected in offered-profile-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-capped-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when ingress reclassification is performed resulting in the traffic entering the policer comprising of hard in/out and uncolored. The offered counters cover in-profile traffic and traffic that has not been explicitly profiled at ingress (uncolored). The traffic explicitly profiled to out-of-profile is counted with the uncolored traffic.

offered-limited-capped-cir is defined, the system creates four forwarding plane offered-output counters in the network processor and four discard counters in the traffic manager.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **offered-limited-capped-cir** mode is similar to the **offered-profile-capped-cir** mode except that it combines **soft in-profile** with **profile in** (InProf) and **profile out** (OutProf) with **soft-out-of-profile** (Uncolor) and eliminates the 'offered undefined' statistic. If trusted out-of-profile packets are not being received, the **offered-limited-capped-cir** is preferred over **offered-profile-capped-cir** because it uses a reduced number of stat resources.

This mode is intended to be used with **profile-capped** configured within the policer.

The impact of using **offered-limited-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used.

The counters displayed in the show output and those collected when **collect-stats** is enabled (the actual fields collected depends on the **record** configured in the applied accounting policy) are described in Table 169.

Table 169 **Ingress Accounting Statistics Collected in offered-limited-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

stat-mode

Syntax **stat-mode** {**no-stats** | **minimal** | **offered-profile-no-cir** | **offered-profile-cir** |

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

offered-total-cir | **offered-limited-capped-cir** | **offered-profile-capped-cir** | **offered-total-cir-exceed** | **offered-four-profile-no-cir** | **offered-total-cir-four-profile**}

no stat mode

Context **[Tree]** (cfg>qos>qgrps>egr>qgrp>policer stat-mode)

Full Context configure qos queue-group-templates egress queue-group policer stat-mode

Description The **sap-egress** QoS policy's policer **stat-mode** command is used to configure the forwarding plane counters that allow offered, forwarded, and dropped accounting to occur for the policer. An egress policer has multiple types of offered packets (soft in-profile and out-of-profile from ingress and hard in-profile, out-of-profile, and exceed-profile due to egress profile overrides) and each of these offered types is interacting with the policer's metering and profiling functions resulting in colored output packets (green, yellow, and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers, for example, will not be configured with a CIR profiling rate and not all policers will receive explicitly reprofiled offered packets. The **stat-mode** command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a **no-stats** mode is supported that prevents any packet accounting, the use of the policer's **parent** command requires that the policer's **stat-mode** to be set at least to the **minimal** setting so that offered stats are available for the policer's Fair Information Rate (FIR) to be calculated. When a policer has been made a child to a parent policer, the **stat-mode** cannot be changed to **no-stats** unless the policer parenting is first removed.

Each time the policer's **stat-mode** is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane's policer counter resources. The total/allocated/free stats can be viewed by using the **tools dump resource-usage card fp** command. If insufficient counters exist to implement a mode on any policer instance, the **stat-mode** change will fail and the previous mode will continue unaffected for all instances of the policer.

The ingress policer stat-modes are described in Table 170.

Table 170 **Egress Policer Stat Mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
no-stats	0	None	None	—
Minimal	1	Single counter entering policer	Single counter for dropped/forwarded exiting policer	—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 170 **Egress Policer Stat Mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-profile-no-cir	2	In/out entering policer	In/out entering policer	Intended for when the policer does not change the profile of packets. Includes only in- and out-of-profile.
offered-profile-cir	4	In/out/uncolored (that corresponds to in- or out-of-profile from the ingress processing) entering policer	In/out exiting policer	Intended for when the policer can change the profile of packets to in- and out-of-profile.
offered-total-cir	2	Single counter entering policer	In/out exiting policer	—
offered-limited-capped-cir	4	In/out entering policer	In/out exiting policer	Intended for when the policer has **profile-capped** configured. The information is limited compared to **offered-profile-capped-cir** with the benefit of using one less stat resource.
offered-profile-capped-cir	5	In/out/uncolored (that corresponds to in- or out-of-profile from the ingress processing) entering policer	In/out exiting policer	Intended for when the policer has **profile-capped** configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 170 **Egress Policer Stat Mode Summary**

Stat Mode	Stat Resources	Traffic Counters (Packet/Octets)		Comments
		Offered	Dropped/ Forwarded	
offered-total-cir-exceed	3	Single counter entering policer	In/out/exceed exiting policer	Intended for when the policer is configured with **enable-exceed-pir** to forward packets that exceed its configured PIR or when traffic is egress reclassified to profile exceed.
offered-four-profile-no-cir	4	Inplus/in/out/ exceed entering policer	Inplus/in/out/ exceed entering policer	Intended to be used when the policer does not change the profile of the packets and traffic is egress reclassified to profile inplus and/or exceed.
offered-total-cir-four-profile	4	Single counter entering policer	Inplus/in/out/ exceed exiting policer	Intended to be used when the policer can change the profile of the packet and traffic is egress reclassified to profile inplus.

The default **stat-mode** when a policer is created within the policy is **minimal**.

The **stat-mode** setting defined for the policer in the QoS policy may be overridden on an **sla-profile** or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the **stat-mode** override command will fail. The previous **stat-mode** setting active for the policer will continue to be used by the policer.

The **no** form of this command attempts to return the policer's **stat-mode** setting to **minimal**. The command will fail if insufficient policer counter resources exist to implement **minimal** where the QoS policer is currently applied and has a forwarding class mapping.

Parameters **no-stats** — Counter resource allocation: 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The policer does not have any forwarding plane counters allocated and cannot provide offered, discard, and forward statistics. A policer using **no-stats** cannot be a child to a parent policer and the policer's **parent** command will fail.

When **collect-stats** is enabled, no statistics are generated.

minimal — Counter resource allocation: 1

This stat-mode provides the minimal accounting resource usage and counter information, and includes only the total offered, dropped and forwarded packet and octet counters for traffic entering (offered) and exiting (dropped/forwarded) the policer.

The default **stat-mode** for a policer is **minimal**. The **minimal** mode allocates one forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types and do not count different profile output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate or using exceed PIR.

The counters displayed in the **show** output and those collected when **collect-stats** is enabled are described in Table 171 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 171 **Egress Accounting Statistics Collected in minimal stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. All	apd	AllPacketsDropped
	aod	AllOctetsDropped
For. All	apf	AllPacketsForwarded
	aof	AllOctetsForwarded

offered-profile-no-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering the policer. inplus-profile traffic is counted with the in-profile counters and exceed-profile traffic is counted with the out-of-of profile counters.

The **offered-profile-no-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **offered-profile-no-cir** mode is most useful when profile-based offered, dropped and forwarded statistics are required from the egress policer, but a CIR or **enable-exceed-pir** is not being used to recolor the soft in-profile and out-of-profile packets. This mode does not prevent the policer from being configured with a CIR rate or using **enable-exceed-pir**.

This mode is intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 172 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 172 **Egress Accounting Statistics Collected in offered-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-cir — Counter resource allocation: 4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer comprises of hard inplus/in/out/exceed and soft in/out. The offered counters cover traffic reclassified to in-profile (that includes traffic reclassified to inplus-profile), traffic reclassified to out-of-profile (that includes traffic reclassified to exceed-profile), and traffic that has not been reclassified at egress (Uncolor). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

The **offered-profile-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-profile-cir** mode is most useful when profile-based offered, dropped and forwarded stats are required from the egress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.

This mode is intended to be used without **profile-capped** or **enable-exceed-pir** configured within the policer as these could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 173 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 173 **Egress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 173 **Egress Accounting Statistics Collected in offered-profile-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-total-cir — Counter resource allocation: 2

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

The **offered-total-cir** mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The **offered-total-cir** mode is most useful when the policer is not receiving trusted in-profile or out-of-profile traffic and both high- and low-priority classifications are not being used on the untrusted packets and the offered packets are being applied to a defined CIR profiling rate. This mode does not prevent the policer from receiving trusted in-profile or out-of-profile packets and does not prevent the use of priority high or low classifications on the untrusted packets.

This mode is intended to be used without **profile-capped** or **enable-exceed-pir** configured within the policer as these could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 174 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 174 **Egress Accounting Statistics Collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 174 **Egress Accounting Statistics Collected in offered-total-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-limited-capped-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer comprises of hard inplus/in/out/exceed and soft in/out. The offered counters cover in-profile traffic (that includes traffic reclassified to inplus-profile) and out-of-profile traffic (that includes traffic reclassified to exceed-profile). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

When **offered-limited-capped-cir** is defined, the system creates four forwarding plane offered-output counters in the network processor and three discard counters in the traffic manager.

The **offered-limited-capped-cir** mode is similar to the **offered-profile-capped-cir** mode except that it combines **soft-in-profile** with **profile in** and **soft-out-of-profile** with **profile out** and eliminates the offered-undefined statistic.

The impact of using **offered-limited-capped-cir** stat-mode while profile-capped mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used and **soft-in-profile** will be treated as offered-in instead of offered-undefined.

This mode is intended to be used with **profile-capped** configured within the policer but without **enable-exceed-pir** configured as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 175 (the actual fields collected depends on the **record** configured in the applied accounting policy).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 175 **Egress Accounting Statistics Collected in offered-limited-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-profile-capped-cir — Counter resource allocation: 5

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer when egress reclassification is performed so that the traffic entering the policer is comprised of hard inplus, hard in, hard out, and hard exceed, as well as soft in and soft out. The offered counters cover traffic reclassified to in-profile (that includes traffic reclassified to inplus-profile), traffic reclassified to out-of-profile (that includes traffic reclassified to exceed-profile), and traffic that has not been reclassified at egress (uncolor). In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter and exceed-profile traffic is counted with the out-of-profile counter.

When **offered-profile-capped-cir** is defined, the system creates five offered-output counters in the forwarding plane and five discard counters in the traffic manager.

The **offered-profile-capped-cir** mode is similar to the **offered-profile-cir** mode except that it includes support for **profile inplus**, **profile in**, and **soft-in-profile** that may be output as out-of-profile due to enabling **profile-capped** mode on the ingress policer.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The impact of using **offered-profile-capped-cir** stat-mode while **profile-capped** mode is disabled is that one of the counting resources in the forwarding plane and traffic manager will not be used and soft-in-profile will be treated as offered-in (hard in-profile) instead of offered-undefined (uncolored).

This mode is intended to be used with **profile-capped** configured within the policer but without **enable-exceed-pir** configured as this could cause the traffic profile to be modified by the policer in a way that is not accounted for in the statistics.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 176 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 176 **Egress Accounting Statistics Collected in offered-profile-capped-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. Uncolor	ucp	UncoloredPacketsOffered
	uco	UncoloredOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded

offered-total-cir-exceed — Counter resource allocation: 3

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. In the dropped and forwarded counters, inplus-profile traffic is counted with the in-profile counter. The **offered-total-cir-exceed** mode allocates three forwarding plane offered counters and three traffic manager discard counters.

The **offered-total-cir-exceed** mode is similar to the **offered-total-cir** mode except that it includes support for forwarded and dropped counters for **profile exceed**.

This mode is intended to be used when the policer is configured with **enable-exceed-pir** to forward packets that exceed its configured PIR or when traffic is egress reclassified to profile exceed. The mode gives the forwarded and dropped counters per profile (in, out, exceed). It is also intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer. This stat-mode is not supported for dynamic policers.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 177 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 177 **Egress Accounting Statistics Collected in offered-total-cir-exceed stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
Dro. ExcProf	xpd	ExceedProfilePktsDropped
	xod	ExceedProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded
For. ExcProf	xpf	ExceedProfilePktsForwarded
	xof	ExceedProfileOctetsForwarded

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

offered-four-profile-no-cir — Counter resource allocation: 4

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering the policer. Offered, dropped, and forwarded counters are provided for inplus-profile, in-profile, out-of-profile, and exceed-profile traffic.

The **offered-four-profile-no-cir** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-four-profile-no-cir** mode is similar to the **offered-profile-no-cir** mode except that it includes support for offered, dropped and forwarded counters for both profile inplus and profile exceed.

This mode is intended to be used when traffic is egress reclassified to profile inplus and/or exceed. It is also intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer. This stat-mode is not supported for dynamic policers.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 178 (the actual fields collected depends on the **record** configured in the applied accounting policy).

Table 178 **Egress Accounting Statistics Collected in offered-four-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. InProf	ipo	InProfilePacketsOffered
	ioo	InProfileOctetsOffered
Off. OutProf	opo	OutOfProfilePacketsOffered
	ooo	OutOfProfileOctetsOffered
Off. ExcProf	xpo	ExceedProfilePacketsOffered
	xoo	ExceedProfileOctetsOffered
Off. InplusProf	ppo	InplusProfilePacketsOffered
	poo	InplusProfileOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
Dro. ExcProf	xpd	ExceedProfilePktsDropped
	xod	ExceedProfileOctetsDropped

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 178 **Egress Accounting Statistics Collected in offered-four-profile-no-cir stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Dro. InplusProf	ppd	InplusProfilePktsDropped
	pod	InplusProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded
For. ExcProf	xpf	ExceedProfilePktsForwarded
	xof	ExceedProfileOctetsForwarded
For. InplusProf	ppf	InplusProfilePktsForwarded
	pof	InplusProfileOctetsForwarded

offered-total-cir-four-profile — Counter resource allocation: 4

This stat-mode provides offered, dropped, and forwarded packet and octet counters corresponding to the profile of traffic entering (offered) and exiting (dropped/forwarded) the policer. All offered traffic is provided in a single counter. There is a separate dropped and forwarded counter for inplus, in, out, and exceed-profile traffic.

The **offered-total-cir-four-profile** mode allocates four forwarding plane offered counters and four traffic manager discard counters.

The **offered-total-cir-four-profile** mode is similar to the **offered-total-cir** except that it includes support for forwarded and dropped counters for both inplus-profile and exceed-profile.

This mode is intended to be used when traffic is egress reclassified to inplus-profile. It is also intended to be used without **profile-capped** configured within the policer as it could cause the traffic profile to be modified by the policer. This stat-mode is not supported for dynamic policers.

The counters displayed in the show output and those collected when **collect-stats** is enabled are described in Table 179 (the actual fields collected depends on the **record** configured in the applied accounting policy).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 179 **Egress Accounting Statistics Collected in offered-total-cir-four-profile stat-mode**

Show Output	Accounting Stats Collected	
	Field	**Field Description**
Off. All	apo	AllPacketsOffered
	aoo	AllOctetsOffered
Dro. InProf	ipd	InProfilePacketsDropped
	iod	InProfileOctetsDropped
Dro. OutProf	opd	OutOfProfilePacketsDropped
	ood	OutOfProfileOctetsDropped
Dro. ExcProf	xpd	ExceedProfilePktsDropped
	xod	ExceedProfileOctetsDropped
Dro. InprofProf	ppd	InplusProfilePktsDropped
	pod	InplusProfileOctetsDropped
For. InProf	ipf	InProfilePacketsForwarded
	iof	InProfileOctetsForwarded
For. OutProf	opf	OutOfProfilePacketsForwarded
	oof	OutOfProfileOctetsForwarded
For. ExcProf	xpf	ExceedProfilePktsForwarded
	xof	ExceedProfileOctetsForwarded
For. InplusProf	ppf	InplusProfilePktsForwarded
	pof	InplusProfileOctetsForwarded

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

stat-mode

Syntax **stat-mode {per-fc | aggregate}**
no stat-mode

Context **[Tree]** (config>router>mpls>lsp>egr-stats stat-mode)
[Tree] (config>router>mpls>lsp>ingr-stats stat-mode)
[Tree] (config>router>mpls>lsp-template>egr-stats stat-mode)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls lsp egress-statistics stat-mode
configure router mpls lsp ingress-statistics stat-mode
configure router mpls lsp-template egress-statistics stat-mode

Description This command sets the mode used for collecting LSP statistics.

The **no** form of this command reverts to the default.

Default stat-mode per-fc

Parameters **per-fc** — Specifies that RSVP-TE statistics will be collected per FC.

aggregate — Specifies that SR-TE statistics will be collected as an aggregate across all FCs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router mpls lsp ingress-statistics stat-mode

All

- configure router mpls lsp egress-statistics stat-mode
- configure router mpls lsp-template egress-statistics stat-mode

23.384 state

state

Syntax [**no**] **state**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query state)

Full Context configure subscriber-mgmt wlan-gw ue-query state

Description This command enables matching on a specific UE state. Multiple states can be provisioned.

The **no** form of this command disables matching on the specified UE state (all UEs match).

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

state

Syntax **state** *state*
no state

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from state)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router policy-options policy-statement entry from state

Description This command identifies in resilient gateways which routes are associated with an active context and which routes are associated with a standby context.

Default no state

Parameters *state* — Specifies the state.

Values
- srrp-master — Used in non-CUPS BNG resiliency. Identifies routes associated with an active SRRP instance.
- srrp-non-master — Used in non-CUPS BNG resiliency. Identifies routes associated with a standby SRRP instance.
- ipsec-master-with-peer — Used in stateful Multi-Chassis IPsec (MC-IPsec) redundancy. Identifies routes associated with an active MC-IPsec node with a reachable peer.
- ipsec-non-master — Used in stateful MC-IPsec redundancy. Identifies routes associated with a standby MC-IPsec node.
- ipsec-master-without-peer — Used in stateful MC-IPsec redundancy. Identifies routes associated with an active MC-IPsec node without a reachable peer.
- fsg-active — Used in BNG CUPS inter-UPF resiliency. Identifies routes associated with an FSG on the active BNG UPF. This covers all session-related routes, including framed routes, IPv6 gateway addresses, and aggregated routes, but not loopback addresses.
- fsg-standby — Used in BNG CUPS inter-UPF resiliency. Identifies routes associated with an FSG on the standby BNG UPF. This covers all session-related routes, including framed routes, IPv6 gateway addresses, and aggregated routes, but not loopback addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.385 state-change

state-change

Syntax [**no**] **state-change**

Context **[Tree]** (debug>dynsvc>scripts>event state-change)
[Tree] (debug>dynsvc>scripts>inst>event state-change)
[Tree] (debug>dynsvc>scripts>script>event state-change)

Full Context debug dynamic-services scripts event state-change
debug dynamic-services scripts instance event state-change
debug dynamic-services scripts script event state-change

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables/disables the generation of a specific dynamic data service script debugging event output: state-change.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

state-change

Syntax [**no**] **state-change**

Context **[Tree]** (debug>vsd>scripts>event state-change)
[Tree] (debug>vsd>scripts>instance state-change)

Full Context debug vsd scripts event state-change
debug vsd scripts instance state-change

Description This command enables/disables the generation of a specific script debugging event output: **state-change**.

Platforms All

23.386 state-timer

state-timer

Syntax **state-timer** *seconds* [**action** *action*]
no state-timer

Context **[Tree]** (config>router>pcep>pcc state-timer)

Full Context configure router pcep pcc state-timer

Description This command configures the state timer for PCE-initiated LSPs. The state timer must be set to a value greater than the redelegation timer.

The **no** form of the command sets this value to the default.

Default state-timer 180 action remove

Parameters *seconds* — Specifies the number of seconds before the state timer expires.

Values 1 to 3600

action — Specifies the actions that are taken on undelegated LSPs upon the state timer expiration.

Values remove, none

Default remove

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.387 stateful

stateful

Syntax [**no**] **stateful**

Context **[Tree]** (config>subscr-mgmt>rtr-adv-plcy>pfx-opt stateful)

Full Context configure subscriber-mgmt router-advertisement-policy prefix-options stateful

Description This command enables the configuration of RA options for stateful DHCP prefixes used by the subscriber host.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.388 stateless

stateless

Syntax [**no**] **stateless**

Context **[Tree]** (config>subscr-mgmt>rtr-adv-plcy>pfx-opt stateless)

Full Context configure subscriber-mgmt router-advertisement-policy prefix-options stateless

Description This command enables the configuration of RA options for stateless SLAAC prefixes used by the subscriber host.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.389 stateless-aps-switchover

stateless-aps-switchover

Syntax [**no**] **stateless-aps-switchover**

Context **[Tree]** (config>port>ml-bundle>mlppp stateless-aps-switchover)

Full Context configure port multilink-bundle mlppp stateless-aps-switchover

Description This command specifies whether the bundle will perform a stateful or a stateless APS switchover.

The value can be changed for APS bundle protection groups of type MLPPP.

A stateless switchover implies that PPP is re-negotiated on each member link after the switchover. PPP negotiations may take a few seconds to complete.

A stateful switchover implies that after an APS switchover the PPP state of the bundle will be restored based on the bpgrp bundle state before the switchover.

The state cannot be changed for normal MLPPP bundles (only applicable for bpgrps).

The **no** form of this command disables stateless APS switchover.

Default no stateless-aps-switchover

Platforms 7450 ESS, 7750 SR-7/12/12e

23.390 static

static

Syntax **static**

Context **[Tree]** (config>service>vpls>sap>igmp-snooping static)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping static)
[Tree] (config>service>vpls>mesh-sdp>igmp-snooping static)
[Tree] (config>service>vpls>sap>mld-snooping static)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping static)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping static)

Full Context configure service vpls mesh-sdp igmp-snooping static
configure service vpls mesh-sdp mld-snooping static
configure service vpls sap igmp-snooping static

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap mld-snooping static
configure service vpls spoke-sdp igmp-snooping static
configure service vpls spoke-sdp mld-snooping static

Description Commands in this context configure static group addresses. Static group addresses can be configured on a SAP or SDP. When present, either as a (*, g) or a (s,g) entry, multicast packets matching the configuration are forwarded even if no join message was registered for the specific group.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>subscr-mgmt>igmp-policy static)
[Tree] (config>subscr-mgmt>mld-policy static)

Full Context configure subscriber-mgmt igmp-policy static
configure subscriber-mgmt mld-policy static

Description Commands in this context configure MLD static group membership parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

static

Syntax **static** *ip-address ieee-address*
no static *ip-address*

Context **[Tree]** (config>service>vpls>proxy-arp static)

Full Context configure service vpls proxy-arp static

Description This command configures static entries to be added to the table. A static MAC-IP entry requires the addition of the MAC address to the FDB as either learned or CStatic (conditional static MAC) in order to become active.

Parameters *ip-address* — Specifies the IPv4 address for the static entry.

ieee-address — Specifies a 48-bit MAC address in the form xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where xx represents a hexadecimal number.

Platforms All

static

Syntax **static** *ipv6-address ieee-address* {**host** | **router**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no static *ipv6-address*

Context **[Tree]** (config>service>vpls>proxy-nd static)

Full Context configure service vpls proxy-nd static

Description This command configures static entries to be added to the table. A static MAC-IP entry requires the addition of the MAC address to the FDB as either dynamic or CStatic (Conditional Static MAC) in order to become active. Along with the IPv6 and MAC, the entry must also be configured as either host or router. This will determine if the received NS for the entry will be replied with the R flag set to 1 (router) or 0 (host).

Parameters *ipv6-address* — Specifies the IPv6 address for the static entry.

ieee-address — Specifies a 48-bit MAC address in the form xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where xx represents a hexadecimal number.

host — Specifies that the entry is type “host”.

router — Specifies that the entry is type “router”.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>service>vprn>igmp>if static)

Full Context configure service vprn igmp interface static

Description This command tests forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>service>vprn>mld>if static)

Full Context configure service vprn mld interface static

Description This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

static

Syntax **static**

Context **[Tree]** (config>service>vprn>pim>rp static)

Full Context configure service vprn pim rp static

Description This command enables access to the context to configure a static rendezvous point (RP) of a PIM-SM protocol instance.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>router>igmp>if static)

Full Context configure router igmp interface static

Description This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>router>igmp>tunnel-interface static)

Full Context configure router igmp tunnel-interface static

Description Commands in this context configure static multicast receiver hosts on a tunnel interface associated with an RSVP P2MP LSP.

When enabled, data is forwarded to an interface without receiving membership reports from host members.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>router>mld>if static)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mld interface static

Description This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Platforms All

static

Syntax **static**

Context **[Tree]** (config>router>pim>rp static)
[Tree] (config>router>pim>rp>ipv6 static)

Full Context configure router pim rp ipv6 static
configure router pim rp static

Description Commands in this context configure static Rendezvous Point (RP) addresses for a multicast group range.

Entries can be created or destroyed. If no IP addresses are configured in the **config>router>pim>rp>static>address** context, then the multicast group to RP mapping is derived from the RP-set messages received from the Bootstrap Router.

Platforms All

static

Syntax **static** *microseconds*
no static

Context **[Tree]** (config>router>if>if-attribute>delay static)

Full Context configure router interface if-attribute delay static

Description This command configures the unidirectional link delay. By default there is no configured delay, the link delay metric TLV is pruned in the IGP.

The **no** form of this command removes the configured unidirectional link delay.

Default no static

Parameters *microseconds* — Specifies the unidirectional link delay in microseconds.

Values 1 to 16777214

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.391 static-aa-sub

static-aa-sub

Syntax **static-aa-sub** *transit-aasub-name*
static-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-aa-sub *transit-aasub-name*

Context **[Tree]** (config>app-assure>group>transit-ip-policy static-aa-sub)

Full Context configure application-assurance group transit-ip-policy static-aa-sub

Description This command configures static transit aa-subs with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context.

The **no** form of this command deletes the named static transit aa-sub from the configuration.

Parameters *transit-aasub-name* — Specifies the name of a transit subscriber up to 32 characters in length.

app-profile-name — Specifies the name of an existing application profile up to 32 characters in length.

create — Keyword used to create a new app-profile entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

static-aa-sub

Syntax **static-aa-sub** *transit-aasub-name*
static-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-aa-sub *transit-aasub-name*

Context **[Tree]** (config>app-assure>group>transit-prefix-policy static-aa-sub)
[Tree] (config>app-assure>group>transit-ip-policy>static static-aa-sub)

Full Context configure application-assurance group transit-ip-policy static static-aa-sub
configure application-assurance group transit-prefix-policy static-aa-sub

Description This command configures a static transit aa-sub with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command deletes the named static transit aa-sub from the configuration.

Parameters *transit-aasub-name* — Specifies a transit aasub-name up to 32 characters.

app-profile-name — Specifies the name of an existing application profile up to 32 characters.

create — Keyword used to create a new app-profile entry

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.392 static-address

static-address

Syntax [**no**] **static-address** {*ip-address* | *ipv6-address*}

Context **[Tree]** (config>app-assure>group>dns-ip-cache>ip-cache static-address)

Full Context configure application-assurance group dns-ip-cache ip-cache static-address

Description This command configures a static address in the cache.

Parameters *ip-address* | *ipv6-address* — Specifies a character string up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.393 static-arp

static-arp

Syntax **static-arp** *ieee-mac-address* **unnumbered**
static-arp *ip-address ieee-mac-address*
no static-arp [*ieee-mac-address*] **unnumbered**
no static-arp *ip-address* [*ieee-mac-address*]

Context **[Tree]** (config>service>ies>if static-arp)
[Tree] (config>service>vprn>if static-arp)

Full Context configure service ies interface static-arp
configure service vprn interface static-arp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface.

If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

Parameters *ip-address* — Specifies the IP address for the static ARP in IP address dotted decimal notation.

ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff, where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

unnumbered — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

Platforms All

static-arp

Syntax **static-arp** *ieee-mac-addr* **unnumbered**
static-arp *ip-address ieee-mac-address*
no static-arp [*ieee-mac-addr*] **unnumbered**
no static-arp *ip-address* [*ieee-mac-address*]

Context **[Tree]** (config>service>vpls>interface static-arp)

Full Context configure service vpls interface static-arp

Description This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. A static ARP can only be configured if it exists on the network attached to the IP interface.

If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

Parameters *ip-address* — Specifies the IP address for the static ARP in dotted decimal notation

ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

unnumbered — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

Platforms All

static-arp

Syntax **static-arp** *ip-address ieee-mac-address*
no static-arp *ip-address*

Context **[Tree]** (config>service>vprn>nw-if static-arp)

Full Context configure service vprn network-interface static-arp

Description This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP will appear in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface. If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

Parameters *ip-address* — Specifies the IP address for the static ARP in IP address dotted decimal notation.

ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

Platforms All

static-arp

Syntax **static-arp** *ip-address ieee-address*
no static-arp *ip-address*
static-arp *ieee-address* **unnumbered**
no static-arp unnumbered

Context **[Tree]** (config>router>if static-arp)

Full Context configure router interface static-arp

Description This command configures a static Address Resolution Protocol (ARP) entry associating an IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If an entry for a specific IP address already exists and a new MAC address is configured for the IP address, the existing MAC address is replaced by the new MAC address.

The number of static-arp entries that can be configured on a single node is limited to 1000.

Static ARP is used when a router needs to know about a device on an interface that cannot or does not respond to ARP requests. Therefore, the router configuration can state that if it has a packet that has a certain IP address to send it to the corresponding ARP address. Use proxy ARP so the router responds to ARP requests on behalf of another device.

The **no** form of this command removes a static ARP entry.

Parameters *ieee-address* — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff*, where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

unnumbered — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

Platforms All

23.394 static-cak

static-cak

Syntax [**no**] **static-cak**

Context **[Tree]** (config>macsec>connectivity-association static-cak)

Full Context configure macsec connectivity-association static-cak

Description This command allows the configuration of a Connectivity Association Key (CAK). The CAK is responsible for managing the MKA.

Platforms All

23.395 static-entry

static-entry

Syntax **static-entry** *ip-prefix/ip-prefix-length* **upto** *prefix-length2* **origin-as** *as-number* [{**valid** |

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

invalid}]
no static-entry *ip-prefix/ip-prefix-length* **upto** *prefix-length2* **origin-as** *as-number*

Context **[Tree]** (config>router>origin-validation static-entry)

Full Context configure router origin-validation static-entry

Description This command configures a static VRP entry indicating that a specific origin AS is either valid or invalid for a specific IP prefix range. Static VRP entries are stored along with dynamic VRP entries (learned from local cache servers using the RPKI-Router protocol) in the origin validation database of the router. This database is used for determining the **origin-validation** state of IPv4 and/or IPv6 BGP routes received over sessions with the **enable-origin-validatio**n command configured.

Static entries can only be configured under the **config**>**router**>**origin-validation** context of the base router.

Parameters *ip-prefix/ip-prefix-length* — Specifies an IPv4 or IPv6 address with a minimum prefix length value.

Values 60 to 3600

prefix-length2 — Specifies the maximum prefix length.

Values 1 to 128

as-number — Specifies as-number.

Values 0 to 4294967295

valid — Specifies a keyword meaning the static entry expresses a valid combination of origin AS and prefix range.

invalid — Specifies a keyword meaning the static entry expresses an invalid combination of origin AS and prefix range.

Platforms All

23.396 static-function

static-function

Syntax **static-function**

Context **[Tree]** (config>router>segment-routing>srv6>locator static-function)

Full Context configure router segment-routing segment-routing-v6 locator static-function

Description Commands in this context configure the function field parameters of a static End, End.X, or service SID assignment.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.397 static-host

static-host

Syntax **static-host ip** *ip-prefix*[*/prefix-length*] [**mac** *ieee-address*] [**create**]
no static-host ip *ip-prefix*[*/prefix-length*] [**mac** *ieee-address*]
no static-host all [**force**]
no static-host ip *ip-prefix*[*/prefix-length*]

Context [Tree] (config>service>ies>sub-if>grp-if>sap static-host)
[Tree] (config>service>vprn>sub-if>grp-if>sap static-host)

Full Context configure service ies subscriber-interface group-interface sap static-host
configure service vprn subscriber-interface group-interface sap static-host

Description This command creates a static subscriber host for the SAP. Static subscriber hosts may be used by the system for various purposes. Applications within the system that make use of static host entries include anti-spoof, ARP reply agent and source MAC population into the VPLS forwarding database.

Multiple static hosts may be defined on the SAP. Each host is identified by either a source IP address, a source MAC address or both a source IP and source MAC address. Every static host definition must have at least one address defined, IP or MAC.

Static hosts can exist on the SAP even with anti-spoof and ARP reply agent features disabled. When enabled, each feature has different requirements for static hosts.

The **no** form of this command removes a static entry from the system. The specified *ip-address* and *mac-address* must match the host's exact IP and MAC addresses as defined when it was created. When a static host is removed from the SAP, the corresponding anti-spoof filter entry and/or FDB entry is also removed.

Parameters *ip-prefix[/prefix-length* — Specifies information for the specified IP address and mask.

mac-address — Specifies a MAC address. The MAC address must be specified for **anti-spoof mac**, and **anti-spoof ip-mac** and arp-reply-agent (**arp-reply-agent** is supported by the 7450 ESS only). Multiple static hosts may be configured with the same MAC address given that each definition is distinguished by a unique IP address.

Every static host definition must have at least one address defined, IP or MAC.

force — Specifies the forced removal of the static host addresses.

create — Keyword used to create the static host instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

static-host

Syntax **static-host ip** *ip-address* [**mac** *ieee-address*] [**create**]
static-host mac *ieee-address* [**create**]
no static-host ip *ip-address* **mac** *ieee-address*
no static-host all [**force**]
no static-host ip *ip-address*

Context **[Tree]** (config>service>ies>if>sap static-host)
[Tree] (config>service>vpls>sap static-host)
[Tree] (config>service>vprn>if>sap static-host)

Full Context configure service ies interface sap static-host
configure service vpls sap static-host
configure service vprn interface sap static-host

Description This command creates a static subscriber host for the SAP. Static subscriber hosts may be used by the system for various purposes. Applications within the system that make use of static host entries include anti-spoof, ARP reply agent and source MAC population into the VPLS forwarding database.

Multiple static hosts may be defined on the SAP. Each host is identified by either a source IP address, a source MAC address or both a source IP and source MAC address. Every static host definition must have at least one address defined, IP or MAC.

Static hosts can exist on the SAP even with anti-spoof and ARP reply agent features disabled. When enabled, each feature has different requirements for static hosts.

The **no** form of this command removes a static entry from the system. The specified *ip-address* and *mac-address* must match the host's exact IP and MAC addresses as defined when it was created. When a static host is removed from the SAP, the corresponding anti-spoof filter entry and/or FDB entry is also removed.

Parameters *ip-address* — Specify this optional parameter when defining a static host. The IP address must be specified for **anti-spoof ip**, **anti-spoof ip-mac** and **arp-reply-agent** (**arp-reply-agent** is supported by the 7450 ESS only). Only one static host may be configured on the SAP with a given IP address.

mac-address — Specify this optional parameter when defining a static host. The MAC address must be specified for **anti-spoof mac**, and **anti-spoof ip-mac** and arp-reply-agent (**arp-reply-agent** is supported by the 7450 ESS only). Multiple static hosts may be configured with the same MAC address given that each definition is distinguished by a unique IP address.

Every static host definition must have at least one address defined, IP or MAC.

force — Specifies the forced removal of the static host addresses.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Keyword used to create the static host instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.398 static-host-mgmt

static-host-mgmt

Syntax **static-host-mgmt**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap static-host-mgmt)
[Tree] (config>service>vprn>sub-if>grp-if>sap static-host-mgmt)

Full Context configure service ies subscriber-interface group-interface sap static-host-mgmt
configure service vprn subscriber-interface group-interface sap static-host-mgmt

Description Commands in this context configure common parameters for static hosts.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.399 static-isid

static-isid

Syntax **static-isid**

Context **[Tree]** (config>service>vpls>sap static-isid)
[Tree] (config>service>vpls>spoke-sdp static-isid)

Full Context configure service vpls sap static-isid
configure service vpls spoke-sdp static-isid

Description This command configures the static-isid context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.400 static-label-range

static-label-range

Syntax **static-label-range** *static-range*
no static-label-range

Context **[Tree]** (config>router>mpls-labels static-label-range)

Full Context configure router mpls-labels static-label-range

Description This command configures the range of MPLS static label values shared among static LSP, MPLS-TP LSP, and static service VC label. Once this range is configured, it is reserved and cannot be used by other protocols such as RSVP, LDP, BGP, or Segment Routing to assign a label dynamically.

Default static-label-range 18400

Parameters *static-range* — Specifies the size of the static label range in number of labels. The minimum label value in the range is 32. The maximum label value is therefore computed as {32+ static-range-1}.

Values 0 to 262112

Default 18400

Platforms All

23.401 static-lsp

static-lsp

Syntax [**no**] **static-lsp** *lsp-name*

Context **[Tree]** (config>router>mpls static-lsp)

Full Context configure router mpls static-lsp

Description This command is used to configure a static LSP on the ingress router. The static LSP is a manually set up LSP where the nexthop IP address and the outgoing label (push) must be specified.

The **no** form of this command deletes this static LSP and associated information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The LSP must be shutdown first in order to delete it. If the LSP is not shut down, the **no static-lsp** *lsp-name* command does nothing except generate a warning message on the console indicating that the LSP is administratively up.

Parameters *lsp-name* — Specifies the name that identifies the LSP.

Values Up to 32 alphanumeric characters.

Platforms All

23.402 static-lsp-fast-retry

static-lsp-fast-retry

Syntax **static-lsp-fast-retry** *seconds*
no static-lsp-fast-retry

Context **[Tree]** (config>router>mpls static-lsp-fast-retry)

Full Context configure router mpls static-lsp-fast-retry

Description This command specifies the value used as the fast retry timer for a static LSP.

When a static LSP is trying to come up, the MPLS request for the ARP entry of the LSP next-hop may fail when it is made while the next-hop is still down or unavailable. In that case, MPLS starts a retry timer before making the next request. This enhancement allows the user to configure the retry timer, so that the LSP comes up as soon as the next-hop is up.

The **no** form of this command reverts to the default.

Default no static-lsp-fast-retry

Parameters *seconds* — Specifies the value (in s), used as the fast retry timer for a static LSP.

Values 1 to 30

Platforms All

23.403 static-mac

static-mac

Syntax **static-mac** *ieee-mac-address* [**create**]
no static-mac *ieee-mac-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vpls>sap static-mac)
[Tree] (config>service>vpls>mesh-sdp static-mac)
[Tree] (config>service>vpls>spoke-sdp static-mac)

Full Context configure service vpls mesh-sdp static-mac
configure service vpls sap static-mac
configure service vpls spoke-sdp static-mac

Description This command creates a remote static MAC entry in the Virtual Private LAN Service (VPLS) forwarding database (FDB) associated with the Service Distribution Point (SDP).

In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Local and remote static MAC entries create a permanent MAC address to SDP association in the forwarding database for the VPLS instance so that MAC address is not learned on the edge device.

Note: Static MAC definitions on one edge device are not propagated to other edge devices participating in the VPLS instance, that is, each edge device has an independent forwarding database for the VPLS.

Only one static MAC entry (local or remote) can be defined per MAC address per VPLS instance.

By default, no static MAC address entries are defined for the SDP.

The **no** form of this command deletes the static MAC entry with the specified MAC address associated with the SDP from the VPLS forwarding database.

Parameters *ieee-mac-address* — Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

create — Keyword used to create the static MAC instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

static-mac

Syntax **static-mac**

Context [Tree] (config>service>vpls static-mac)

Full Context configure service vpls static-mac

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description A set of conditional static MAC addresses can be created within a VPLS supporting BGP-EVPN. Conditional Static Macs are also supported in B-VPLS with SPBs. Unless they are configured as **black-hole**, conditional Static Macs are dependent on the SAP/SDP state.

This command allows the assignment of a set of conditional Static MAC addresses to a SAP/spoke-SDP or **black-hole**. In the FDB, the static MAC is then associated with the active SAP or spoke-SDP.

When configured in conjunction with SPBM services, Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

Static MACs configured in a BGP-EVPN service are advertised as protected (EVPN will signal the MAC as protected).

Platforms All

static-mac

Syntax **static-mac**

Context **[Tree]** (config>service>vpls>interface static-mac)

Full Context configure service vpls interface static-mac

Description A set of conditional static MAC addresses can be created within a VPLS supporting bgp-evpn. Conditional static macs are also supported in B-VPLS with SPBM. Conditional Static MACs are dependent on the SAP/SDP state.

This command allows assignment of a set of conditional static MAC addresses to a SAP/spoke-SDP. In the FDB, the static MAC is then associated with the active SAP or spoke-SDP.

Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

Static MACs configured in a bgp-evpn service are advertised as protected (EVPN will signal the mac as protected).

static-mac

Syntax **static-mac** *ieee-address* [**create**]
no static-mac *ieee-address*

Context **[Tree]** (config>service>vpls>endpoint static-mac)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls endpoint static-mac

Description This command assigns a static MAC address to the endpoint. In the FDB, the static MAC is then associated with the active spoke-SDP.

Parameters *ieee-address* — Specifies the static MAC address to the endpoint

Values 6-byte mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) Cannot be all zeros

create — This keyword is mandatory while creating a static MAC

Platforms All

23.404 static-policer

static-policer

Syntax [**no**] **static-policer** *policer-name* [**create**]

Context **[Tree]** (config>sys>security>dist-cpu-protection>policy static-policer)

Full Context configure system security dist-cpu-protection policy static-policer

Description Configures a static enforcement policer that can be referenced by one or more protocols in the policy. Once this **policer-name** is referenced by a protocol, then this policer will be instantiated for each object (for example, a SAP or network interface) that is created and references this policy. If there is no policer resource available on the associated card or fp then the object is be blocked from being created. Multiple protocols can use the same **static-policer**.

Parameters *policy-name* — Specifies the name of the policy, up to 32 characters.

Platforms All

23.405 static-policy

static-policy

Syntax [**no**] **static-policy** *policy-name*

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>p2mp-sr static-policy)
[Tree] (config>service>vprn>mvpn>pt>selective>multistream-spmsi static-policy)
[Tree] (config>service>vprn>mvpn>pt>selective>p2mp-sr static-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn mvpn provider-tunnel inclusive p2mp-sr static-policy
configure service vprn mvpn provider-tunnel selective multistream-spmsi static-policy
configure service vprn mvpn provider-tunnel selective p2mp-sr static-policy

Description This command assigns the specified static policy to the MVPN tunnel.

The **no** form of this command removes the static policy from the MVPN tunnel.

Default no static-policy

Parameters *policy-name* — Specifies the policy name, up to 32 characters.

Platforms All

static-policy

Syntax **static-policy** *name* [**create**]
no static-policy *name*

Context **[Tree]** (config>router>segment-routing>sr-policies static-policy)

Full Context configure router segment-routing sr-policies static-policy

Description This command creates a context to configure a segment routing policy. The resulting segment routing policy is targeted for local installation or propagation by BGP to another router.

The **no** form of this command deletes the statically defined segment routing policy.

Default no static-policy

Parameters *name* — Specifies the name assigned to the statically defined segment routing policy, up to 64 characters.

create — Keyword used to create the policy.

Platforms All

23.406 static-remote-aa-sub

static-remote-aa-sub

Syntax **static-remote-aa-sub** *transit-aasub-name*
static-remote-aa-sub *transit-aasub-name* **app-profile** *app-profile-name* [**create**]
no static-remote-aa-sub *transit-aasub-name*

Context **[Tree]** (config>app-assure>group>transit-prefix-policy static-remote-aa-sub)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group transit-prefix-policy static-remote-aa-sub

Description This command configures static remote transit aa-subs with a name and an app-profile. Remote transit subscribers are configured for sites on the opposite side of the system as the parent SAP/spoke- SDP. A new remote transit sub with both a name and an app-profile is configured with the create command. Static remote transit aa-subs must have an explicitly assigned app-profile. An existing remote transit sub can optionally be assigned a different app-profile.

The **no** form of this command removes the name from the transit prefix policy.

Parameters *transit-aasub-name* — Specifies a transit aasub-name up to 32 characters.

app-profile-name — Specifies the name of an existing application profile up to 32 characters.

create — Keyword used to create a new app-profile entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.407 static-route

static-route

Syntax [**no**] **static-route** *route-name*

Context **[Tree]** (config>service>pw-routing static-route)

Full Context configure service pw-routing static-route

Description This command configures a static route to a next hop S-PE or T-PE. Static routes may be configured on either S-PEs or T-PEs.

A default static route is entered as follows:

static-route 0:0:next_hop_ip_addresss

or

static-route 0:0.0.0.0:next_hop_ip_address

The **no** form of this command removes a previously configured static route.

Parameters *route-name* — Specifies the static pseudowire route.

Values

route-name	<global-id>:<prefix>:<next-hop-ip_addr>
global-id	0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

prefix	a.b.c.d | 0 to 4294967295
next-hop-ip_addr	a.b.c.d

Platforms All

static-route

Syntax [**no**] **static-route** *ip-prefix/ip-prefix-length* **next-hop** *ip-address*

Context **[Tree]** (bof static-route)

Full Context bof static-route

Description This command creates a **static route** entry for the CPM management Ethernet port in the running configuration and the Boot Option File (BOF).

This command allows manual configuration of static routing table entries. These static routes are only used by traffic generated by the CPM Ethernet port. To reduce configuration, manual address aggregation should be applied where possible.

A maximum of 10 static routes can be configured on the CPM port.

The **no** form of this command deletes the static route.

Default no static-route

Parameters *ip-prefix/ip-prefix-length* — Specifies the destination address of the static route in dotted decimal notation.

Values

ip-prefix/ip-prefix-length	ipv4-prefix	a.b.c.d (host bits must be 0)
	ipv4-prefix-le	0 to 32
	ipv6-prefix	*x:x:x:x:x:x:x:x* (eight 16-bit pieces) *x:x:x:x:x:x:d.d.d.d* *x*: [0 to FFFF]H *d*: [0to 255]D
	ipv6-prefix-le	0 to128
ip-address	ipv4-address	a.b.c.d
	ipv6-address	*x:x:x:x:x:x:x:x* (eight 16-bit pieces) *x:x:x:x:x:x:d.d.d.d* *x*: [0 to FFFF]H *d*: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: IPv6 is applicable to the 7750 SR and 7950 XRS only.

mask — Specifies the subnet mask, expressed as an integer or in dotted decimal notation.

Values 1 to 32 (mask length), 128.0.0.0 to255.255.255.255 (dotted decimal)

ip-address — Specifies the next hop IP address used to reach the destination.

Platforms All

23.408 static-route-entry

static-route-entry

Syntax **static-route-entry** *ip-prefix*/*prefix-length* [**mcast**]
no static-route-entry *ip-prefix*/*prefix-length* [**mcast**]

Context **[Tree]** (config>service>vprn static-route-entry)

Full Context configure service vprn static-route-entry

Description This command creates a static route entry for both the network and access routes. A prefix and netmask must be specified.

Once the static route context for the specified prefix and netmask has been created, additional parameters associated with the static route(s) may be specified through the inclusion of additional static-route parameter commands.

The **no** form of this command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, then as many parameters to uniquely identify the static route must be entered.

IPv6 static routes are not supported on the 7450 ESS except in mixed mode.

Default No static routes are defined.

Parameters *ip-prefix/prefix-length* — The destination address of the static route.

Values The following values apply to the 7750 SR and 7950 XRS:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-length	0 to 128

Values The following values apply to the 7450 ESS:

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32

mcast — Specifies that the associated static route should be populated in the associated VPRN multicast route table.

Platforms All

static-route-entry

Syntax [**no**] **static-route-entry** *ip-prefix*/*prefix-length* [**mcast**]

Context **[Tree]** (config>router static-route-entry)

Full Context configure router static-route-entry

Description This command creates a static route entry for both the network and access routes. A prefix and netmask must be specified.

After the static route context for the specified prefix and netmask has been created, additional parameters associated with the static routes may be specified through the inclusion of additional static route parameter commands.

The **no** form of this command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, then as many parameters to uniquely identify the static route must be entered.

Default No static routes are defined.

Parameters *ip-prefix/prefix-length* — Specifies the destination address of the static route.

Values The following values apply to the 7750 SR and 7950 XRS:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv4-prefix	a.b.c.d (host bits must be 0)	
ipv4-prefix-length	0 to 32	
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x	[0 to FFFF]H
	d	[0 to 255]D
ipv6-prefix-length	0 to 128	

Values The following values apply to the 7450 ESS:

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32

ip-address — Specifies the IP address of the IP interface. The *ip-addr* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values The following values apply to the 7750 SR and 7950 XRS:

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 characters maximum, mandatory for link local addresses

Values The following value applies to the 7450 ESS:

ipv4-address	a.b.c.d (host bits must be 0)

mcast — Indicates that static route being configured is used for multicast table only.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.409 static-route-hold-down

static-route-hold-down

Syntax **static-route-hold-down initial** *initial* **multiplier** *multiplier* **max-value** *max-value*
no static-route-hold-down

Context **[Tree]** (config>router static-route-hold-down)

Full Context configure router static-route-hold-down

Description This command enables the hold down time feature globally for static routes in the system.

The **no** form of this command disables the hold down time feature globally for static routes in the system.

Default no static-route-hold-down

Parameters *initial* — Specifies the initial value of the hold down time feature globally for static routes in the system.

Values 1 to 65535

multiplier — Specifies the multiplier value of the hold down time feature globally for static routes in the system.

Values 1 to 10

max-value — Specifies the maximum value of the hold down time feature globally for static routes in the system.

Values 1 to 65535

Platforms All

23.410 static-sa

static-sa

Syntax **static-sa** *sa-name* [**create**]
no static-sa *sa-name*

Context **[Tree]** (config>ipsec static-sa)

Full Context configure ipsec static-sa

Description This command configures an IPsec static SA.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.411 static-string

static-string

Syntax **static-string** *static-string*
no static-string

Context **[Tree]** (config>app-assure>group>http-enrich>field static-string)

Full Context configure application-assurance group http-enrich field static-string

Description This command configures an HTTP header enrichment template field static string.

The **no** form of this command removes the template field static string.

Default no static-string

Parameters *static-string* — Specifies a static string.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.412 static-tunnel-redundant-next-hop

static-tunnel-redundant-next-hop

Syntax **static-tunnel-redundant-next-hop** *ip-address*
no static-tunnel-redundant-next-hop

Context **[Tree]** (config>service>ies>if static-tunnel-redundant-next-hop)
[Tree] (config>service>vprn>if static-tunnel-redundant-next-hop)

Full Context configure service ies interface static-tunnel-redundant-next-hop
configure service vprn interface static-tunnel-redundant-next-hop

Description This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for static IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them. Refer to the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter and Extended Services Appliance Guide* for information about IPsec commands and descriptions.

The next-hop address will be resolved in routing table of corresponding service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the address from the interface configuration.

Parameters *ip-address* — Specifies the static ISA tunnel redundant next-hop address.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.413 station

station

Syntax **station** *station-name* [**create**]
no station *station-name*

Context **[Tree]** (config>bmp station)

Full Context configure bmp station

Description The command configures the BMP monitoring station name.

The **no** form of this command removes the station name from the configuration.

Parameters *station-name* — Specifies the station name of the BMP monitoring station up to 32 characters.

create — Keyword used to create the station name. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

station

Syntax **station all**
station *name* [*name*]
no station

Context **[Tree]** (config>router>bgp>group>monitor station)
[Tree] (config>router>bgp>group>neighbor>monitor station)
[Tree] (config>router>bgp>monitor station)
[Tree] (config>service>vprn>bgp>group>monitor station)
[Tree] (config>service>vprn>bgp>group>neighbor>monitor station)

Full Context configure router bgp group monitor station
configure router bgp group neighbor monitor station
configure router bgp monitor station
configure service vprn bgp group monitor station
configure service vprn bgp group neighbor monitor station

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the set of BMP monitoring stations for which BMP messages are to be sent, at the global BGP instance level, per group or for a particular neighbor.

Whatever value is configured for the station parameter at the most specific BGP hierarchy level is used.

- If a station list or the **no station** command is configured at a neighbor context, then that value is used.
- If **no station** command is configured at the neighbor context, the group value is used.
- If a station list or the **no station** command is configured at a group context, then that value is used.
- If **no station** command is configured at the group context, the global value is used.
- If a station list or the **no station** command is configured at the global context, then that value is used.
- If **no station** command is configured at the global context, then a **no station** is assumed.

The **no** form of this command disables sending BMP messages to BMP monitoring stations.

Parameters *name* — Specifies up to eight station names up to 32 characters. Allowed values are any string up to 32 characters long composed of printable,7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

all — Specifies all configured stations.

Platforms All

23.414 station-address

station-address

Syntax **station-address** *ip-address* | *ipv6-address* **port** *port*
no station-address

Context **[Tree]** (config>bmp>station>connection station-address)

Full Context configure bmp station connection station-address

Description This command configures the IP address and TCP port number of the remote BMP monitoring station. This is a mandatory parameter and must be configured before the associated station can transitioned out of the shut down state.

The **no** form of this command removes the configured station IP address and port number for the BMP session. The **no station-address** command cannot be accepted unless the BMP or station instance is shut down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the station address expressed in dotted decimal notation. Allowed value is a valid routable IP address on the router, either an interface or system IP address.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address — Specifies the station address expressed in dotted decimal notation. Allowed value is a valid routable IPv6 address on the router, either an interface or system IPv6 address.

Values ipv6-address:
- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

port — Specifies the TCP (destination) port number to be used when establishing the connection to the associated BMP station.

Values 1 to 65535

Platforms All

23.415 statistic

statistic

Syntax **statistic type** *type* **name** *name*
no statistic

Context **[Tree]** (debug>wlan-gw>group statistic)

Full Context debug wlan-gw group statistic

Description This command enables debugging of the specified statistic. The first packet that causes an increase of the specified statistic is shown in debug output. After the first packet, debugging of the counter is stopped.

Parameters *type* — Displays the type of statistic to be debugged; for example, DHCP or RADIUS.

Values packet-errors, host-errors, bd-errors, forwarding, reassembly, aa, radius, arp, dhcp, dhcp6, icmp, icmp6

name — Specifies the name, up to 256 characters, of the statistic within that group. For a complete list, see the command **show isa wlan-gw-group** *wlan-gw-group-id* **member** *member-id* **statistics**.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.416 statistics

statistics

Syntax **statistics**

Context **[Tree]** (config>app-assure>group statistics)

Full Context configure application-assurance group statistics

Description Commands in this context configure accounting and billing statistics for this AA ISA group.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

statistics

Syntax **statistics**

Context **[Tree]** (config>isa>aa-grp statistics)

Full Context configure isa application-assurance-group statistics

Description Commands in this context configure statistics generation.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.417 stats-collection

stats-collection

Syntax **stats-collection**

Context **[Tree]** (config>isa>tunnel-grp stats-collection)

Full Context configure isa tunnel-group stats-collection

Description Commands in this context configure ISA statistics collection parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.418 stats-report-interval

stats-report-interval

Syntax **stats-report-interval** [*seconds*]
no stats-report-interval

Context **[Tree]** (config>bmp>station stats-report-interval)

Full Context configure bmp station stats-report-interval

Description This command configures the frequency of sending statistics reporting messages to the BMP monitoring station.

The **no** form of this command removes the interval from the configuration.

Parameters *seconds* — Specifies the frequency of sending statistics reporting messages, in seconds, to the BMP monitoring station.

Values 15 to 65535

Platforms All

23.419 stats-type

stats-type

Syntax **stats-type** {**time** | **volume-time**}
no stats-type

Context **[Tree]** (config>service>dynsvc>acct-1 stats-type)
[Tree] (config>service>dynsvc>acct-2 stats-type)

Full Context configure service dynamic-services dynamic-services-policy accounting-1 stats-type
configure service dynamic-services dynamic-services-policy accounting-2 stats-type

Description This command configures the type of statistics to be reported in dynamic data services RADIUS accounting. A RADIUS specified Stats Type overrides the CLI configured value.

The **no** form of this command resets the default value.

Default stats-type volume-time

Parameters **time** — Only report Session-Time in the RADIUS Accounting Interim-Update and Stop message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

volume-time — Report both Session-Time and Volume counter attributes in the RADIUS. Accounting Interim-Update and Stop messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

stats-type

Syntax **stats-type** {**volume-time** | **time**}
no stats-type

Context **[Tree]** (config>service>dynsvc>ladb>user>idx>acct stats-type)

Full Context configure service dynamic-services local-auth-db user-name index accounting stats-type

Description This command specifies whether dynamic service accounting should be enabled or disabled for this destination. RADIUS accounting is enabled by specifying the stats type: volume and time or time only. This command overrides the local configured value in the dynamic services policy.

The **no** form of this command disables RADIUS accounting (**stats-type** off).

Parameters **volume-time | time** — Enables RADIUS accounting for this dynamic service and specifies if volume counters should be included (**volume-time**) or time only (**time**) in the RADIUS accounting messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.420 status-verify

status-verify

Syntax **status-verify**

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>dyn>cert status-verify)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn>cert status-verify)
[Tree] (config>service>ies>if>sap>ipsec-gw>cert status-verify)
[Tree] (config>service>vprn>if>sap>ipsec-gw>cert status-verify)
[Tree] (config>service>vprn>if>sap>ipsec-tun>dyn>cert status-verify)
[Tree] (config>router>if>ipsec>ipsec-tun>dyn>cert status-verify)
[Tree] (config>ipsec>trans-mode-prof>dyn>cert status-verify)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying cert status-verify
configure router interface ipsec ipsec-tunnel dynamic-keying cert status-verify
configure service ies interface ipsec ipsec-tunnel dynamic-keying cert status-verify
configure service ies interface sap ipsec-gw cert status-verify
configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert status-verify

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ipsec-gw cert status-verify
configure service vprn interface sap ipsec-tunnel dynamic-keying cert status-verify

Description Commands in this context configure Certificate Status Verification (CSV) parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-gw cert status-verify
- configure service vprn interface sap ipsec-tunnel dynamic-keying cert status-verify
- configure service ies interface sap ipsec-gw cert status-verify
- configure ipsec ipsec-transport-mode-profile dynamic-keying cert status-verify

VSR

- configure router interface ipsec ipsec-tunnel dynamic-keying cert status-verify
- configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert status-verify
- configure service ies interface ipsec ipsec-tunnel dynamic-keying cert status-verify

23.421 std-acct-attributes

std-acct-attributes

Syntax [**no**] **std-acct-attributes**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute std-acct-attributes)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute std-acct-attributes

Description This command enables reporting of aggregated forwarded IPv4 and IPv6 octet, packet and gigaword counters using standard RADIUS attributes. This attribute is by default. It can be enabled simultaneously with detailed per queue or policer counters (**detailed-acct-attributes**).

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.422 std-port-class-pools

std-port-class-pools

Syntax **std-port-class-pools**

Context **[Tree]** (config>qos>hs-port-pool-policy std-port-class-pools)

Full Context configure qos hs-port-pool-policy std-port-class-pools

Description Commands in this context configure standard port-class pools parameters. Within this context, the corresponding port-class pools can be associated with a mid-pool, explicitly sized as a percentage of the mid-pool size, dynamically-sized based on relative port bandwidth, or have a slope policy applied.

Platforms 7750 SR-7/12/12e

23.423 steering-profile

steering-profile

Syntax **steering-profile** *steering-profile-name*
no steering-profile

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host steering-profile)

Full Context configure subscriber-mgmt local-user-db ppp host steering-profile

Description This command configures the steering profile for the specific host.

The **no** form of this command removes the steering profile for the host.

Parameters *steering-profile-name* — Specifies the name of the steering profile, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

steering-profile

Syntax **steering-profile** *steering-profile-name* [**create**]
no steering-profile *steering-profile-name*

Context **[Tree]** (config>subscr-mgmt steering-profile)

Full Context configure subscriber-mgmt steering-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a steering profile mapping. A steering profile can be applied to each L2TP LAC subscriber host that requires traffic steering.

The **no** form of this command removes the specified steering profile.

Parameters *steering-profile-name* — Specifies the name of the steering profile, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

steering-profile

Syntax [**no**] **steering-profile**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute steering-profile)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute steering-profile

Description This command enables including the Alc-Steering-Profile RADIUS attribute.

The **no** form of the command disables including the Alc-Steering-Profile RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.424 steering-route

steering-route

Syntax **steering-route** *ip-prefix/length*
no steering-route

Context **[Tree]** (config>service>vprn>nat>inside>redundancy steering-route)

Full Context configure service vprn nat inside redundancy steering-route

Description This command configures specifies the IP address and prefix length of the steering route. The steering route is used in the realm of this virtual router instance as an indirect next-hop for all the traffic that must be routed to the large scale NAT function.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

steering-route

Syntax **steering-route** *ip-prefix/length*
no steering-route

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>nat>inside>redundancy steering-route)

Full Context configure router nat inside redundancy steering-route

Description This command is optionally used in LSN44 multi-chassis redundancy when filters are used on the inside to send traffic destined for the LSN44 function to MS-ISA, where NAT is performed.

If configured, the steering-route is advertised only from the active LSN44 node: the purpose is to bring the LSN44 node activity awareness to downstream routers. In this fashion, downstream routers can make a more intelligent decision when forwarding traffic in the upstream direction. Based on the steering-route, traffic can be sent directly towards the active LSN44 node. This route avoids an extra forwarding hop which would ensue in the case without LSN44 activity awareness, where the upstream traffic can be forwarded to the standby LSN44 node and then to the active LSN44 node.

LSN44 node activity (active/standby) is evaluated per isa-group based on monitoring routes advertised on the outside.

The **no** form of the command removes the ip-prefix/length from the configuration.

Default none

Parameters *ip-prefix/length* — Specifies the IP address and length of the steering route.

Values

ip-prefix:	a.b.c.d
ip-prefix-length:	0 to 32

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.425 sticky-dest

sticky-dest

Syntax **sticky-dest** *hold-time-up*
sticky-dest no-hold-time-up
no sticky-dest

Context [Tree] (config>filter>ip-filter>entry sticky-dest)
[Tree] (config>filter>ipv6-filter>entry sticky-dest)
[Tree] (config>filter>mac-filter>entry sticky-dest)
[Tree] (config>filter>redirect-policy sticky-dest)

Full Context configure filter ip-filter entry sticky-dest
configure filter ipv6-filter entry sticky-dest

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure filter mac-filter entry sticky-dest
configure filter redirect-policy sticky-dest

Description This command configures sticky destination behavior for redundant PBR/PBF actions. Configuring sticky destination has an effect on PBR/PBF actions whether a secondary action is configured.

The *hold-time-up* parameter allows the operator to delay programming of a PBR/PBF action for a specified amount of time. The timer is only started when transitioning from all configured targets being down (that is, the primary target if no secondary target is configured, or both the primary and secondary targets when both are configured) to at least one target being up.

When the timer expires, the primary PBR/PBF action is programmed if its target is up. If the primary PBR/PBF target is down and a secondary PBR/PBF action has been configured and its target is up, then this secondary PBR/PBF action is programmed. In all other cases, no specific programming occurs when the timer expires.

When sticky destination is configured and the secondary PBR/PBF target is up and its associated action is programmed, it is not automatically replaced by the primary PBR/PBF action when its target transitions from down to up. In this situation, programming the primary PBR/PBF action can be forced using the **activate-primary-action** tools command.

Changing the value of the timer while the timer is running takes effect immediately (that is, the timer is restarted immediately using the new value).

The **no** form of the command disables sticky destination behavior.

Default no sticky-dest

Parameters *hold-time-up* — Specifies the initial delay in seconds. Zero is equivalent to **no-hold-time-up** (no delay).

Values 0 to 65535 seconds

Platforms All

23.426 sticky-dr

sticky-dr

Syntax **sticky-dr** [**priority** *dr-priority*]
no sticky-dr

Context **[Tree]** (config>service>vprn>pim>if sticky-dr)

Full Context configure service vprn pim interface sticky-dr

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables sticky-dr operation on this interface. When enabled, the priority in PIM hellos sent on this interface when elected as the designated router (DR) is modified to the value configured in *dr-priority*. This is done to avoid the delays in forwarding caused by DR recovery, when switching back to the old DR on a LAN when it comes back up.

By enabling **sticky-dr** on this interface, it will continue to act as the DR for the LAN even after the old DR comes back up.

The **no** form of this command disables sticky-dr operation on this interface.

Default no sticky-dr

Parameters **priority** *dr-priority* — Sets the DR priority to be sent in PIM Hello messages following the election of that interface as the DR, when sticky-dr operation is enabled.

Values 1 to 4294967295

Platforms All

sticky-dr

Syntax **sticky-dr** [**priority** *dr-priority*]
no sticky-dr

Context **[Tree]** (config>router>pim>interface sticky-dr)

Full Context configure router pim interface sticky-dr

Description This command enables sticky-dr operation on this interface. When enabled, the priority in PIM hellos sent on this interface when elected as the designated router (DR) will be modified to the value configured in *dr-priority*. This is done to avoid the delays in forwarding caused by DR recovery, when switching back to the old DR on a LAN when it comes back up.

By enabling **sticky-dr** on this interface, it will continue to act as the DR for the LAN even after the old DR comes back up.

The **no** form of this command disables sticky-dr operation on this interface.

Default no sticky-dr

Parameters **priority** *dr-priority* — Sets the DR priority to be sent in PIM Hello messages following the election of that interface as the DR, when sticky-dr operation is enabled.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.427 sticky-ecmp

sticky-ecmp

Syntax **sticky-ecmp**
no sticky-ecmp

Context **[Tree]** (config>router>policy-options>policy-statement>entry>action sticky-ecmp)
[Tree] (config>router>policy-options>policy-statement>default-action sticky-ecmp)

Full Context configure router policy-options policy-statement default-action sticky-ecmp
configure router policy-options policy-statement entry action sticky-ecmp

Description This command specifies that BGP routes matching an entry or default-action of a route policy should be tagged internally as requiring sticky ECMP behavior. When a BGP route with multiple equal-cost BGP next-hops is programmed for sticky ECMP the failure of one or more of its BGP next-hops causes only the affected traffic flows to be re-distributed to the remaining next-hops; by default (without sticky-ECMP) all flows are potentially affected, even those using a next-hop that did not fail.

Default no sticky-ecmp

Platforms All

23.428 sticky-msaps

sticky-msaps

Syntax **sticky-msaps** [**idle-timeout** *seconds*]
no sticky-msaps

Context **[Tree]** (config>subscr-mgmt>msap-policy sticky-msaps)

Full Context configure subscriber-mgmt msap-policy sticky-msaps

Description This command prevents MSAPs associated with the specified MSAP policy from being deleted unless a manual **clear** command is issued. If this command is not enabled, an MSAP is deleted when a host creation fails or when a subscriber is no longer associated with the MSAP, for example, when a subscriber ends the session. This feature is useful for an operator who wants to keep historical statistics on MSAPs. It can also speed up host creation on an MSAP since the MSAP is already created. The **idle-timeout** parameter allows the removal of MSAPs that are idle for longer than the specified time.

The **no** form of this command allows an MSAP to be deleted when a host creation fails or when a subscriber is no longer associated with the MSAP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no sticky-msaps

Parameters *seconds* — Specifies the idle timeout, in seconds.

Values 5 to 604800

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.429 stp

stp

Syntax [**no**] **stp**

Context **[Tree]** (config>service>vpls>pbb>backbone-vpls stp)

Full Context configure service vpls pbb backbone-vpls stp

Description This command enables or disable STP through B-VPLS service.

Platforms All

stp

Syntax [**no**] stp

Context **[Tree]** (config>service>vpls>backbone-vpls stp)

Full Context configure service vpls backbone-vpls stp

Description This command enables STP on the backbone VPLS service.

The **no** form of this command disables STP on the backbone VPLS service.

stp

Syntax **stp**

Context **[Tree]** (config>service>vpls stp)
[Tree] (config>service>vpls>sap stp)
[Tree] (config>service>vpls>spoke-sdp stp)
[Tree] (config>service>template>vpls-sap-template stp)
[Tree] (config>service>template>vpls-template stp)

Full Context configure service template vpls-sap-template stp
configure service template vpls-template stp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap stp
configure service vpls spoke-sdp stp
configure service vpls stp

Description Commands in this context configure the Spanning Tree Protocol (STP) parameters. Nokia's STP is simply the Spanning Tree Protocol (STP) with a few modifications to better suit the operational characteristics of VPLS services. The most evident change is to the root bridge election. Since the core network operating between Nokia's service routers should not be blocked, the root path is calculated from the core perspective.

Platforms All

stp

Syntax [**no**] **stp**

Context **[Tree]** (debug>service>id stp)

Full Context debug service id stp

Description Commands in this context debug STP.

The **no** form of the command disables debugging.

Platforms All

stp

Syntax **stp**

Context **[Tree]** (config>service>pw-template stp)

Full Context configure service pw-template stp

Description Commands in this context configure the Spanning Tree Protocol (STP) parameters. The STP is simply the Spanning Tree Protocol (STP) with a few modifications to better suit the operational characteristics of VPLS services. The most evident change is to the root bridge election. Since the core network operating between service routers should not be blocked, the root path is calculated from the core perspective.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.430 stream-selection

stream-selection

Syntax [**no**] **stream-selection**

Context **[Tree]** (config>isa>video-group stream-selection)

Full Context configure isa video-group stream-selection

Description This command specifies whether or not stream selection is enabled on this video group.

The **no** form of the command disables **stream-selection** for the group.

Default no stream-selection

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

23.431 streaming

streaming

Syntax **streaming**

Context **[Tree]** (config>oam-pm streaming)

Full Context configure oam-pm streaming

Description This command specifies the context to configure the OAM-PM streaming template and its associated parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

streaming

Syntax **streaming**

Context **[Tree]** (config>system>snmp streaming)

Full Context configure system snmp streaming

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the proprietary SNMP request/response bundling and TCP-based transport mechanism for optimizing network management of the router nodes. In higher latency networks, synchronizing router MIBs from network management via streaming takes less time than synchronizing via classic SNMP UDP requests. Streaming operates on TCP port 1491 and runs over IPv4 or IPv6.

Platforms All

23.432 strict

strict

Syntax [**no**] **strict**

Context **[Tree]** (config>app-assure>group>tcp-validate strict)

Full Context configure application-assurance group tcp-validate strict

Description This command specifies whether enforcement of TCP sequence and acknowledgment numbers is applied. If a packet does not meet the expected sequence or acknowledgment number, it is dropped.

This command should only be enabled if the expected bit error rate or packet loss is low. For example, if acknowledgments are lost before being detected by AA, the server timeouts are triggered and retransmissions occur. If **strict** is enabled, these retransmissions would resemble a reply attack and would be dropped by AA.

The **no** form of this command removes TCP sequence and acknowledgment number enforcement.

Default no strict

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.433 strict-adjacency-check

strict-adjacency-check

Syntax [**no**] **strict-adjacency-check**

Context **[Tree]** (config>service>vprn>isis strict-adjacency-check)

Full Context configure service vprn isis strict-adjacency-check

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables strict checking of address families (IPv4 and IPv6) for IS-IS adjacencies. When enabled, adjacencies do not come up unless both routers have exactly the same address families configured. If there is an existing adjacency with unmatched address families, it is torn down.

This command is used to prevent black-holing traffic when IPv4 and IPv6 topologies are different. When disabled (**no strict-adjacency-check**) a BFD session failure for either IPv4 or IPv6 will cause the routes for the other address family to be removed as well.

When disabled (**no strict-adjacency-check**), both routers only need to have one common address family to establish the adjacency.

Default no strict-adjacency-check

Platforms All

strict-adjacency-check

Syntax [**no**] **strict-adjacency-check**

Context **[Tree]** (config>router>isis strict-adjacency-check)

Full Context configure router isis strict-adjacency-check

Description This command enables strict checking of address families (IPv4 and IPv6) for IS-IS adjacencies. When enabled, adjacencies will not come up unless both routers have exactly the same address families configured. If there is an existing adjacency with unmatched address families, it will be torn down. This command is used to prevent black-holing traffic when IPv4 and IPv6 topologies are different. When disabled (no strict-adjacency-check) a BFD session failure for either IPv4 or Ipv6 will cause the routes for the other address family to be removed as well.

When disabled (**no strict-adjacency-check**), both routers only need to have one common address family to establish the adjacency.

Platforms All

23.434 strict-lsa-checking

strict-lsa-checking

Syntax [**no**] **strict-lsa-checking**

Context **[Tree]** (config>service>vprn>ospf>graceful-restart strict-lsa-checking)
[Tree] (config>service>vprn>ospf3>graceful-restart strict-lsa-checking)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ospf graceful-restart strict-lsa-checking
configure service vprn ospf3 graceful-restart strict-lsa-checking

Description This command indicates whether an OSPF restart helper should terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router during the restart process.

The default OSPF behavior is to terminate a graceful restart if an LSA changes, which causes the OSPF neighbor to go down.

The **no strict-lsa-checking** command disables strict LSA checking.

Default strict-lsa-checking

Platforms All

strict-lsa-checking

Syntax [**no**] **strict-lsa-checking**

Context **[Tree]** (config>router>ospf>graceful-restart strict-lsa-checking)
[Tree] (config>router>ospf3>graceful-restart strict-lsa-checking)

Full Context configure router ospf graceful-restart strict-lsa-checking
configure router ospf3 graceful-restart strict-lsa-checking

Description This command indicates whether an OSPF restart helper should terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router during the restart process.

The default OSPF behavior is to terminate a graceful restart if an LSA changes, which causes the OSPF neighbor to go down.

The **no** form of this command disables strict LSA checking.

Default strict-lsa-checking

Platforms All

23.435 strict-mode

strict-mode

Syntax [**no**] **strict-mode**

Context **[Tree]** (config>service>upnp>upnp-policy strict-mode)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service upnp upnp-policy strict-mode

Description This command enable UPnP strict mode. With strict-mode, system only allows changes to existing UPnP mapping if the request comes from same UPnP client.

Default no strict-mode

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.436 string

string

Syntax **string** *string*
no string

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident string)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification string

Description This command specifies the string from the Nokia vendor-specific sub-option (VSO) in Option 82 to match when the LUDB is accessed using a DHCPv4 server.

Note: This command is only used when **string** is configured as one of the **match-list** parameters.

The **no** form of this command removes the host identification string from the configuration.

Parameters *string* — Specifies the VSO string of this host, up to 255 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

string

Syntax [**no**] **string** *text*

Context **[Tree]** (config>service>vpls>sap>dhcp>option>vendor string)
[Tree] (config>service>vprn>if>dhcp>option>vendor string)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option>vendor string)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option>vendor string)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option>vendor string)

Full Context configure service ies subscriber-interface group-interface dhcp option vendor-specific-option string

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap dhcp option vendor-specific-option string
configure service vprn interface dhcp option vendor-specific-option string
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option string
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option string

Description This command specifies the string in the Nokia vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command reverts to the default.

Parameters *text* — Specifies a string that can be any combination of ASCII characters, up to 32 characters. If spaces are used in the string, enclose the entire string in quotation marks (“ “).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option string
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option string
- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option string

All

- configure service vpls sap dhcp option vendor-specific-option string
- configure service vprn interface dhcp option vendor-specific-option string

string

Syntax [**no**] **string** *text*

Context **[Tree]** (config>router>if>dhcp>option>vendor-specific-option string)

Full Context configure router interface dhcp option vendor-specific-option string

Description This command specifies the vendor-specific sub-option string of the DHCP relay packet.

The **no** form of this command returns the default value.

Default no string

Parameters *text* — Specifies a string that can be any combination of ASCII characters, up to 32 characters in length. If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.437 strings-from-option

strings-from-option

Syntax **strings-from-option** *dhcp-option-number*
no strings-from-option

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol strings-from-option)

Full Context configure subscriber-mgmt sub-ident-policy strings-from-option

Description This command enables DHCPv4 option processing on DHCP ACK for subscriber host identification.

The parameter *dhcp-option-number* specifies the DHCPv4 option number containing subscriber host identification strings such as subscriber ID, sub-profile, sla-profile strings, and so on. The identification strings can be inserted by an SR OS based DHCPv4 server via a local user database lookup.

Applicable to DHCPv4 hosts and PPP hosts that use the internal DHCP client to get an IPv4 address from an SR OS based DHCPv4 server.

The **no** form of this command reverts to the default.

Default no strings-from-option

Parameters *dhcp-option-number* — Specifies the DHCPv4 option number containing subscriber host identification strings.

Values 1 to 254

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.438 strip-label

strip-label

Syntax [**no**] **strip-label**

Context **[Tree]** (config>router>if strip-label)

Full Context configure router interface strip-label

Description This command forces packets to be stripped of all (max 5) MPLS labels before the packets are handed over for possible filter (PBR) processing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the packets do not have an IP header immediately following the MPLS label stack after the strip, they are discarded. Only MPLS encapsulated IP, IGP shortcuts and VPRN over MPLS packets will be processed. However, IPv4 and IPv6 packets that arrive without any labels are supported on an interface with **strip-label** enabled.

This command operates in promiscuous mode. This means that the router does not filter on the destination MAC address of the Ethernet frames. In some network designs, multiple ports may be tapped and combined into interface toward the router. Promiscuous mode allows all of these flows to be processed without requiring the destination MAC address to be updated to match the router address.

This command is supported on:

- Optical ports for the 7750 SR and 7450 ESS
- IOM3-XP cards for the 7750 SR and 7450 ESS
- Null/Dot1q encaps
- Network ports
- IPv4
- IPv6

In order to associate an interface that is configured with the strip-label parameter with a port, the port must be configured as single-fiber for the command to be valid.

Packets that are subject to the strip-label action and are mirrored (using mirrors or lawful interception) will contain the original MPLS labels (and other L2 encapsulation) in the mirrored copy of the packet, as they appeared on the wire, when the mirror-dest type is the default type “ether”. If the mirror-dest type is “ip-only”, then the mirrored copy of the packet will not contain the original L2 encapsulation or the stripped MPLS labels.

The **no** form of this command removes the strip-label command.

Default no strip-label

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.439 strip-srv6-tlvs

strip-srv6-tlvs

Syntax **[no] strip-srv6-tlvs**

Context **[Tree]** (config>router>bgp>group>srv6>route>fam strip-srv6-tlvs)
[Tree] (config>router>bgp>group>neighbor>srv6>route>family strip-srv6-tlvs)

Full Context configure router bgp group neighbor segment-routing-v6 route-advertisement family strip-srv6-tlvs

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router bgp group segment-routing-v6 route-advertisement family strip-srv6-tlvs

Description This command specifies that BGP routes that belong to the address family configured in the **family** command are advertised to peers with SRv6 TLVs removed. Locally or remotely added SRv6 TLVs can be removed.

The **no** form of this command configures the router not to strip SRv6 TLVs from the BGP routes advertised to peers.

Default no strip-srv6-tlvs

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

23.440 stub

stub

Syntax [**no**] **stub**

Context **[Tree]** (config>service>vprn>ospf>area stub)
[Tree] (config>service>vprn>ospf3>area stub)

Full Context configure service vprn ospf area stub
configure service vprn ospf3 area stub

Description This command enables access to the context to configure an OSPF stub area and adds/removes the stub designation from the area. External routing information is not flooded into stub areas. All routers in the stub area must be configured with the **stub** command. An OSPF area cannot be both an NSSA and a stub area. Existing virtual links of a non STUB or NSSA area will be removed when its designation is changed to NSSA or STUB.

By default, an area is not a stub area.

The **no** form of this command removes the stub designation and configuration context from the area.

Default no stub — The area is not configured as a stub area.

Platforms All

stub

Syntax [**no**] **stub**

Context **[Tree]** (config>router>ospf>area stub)
[Tree] (config>router>ospf3>area stub)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router ospf area stub
configure router ospf3 area stub

Description This command enables access to the context to configure an OSPF or OSPF3 stub area and adds/removes the stub designation from the area.

External routing information is not flooded into stub areas. All routers in the stub area must be configured with the **stub** command. An OSPF or OSPF3 area cannot be both an NSSA and a stub area.

Existing virtual links of a non STUB or NSSA area will be removed when its designation is changed to NSSA or STUB.

By default, an area is not a stub area.

The **no** form of this command removes the stub designation and configuration context from the area.

Default no stub

Platforms All

23.441 sub-domain

sub-domain

Syntax **sub-domain** *sub-domain*
no sub-domain

Context **[Tree]** (config>service>vprn>mvpn>provider-tunnel>inclusive>bier sub-domain)
[Tree] (config>service>vprn>mvpn>provider-tunnel>selective>bier sub-domain)

Full Context configure service vprn mvpn provider-tunnel inclusive bier sub-domain
configure service vprn mvpn provider-tunnel selective bier sub-domain

Description This command sets the sub-domain used to attach the BIER provider tunnel. Both PMSI within the MVPN need to have the same sub-domain.

The **no** form of this command removes the sub-domain.

Parameters *sub-domain* — The identifier of the sub-domain.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-domain

Syntax [**no**] **sub-domain** *sub-domain*
[**no**] **sub-domain start** *sub-domain* **end** *sub-domain*

Context **[Tree]** (config>router>bier>template sub-domain)

Full Context configure router bier template sub-domain

Description This command creates a BIER sub-domain or range of sub-domains. For example, for IS-IS each sub-domain is associated with a single IS-IS topology, which may be any of the topologies supported by IS-IS.

The **no** form of this command removes a sub-domain.

Default sub-domain 0

Parameters *sub-domain* — The ID of the sub-domain to be created or removed.

Values 0 to 255

Platforms All

23.442 sub-host-trk

sub-host-trk

Syntax [**no**] **sub-host-trk**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync sub-host-trk)

Full Context configure redundancy multi-chassis peer sync sub-host-trk

Description This command specifies whether subscriber host tracking information should be synchronized with the multi-chassis peer.

Default no sub-host-trk

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.443 sub-hosts-only

sub-hosts-only

Syntax [**no**] **sub-hosts-only**

Context **[Tree]** (config>service>vprn>igmp>grp-if sub-hosts-only)

Full Context configure service vprn igmp group-interface sub-hosts-only

Description This command enables the IGMP traffic from known hosts only.

The **no** form of this command disable the IGMP traffic from known hosts only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-hosts-only

Syntax [**no**] **sub-hosts-only**

Context **[Tree]** (config>router>igmp>group-interface sub-hosts-only)

Full Context configure router igmp group-interface sub-hosts-only

Description This command disables the processing of IGMP messages outside of the subscriber-host context. No other hosts outside of the subscriber-hosts can create IGMP states.

Disabling this command allows the creation of the IGMP states that correspond to the AN that operate in IGMP proxy mode. In this mode, the AN will hide source IP addresses of IGMP messages and will source IGMP messages with its own IP address. In this case, an IGMP state can be created under the **sap** context. This IGMP state creation under the SAP is controlled via the import policy under the group-interface.

The IGMP state processing for regular subscriber-hosts is unaffected by this command.

The **no** form of the command disables the command.

Default sub-hosts-only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-hosts-only

Syntax [**no**] **sub-hosts-only**

Context **[Tree]** (config>router>mld>group-interface sub-hosts-only)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mld group-interface sub-hosts-only

Description This command processes the handling of MLD joins received from hosts that are not known in subscriber management or on which no MLD policy is applied.

Disabling this command allows the creation of the MLD states that correspond to the AN that operate in MLD proxy mode. In this mode, the AN will hide source IP addresses of MLD messages and will source MLD messages with its own IP address. In this case, an MLD state can be created under the **sap** context. This MLD state creation under the SAP is controlled via the import policy under the group-interface.

The MLD state processing for regular subscriber-hosts is unaffected by this command.

The **no** form of the command enables the command.

Default sub-hosts-only

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.444 sub-id

sub-id

Syntax [**no**] **sub-id**

Context **[Tree]** (config>service>nat>syslog>syslog-export-policy>include sub-id)

Full Context configure service nat syslog syslog-export-policy include sub-id

Description This command includes the **sub-id** string in the flow log. The **sub-id** is applicable only in subscriber-aware NAT. If subscriber-aware NAT is not enabled, the **sub-id** string is set to '-'.

The **no** form of the command disables the feature.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.445 sub-ident-policy

sub-ident-policy

Syntax [**no**] **sub-ident-policy** *sub-ident-policy-name*

Context **[Tree]** (config>subscr-mgmt sub-ident-policy)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt sub-ident-policy

Description This command configures a subscriber identification policy. Each subscriber identification policy can have a default subscriber profile defined. The subscriber identification policy default subscriber profile overrides the system default and the subscriber SAP default subscriber profiles. Defining a subscriber identification policy default subscriber profile is optional.

The subscriber identification policy default subscriber profile cannot be defined with the subscriber profile name default.

Defining a subscriber profile as a subscriber identification policy default subscriber profile will cause all active subscribers currently associated with a subscriber SAP using the policy and associated with a subscriber policy through the system default or subscriber SAP default subscriber profiles to be reassigned to the subscriber policy defined as default on the subscriber identification policy.

Attempting to delete a subscriber profile that is currently defined as a default for a subscriber identification policy will fail.

When attempting to remove a subscriber identification policy default subscriber profile definition, the system will evaluate each active subscriber on all subscriber SAPs the subscriber identification policy is currently associated with that are using the default definition to determine whether the active subscriber can be either reassigned to a subscriber SAP default or the system default subscriber profile. If all active subscribers cannot be reassigned, the removal attempt will fail.

The **no** form of this command reverts to the default.

Parameters *sub-ident-policy-name* — Specifies the name of the subscriber identification policy, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-ident-policy

Syntax **sub-ident-policy** *sub-ident-policy-name*

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>sub-sla-mgmt sub-ident-policy)
[Tree] (config>service>ies>sub-if>grp-if>sap-parameters>sub-sla-mgmt sub-ident-policy)
[Tree] (config>subscr-mgmt>msap-policy>sub-sla-mgmt sub-ident-policy)
[Tree] (config>service>vpls>sap>sub-sla-mgmt sub-ident-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap>sub-sla-mgmt sub-ident-policy)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters>sub-sla-mgmt sub-ident-policy)

Full Context configure service ies subscriber-interface group-interface sap sub-sla-mgmt sub-ident-policy
configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt sub-ident-policy
configure service vpls sap sub-sla-mgmt sub-ident-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface sap sub-sla-mgmt sub-ident-policy
configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt sub-ident-policy
configure subscriber-mgmt msap-policy sub-sla-mgmt sub-ident-policy

Description This command associates a subscriber identification policy to this SAP. The subscriber identification policy must be defined prior to associating the profile with a SAP in the **config>subscr-mgmt>sub-ident-policy** context.

Subscribers are managed by the system through the use of subscriber identification strings such as a subscriber identifier, an sla-profile string, a sub-profile string and an app-profile string.

The subscriber identification policy performs following functions for subscriber hosts and sessions associated with the SAP or MSAP:

- mapping of sla-profile, sub-profile and app-profile strings obtained from authentication (for example, LUDB, RADIUS, Diameter, or Python) into profile names that are configured on the router
- for IPoE DHCPv4 hosts, the subscriber identification strings can be derived from the DHCP ACK message sent to the subscriber host using a Python script referenced in the sub-ident-policy
- for PPPoE hosts that get an IPv4 address via the PPPoE DHCPv4 client and for IPoE DHCPv4 hosts, an SR OS DHCPv4 server in combination with an LUDB returns the identification strings in a DHCPv4 option. The **strings-from-option** command in the sub-ident-policy tells the system from which option to extract the identification strings.

The **no** form of this command removes the default subscriber identification policy from the SAP configuration.

Parameters *sub-ident-policy-name* — Specifies a subscriber identification policy for this SAP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap sub-sla-mgmt sub-ident-policy
- configure service vpls sap sub-sla-mgmt sub-ident-policy
- configure service vprn subscriber-interface group-interface sap sub-sla-mgmt sub-ident-policy
- configure subscriber-mgmt msap-policy sub-sla-mgmt sub-ident-policy

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt sub-ident-policy
- configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt sub-ident-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-ident-policy

Syntax [**no**] **sub-ident-policy** *policy-name*

Context **[Tree]** (debug>subscr-mgmt sub-ident-policy)

Full Context debug subscriber-mgmt sub-ident-policy

Description This command debugs subscriber identification policies.

The **no** form of this command disables debugging.

Parameters *policy-name* — Specifies the subscriber identification policy to debug.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-ident-policy

Syntax **sub-ident-policy** *sub-ident-policy-name*
no sub-ident-policy

Context **[Tree]** (config>app-assure>group>transit-ip-policy sub-ident-policy)

Full Context configure application-assurance group transit-ip-policy sub-ident-policy

Description This command associates a subscriber identification policy to this SAP. The subscriber identification policy must be defined prior to associating the profile with a SAP in the **config>subscribermgmt>sub-ident-policy** context.

Subscribers are managed by the system through the use of subscriber identification strings. A subscriber identification string uniquely identifies a subscriber. For static hosts, the subscriber identification string is explicitly defined with each static subscriber host.

For dynamic hosts, the subscriber identification string must be derived from the DHCP ACK message sent to the subscriber host. The default value for the string is the content of Option 82 CIRCUIT-ID and REMOTE-ID fields interpreted as an octet string. As an option, the DHCP ACK message may be processed by a subscriber identification policy which has the capability to parse the message into an alternative ASCII or octet string value.

When multiple hosts on the same port are associated with the same subscriber identification string they are considered to be host members of the same subscriber.

A sub-ident-policy can also be used for identifying dynamic transit subscriber names.

The **no** form of this command removes the default subscriber identification policy from the SAP configuration.

Default no sub-ident-policy

Parameters *sub-ident-policy-name* — Specifies the subscriber identification policy name, up to 32 characters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.446 sub-insert-credit-control

sub-insert-credit-control

Syntax **sub-insert-credit-control start-entry** *entry-id* **count** *count*
no sub-insert-credit-control

Context **[Tree]** (config>filter>ip-filter sub-insert-credit-control)
[Tree] (config>filter>ipv6-filter sub-insert-credit-control)

Full Context configure filter ip-filter sub-insert-credit-control
configure filter ipv6-filter sub-insert-credit-control

Description This command inserts point information for credit control for the filter.

The **no** form of the command reverts to the default.

Default no sub-insert-credit-control

Parameters *entry-id* — Identifies a filter on this system.

Values 1 to 2097151

count — Specifies the count

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.447 sub-insert-radius

sub-insert-radius

Syntax **sub-insert-radius start-entry** *entry-id* **count** *count*
no sub-insert-radius

Context **[Tree]** (config>filter>ip-filter sub-insert-radius)
[Tree] (config>filter>ipv6-filter sub-insert-radius)

Full Context configure filter ip-filter sub-insert-radius
configure filter ipv6-filter sub-insert-radius

Description This command inserts point information for RADIUS for the filter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command reverts to the default.

Default no sub-insert-radius

Parameters *entry-id* — Specifies at what place the filter entries received from RADIUS will be inserted in the filter.

Values 1 to 2097151

count — Specifies the count.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.448 sub-insert-shared-pccrule

sub-insert-shared-pccrule

Syntax **sub-insert-shared-pccrule start-entry** *entry-id* **count** *count*
no sub-insert-shared-pccrule

Context **[Tree]** (config>qos>sap-egress sub-insert-shared-pccrule)
[Tree] (config>qos>sap-ingress sub-insert-shared-pccrule)

Full Context configure qos sap-egress sub-insert-shared-pccrule
configure qos sap-ingress sub-insert-shared-pccrule

Description This command defines the range of filter and QoS policy entries that are reserved for shared entries received in Flow-Information AVP via Gx interface (PCC rules – Policy and Charging Control).

The **no** form of this command disables the insertion, which will result in a failure of PCC rule installation.

Default no sub-insert-shared-pccrule

Parameters *entry-id* — Specifies the lowest entry in the range.

Values 1 to 65535

count — Specifies the number of entries in the range.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-insert-shared-pccrule

Syntax **sub-insert-shared-pccrule start-entry** *entry-id* **count** *count*
no sub-insert-shared-pccrule

Context **[Tree]** (config>filter>ip-filter sub-insert-shared-pccrule)
[Tree] (config>filter>ipv6-filter sub-insert-shared-pccrule)

Full Context configure filter ip-filter sub-insert-shared-pccrule
configure filter ipv6-filter sub-insert-shared-pccrule

Description This command defines the range of filter and QoS policy entries that are reserved for shared entries received in Flow-Information AVP via Gx interface (PCC rules – Policy and Charging Control). The **no** form of this command disables the insertion, which will result in a failure of PCC rule installation.

Default no sub-insert-shared-pccrule

Parameters *entry-id* — Specifies the lowest entry in the range.

Values 1 to 2097151

count — Specifies the number of entries in the range.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.449 sub-insert-shared-radius

sub-insert-shared-radius

Syntax **sub-insert-shared-radius start-entry** *entry-id* **count** *count*
no sub-insert-shared-radius

Context **[Tree]** (config>filter>ip-filter sub-insert-shared-radius)
[Tree] (config>filter>ipv6-filter sub-insert-shared-radius)

Full Context configure filter ip-filter sub-insert-shared-radius
configure filter ipv6-filter sub-insert-shared-radius

Description This command configures the insert point for shared host rules from RADIUS.

Default no sub-insert-shared-radius

Parameters *entry-id* — Identifies a filter on this system.

Values 1 to 2097151

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

count — Specifies the count.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.450 sub-insert-wmark

sub-insert-wmark

Syntax **sub-insert-wmark low** *low-watermark* **high** *high-watermark*
no sub-insert-wmark

Context **[Tree]** (config>filter>ip-filter sub-insert-wmark)
[Tree] (config>filter>ipv6-filter sub-insert-wmark)

Full Context configure filter ip-filter sub-insert-wmark
configure filter ipv6-filter sub-insert-wmark

Description This command configures the low and high watermark percentage for inserted filter entry usage reporting.

The **no** form of the command reverts to the default.

Default sub-insert-wmark low 90 high 95

Parameters *low-watermark* — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be cleared by the agent.

Values 0 to 100

high-watermark — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be raised by the agent.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.451 sub-mcac-policy

sub-mcac-policy

Syntax **sub-mcac-policy** *sub-mcac-policy-name* [**create**]
no sub-mcac-policy *b*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt sub-mcac-policy)

Full Context configure subscriber-mgmt sub-mcac-policy

Description This command creates a policy template with MCAC bandwidth limits that are applied to the subscriber.

Per interface mcac bandwidth limits are set directly under the interface (regular interface or group-interface) and no such policy templates are needed.

The need for a separate policy template for subscribers is due to the fact that groups of subscribers under the same group-interface can share certain settings that can be configured via this template.

To summarize, the MCAC bandwidth constraints for subscribers are defined in the sub-mcac-policy while the mcac bandwidth constraints for the interface are configured directly under the **igmp>interface>mcac** or **igmp>grp-if>mcac** context without the need for policy templates.

Note: The sub-mcac-policy only deals with the mcac bandwidth limits and not the channel bandwidth definitions. Channels bandwidth is defined in a different policy (in the **config>router>mcac** context) and that policy is applied on the interface level as follows:

- For group-interface: under the **config>service>vprn>igmp>grp-if>mcac** context
- For regular interface: under the **config>service/router>igmp>interface>mcac** context.

In case of HQoS Adjustment, it is mandatory that the sub-mcac-policy be created and applied to the subscriber. The sub-mac-policy does not have to contain any bandwidth constrains, but it has to be in a no shutdown state in order for HQoS Adjustment to work.

The **no** form of this command reverts to the default.

Parameters *policy-name* — Specifies the name of the policy up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

sub-mcac-policy

Syntax **sub-mcac-policy** *policy-name*
no sub-mcac-policy

Context [Tree] (config>subscr-mgmt>sub-prof sub-mcac-policy)

Full Context configure subscriber-mgmt sub-profile sub-mcac-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command references the policy template in which the mcac bandwidth limits are defined. Mcac for the subscriber is effectively enabled with this command when the sub-profile is applied to the subscriber. The bandwidth of the channels is defined in a different policy (under the **config>router>mcac** context) and this policy is applied on the interface level as follows:

- For group-interfaces under the **config>service>vprn>igmp>grp-if>mcac** context
- For regular interfaces under the **config>service/router>igmp>interface>mcac** context

In case of HQoS Adjustment, it is mandatory that the sub-mcac-policy be created and applied to the subscriber. The sub-mac-policy does not have to contain any bandwidth constrains, but it has to be in a no shutdown state in order for HQoS Adjustment to work.

The **no** form of this command removes the policy from the configuration.

Parameters *policy-name* — Specifies the policy name configured in the config>subscr-mgmt>sub-mcac-policy context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

23.452 sub-mgmt

sub-mgmt

Syntax **sub-mgmt** [**ipoe**] [**pppoe**]
no sub-mgmt

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync sub-mgmt)

Full Context configure redundancy multi-chassis peer sync sub-mgmt

Description This command specifies whether subscriber management information should be synchronized with the multi-chassis peer.

Default no sub-mgmt

Parameters **ipoe** — Specifies to synchronize IPoE subscribers. The use of the keyword must match on both nodes, otherwise the subscriber synchronization fails.

pppoe — Specifies to synchronize PPPoE subscribers. The use of the keyword must match on both nodes, otherwise the subscriber synchronization fails.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

sub-mgmt

Syntax [**no**] **sub-mgmt**

Context **[Tree]** (config>redundancy>multi-chassis>options sub-mgmt)

Full Context configure redundancy multi-chassis options sub-mgmt

Description This command enables the CLI context to configure subscriber management multi-chassis options parameters.

Default sub-mgmt

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.453 sub-mgmt-extensions

sub-mgmt-extensions

Syntax [**no**] **sub-mgmt-extensions**

Context **[Tree]** (config>fwd-path-ext>fpe sub-mgmt-extensions)

Full Context configure fwd-path-ext fpe sub-mgmt-extensions

Description This command configures FPE for subscriber management extensions. The FPE cannot be used for other applications but can be used for multiple subscriber management applications.

The **no** version of this command disables FPE for subscriber management extensions.

Default no sub-mgmt-extensions

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.454 sub-port

sub-port

Syntax **sub-port** *port-id* [**create**]
no sub-port *port-id*

Context **[Tree]** (config>port>ethernet>dot1x>macsec sub-port)

Full Context configure port ethernet dot1x macsec sub-port

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a MACsec instance on a physical port, targeting the specific subset of traffic defined by the **encap-match** command.

The **no** form of this command removes the MACsec instance.

Parameters *port-id* — Specifies the sub-port id index.

Values 1 to 1023

create — Creates a new sub-port.

Platforms All

23.455 sub-profile

sub-profile

Syntax [**no**] **sub-profile**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute sub-profile)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute sub-profile

Description This command specifies that subscriber profile attributes should be included into RADIUS accounting messages.

The **no** form of this command excludes subscriber profile attributes into RADIUS accounting messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-profile

Syntax **sub-profile** *sub-profile-name*
no sub-profile

Context **[Tree]** (config>service>ies>if>sap>static-host sub-profile)
[Tree] (config>service>vpls>sap>static-host sub-profile)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host sub-profile)
[Tree] (config>service>vprn>if>sap>static-host sub-profile)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host sub-profile)

Full Context configure service ies interface sap static-host sub-profile
configure service ies subscriber-interface group-interface sap static-host sub-profile
configure service vpls sap static-host sub-profile
configure service vprn interface sap static-host sub-profile
configure service vprn subscriber-interface group-interface sap static-host sub-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies an existing subscriber profile name to be associated with the static subscriber host.

The **no** form of this command reverts to the default.

Parameters *sub-profile-name* — Specifies the sub-profile name.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-profile

Syntax [**no**] **sub-profile** *subscriber-profile-name*

Context **[Tree]** (config>subscr-mgmt sub-profile)

Full Context configure subscriber-mgmt sub-profile

Description Commands in this context configure a subscriber profile. A subscriber profile is a template used to define the aggregate QoS for all hosts within a subscriber context. This is done through the definition of the egress and ingress scheduler policies that govern the aggregate SLA for subscribers using the subscriber profile. Subscriber profiles also allow for specific SLA profile definitions when the default definitions from the subscriber identification policy must be overridden.

Subscribers are either explicitly mapped to a subscriber profile template or are dynamically associated by one of various non-provisioned subscriber profile definitions.

A subscriber host can be associated with a subscriber profile in the following ways, listed from lowest to highest precedence:

1. The subscriber profile named default.
2. The subscriber profile defined as the subscriber SAP default.
3. The subscriber profile found by the subscriber identification policy sub-profile-map.
4. The subscriber profile found by the subscriber identification policy explicit map.

In the event that no defaults are defined and the subscriber identification string is not explicitly provisioned to map to a subscriber profile, either the static subscriber host creation will fail or the dynamic subscriber host DHCP ACK is discarded.

Default Subscriber profile:

When a subscriber profile is created with the *subscriber-profile-name* default, it is used when no other subscriber profile is associated with the subscriber host by the system. Creating a subscriber profile with the *subscriber-profile-name* default is optional. If a default subscriber profile is not created, all subscriber hosts subscriber identification strings must match either a non-provisioned default or be provisioned as an explicit match to a subscriber profile.

The default profile has no effect on existing active subscriber on the system as they exist due to higher precedence mappings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Attempting to delete any subscriber profile (including the profile named default) while in use by existing active subscribers will fail.

The **no** form of this command reverts to the default.

Parameters *subscriber-profile-name* — Specifies the name of the subscriber profile, up to 32 characters.

create — Keyword used to create the subscriber profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.456 sub-profile-map

sub-profile-map

Syntax **sub-profile-map**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol sub-profile-map)

Full Context configure subscriber-mgmt sub-ident-policy sub-profile-map

Description Commands in this context configure subscriber profile mapping parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.457 sub-profile-string

sub-profile-string

Syntax **sub-profile-string** *sub-profile-string*
no sub-profile-string

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings sub-profile-string)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings sub-profile-string)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings sub-profile-string
configure subscriber-mgmt local-user-db ppp host identification-strings sub-profile-string

Description This command specifies the subscriber profile string which is encoded in the identification strings.

The **no** form of this command returns to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sub-profile-string* — Specifies the subscriber profile string, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-profile-string

Syntax **sub-profile-string** *string*
no sub-profile-string

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile sub-profile-string)

Full Context configure subscriber-mgmt vrgw brg brg-profile sub-profile-string

Description This string will be used as a default for subscriber-profile lookup. This string can be overridden during BRG or host authentication. The **no** form of the command removes the string from the configuration.

Default no sub-profile-string

Parameters *string* — Specifies the string used to look up the subscriber profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.458 sub-ring

sub-ring

Syntax [**no**] **sub-ring** {**virtual-link** | **non-virtual-link**}

Context **[Tree]** (config>eth-ring sub-ring)

Full Context configure eth-ring sub-ring

Description This command specifies this ring-id to be sub-ring as defined in G.80312. By declaring this ring as a sub-ring object, this ring will only have one valid path and the sub-ring will be connected to a major ring or a VPLS instance.

The **virtual-link** keyword declares that a sub-ring is connected to another ring and control messages can be sent over the attached ring to the other side of the sub-ring.

The **non-virtual-link** channel parameter declares that a sub-ring may be connected to another ring or to a VPLS instance but no control messages from the sub-ring use the attached ring or VPLS instance. The non-virtual channel behavior is standard G.8032 capability.

The **no** form of this command deletes the sub-ring and its virtual channel associations.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no sub-ring

Parameters **virtual-link** — Specifies that the interconnection is to a ring and a virtual link will be used.

non-virtual-link — Specifies that the interconnection is to a ring or a VPLS instance and a virtual link will not be used.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.459 sub-sla-mgmt

sub-sla-mgmt

Syntax [**no**] **sub-sla-mgmt**

Context **[Tree]** (config>service>vpls>sap sub-sla-mgmt)
[Tree] (config>service>ies>if>sap sub-sla-mgmt)
[Tree] (config>service>ies>sub-if>grp-if>sap sub-sla-mgmt)
[Tree] (config>service>vprn>if>sap sub-sla-mgmt)
[Tree] (config>service>vprn>sub-if>grp-if>sap sub-sla-mgmt)
[Tree] (config>subscr-mgmt>msap-policy sub-sla-mgmt)

Full Context configure service ies interface sap sub-sla-mgmt
configure service ies subscriber-interface group-interface sap sub-sla-mgmt
configure service vpls sap sub-sla-mgmt
configure service vprn interface sap sub-sla-mgmt
configure service vprn subscriber-interface group-interface sap sub-sla-mgmt
configure subscriber-mgmt msap-policy sub-sla-mgmt

Description Commands in this context configure subscriber management parameters for this SAP.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

sub-sla-mgmt

Syntax [**no**] **sub-sla-mgmt**

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap-parameters sub-sla-mgmt)
[Tree] (config>service>vprn>sub-if>grp-if>sap-parameters sub-sla-mgmt)

Full Context configure service ies subscriber-interface group-interface sap-parameters sub-sla-mgmt
configure service vprn subscriber-interface group-interface sap-parameters sub-sla-mgmt

Description Commands in this context configure subscriber management parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the parameters from the configuration.

Default sub-sla-mgmt

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.460 subject

subject

Syntax **subject** {**eq** | **neq**} *subject* [*regexp*]
no subject

Context **[Tree]** (config>service>vprn>log>filter>entry>match subject)

Full Context configure service vprn log filter entry match subject

Description This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case the port-id string would be the subject. Only one **subject** command can be entered per event filter entry. The latest **subject** command overwrites the previous command.

The **no** form of this command removes the subject match criterion.

Default no subject

Parameters **eq | neq** — This operator specifies the type of match. Valid operators are listed below.

Values

Operator	Notes
eq	equal to
neq	not equal to

subject — A string used as the subject match criterion.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regexp** keyword is specified, the string in the **subject** command is a regular expression string that will be matched against the subject string in the log event being filtered.

When **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

subject

Syntax **subject** {**eq** | **neq**} *subject* [*regexp*]
no subject

Context **[Tree]** (config>log>filter>entry>match subject)

Full Context configure log filter entry match subject

Description This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case the port-id string would be the subject. Only one **subject** command can be entered per event filter entry. The latest **subject** command overwrites the previous command.

The **no** form of this command removes the subject match criterion.

Parameters **eq** | **neq** — Specifies the match type. Valid operators are listed in Table 180.

Table 180 **Valid Operators**

Operator	Notes
eq	equal to
neg	not equal to

subject — Specifies a string up to 32 characters, used as the subject match criterion.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regexp** keyword is specified, the string in the **subject** command is a regular expression string that will be matched against the subject string in the log event being filtered. When the **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

Platforms All

23.461 subnet

subnet

Syntax **subnet** {*ip-address*/*mask* | *ip-address netmask*} [**create**]
no subnet {*ip-address*/*mask* | *ip-address netmask*}

Context **[Tree]** (config>router>dhcp>server>pool subnet)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>dhcp>server>pool subnet)

Full Context configure router dhcp local-dhcp-server pool subnet
configure service vprn dhcp local-dhcp-server pool subnet

Description This command creates a subnet of IP addresses to be served from the pool. The subnet cannot include any addresses that were assigned to subscribers without those addresses specifically excluded. When the subnet is created, no IP addresses are made available until a range is defined.

The **no** form of the removes the subnet parameters from the configuration.

Parameters *ip-prefix/mask* — Specifies the address prefix and mask. A mask of 255.255.255.255 is reserved for system IP addresses.

Values ip-prefix: a.b.c.d
mask: 8 to 32

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

Values a.b.c.d, any mask expressed as dotted quad

create — Keyword used to create the subnet. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.462 subnet-check

subnet-check

Syntax [**no**] **subnet-check**

Context [Tree] (config>service>vprn>igmp>grp-if subnet-check)
[Tree] (config>service>vprn>igmp>if subnet-check)

Full Context configure service vprn igmp group-interface subnet-check
configure service vprn igmp interface subnet-check

Description This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.

The **no** form of this command disables local subnet checking for IGMP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn igmp group-interface subnet-check

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn igmp interface subnet-check

subnet-check

Syntax [**no**] **subnet-check**

Context **[Tree]** (config>router>igmp>group-interface subnet-check)
[Tree] (config>router>igmp>if subnet-check)

Full Context configure router igmp group-interface subnet-check
configure router igmp interface subnet-check

Description This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.

Default subnet-check

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface subnet-check

All

- configure router igmp interface subnet-check

subnet-check

Syntax [**no**] **subnet-check**

Context **[Tree]** (config>router>mld>group-interface subnet-check)

Full Context configure router mld group-interface subnet-check

Description This command enables subnet checking for MLD messages received on this interface. All MLD packets with a source address that is not in the local subnet are dropped.

Default subnet-check

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.463 subnet-mask

subnet-mask

Syntax **subnet-mask** *ip-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no subnet-mask

Context [Tree] (config>router>dhcp>server>pool>subnet>options subnet-mask)
[Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>options subnet-mask)

Full Context configure router dhcp local-dhcp-server pool subnet options subnet-mask
configure subscriber-mgmt local-user-db ipoe host options subnet-mask

Description This command specifies the subnet-mask option to the client. The mask can either be defined (for supernetting) or taken from the pool address.

The **no** form of this command removes the address from the configuration.

Parameters *ip-address* — Specifies the IP address of the subnet mask. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.464 subrate

subrate

Syntax **subrate** {**digital-link** | **larscom**} *rate-step*
no subrate

Context [Tree] (config>port>tdm>ds3 subrate)

Full Context configure port tdm ds3 subrate

Description This command configures the channel service unit (CSU) compatibility mode to interoperate with existing DS-3 subrate standards.

This configuration applies only for non-channelized DS-3s on ASAP TDM MDAs.

The **no** form of this command remove the subrate functionality.

Default no subrate

Parameters **digital-link** — Enables the Digital-Link (Quick Eagle) CSU compatibility mode.

larscom — Enables the Larscom CSU compatibility mode.

rate-step — Specifies the subrate value for the associated DS-3.

Values 1 to 147 (digital-link) 1 to 14 (larscom)

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.465 subscriber

subscriber

Syntax **subscriber** *sub-ident*
no subscriber

Context **[Tree]** (config>service>ies>if>sap>static-host subscriber)
[Tree] (config>service>vpls>sap>static-host subscriber)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host subscriber)
[Tree] (config>service>vprn>if>sap>static-host subscriber)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host subscriber)

Full Context configure service ies interface sap static-host subscriber
configure service ies subscriber-interface group-interface sap static-host subscriber
configure service vpls sap static-host subscriber
configure service vprn interface sap static-host subscriber
configure service vprn subscriber-interface group-interface sap static-host subscriber

Description This command specifies an existing subscriber identification profile to be associated with the static subscriber host.

Parameters *sub-ident* — Specifies the subscriber identification.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

subscriber

Syntax **subscriber** *sub-ident-string* [**sap** *sap-id*] [**ip** *ip-address*] [{[**mac** *ieee-address*] | **sla-profile** *sla-profile-name*}] [**fc** {[**be**] [**l2**] [**af**] [**l1**] [**h2**] [**ef**] [**h1**] [**nc**]}] {[**ingress**] [**egress**]} [**host-type** *host-type*] [**family** *family*]
no subscriber *sub-ident-string*

Context **[Tree]** (config>mirror>mirror-source subscriber)

Full Context configure mirror mirror-source subscriber

Description This command adds hosts of a subscriber to mirroring service.

Parameters *sub-ident-string* — Specifies the name of the subscriber identification policy.

sap-id — Specifies the physical port identifier portion of the SAP definition.

ip-address — Specifies the service IP address (system IP address) of the remote device sending LI traffic. If 0.0.0.0 is specified, any remote router is allowed to send to this service.

Values 1.0.0.1 to 223.255.255.254

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ieee-address — Specify this optional parameter when defining a static host. The MAC address must be specified for **anti-spoof ip-mac** and **arp-populate**. Multiple static hosts may be configured with the same MAC address given that each definition is distinguished by a unique IP address.

sla-profile-name — Each host of a subscriber can use a different sla-profile. This option allows interception of only the hosts using the specified sla-profile. In some deployments sla-profiles are assigned per type of traffic. There can be, for example, a specific sla-profile for voice traffic (which could be used for all SIP-hosts). The name can have up to 32 characters.

fc — Specifies the name of the forwarding class with which to associate traffic. The forwarding class name must already be defined within the system. If the *fc-name* does not exist, an error will be returned and the **fc** command will have no effect. If the *fc-name* does exist, the forwarding class associated with *fc-name* will override the default forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

egress — Specifies that packets egressing the SAP should be mirrored. Egress packets are mirrored to the mirror destination after egress packet modification.

ingress — Specifies that packets ingressing the SAP should be mirrored. Ingress packets are mirrored to the mirror destination prior to ingress packet modification.

host-type — Specifies the host type for mirroring. The anti-spoof filter on the SAP must be configured as **ip-mac**.

Values any, ipoe, ppp

family — Specifies the IP family for mirroring. The anti-spoof filter on the SAP must be configured as **ip-mac**.

Values any, ipv4, ipv6

Platforms All

subscriber

Syntax **subscriber** *sub-ident-string* [**sap** *sap-id* [**ip** *ip-address*] [**mac** *ieee-address*] | **sla-profile** *sla-profile-name*] [**fc** {[**be**] [**l2**] [**af**] [**l1**] [**h2**] [**ef**] [**h1**] [**nc**]}] [**intercept-id** *intercept-id*] [**session-id** *session-id*] {[**ingress**] [**egress**]} [**host-type** *host-type*] [**family** *ip-family*]

no subscriber *sub-ident-string*

Context **[Tree]** (config>li>li-source subscriber)

Full Context configure li li-source subscriber

Description This command adds hosts of a subscriber to mirroring service.

Parameters *sub-ident-string* — Specifies the name of the subscriber identification policy.

sap-id — Specifies the physical port identifier portion of the SAP definition.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address — Specifies the service IP address (system IP address) of the remote device sending LI traffic. If 0.0.0.0 is specified, any remote router is allowed to send to this service.

Values 1.0.0.1 to 223.255.255.254

ieee-address — Specifies a MAC address when defining a static host. The MAC address must be specified for **anti-spoof ip-mac** and **arp-populate**. Multiple static hosts may be configured with the same MAC address given that each definition is distinguished by a unique IP address.

sla-profile-name — Specifies an SLA profile name, up to 32 characters. Each host of a subscriber can use a different sla-profile. This option allows interception of only the hosts using the specified sla-profile. In some deployments sla-profiles are assigned per type of traffic. There can be, for example, a specific sla-profile for voice traffic (which could be used for all SIP-hosts).

fc — The name of the forwarding class with which to associate LI traffic. The forwarding class name must already be defined within the system. If the *fc-name* does not exist, an error will be returned and the **fc** command will have no effect. If the *fc-name* does exist, the forwarding class associated with *fc-name* will override the default forwarding class.

Values be, l2, af, l1, h2, ef, h1, nc

intercept-id — Specifies the intercept-id that is inserted into the packet header for all mirrored packets of the associated li-source entry. This *intercept-id* can be used (for example by a downstream LI Gateway) to identify the particular LI session to which the packet belongs.

For all types of **li-source** entries (**filter**, **nat**, **sap**, or **subscriber**), when the mirror service is configured with **ip-udp-shim** routable encap, an *intercept-id* field (as part of the routable encap) is always present in the mirrored packets. If there is no *intercept-id* configured for an **li-source** entry, then the default value will be inserted. When the mirror service is configured with **ip-gre** routable encap, no *intercept-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4294967295 (32b) For **nat li-source** entries that are using a mirror service that is not configured with routable encap

Values 1 to 1,073,741,824 (30b) For all types of li-source entries that are using a mirror service with routable **ip-udp-shim** encapsulation and no direction-bit.

Values 1 to 536,870,912 (29b) For all types of li-source entries that are using a mirror service with routable **ip-udp-shim** encapsulation and with the direction-bit enabled.

session-id — Specifies the *session-id* that is inserted into the packet header for all mirrored packets of the associated **li-source** entry. This *session-id* can be used (for example by a downstream LI gateway) to identify the particular LI session to which the packet belongs. The *session-id* is only valid and used for mirror services that are configured with **ip-udp-shim** routable encapsulation (**config>mirror>mirror-dest>encap>ip-udp-shim**).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For all types of **li-source** entries (**filter**, **nat**, **sap**, or **subscriber**), when the mirror service is configured with **ip-udp-shim** routable encap, a *session-id* field (as part of the routable encapsulation) is always present in the mirrored packets. If there is no *session-id* configured for an **li-source** entry, then the default value will be inserted. When a mirror service is configured with **ip-gre** routable encap, no *session-id* is inserted and none should be specified against the **li-source** entries.

Values 1 to 4,294,967,295 (32b)

ingress — Specifies information for the ingress policy.

egress — Specifies information for the egress policy.

host-type — Specifies the host type for lawful intercept. The anti-spoof filter on the SAP must be configured as **ip-mac**.

Values any, ipoe, ppp

ip-family — Specifies the IP family for lawful intercept. The anti-spoof filter on the SAP must be configured as **ip-mac**.

Values any, ipv4, ipv6

Platforms All

subscriber

Syntax **subscriber** *sub-ident-string* [**sap** *sap-id*] [**ip** *ip-address*] [{**mac** *ieee-address*] | **sla-profile** *sla-profile-name*}] [**fc** {[**be**] [**l2**] [**af**] [**l1**] [**h2**] [**ef**] [**h1**] [**nc**]}] {[**ingress**] [**egress**]}
no subscriber *sub-ident-string*

Context **[Tree]** (debug>mirroring-source subscriber)

Full Context debug mirroring-source subscriber

Description This command adds hosts of a subscriber to mirroring service.

Parameters *sub-ident-string* — Specifies the name of the subscriber identification policy.

sap-id — Specifies the physical port identifier portion of the SAP definition.

ip-address — The service IP address (system IP address) of the remote 7750 SR or 7450 ESS device sending LI traffic.

Values 1.0.0.1 to 223.255.255.254

ieee-address — Specify this optional parameter when defining a static host. The MAC address must be specified for **anti-spoof ip-mac** and **arp-populate**. Multiple static hosts may be configured with the same MAC address given that each definition is distinguished by a unique IP address.

sla-profile-name — Specifies the SLA profile name, up to 32 characters.

fc — Specifies name of the forwarding class with which to associate LI traffic.

Values be, l2, af, l1, h2, ef, h1, nc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ingress — Specifies information for the ingress policy.

egress — Specifies information for the egress policy.

23.466 subscriber-bw-limit

subscriber-bw-limit

Syntax **subscriber-bw-limit** *bandwidth*
no subscriber-bw-limit

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>video-policy>video-if subscriber-bw-limit)

Full Context configure mcast-management multicast-info-policy video-policy video-interface subscriber-bw-limit

Description This command configures of an egress per-subscriber bandwidth limit for the combined retransmission and Fast Channel Change (FCC) replies for requests received directed to the IP address. If the bandwidth for a request will exceed the bandwidth limit, the request is logged and dropped.

The **no** form of the command disables enforcement of an egress bandwidth limit.

Default no subscriber-bw-limit

Parameters *bandwidth* — The per-subscriber egress bandwidth limit for retransmission and FCC packets in kilobits per second expressed as an integer indicates infinity or no limit.

Values 1 to 4294967295 kb/s

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

23.467 subscriber-data

subscriber-data

Syntax [**no**] **subscriber-data**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes subscriber-data)

Full Context configure aaa isa-radius-policy acct-include-attributes subscriber-data

Description This command enables the inclusion of subscriber data attributes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the command excludes subscriber data attributes.

Default no subscriber-data

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.468 subscriber-id

subscriber-id

Syntax **subscriber-id** *sub-ident-string*
no subscriber-id

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ident-strings subscriber-id)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ident-strings subscriber-id)

Full Context configure subscriber-mgmt local-user-db ipoe host identification-strings subscriber-id
configure subscriber-mgmt local-user-db ppp host identification-strings subscriber-id

Description This command specifies the subscriber ID which is encoded in the identification strings.

The **no** form of this command returns to the default.

Parameters *sub-ident-string* — Specifies the subscriber ID string, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

subscriber-id

Syntax [**no**] **subscriber-id**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute subscriber-id)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute subscriber-id

Description This command specifies that subscriber ID attributes should be included into RADIUS accounting messages.

The **no** form of this command excludes subscriber ID attributes into RADIUS accounting messages.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

subscriber-id

Syntax [**no**] **subscriber-id**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes subscriber-id)

Full Context configure aaa isa-radius-policy acct-include-attributes subscriber-id

Description This command specifies that subscriber ID attributes should be included into RADIUS accounting messages.

Default no subscriber-id

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.469 subscriber-identification

subscriber-identification

Syntax **subscriber-identification**

Context **[Tree]** (config>router>nat>inside subscriber-identification)

Full Context configure router nat inside subscriber-identification

Description Commands in this context configure subscriber identification for Large Scale NAT.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.470 subscriber-interface

subscriber-interface

Syntax **subscriber-interface** *ip-int-name* [**create**] [**wan-mode** *mode*]
subscriber-interface *ip-int-name* [**create**] **fwd-service** *service-id* **fwd-subscriber-interface** *fwd-int-name* [**wan-mode** *mode*]
no subscriber-interface *ip-int-name*

Context **[Tree]** (config>service>ies subscriber-interface)
[Tree] (config>service>vprn subscriber-interface)

Full Context configure service ies subscriber-interface
configure service vprn subscriber-interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows the operator to create special subscriber-based interfaces. It is used to contain multiple group interfaces. Multiple subnets associated with the subscriber interface can be applied to any of the contained group interfaces in any combination. The subscriber interface allows subnet sharing between group interfaces.

The **no** form of this command reverts to the default.

Parameters *ip-int-name* — Specifies the interface name of a subscriber interface, up to 32 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — Keyword used to create the subscriber interface.

fwd-service *service-id* — Specifies the wholesale service ID or service name.

Values *service-id*: 1 to 214748364
svc-name: A string up to 64 characters

ip-int-name — Specifies the wholesale subscriber interface.

wan-mode *mode* — Specifies the WAN mode as 64-bit or 128-bit. To change the WAN mode after creation, the interface must first be removed then recreated.

Values *mode64*, *mode128*

Default *mode64*

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.471 subscriber-interface-statistics

subscriber-interface-statistics

Syntax **subscriber-interface-statistics**

Context **[Tree]** (config>subscr-mgmt subscriber-interface-statistics)

Full Context configure subscriber-mgmt subscriber-interface-statistics

Description Commands in this context enable or disable the collection of subscriber interface statistics.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.472 subscriber-limit

subscriber-limit

Syntax **subscriber-limit** *limit*
no subscriber-limit

Context **[Tree]** (config>service>vprn>nat>outside>pool subscriber-limit)

Full Context configure service vprn nat outside pool subscriber-limit

Description This command configures the maximum number of subscribers per outside IP address.

If multiple port blocks per subscriber are used, the block size is typically small; all blocks assigned to a given subscriber belong to the same IP address; the subscriber limit guarantees that any subscriber can get a minimum number of ports.

Parameters *limit* — Specifies the maximum number of subscribers per outside IP address.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.473 subscriber-mgmt

subscriber-mgmt

Syntax **subscriber-mgmt**

Context **[Tree]** (config>service>ies subscriber-mgmt)
[Tree] (config>service>vprn subscriber-mgmt)

Full Context configure service ies subscriber-mgmt
configure service vprn subscriber-mgmt

Description Commands in this context configure per service subscriber management parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

subscriber-mgmt

Syntax **subscriber-mgmt**

Context **[Tree]** (config subscriber-mgmt)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt

Description Commands in this context configure subscriber management entities. A subscriber is uniquely identified by a subscriber identification string. Each subscriber can have several DHCP sessions active at any time. Each session is referred to as a subscriber host and is identified by its IP address and MAC address.

All subscriber hosts belonging to the same subscriber are subject to the same hierarchical QoS (HQoS) processing. The HQoS processing is defined in the sub-profile (the subscriber profile). A sub-profile refers to an existing scheduler policy (configured in **the config>qos>scheduler-policy** context) and offers the possibility to overrule the rate of individual schedulers within this policy.

Because all subscriber hosts use the same scheduler policy instance, they must all reside on the same complex.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

subscriber-mgmt

Syntax **subscriber-mgmt**

Context **[Tree]** (config>system>persistence subscriber-mgmt)

Full Context configure system persistence subscriber-mgmt

Description This command configures subscriber management persistence parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.474 subscriber-prefix-length

subscriber-prefix-length

Syntax **subscriber-prefix-length** *prefix-length*
no subscriber-prefix-length

Context **[Tree]** (config>service>vprn>nat>inside>dslite subscriber-prefix-length)

Full Context configure service vprn nat inside dual-stack-lite subscriber-prefix-length

Description This command configures the IPv6 prefix length of the DS-Lite subscribers.

The **no** form of this command reverts the default.

Default subscriber-prefix-length 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **prefix-length** *prefix-length* — Specifies the IPv6 prefix length of the DS-Lite subscriber.

Values 32 to 64, 128

Default 128

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

subscriber-prefix-length

Syntax **subscriber-prefix-length** *prefix-length*
no subscriber-prefix-length

Context **[Tree]** (config>router>nat>inside>dual-stack-lite subscriber-prefix-length)

Full Context configure router nat inside dual-stack-lite subscriber-prefix-length

Description This command sets the value for the number of high order bits of the source IPv6 address that will be considered as DS-Lite subscriber. The remaining bits of the source IPv6 address will be masked off, effectively aggregation all IPv6 source addresses under the configured prefix length into a single DS-Lite subscriber. Source IPv4 addresses/ports of the traffic carried within the DS-Lite subscriber will be translated into a single outside IPv4 address and the corresponding deterministic port-block (port-blocks can be extended).

The range of values for subscriber-prefix-length in non-deterministic DS-Lite is limited from 32 to 64 (a prefix will be considered as a DS-Lite subscriber) or it can be set to a value of 128 (the source IPv6 address is considered as a DS-Lite subscriber).

In cases where deterministic DS-Lite is enabled in a giver inside routing context, the range of values of the **subscriber-prefix-length** depends on the value of *dslite-max-subscriber-limit* parameter as follows:

subscriber-prefix-length – n = [32..64,128]

where n = log2(dslite-max-subscriber-limit)

[or in an alternate form: dslite-max-subscriber-limit = 2^n.]

In other words the largest prefix length for the deterministic DS-Lite subscriber will be 32+n, where n = log2(dslite-max-subscriber-limit). The subscriber prefix length can extend up to 64 bits. Beyond 64 bits for the subscriber prefix length, there only one value is allowed: 128. In the case n must be 0, which means that the mapping between B4 elements (or IPv6 address) and the IPv4 outside addresses is in 1:1 ratio (no sharing of outside IPv4 addresses).

This parameter can be changed only when there are no deterministic prefixes configured in the same routing context.

The **no** form of the command reverts to the default.

Default 128

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *prefix-length* — In non-deterministic DS-Lite this value can be [32..64,128], assuming that the deterministic DS-Lite is not concurrently enabled in the same inside routing context. In case that deterministic DS-Lite is enabled, this value can be within the range [(32+n)..64,128] where n = log2(dslite-max-subscriber-limit). The value of 128 is allowed only when n=0 (each subscriber is mapped to a single outside IPv4 IP address).

Values 32 to 64

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

subscriber-prefix-length

Syntax **subscriber-prefix-length** *prefix-length*
no subscriber-prefix-length

Context [Tree] (config>service>vprn>nat>inside>nat64 subscriber-prefix-length)
[Tree] (config>router>nat>inside>nat64 subscriber-prefix-length)

Full Context configure router nat inside nat64 subscriber-prefix-length
configure service vprn nat inside nat64 subscriber-prefix-length

Description This command specifies the IPv6 address prefix length to be used for the NAT64 subscribers in this virtual router instance.

Default subscriber-prefix-length128

Parameters *prefix-length* — Specifies the subscriber identification for Large Scale NAT.

Values 32 to 64, 128

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.475 subscriber-prefixes

subscriber-prefixes

Syntax **subscriber-prefixes**

Context [Tree] (config>service>ies>sub-if>ipv6 subscriber-prefixes)
[Tree] (config>service>vprn>sub-if>ipv6 subscriber-prefixes)

Full Context configure service ies subscriber-interface ipv6 subscriber-prefixes
configure service vprn subscriber-interface ipv6 subscriber-prefixes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure aggregate off-link subscriber prefixes associated with this subscriber interface. Individual prefixes are specified under the prefix context list aggregate routes in which the next hop is indirect via the subscriber interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.476 subscriber-retention

subscriber-retention

Syntax **subscriber-retention** [**hrs** *hours*] [**min** *minutes*]
no subscriber-retention

Context **[Tree]** (config>service>nat>nat-policy>timeouts subscriber-retention)
[Tree] (config>service>nat>up-nat-policy>timeouts subscriber-retention)

Full Context configure service nat nat-policy timeouts subscriber-retention
configure service nat up-nat-policy timeouts subscriber-retention

Description This command specifies the subscriber retention timeout, which is the time a NAT subscriber and its associated IP address are kept after all hosts and associated port blocks have expired. If a NAT subscriber host appears before the retention timeout has elapsed, it is given the same outside IP address.

Default no subscriber-retention

Parameters **hrs** *hours* — Specifies the hours a subscriber's IP address is kept after all hosts and port blocks have expired.

Values 1 to 24

min *minutes* — Specifies the minutes a subscriber's IP address is kept after all hosts and port blocks have expired.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.477 subscriber-sap-id

subscriber-sap-id

Syntax [**no**] **subscriber-sap-id**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if>sap>static-host subscriber-sap-id)
[Tree] (config>service>ies>sub-if>grp-if>sap>static-host subscriber-sap-id)
[Tree] (config>service>vpls>sap>static-host subscriber-sap-id)
[Tree] (config>service>vprn>if>sap>static-host subscriber-sap-id)
[Tree] (config>service>vprn>sub-if>grp-if>sap>static-host subscriber-sap-id)

Full Context configure service ies interface sap static-host subscriber-sap-id
configure service ies subscriber-interface group-interface sap static-host subscriber-sap-id
configure service vpls sap static-host subscriber-sap-id
configure service vprn interface sap static-host subscriber-sap-id
configure service vprn subscriber-interface group-interface sap static-host subscriber-sap-id

Description This command enables using the SAP ID as the subscriber ID.

Parameters **subscriber-sap-id** — Specifies to use the sap-id as the subscriber-id.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.478 subscription

subscription

Syntax **subscription** *percentage*
no subscription

Context [Tree] (config>router>rsvp>interface subscription)

Full Context configure router rsvp interface subscription

Description This command configures the percentage of the link bandwidth that RSVP can use for reservation and sets a limit for the amount of over-subscription or under-subscription allowed on the interface.

When the **subscription** is set to zero, no new sessions are permitted on this interface. If the *percentage* is exceeded, the reservation is rejected and a log message is generated.

The **no** form of this command reverts the *percentage* to the default value.

Default subscription 100

Parameters *percentage* — Specifies the percentage of the interface's bandwidth that RSVP allows to be used for reservations.

Values 0 to 1000

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

subscription

Syntax **subscription** *subscription-id* **cancel**

Context **[Tree]** (admin>system>telemetry>grpc subscription)

Full Context admin system telemetry grpc subscription

Description This command cancels an active telemetry subscription.

Parameters *subscription-id* — Specifies the ID of the Telemetry subscription to cancel.

Values 0 to 4294967295

Platforms All

subscription

Syntax **subscription** *name* [**create**]
no subscription *name*

Context **[Tree]** (config>system>telemetry>persistent-subscriptions subscription)

Full Context configure system telemetry persistent-subscriptions subscription

Description Commands in this context configure persistent subscription commands.

The **no** form of this command removes the configuration.

Parameters *name* — Specifies the subscription name, up to 32 characters.

create — Keyword used to create the subscription.

Platforms All

23.479 subscription cancel-all

subscription cancel-all

Syntax **subscription cancel-all**

Context **[Tree]** (admin>system>telemetry>grpc subscription cancel-all)

Full Context admin system telemetry grpc subscription cancel-all

Description This command cancels all active Telemetry subscriptions.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.480 subtype

subtype

Syntax [**no**] **subtype** *tls extension subtype*

Context **[Tree]** (config>app-assure>group>http-enrich>tls-extension subtype)

Full Context configure application-assurance group http-enrich tls-extension subtype

Description This command configures a TLS subtype.

The **no** form of this command removes the TLS subtype from the configuration.

Parameters *tls extension subtype* — Specifies a TLS subtype, up to 32 characters

23.481 suggest-internal-objects

suggest-internal-objects

Syntax [**no**] **suggest-internal-objects**

Context **[Tree]** (environment suggest-internal-objects)

Full Context environment suggest-internal-objects

Description This command enables suggesting of internally created objects while auto completing.

The **no** form of the command disables the command.

Platforms All

23.482 summaries

summaries

Syntax [**no**] **summaries**

Context **[Tree]** (config>service>vprn>ospf>area>nssa summaries)
[Tree] (config>service>vprn>ospf>area>stub summaries)
[Tree] (config>service>vprn>ospf3>area>nssa summaries)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ospf area nssa summaries
configure service vprn ospf area stub summaries
configure service vprn ospf3 area nssa summaries

Description This command enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR). This parameter is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or nssa area. By default, summary route advertisements are sent into the stub area or NSSA.

The **no** form of this command disables sending summary route advertisements and, for stub areas, only the default route is advertised by the ABR.

Default summaries — Summary routes are advertised by the ABR into the stub area or NSSA.

Platforms All

summaries

Syntax [**no**] **summaries**

Context **[Tree]** (config>router>ospf>area>nssa summaries)
[Tree] (config>router>ospf>area>stub summaries)
[Tree] (config>router>ospf3>area>nssa summaries)
[Tree] (config>router>ospf3>area>stub summaries)

Full Context configure router ospf area nssa summaries
configure router ospf area stub summaries
configure router ospf3 area nssa summaries
configure router ospf3 area stub summaries

Description This command enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR).

This parameter is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or NSSA area (default: summary).

By default, summary route advertisements are sent into the stub area or NSSA.

The **no** form of this command disables sending summary route advertisements and, for stub areas; only the default route is advertised by the ABR.

Default summaries

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.483 summary

summary

Syntax **summary**

Context **[Tree]** (config>filter>log summary)

Full Context configure filter log summary

Description Commands in this context configure log summarization. These settings will only be taken into account when syslog is the log destination.

Platforms All

summary

Syntax **summary** [*ip-address*]
no summary

Context **[Tree]** (debug>router>isis summary)

Full Context debug router isis summary

Description This command enables debugging for ISIS summary addresses.

The **no** form of the command disables the debugging.

Parameters *ip-address* — When specified, only packets with the specified address are debugged.

Platforms All

23.484 summary-address

summary-address

Syntax **summary-address** {*ip-prefix/mask* | *ip-prefix* [*netmask*]} [*level*] [**tag** *tag*]
no summary-address {*ip-prefix/mask* | *ip-prefix* [*netmask*]}

Context **[Tree]** (config>service>vprn>isis summary-address)

Full Context configure service vprn isis summary-address

Description This command creates summary-addresses for the specified router or VPRN instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-prefix/mask* — Specifies information for the specified IP prefix and mask length.

Values

ip-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
ipv6-prefix-length	0 to 128

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

level — Specifies IS-IS level area attributes. If no level parameter is specified, the default is level-1/2.

Values level-1, level-2, level-1/2

tag *tag* — Assigns a route tag to the summary address.

Values 1 to 4294967295

Platforms All

summary-address

Syntax **summary-address** {*ip-prefix/ip-prefix-length* | *ip-prefix netmask*} [*level*] [**tag** *tag*] [**algorithm** *algo-id*]
no summary-address {*ip-prefix/ip-prefix-length* | *ip-prefix netmask*}

Context **[Tree]** (config>router>isis summary-address)

Full Context configure router isis summary-address

Description This command creates summary-addresses.

Default no summary-address

Parameters *ip-prefix/ip-prefix-length* — Specifies the IP prefix and prefix length of the summary address.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)
ipv4-prefix-length	0 to 32
ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	d: [0 to 255]D
ipv6-prefix-length	0 to 128

netmask — Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

level — Specifies IS-IS level area attributes. If no level parameter is specified, the default is level-1/2.

Values level-1, level-2, level-1/2

tag — Assigns a route tag to the summary address.

Values 1 to 4294967295

algo-id — Specifies the algorithm topology applied for the summary address. If no algo-id parameter is specified, the default is 0.

Values 0, 128 to 255

Platforms All

23.485 summary-crit

summary-crit

Syntax **summary-crit dst-addr**
summary-crit src-addr
no summary-crit

Context **[Tree]** (config>filter>log>summary summary-crit)

Full Context configure filter log summary summary-crit

Description This command defines the key of the index of the mini-table. If key information is changed while summary is administratively enabled (no shutdown), the filter summary mini-table is flushed and recreated with different key information. Log packets received during the reconfiguration time will be handled as if summary was not active.

The **no** form of the command reverts to the default parameter.

Default summary-crit src-addr

Parameters **dst-addr** — Specifies that received log packets are summarized based on the destination IPv4, IPv6, or MAC address.

src-addr — Specifies that received log packets are summarized based on the source IPv4, IPv6 or MAC address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.486 super-backbone

super-backbone

Syntax [**no**] **super-backbone**

Context **[Tree]** (config>service>vprn>ospf super-backbone)

Full Context configure service vprn ospf super-backbone

Description This command specifies whether CE-PE functionality is required or not. The OSPF super backbone indicates the type of the LSA generated as a result of routes redistributed into OSPF. When enabled, the redistributed routes are injected as summary, external or NSSA LSAs. When disabled, the redistributed routes are injected as either external or NSSA LSAs only.

Default no super-backbone

Platforms All

23.487 supplicant-timeout

supplicant-timeout

Syntax **supplicant-timeout** *seconds*
no supplicant-timeout

Context **[Tree]** (config>port>ethernet>dot1x supplicant-timeout)

Full Context configure port ethernet dot1x supplicant-timeout

Description This command configures the period during which the router waits for a client to respond to its EAPOL messages. When the supplicant-timeout expires, the 802.1x authentication session is considered to have failed.

The **no** form of this command returns the value to the default.

Default supplicant-timeout 30

Parameters *seconds* — Specifies the server timeout period in seconds.

Values 1 to 300

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.488 supported-features

supported-features

Syntax [**no**] **supported-features**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp supported-features)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp supported-features

Description This command includes the **supported-features** in CCR messages.

The **no** form of this command resets the command to the default setting.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.489 suppress

suppress

Syntax **suppress** *integer*
no suppress

Context **[Tree]** (config>router>policy-options>damping suppress)

Full Context configure router policy-options damping suppress

Description This command configures the suppression parameter for the route policy damping profile.

A route is suppressed when it has flapped frequently enough to increase the Figure of Merit (FoM) value to exceed the **suppress** threshold limit. When the **FoM** value exceeds the **suppress** threshold limit, the route is removed from the route table or inclusion in advertisements.

The **no** form of this command removes the suppress parameter from the damping profile.

Default no suppress

Parameters *integer* — Specifies the suppress value expressed as a decimal integer.

Values 1 to 20000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.490 suppress-attached-bit

suppress-attached-bit

Syntax [**no**] **suppress-attached-bit**

Context **[Tree]** (config>service>vprn>isis suppress-attached-bit)

Full Context configure service vprn isis suppress-attached-bit

Description This command configures IS-IS to suppress setting the attached bit on originated Level 1 LSPs to prevent all L1 routers in the area from installing a default route to it.

Platforms All

suppress-attached-bit

Syntax [**no**] **suppress-attached-bit**

Context **[Tree]** (config>router>isis suppress-attached-bit)

Full Context configure router isis suppress-attached-bit

Description This command configures IS-IS to suppress setting the attached bit on originated Level 1 LSPs to prevent all L1 routers in the area from installing a default route to it.

Default no suppress-attached-bit

Platforms All

23.491 suppress-dn-bit

suppress-dn-bit

Syntax [**no**] **suppress-dn-bit**

Context **[Tree]** (config>service>vprn>ospf suppress-dn-bit)
[Tree] (config>service>vprn>ospf3 suppress-dn-bit)

Full Context configure service vprn ospf suppress-dn-bit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn ospf3 suppress-dn-bit

Description This command specifies whether to suppress the setting of the DN bit for OSPF LSA packets generated by this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets generated by this instance of the OSPF router will not be set. When disabled, this instance of the OSPF router will follow the normal procedure to determine whether to set the DN bit.

Default no suppress-dn-bit

Platforms All

23.492 suppress-lo-alarm

suppress-lo-alarm

Syntax [**no**] **suppress-lo-alarm**

Context **[Tree]** (config>port>sonet-sdh suppress-lo-alarm)

Full Context configure port sonet-sdh suppress-lo-alarm

Description This command enables the suppression of lower order alarms on SONET/SDH port such as MLPPP bundle alarms, DS1/E1 links alarms and 336 APS channel groups alarms.

The **no** form of this command disables the suppression of lower order alarms on SONET/SDH port.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.493 suppress-lsn-events

suppress-lsn-events

Syntax [**no**] **suppress-lsn-events**

Context **[Tree]** (configure>isa>wlan-gw-group>nat suppress-lsn-events)

Full Context configure isa wlan-gw-group nat suppress-lsn-events

Description This command suppresses the generation of Large Scale NAT (LSN) events when RADIUS accounting is enabled.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

By default, only one logging facility for tracking subscribers in LSN44, DS-Lite, and NAT64 can be enabled at the time, either the SR OS event logging facility or the RADIUS logging facility. Note that SR OS event logs can be sent to multiple destinations, such as the console session, a telnet or SSH session, memory logs, file destinations, SNMP trap groups, and syslog destinations.

If RADIUS logging is enabled, the NAT logs are sent to the RADIUS destination and the NAT logs are suppressed in the SR OS event logging facility, for example, NAT logs are not sent to the syslog server.

If RADIUS logging is disabled, the NAT logs are sent to the SR OS event logging facility, for example, syslog, assuming that the events are enabled via the SR OS event-control (**config> log>event-control nat event generate**).

The **no** form of this command, the NAT logs can be sent to both logging facilities simultaneously, the SR OS event logging facility and RADIUS logging facility.

Default suppress-lsn-events

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

suppress-lsn-events

Syntax [**no**] **suppress-lsn-events**

Context **[Tree]** (config>isa>nat-group suppress-lsn-events)

Full Context configure isa nat-group suppress-lsn-events

Description This command suppresses the generation of Large Scale NAT (LSN) events when RADIUS accounting is enabled.

By default, only one logging facility for tracking subscribers in LSN44, DS-Lite, and NAT64 can be enabled at the time: either the SR OS event logging facility or the RADIUS logging facility. SR OS event logs can be sent to multiple destinations, such as the console session, a telnet or SSH session, memory logs, file destinations, SNMP trap groups, and syslog destinations.

If RADIUS logging is enabled, the NAT logs are sent to the RADIUS destination and the NAT logs are suppressed in the SR OS event logging facility, for example, NAT logs are not sent to the syslog server.

If RADIUS logging is disabled, the NAT logs are sent to the SR OS event logging facility; for example, syslog, assuming that the events are enabled via the event-control command (**config> log>event-control nat event generate**).

By explicitly disabling this command (**no suppress-lsn-events**), the NAT logs can be sent to both logging facilities simultaneously, the SR OS event logging facility, and the RADIUS logging facility.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default suppress-lsn-events

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.494 suppress-lsn-sub-blks-free

suppress-lsn-sub-blks-free

Syntax [**no**] **suppress-lsn-sub-blks-free**

Context **[Tree]** (configure>isa>wlan-gw-group>nat suppress-lsn-sub-blks-free)

Full Context configure isa wlan-gw-group nat suppress-lsn-sub-blks-free

Description This command suppresses the tmnxNatLsnSubBlksFree summary notification and use the tmnxNatPlBlockAllocationLsn notifications. When the SR OS node is in a state of excessive logging, the queue associated with the transmission of logs on the MS-ISA can become congested. This event further delays the generation of logs, and with this, further allocations and deallocations of NAT resources (port-blocks) is stalled until the queue is relieved of congestion. For example, an excessive logging state in the system can be caused by issuing a command to clear a large number of NAT subscribers where a large number of resources (port-blocks) are released at once.

The **suppress-lsn-sub-blks-free** command enables the generation of individual logs carried in event-id 2012 for every released port block regardless of the state of the transmission queue (whether congested or not). If NAT subscribers have a large number of allocated port blocks (this could be hundreds of port blocks per subscriber), generating individual logs per port-block release contributes to the congestion.

To alleviate transmission queue congestion, this behavior can be changed by disabling this command (**no suppress-lsn-sub-blks-free**). This causes the suppression of logs related to the release of individual port blocks of a NAT subscriber when the transmission queue is congested. As a result, only a summarized release log via event-id 2021 for the subscriber is generated. The purpose of this new log is to inform the operator in a single message that all ports blocks for the subscriber are released. For example, the log message for LSN is “LSN subscriber all blocks freed”. The benefit of such summarization (or log aggregation) is to alleviate the congestion of the transmission queue and consequently accelerate resource releases. An effect is the decreased granularity of information.

If summarization is enabled (**no suppress-lsn-sub-blks-free**) while there is no logging congestion in the system, the port block releases continue to be logged individually via the event-id 2012 (assuming that this is enabled in the event control), except for the last port block of the subscriber. When the last port block is released, the log with event-id 2021 is generated indicating that all port blocks for the subscriber are now released without carrying the specific information about this last port block that is released.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

suppress-lsn-sub-blks-free

Syntax [**no**] **suppress-lsn-sub-blks-free**

Context **[Tree]** (config>isa>nat-group suppress-lsn-sub-blks-free)

Full Context configure isa nat-group suppress-lsn-sub-blks-free

Description This command suppresses the tmnxNatLsnSubBlksFree summary notification and use the tmnxNatPlBlockAllocationLsn notifications. When the SR OS node is in a state of excessive logging, the queue associated with the transmission of logs on the MS-ISA can become congested. This event further delays the generation of logs, and with this, further allocations and deallocations of NAT resources (port-blocks) will be stalled until the queue is relieved of congestion. For example, an excessive logging state in the system can be caused by issuing a command to clear a large number of NAT subscribers where a large number of resources (port-blocks) are released at once.

The **suppress-lsn-sub-blks-free** command enables the generation of individual logs carried in event-id 2012 for every released port block regardless of the state of the transmission queue (whether congested or not). If NAT subscribers have a large number of allocated port blocks (this could be hundreds of port blocks per subscriber), generating individual logs per port-block release contributes to the congestion.

To alleviate transmission queue congestion, this behavior can be changed by disabling this command (**no suppress-lsn-sub-blks-free**). This causes the suppression of logs related to the release of individual port blocks of a NAT subscriber when the transmission queue is congested. As a result, only a summarized release log via event-id 2021 for the subscriber is generated. The purpose of this new log is to inform the operator in a single message that all ports blocks for the subscriber are released. For example, the log message for LSN will be “LSN subscriber all blocks freed”. The benefit of such summarization (or log aggregation) is to alleviate the congestion of the transmission queue and consequently accelerate resource releases. An effect is the decreased granularity of information.

If summarization is enabled (**no suppress-lsn-sub-blks-free**) while there is no logging congestion in the system, the port block releases continue to be logged individually via the event-id 2012 (assuming that this is enabled in the event control), except for the last port block of the subscriber. When the last port block is released, the log with event-id 2021 is generated indicating that all port blocks for the subscriber are now released without carrying the specific information about this last port block that is released.

Default no suppress-lsn-sub-blks-free

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.495 suppress-standby-signaling

suppress-standby-signaling

Syntax [**no**] **suppress-standby-signaling**

Context **[Tree]** (config>service>vpls>endpoint suppress-standby-signaling)

Full Context configure service vpls endpoint suppress-standby-signaling

Description When this command is enabled, the pseudowire standby bit (value 0x00000020) will not be sent to T-LDP peer when the specified spoke is selected as a standby. This allows faster switchover as the traffic will be sent over this SDP and discarded at the blocking side of the connection. This is particularly applicable to multicast traffic.

Default suppress-standby-signaling

Platforms All

23.496 suppress-threshold

suppress-threshold

Syntax **suppress-threshold** *suppress-penalties* **reuse-threshold** *reuse-penalties*

Context **[Tree]** (config>port>ethernet>dampening suppress-threshold)

Full Context configure port ethernet dampening suppress-threshold

Description This command configures the penalties thresholds at which the port state events to the upper layer are dampened (suppress threshold) and then permitted (reuse threshold).

Parameters *suppress-penalties* — Specifies the threshold at which the port up state is suppressed until the accumulated penalties drop below the reuse threshold again.

Values 1 to 20000

Default 2000

reuse-penalties — Specifies the threshold at which the port up state is no longer suppressed, after the port has been in a suppressed state and the accumulated penalties decay drops below this threshold. The reuse threshold value must be less than the suppress threshold value.

Values 1 to 20000

Default 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.497 svc-id

svc-id

Syntax **svc-id** *service-id*
no svc-id

Context **[Tree]** (config>system>security>mgmt-access-filter>mac-filter>entry>match svc-id)

Full Context configure system security management-access-filter mac-filter entry match svc-id

Description This command specifies an existing svc-id to use as a match condition.

Parameters *service-id* — Specifies a service-id to match.

Values *service-id*: 1 to 2147483647*svc-name*: 64 characters maximum

Platforms All

23.498 svc-path

svc-path

Syntax **svc-path** *path-id* **svc-index** *service-index*
no svc-path

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>vas-filter>entry>action>insert-nsh svc-path)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter entry action insert-nsh svc-path

Description This command configures the service path identifier and service index to be inserted in NSH in the steered traffic if the forward action indicates NSH insertion.

The **no** form of this command removes the parameters from the configuration.

Parameters *path-id* — Specifies the 24-bit path ID in the base part of NSH.

Values 0 to 16777215

service-index — Specifies the 8-bit service index inserted in the base part of NSH.

Values 0 to 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

23.499 svc-ping

svc-ping

Syntax **svc-ping** *ip-address* [**service** *service-id*] [**local-sdp**] [**remote-sdp**]

Context **[Tree]** (oam svc-ping)

Full Context oam svc-ping

Description This command tests a service ID for correct and consistent provisioning between two service end points.

The **svc-ping** command accepts a far-end IP address and a service ID for local and remote service testing. The following information can be determined from **svc-ping**:

Local and remote service existence

- Local and remote service state
- Local and remote service type correlation
- Local and remote customer association
- Local and remote service-to-SDP bindings and state
- Local and remote ingress and egress service label association

Unlike **sdp-ping**, only a single message is sent per command; no count nor interval parameter is supported and round trip time is not calculated. A time out value of 10 seconds is used before failing the request. The forwarding class is assumed to be Best-Effort Out-of-Profile.

If no request is sent or a reply is not received, all remote information is shown as N/A.

To terminate a **svc-ping** in progress, use the CLI break sequence <Ctrl-C>.

Upon request time out, message response, request termination, or request error the following local and remote information is displayed. See Table 181. Local and remote information is dependent upon service existence and reception of reply.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Request Result	The result of the **svc-ping** request message.	Sent - Request Timeout
		Sent - Request Terminated
		Sent - Reply Received
		Not Sent - Non-Existent Service-ID
		Not Sent - Non-Existent SDP for Service
		Not Sent - SDP For Service Down
		Not Sent - Non-existent Service Egress Label
Service-ID	The ID of the service being tested.	service-id
Local Service Type	The type of service being tested. If *service-id* does not exist locally, N/A is displayed.	Epipe, Ipipe, Fpipe, Apipe
		TLS
		IES
		Mirror-Dest
		—
Local Service Admin State	The local administrative state of *service-id*. If the service does not exist locally, the administrative state is Non-Existent.	Admin-Up
		Admin-Down
		Non-Existent
Local Service Oper State	The local operational state of *service-id*. If the service does not exist locally, the state is N/A.	Oper-Up
		Oper-Down
		—
Remote Service Type	The remote type of service being tested. If *service-id* does not exist remotely, N/A is displayed.	Epipe, Ipipe, Fpipe, Apipe
		TLS
		IES
		Mirror-Dest
		—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Remote Service Admin State	The remote administrative state of *service-id*. If the service does not exist remotely, the administrative state is Non-Existent.	Up
		Down
		Non-Existent
Local Service MTU	The local **service-mtu** for *service-id*. If the service does not exist, N/A is displayed.	*service-mtu*
		—
Remote Service MTU	The remote **service-mtu** for *service-id*. If the service does not exist remotely, N/A is displayed.	*remote-service-mtu*
		—
Local Customer ID	The local *customer-id* associated with *service-id*. If the service does not exist locally, N/A is displayed.	*customer-id*
		—
Remote Customer ID	The remote *customer-id* associated with *service-id*. If the service does not exist remotely, N/A is displayed.	*customer-id*
		—
Local Service IP Address	The local system IP address used to terminate remotely configured SDP-ID (as the **far-end** address). If an IP interface has not been configured to be the system IP address, N/A is displayed.	*system-ip-address*
		—
Local Service IP Interface Name	The name of the local system IP interface. If the local system IP interface has not been created, N/A is displayed.	*system-interface-name*
		—
Local Service IP Interface State	The state of the local system IP interface. If the local system IP interface has not been created, Non-Existent is displayed.	Up
		Down
		Non-Existent
Expected Far-end Address	The expected IP address for the remote system IP interface. This must be the **far-end** address entered for the **svc-ping** command.	*orig-sdp-far-end-addr*
		dest-ip-addr
		—
Actual Far-end Address	The returned remote IP address. If a response is not received, the displayed value is N/A. If the far-end service IP interface is down or non-existent, a message reply is not expected. **sdp-ping** should also fail.	*resp-ip-addr*
		—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Responders Expected Far-end Address	The expected source of the originator's *sdp-id* from the perspective of the remote router terminating the *sdp-id*. If the far-end cannot detect the expected source of the ingress *sdp-id* or the request is transmitted outside the *sdp-id*, N/A is displayed.	*resp-rec-tunnel-far-end-address*
		—
Originating SDP-ID	The *sdp-id* used to reach the **far-end** IP address if **sdp-path** is defined. The originating *sdp-id* must be bound to the *service-id* and terminate on the **far-end** IP address. If an appropriate originating *sdp-id* is not found, Non-Existent is displayed.	orig-sdp-id
		Non-Existent
Originating SDP-ID Path Used	Whether the Originating router used the originating *sdp-id* to send the **svc-ping** request. If a valid originating *sdp-id* is found, operational and has a valid egress service label, the originating router should use the *sdp-id* as the requesting path if **sdp-path** has been defined. If the originating router uses the originating *sdp-id* as the request path, Yes is displayed. If the originating router does not use the originating *sdp-id* as the request path, No is displayed. If the originating *sdp-id* is non-existent, N/A is displayed.	Yes
		No
		—
Originating SDP-ID Administrative State	The local administrative state of the originating *sdp-id*. If the *sdp-id* has been shutdown, Admin-Down is displayed. If the originating *sdp-id* is in the no shutdown state, Admin-Up is displayed. If an originating *sdp-id* is not found, N/A is displayed.	Admin-Up
		Admin-Up
		—
Originating SDP-ID Operating State	The local operational state of the originating *sdp-id*. If an originating *sdp-id* is not found, N/A is displayed.	Oper-Up
		Oper-Down
		—
Originating SDP-ID Binding Admin State	The local administrative state of the originating *sdp-id*s binding to *service-id*. If an *sdp-id* is not bound to the service, N/A is displayed.	Admin-Up
		Admin-Up
		—
Originating SDP-ID Binding Oper State	The local operational state of the originating *sdp-id*s binding to *service-id*. If an *sdp-id* is not bound to the service, N/A is displayed.	Oper-Up
		Oper-Down
		—

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Responding SDP-ID	The *sdp-id* used by the far end to respond to the **svc-ping** request. If the request was received without the **sdp-path** parameter, the responding router does not use an *sdp-id* as the return path, but the appropriate responding *sdp-id* is displayed. If a valid *sdp-id* return path is not found to the originating router that is bound to the *service-id*, Non-Existent is displayed.	*resp-sdp-id* Non-Existent
Responding SDP-ID Path Used	Whether the responding router used the responding *sdp-id* to respond to the **svc-ping** request. If the request was received via the originating *sdp-id* and a valid return *sdp-id* is found, operational and has a valid egress service label, the far-end router should use the *sdp-id* as the return *sdp-id*. If the far end uses the responding *sdp-id* as the return path, Yes is displayed. If the far end does not use the responding *sdp-id* as the return path, No is displayed. If the responding *sdp-id* is non-existent, N/A is displayed.	Yes No —
Responding SDP-ID Administrative State	The administrative state of the far-end *sdp-id* associated with the return path for *service-id*. When a return path is administratively down, Admin-Down is displayed. If the return *sdp-id* is administratively up, Admin-Up is displayed. If the responding *sdp-id* is non-existent, N/A is displayed.	Admin-Up Admin-Up N/A
Responding SDP-ID Operational State	The operational state of the far-end *sdp-id* associated with the return path for *service-id*. When a return path is operationally down, Oper-Down is displayed. If the return *sdp-id* is operationally up, Oper-Up is displayed. If the responding *sdp-id* is non-existent, N/A is displayed.	Oper-Up Oper-Down —
Responding SDP-ID Binding Admin State	The local administrative state of the responder's *sdp-id* binding to *service-id*. If an *sdp-id* is not bound to the service, N/A is displayed.	Admin-Up Admin-Down —
Responding SDP-ID Binding Oper State	The local operational state of the responder's *sdp-id* binding to *service-id*. If an *sdp-id* is not bound to the service, N/A is displayed.	Oper-Up Oper-Down —
Originating VC-ID	The originator's VC-ID associated with the *sdp-id* to the far-end address that is bound to *service-id*. If the *sdp-id* signaling is off, *originator-vc-id* is 0. If the *originator-vc-id* does not exist, N/A is displayed.	*originator-vc-id* —

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Responding VC-ID	The responder's VC-ID associated with the *sdp-id* to *originator-id* that is bound to *service-id*. If the *sdp-id* signaling is off or the service binding to *sdp-id* does not exist, *responder-vc-id* is 0. If a response is not received, N/A is displayed.	*responder-vc-id* —
Originating Egress Service Label	The originating service label (VC-Label) associated with the *service-id* for the originating *sdp-id*. If *service-id* does not exist locally, N/A is displayed. If *service-id* exists, but the egress service label has not been assigned, Non-Existent is displayed.	*egress-vc-label* — Non-Existent
Originating Egress Service Label Source	The originating egress service label source. If the displayed egress service label is manually defined, Manual is displayed. If the egress service label is dynamically signaled, Signaled is displayed. If the *service-id* does not exist or the egress service label is non-existent, N/A is displayed.	Manual Signaled —
Originating Egress Service Label State	The originating egress service label state. If the originating router considers the displayed egress service label operational, Up is displayed. If the originating router considers the egress service label inoperative, Down is displayed. If the *service-id* does not exist or the egress service label is non-existent, N/A is displayed.	Up Down —
Responding Service Label	The actual responding service label in use by the far-end router for this *service-id* to the originating router. If *service-id* does not exist in the remote router, N/A is displayed. If *service-id* does exist remotely but the remote egress service label has not been assigned, Non-Existent is displayed.	*rec-vc-label* — Non-Existent
Responding Egress Service Label Source	The responder's egress service label source. If the responder's egress service label is manually defined, Manual is displayed. If the responder's egress service label is dynamically signaled, Signaled is displayed. If the *service-id* does not exist on the responder or the responder's egress service label is non-existent, N/A is displayed.	Manual Signaled —

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Responding Service Label State	The responding egress service label state. If the responding router considers its egress service label operational, Up is displayed. If the responding router considers its egress service label inoperative, Down is displayed. If the *service-id* does not exist or the responder's egress service label is non-existent, N/A is displayed.	Up Down —
Expected Ingress Service Label	The locally assigned ingress service label. This is the service label that the far-end is expected to use for *service-id* when sending to the originating router. If *service-id* does not exist locally, N/A is displayed. If *service-id* exists but an ingress service label has not been assigned, Non-Existent is displayed.	*ingress-vc-label* — Non-Existent
Expected Ingress Label Source	The originator's ingress service label source. If the originator's ingress service label is manually defined, Manual is displayed. If the originator's ingress service label is dynamically signaled, Signaled is displayed. If the *service-id* does not exist on the originator or the originators ingress service label has not been assigned, N/A is displayed.	Manual Signaled —
Expected Ingress Service Label State	The originator's ingress service label state. If the originating router considers its ingress service label operational, Up is displayed. If the originating router considers its ingress service label inoperative, Down is displayed. If the *service-id* does not exist locally, N/A is displayed.	Up Down —
Responders Ingress Service Label	The assigned ingress service label on the remote router. This is the service label that the far end is expecting to receive for *service-id* when sending to the originating router. If *service-id* does not exist in the remote router, N/A is displayed. If *service-id* exists, but an ingress service label has not been assigned in the remote router, Non-Existent is displayed.	*resp-ingress-vc-label* — Non-Existent
Responders Ingress Label Source	The assigned ingress service label source on the remote router. If the ingress service label is manually defined on the remote router, Manual is displayed. If the ingress service label is dynamically signaled on the remote router, Signaled is displayed. If the *service-id* does not exist on the remote router, N/A is displayed.	Manual Signaled —

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 181 **Svc-ping**

Field	Description	Values
Responders Ingress Service Label State	The assigned ingress service label state on the remote router. If the remote router considers its ingress service label operational, Up is displayed. If the remote router considers its ingress service label inoperative, Down is displayed. If the *service-id* does not exist on the remote router or the ingress service label has not been assigned on the remote router, N/A is displayed.	Up
		Down
		—

Parameters *ip-address* — Specifies the far-end IP address to which to send the **svc-ping** request message in dotted decimal notation.

Values a.b.c.d

service-id — Specifies the service ID of the service being tested must be indicated with this parameter. The service ID need not exist on the local router to receive a reply message.

Values 1 to 2147483647, service-name: up to 64 characters

local-sdp — Specifies the **svc-ping** request message should be sent using the same service tunnel encapsulation labeling as service traffic. If **local-sdp** is specified, the command attempts to use an egress *sdp-id* bound to the service with the specified **far-end** IP address with the VC-Label for the service. The far-end address of the specified *sdp-id* is the expected *responder-id* within the reply received. The *sdp-id* defines the encapsulation of the SDP tunnel encapsulation used to reach the far end; this can be IP/GRE or MPLS. On originator egress, the service-ID must have an associated VC-Label to reach the far-end address of the *sdp-id* and the *sdp-id* must be operational for the message to be sent.

If **local-sdp** is not specified, the **svc-ping** request message is sent with GRE encapsulation with the OAM label.

Table 182 indicates whether a message is sent and how the message is encapsulated based on the state of the service ID.

Table 182 **Message Encapsulation**

Local Service State	local-sdp Not Specified		local-sdp Specified	
	Message Sent	Message Encapsulation	Message Sent	Message Encapsulation
Invalid Local Service	Yes	Generic IP/GRE OAM (PLP)	No	None
No Valid SDP-ID Bound	Yes	Generic IP/GRE OAM (PLP)	No	None

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 182 **Message Encapsulation**

Local Service State	local-sdp Not Specified		local-sdp Specified	
	Message Sent	Message Encapsulation	Message Sent	Message Encapsulation
SDP-ID Valid But Down	Yes	Generic IP/GRE OAM (PLP)	No	None
SDP-ID Valid and Up, But No Service Label	Yes	Generic IP/GRE OAM (PLP)	No	None
SDP-ID Valid, Up and Egress Service Label	Yes	Generic IP/GRE OAM (PLP)	Yes	SDP Encapsulation with Egress Service Label (SLP)

remote-sdp — Specifies **svc-ping** reply message from the **far-end** should be sent using the same service tunnel encapsulation labeling as service traffic.

If **remote-sdp** is specified, the **far-end** responder attempts to use an egress *sdp-id* bound to the service with the message originator as the destination IP address with the VC-Label for the service. The *sdp-id* defines the encapsulation of the SDP tunnel encapsulation used to reply to the originator; this can be IP/GRE or MPLS. On responder egress, the service-ID must have an associated VC-Label to reach the originator address of the *sdp-id* and the *sdp-id* must be operational for the message to be sent.

If **remote-sdp** is not specified, the **svc-ping** request message is sent with GRE encapsulation with the OAM label.

Table 183 indicates how the message response is encapsulated based on the state of the remote service ID.

Table 183 **Message Response Encapsulation**

Remote Service State	Message Encapsulation	
	remote-sdp Not Specified	remote-sdp Specified
Invalid Ingress Service Label	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
Invalid Service-ID	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
No Valid SDP-ID Bound on Service-ID	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid But Down	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid and Up, but No Service Label	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 183 **Message Response Encapsulation**

Remote Service State	Message Encapsulation	
	remote-sdp Not Specified	**remote-sdp Specified**
SDP-ID Valid and Up, Egress Service Label, but VC-ID Mismatch	Generic IP/GRE OAM (PLP)	Generic IP/GRE OAM (PLP)
SDP-ID Valid and Up, Egress Service Label, but VC-ID Match	Generic IP/GRE OAM (PLP)	SDP Encapsulation with Egress Service Label (SLP)

Output

Sample Output

```
*A:router1> svc-ping far-end 10.10.10.10 service 101 local-sdp remote-sdp
Request Result: Sent - Reply Received

Service-ID: 101

Err       Basic Info              Local     Remote
---       -----------------       ------    ------
__        Type:                   TLS       TLS
__        Admin State:            Up        Up
__        Oper State:             Up        Up
__        Service-MTU:            1514      1514
__        Customer ID:            1001      1001

Err       System IP Interface Info
---       ------------------------------------------------------------
Local Interface Name: "7750 SR-System-IP-Interface (Up to 32 chars)…"
__        Local IP Interface State:         Up
__        Local IP Address:                 10.10.10.11
__        IP Address Expected By Remote:    10.10.10.11
__        Expected Remote IP Address:       10.10.10.10
__        Actual Remote IP Address:         10.10.10.10

Err       SDP-ID Info             Local     Remote
---       -----------------       ------    ------
__        Path Used:              Yes       Yes
__        SDP-ID:                 123       325
__        Administrative State:   Up        Up
__        Operative State:        Up        Up
__        Binding Admin State:    Up        Up
__        Binding Oper State:     Up        Up
__        Binding VC-ID:          101       101

Err       Service Label Information   Label     Source        State
---       -------------------------   -----     -----------   -----
__        Local Egress Label:         45        Signaled      Up
__        Remote Expected Ingress:    45        Signaled      Up
__        Remote Egress:              34        Signaled      Up
__        Local Expected Ingress:     34        Signaled      Up
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.500 svlan-statistics

svlan-statistics

Syntax **svlan-statistics**

Context **[Tree]** (config>subscr-mgmt svlan-statistics)

Full Context configure subscriber-mgmt svlan-statistics

Description Commands in this context enable subscriber VLAN statistics collection.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.501 swap

swap

Syntax **swap** {*out-label* | **implicit-null-label**} **nexthop** *ip-address*
no swap

Context **[Tree]** (config>router>mpls>if>label-map swap)

Full Context configure router mpls interface label-map swap

Description This command swaps the incoming label and specifies the outgoing label and next hop IP address on an LSR for a static LSP.

The **no** form of this command removes the swap action associated with the *in-label*.

Parameters *implicit-null-label* — Specifies the use of the implicit label value for the outgoing label of the swap operation.

out-label — Specifies the label value to be swapped with the in-label. Label values 16 through 1,048,575 are defined as follows:

- label values 16 through 31 are reserved
- label values 32 through 1,023 are available for static assignment
- label values 1,024 through 2,047 are reserved for future use
- label values 2,048 through 18,431 are statically assigned for services

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- label values 28,672 through 131,071 are dynamically assigned for both MPLS and services
- label values 131,072 through 1,048,575 are reserved for future use

Values 16 to 1048575

nexthop *ip-address* — Specifies the IP address to forward to. If an ARP entry for the next hop exists, then the static LSP will be marked operational. If ARP entry does not exist, software will set the operational status of the static LSP to down and continue to ARP for the configured nexthop. Software will continuously try to ARP for the configured nexthop at a fixed interval.

Platforms All

23.502 sweep

sweep

Syntax **sweep start** *dispersion-start* **end** *dispersion-end*

Context **[Tree]** (config>port>dwdm>coherent sweep)

Full Context configure port dwdm coherent sweep

Description This command allows users to configure the dispersion sweep ‘start’ and ‘end’ values for the automatic mode of coherent control. If the user knows the approximate or theoretical residual dispersion of the link, this command can be used to limit the range of sweeping for the automatic control mode and thus achieve faster link up.

Parameters *dispersion-start* — Specifies the lower range limit for the dispersion compensation.

Values -50000 to 50000

Default -25500

dispersion-end — Specifies the upper range limit for the dispersion compensation.

Values -50000 to 50000

Default 2000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.503 switch-defined-cookie

switch-defined-cookie

Syntax [**no**] **switch-defined-cookie**

Context **[Tree]** (config>open-flow>of-switch>flowtable switch-defined-cookie)

Full Context configure open-flow of-switch flowtable switch-defined-cookie

Description This command enables OpenFlow switch-defined Flow Table cookie encoding for flowtable 0 that allows multi-service operation.

The **no** form of the command disables the above function.

Default no switch-defined-cookie

Platforms All

23.504 switch-fabric

switch-fabric

Syntax **switch-fabric**

Context **[Tree]** (config>system switch-fabric)

Full Context configure system switch-fabric

Description Commands in this context configure switch fabric parameters.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7, 7750 SR-7s, 7950 XRS

23.505 switching-mode

switching-mode

Syntax **switching-mode** {**bi-directional** | **uni-directional**}

Context **[Tree]** (config>port>aps switching-mode)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port aps switching-mode

Description This command configures the switching mode for the APS group.

Parameters **bi-directional** — Configures the group to operate in Bidirectional 1+1 Signaling APS mode.

uni-directional — Configures the group to operate in Unidirectional 1+1 Signaling APS mode.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

23.506 switching-type

switching-type

Syntax **switching-type** *switching-type*
no switching-type

Context **[Tree]** (config>router>gmpls>lsp switching-type)

Full Context configure router gmpls lsp switching-type

Description This command configures the type of switching required for the gLSP. As defined in RFC 3471. The default CLI value is **dcsc**, which indicates that Digital Channel Switch Capable (DCSC) should be signaled.

Default switching-type dcsc

Parameters *switching-type* — Specifies the required type of switching.

Values dcsc

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.507 switchover-exec

switchover-exec

Syntax **switchover-exec** *file-url*
no switchover-exec

Context **[Tree]** (config>system switchover-exec)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system switchover-exec

Description This command specifies the location and name of the CLI script file executed following a redundancy switchover from the previously active CPM card. A switchover can happen because of a fatal failure or by manual action.

The CLI script file can contain commands for environment settings, debug (excluding mirroring settings), and other commands not maintained by the configuration redundancy.

The following commands are not supported in the switchover-exec file: clear, configure, candidate, oam, tools, oam, ping, traceroute, mstat, mtrace and mrinfo.

When the *file-url* parameter is not specified, no CLI script file is executed.

Default no switch-over-exec

Parameters *file-url* — Specifies the location and name of the CLI script file.

Values

local-url | *remote-url*	
local-url	[*cflash-id*/][*file-path*] 200 chars max, including cflash-id directory length 99 chars max each
remote-url	[{ftp:// | tftp://}*login:pswd@remote-locn*/][*file-path*] 243 chars max directory length 99 chars max each
remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - 32 chars max, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

23.508 symbol-monitor

symbol-monitor

Syntax **symbol-monitor**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>ethernet symbol-monitor)

Full Context configure port ethernet symbol-monitor

Description This command configures Ethernet Symbol Monitoring parameters. Support for symbol monitoring is hardware dependent. An error message indicating that the port setting cannot be modified will be presented when attempting to enable the feature or configure the individual parameters on unsupported hardware.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.509 sync

sync

Syntax [**no**] **sync**

Context [Tree] (config>redundancy>multi-chassis>peer sync)

Full Context configure redundancy multi-chassis peer sync

Description Commands in this context configure synchronization parameters.

Default no sync

Platforms All

23.510 sync-boot-env

sync-boot-env

Syntax **sync-boot-env**

Context [Tree] (admin>satellite>eth-sat sync-boot-env)

Full Context admin satellite eth-sat sync-boot-env

Description The command forces the specified Ethernet-satellite chassis to synchronize the boot image.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.511 sync-e

sync-e

Syntax [**no**] **sync-e**

Context **[Tree]** (config>card>mda sync-e)
[Tree] (config>card>xiom>mda sync-e)

Full Context configure card mda sync-e
configure card xiom mda sync-e

Description This command enables synchronous Ethernet on the MDA. Then any port on the MDA can be used as a source port in the sync-if-timing configuration.

The **no** form of this command disables synchronous Ethernet on the MDA.

Platforms 7750 SR-s

- configure card xiom mda sync-e

All

- configure card mda sync-e

sync-e

Syntax [**no**] **sync-e**

Context **[Tree]** (config>system>satellite>eth-sat sync-e)

Full Context configure system satellite eth-sat sync-e

Description This command enables the Ethernet satellite for synchronous Ethernet operation so that the transmit timing of the satellite access ports use the frequency of the host router's central clock.

To enable this functionality, both host ports on the router that connect to the U1 and U2 ports of the satellite must be synchronous Ethernet-capable ports.

When the Ethernet satellite is configured for synchronous Ethernet, ESMC frames are enabled on the host ports. The SSM code-type used between the host and the satellite should be manually configured on the host ports to match the code-type desired on the satellite client ports. The code-type setting on the host ports does not restrict the code-type used on the satellite client ports, as those may be configured on an individual port basis.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.512 sync-if-timing

sync-if-timing

Syntax **sync-if-timing**

Context **[Tree]** (config>system sync-if-timing)

Full Context configure system sync-if-timing

Description This command creates or edits the context to create or modify timing reference parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

sync-if-timing

Syntax **sync-if-timing**

Context **[Tree]** (debug sync-if-timing)

Full Context debug sync-if-timing

Description The context to debug synchronous interface timing references.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

23.513 synce

synce

Syntax **synce**

Context **[Tree]** (config>system>sync-if-timing synce)

Full Context configure system sync-if-timing synce

Description Commands in this context configure attributes related to the CPM/CCM SyncE/1588 ports.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.514 synchronize

synchronize

Syntax **synchronize** {**boot-env** | **config**}

Context **[Tree]** (config>redundancy synchronize)

Full Context configure redundancy synchronize

Description This command performs a synchronization of the standby CPMs images and/or config files to the active CPM. Either the **boot-env** or **config** parameter must be specified. In the **config>redundancy** context, this command performs an automatically triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPMs have identical operational parameters. This includes the saved configuration, CPM, XCM, and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM.

If synchronization fails, alarms and log messages that indicate the type of error that caused the failure of the synchronization operation are generated. When the error condition ceases to exist, the alarm is cleared.

Only files stored on the router are synchronized. If a configuration file or image is stored in a location other than on a local compact flash, the file is not synchronized (for example, storing a configuration file on an FTP server).

Default no synchronize

Parameters **boot-env** — Synchronizes all files required for the boot process (loader, BOF, images, and config).

config — Synchronizes only the primary, secondary, and tertiary configuration files.

Default config

Platforms All

synchronize

Syntax **synchronize cert**
synchronize {**boot-env** | **config**}

Context **[Tree]** (admin>redundancy synchronize)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context admin redundancy synchronize

Description This command performs a synchronization of the standby CPM's images and/or configuration files to the active CPM. Either the **boot-env** or **config** parameter must be specified.

In the **admin>redundancy** context, this command performs a manually triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPM have identical operational parameters. This includes the saved configuration, CPM, XCM, and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM. If synchronization fails, alarms and log messages that indicate the type of error that caused the failure of the synchronization operation are generated. When the error condition ceases to exist, the alarm is cleared.

Only files stored on the router are synchronized. If a configuration file or image is stored in a location other than on a local compact flash, the file is not synchronized (for example, storing a configuration file on an FTP server).

The **no** form of the command removes the parameter from the configuration.

Default no synchronize

Parameters **cert** — Synchronizes the imported certificate/key/CRL files to the standby CPM.

boot-env — Synchronizes all files required for the boot process (loader, BOF, images, and config).

config — Synchronizes only the primary, secondary, and tertiary configuration files.

Platforms All

23.515 synchronous-execution

synchronous-execution

Syntax **synchronous-execution** *seconds*
synchronous-execution never

Context **[Tree]** (config>system>management-interface>ops>global-timeouts synchronous-execution)

Full Context configure system management-interface operations global-timeouts synchronous-execution

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the period of time that operations launched as "'synchronous" (the default method for all operations) are allowed to execute before they are automatically stopped, and their associated data is deleted.

If a specific execution timeout is not included in the request for a particular synchronous operation, this system-level timeout applies.

Note: This execution timeout is part of the general global operations infrastructure and is separate and independent from any operation-specific timeouts (for example, the **ping** operation also has its own **timeout** parameter).

Caution: This timeout also applies to operations requested in the MD-CLI interface (for example, ping, file dir, and so on). If **synchronous-execution** is enabled with a specific time value, MD-CLI operations are subject to this timeout and are interrupted if they execute longer than the configured **synchronous-execution** time.

Default synchronous-execution never

Parameters *seconds* — Specifies the period of time, in seconds, that synchronous operations are allowed to execute.

Values 1 to 604800

never — Keyword to specify that an execution timeout is not applied to synchronous operations.

Platforms All

23.516 syslog

syslog

Syntax **syslog script** *name*
no syslog

Context **[Tree]** (config>python>py-policy syslog)

Full Context configure python python-policy syslog

Description This command enables Python script to process syslog related messages and events.

The **no** form of this command disables the Python script to process syslog related messages and events.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

syslog

Syntax **syslog** *syslog-id* [**name** *syslog-name*]
no syslog *syslog-id*

Context **[Tree]** (config>service>vprn>log syslog)

Full Context configure service vprn log syslog

Description This command creates the context to configure a Syslog target host that is capable of receiving selected Syslog messages from this network element.

A valid *syslog-id* must have the target Syslog host address configured.

A maximum of 30 Syslog IDs can be configured.

No log events are sent to a Syslog target address until the syslog-id has been configured as the log destination (**to**) in the log-id node.

The Syslog ID configured in the **configure**>**service**>**vprn** context has a local VPRN scope and only needs to be unique within the specific VPRN instance. The same ID can be reused under a different VPRN service or in the global log context under **config>log**.

Default No syslog IDs are defined.

Parameters *syslog-id* — Specifies the Syslog ID for the Syslog destination.

Values 1 to 30

name *syslog-name* — Specifies an optional Syslog name, up to 64 characters, that can be used to refer to the Syslog destination after it is created.

Platforms All

syslog

Syntax **syslog**

Context **[Tree]** (config>app-assure>group>evt-log syslog)

Full Context configure application-assurance group event-log syslog

Description Commands in this context configure the target syslog server.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

syslog

Syntax **syslog**

Context **[Tree]** (config>service>nat syslog)

Full Context configure service nat syslog

Description Commands in this context configure syslog reporting of NAT flow parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

syslog

Syntax **syslog** *syslog-id* [**name** *syslog-name*]
no syslog *syslog-id*

Context **[Tree]** (config>log syslog)

Full Context configure log syslog

Description Commands in this context configure a Syslog target host capable of receiving selected syslog messages from this network element.

A valid *syslog-id* must have the target Syslog host address configured.

A maximum of 10 Syslog IDs can be configured.

Log events are not sent to a Syslog target address until the *syslog-id* is configured as the log destination (**to**) in the node specified by the Log ID.

The Syslog ID configured in the **config**>**service**>**vprn** context has a local VPRN scope and only needs to be unique within the specific VPRN instance. The same ID can be reused under a different VPRN service or in the global log context under **config**>**log**.

The **no** form of this command removes the Syslog configuration.

Parameters *syslog-id* — Specifies the Syslog ID for the Syslog destination.

Values 1 to 10

name *syslog-name* — Configures an optional Syslog name, up to 64 characters, that can be used to refer to the Syslog destination after it is created.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.517 syslog-export-policy

syslog-export-policy

Syntax **syslog-export-policy** *policy-name*
no syslog-export-policy

Context **[Tree]** (config>service>nat>nat-policy syslog-export-policy)

Full Context configure service nat nat-policy syslog-export-policy

Description This command creates a syslog export policy with a set of transport parameters that will be used to transmit NAT flow records in syslog format to an external collector node. This policy name is then referenced from the nat-policy applied to an inside routing context.

Default no syslog-export-policy

Parameters *policy-name* — Specifies the name of the syslog export policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

syslog-export-policy

Syntax **syslog-export-policy** *name* [**create**]
no syslog-export-policy *name*

Context **[Tree]** (config>service>nat>syslog syslog-export-policy)

Full Context configure service nat syslog syslog-export-policy

Description This command creates a syslog export policy with a set of transport parameters that are used to transmit NAT flow records in syslog format to an external collector node. This policy name is then referenced from the NAT policy applied to an inside routing context.

The **no** form of the command removes the policy name from the configuration.

Parameters *name* — Specifies the syslog export policy name, up to 32 characters.

create — Keyword used to create the syslog export policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

23.518 system

system

Syntax **system**

Context **[Tree]** (admin>system system)

Full Context admin system system

Description Commands in this context configure system operations.

system

Syntax **system**

Context **[Tree]** (config>eth-cfm system)

Full Context configure eth-cfm system

Description Commands in this context configure Connectivity Fault Management General System parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

system

Syntax [**no**] **system**

Context **[Tree]** (debug system)

Full Context debug system

Description This command displays system debug information.

Platforms All

23.519 system-base-mac

system-base-mac

Syntax **system-base-mac** *mac-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no system-base-mac

Context [Tree] (bof system-base-mac)

Full Context bof system-base-mac

Description This command is used to specify the base MAC address for a VSR-based system. The specified MAC address is used as the first MAC address by the system to assign MAC addresses to individual interfaces.

It is strongly recommended that a unique base MAC address is assigned to each VSR instance with a minimum gap of 1024 between base addresses to avoid a MAC address overlap.

The **no** form of this command removes the configured system base MAC address.

Default no system-base-mac

Parameters *mac-address* — Specifies the MAC address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS-20, 7950 XRS-20e, VSR

23.520 system-behavior

system-behavior

Syntax **system-behavior**

Context [Tree] (config>subscr-mgmt system-behavior)

Full Context configure subscriber-mgmt system-behavior

Description Commands in this context configure system-wide subscriber management behavior parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

23.521 system-filter

system-filter

Syntax **system-filter**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter system-filter)

Full Context configure filter system-filter

Description Commands in this context activate system filter policies.

Platforms All

23.522 system-id

system-id

Syntax **system-id** *system-id*
no system-id

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host>host-ident system-id)

Full Context configure subscriber-mgmt local-user-db ipoe host host-identification system-id

Description This command specifies the system ID to match for a host lookup. When the LUDB is accessed through a DHCPv4 server, the system ID is matched against the Nokia vendor specific sub-option in DHCP Option 82.

Note: This command is only used when **system-id** is configured as one of the **match-list** parameters.

The **no** form of this command removes the system ID from the configuration.

Parameters *system-id* — Specifies the system ID, up to 255 characters

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

system-id

Syntax [**no**] **system-id**

Context [Tree] (config>service>vpls>sap>dhcp>option>vendor system-id)
[Tree] (config>service>vprn>if>dhcp>option>vendor system-id)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option>vendor system-id)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option>vendor system-id)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only>dhcp>option>vendor system-id)

Full Context configure service ies subscriber-interface group-interface dhcp option vendor-specific-option system-id

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls sap dhcp option vendor-specific-option system-id
configure service vprn interface dhcp option vendor-specific-option system-id
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option system-id
configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option system-id

Description This command specifies whether the system-id is encoded in the Nokia vendor-specific sub-option of Option 82.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option system-id
- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option system-id
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option system-id

All

- configure service vpls sap dhcp option vendor-specific-option system-id
- configure service vprn interface dhcp option vendor-specific-option system-id

system-id

Syntax **system-id** *name*
no system-id

Context **[Tree]** (config>system>vsd system-id)

Full Context configure system vsd system-id

Description This command configures the DC GW system-id that is used for the configuration from VSD. VSD will identify the DC GW based on this identifier, hence it must be unique per VSD.

Parameters *name* — Specifies the name of the DC GW.

Platforms All

system-id

Syntax **system-id** *isis-system-id*
no system-id

Context **[Tree]** (config>service>vprn>isis system-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn isis system-id

Description This command configures the IS-IS system ID. The system ID has a fixed length of 6 octets; it is determined using the following preference order:

1. **config>service>vprn>isis>system-id**
2. **config>service>vprn>isis>router-id**
3. **config>service>vprn>router-id**
4. **config>service>vprn>if>address**
5. The default system ID 2550.0000.0000, based on the default router ID 255.0.0.0

The system ID is integral to IS-IS; therefore, for the **system-id** command to take effect, a **shutdown** and then **no shutdown** must be performed on the IS-IS instance. This will ensure that the configured and operational system ID are always the same.

The **no** form of this command removes the system ID from the configuration. The router ID is used when no system ID is specified.

Default no system-id

Parameters *isis-system-id* — 12 hexadecimal characters in dotted-quad notation.

Values aaaa.bbbb.cccc, where aaaa, bbbb, and cccc are hexadecimal numbers

Platforms All

system-id

Syntax [**no**] **system-id**

Context **[Tree]** (config>router>if>dhcp>option>vendor-specific-option system-id)

Full Context configure router interface dhcp option vendor-specific-option system-id

Description This command specifies whether the system-id is encoded in the Nokia vendor-specific sub-option of Option 82.

Default no system-id

Platforms All

system-id

Syntax **system-id** *isis-system-id*
no system-id

Context **[Tree]** (config>router>isis system-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router isis system-id

Description This command configures the IS-IS system ID. The system ID has a fixed length of 6 octets; it is determined using the following preference:

1. **config>router>isis>system-id**
2. **config>router>isis>router-id**
3. **config>router>router-id**
4. **config>router>interface>system>address**
5. The default system ID 2550.0000.0000, based on the default router ID 255.0.0.0

The system ID is integral to IS-IS; therefore, for the **system-id** command to take effect, the IS-IS instance must be **shutdown** and then **no shutdown**. This will ensure that the configured and operational system ID are always the same.

The **no** form of this command removes the system ID from the configuration. The router ID is used when no system ID is specified.

Parameters *isis-system-id* — Specifies 12 hexadecimal characters in dotted-quad notation.

Values aaaa.bbbb.cccc, where aaaa, bbbb, and cccc are hexadecimal numbers

Platforms All

23.523 system-ip-load-balancing

system-ip-load-balancing

Syntax [**no**] **system-ip-load-balancing**

Context **[Tree]** (config>system>load-balancing system-ip-load-balancing)

Full Context configure system load-balancing system-ip-load-balancing

Description This command enables the use of the system IP address in the ECMP hash algorithm to add a per system variable. This can help guard against cases where multiple routers, in series, will end up hashing traffic to the same ECMP/LAG path.

This command is set at a system wide basis, however if certain IOMs do not support the new load-balancing algorithm, they will continue to use the default algorithm. By default, the IPv4 system IP address is used in the hash algorithm. When no IPv4 system IP address is configured, the IPv6 system IP address, when configured, is used in the hash algorithm.

The **no** form of the command resets the system wide algorithm to default.

Default no system-ip-load-balancing

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

23.524 system-mac

system-mac

Syntax **system-mac** *mac-address*
no system-mac

Context **[Tree]** (config>system>ned>profile system-mac)

Full Context configure system network-element-discovery profile system-mac

Description This command configures the MAC address to be advertised.

The **no** form of this command removes any explicitly defined MAC address and chassis MAC address will be advertised.

Default no system-mac

Parameters *mac-address* — Specifies the MAC address to be associated with the profile in *xx:xx:xx:xx:xx:xx* or *xx-xx-xx-xx-xx-xx* format.

Platforms All

23.525 system-priority

system-priority

Syntax **system-priority** *value*
no system-priority

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ep system-priority)

Full Context configure redundancy multi-chassis peer mc-endpoint system-priority

Description This command allows the operator to set the system priority. The peer configured with the lowest value is chosen to be the master. If system-priority are equal then the one with the highest system-id (chassis MAC address) is chosen as the master.

The **no** form of this command sets the system priority to default.

Default no system-priority

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the priority assigned to the local MC-EP peer.

Values 1 to 255

Platforms All

23.526 system-profile

system-profile

Syntax **system-profile** {**profile-a** | **profile-b**}
no system-profile

Context **[Tree]** (bof system-profile)

Full Context bof system-profile

Description This command configures the system profile in the BOF.

System profile none represents the existing system capabilities and allows FP3- and FP4-based hardware to co-exist within a system. This is indicated by the omission of the **system-profile** parameter in the BOF, except on 7750 SR-1 systems.

System profile **profile-a** is primarily targeted at subscriber services and layer 2 and 3 VPN business services.

System profile **profile-b** is primarily targeted at infrastructure routing, core, peering, and DC-GW applications.

System profile **profile-a** and **profile-b** are supported on 7950 XRS-20/20e, 7750 SR-1 and 7750 SR-12e systems, and support only FP4-based line cards.

The system profile on 7750 SR-1 systems should be set to **profile-a**. It is set by default to **profile-a** when the **system-profile** parameter is omitted from the BOF, or configured to an invalid value.

On 7950 XRS-20/20e and 7750 SR-12e systems, default system profile is none.

On all other systems, the **system-profile** parameter must not be configured in the BOF which sets the system profile to none.

The **no** form of this command removes the **system-profile** parameter from the BOF.

Default none

Parameters **profile-a** — Specifies that the system profile is for subscriber services and Layer 2 and 3 VPN business services.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

profile-b — Specifies that the system profile is primarily targeted at infrastructure routing, core, peering, and DC-GW applications.

Platforms All

23.527 system-reserve

system-reserve

Syntax **system-reserve** *percent-of-buffers*
no system-reserve

Context **[Tree]** (config>qos>hs-pool-policy system-reserve)

Full Context configure qos hs-pool-policy system-reserve

Description This command defines the amount of HSQ IOM buffers that is set aside for internal system use. By default, 5% of the total buffer space is reserved for system internal queues. The command is provided for the case where the reserved buffer space is either insufficient or excessive. Exercise care when modifying this value.

When the system reserve value is changed, all the provisioned port-class, mid-tier, and root pool sizes are reevaluated and possibly changed.

Use the **show hs-pools** *card-slot-number* **fp** *forwarding-plane* **egress** command to display the current buffer allocation and buffer usage conditions on an HSQ IOM.

The **no** form of the command reverts to the default system reserve value.

Default system-reserve 5.0

Parameters *percent-of-buffers* — Specifies the percentage of HS buffers that are reserved for internal system use. This parameter is required when executing the **system-reserve** command. The parameter accepts a percent value with two decimal places (100th of a percent).

Values 1.00 to 30.00

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24 t Commands

24.1 t2-paths

t2-paths

Syntax **t2-paths**

Context **[Tree]** (config>mcast-mgmt>bw-plcy t2-paths)

Full Context configure mcast-management bandwidth-policy t2-paths

Description Commands in this context configure T2 path queuing parameters for primary and secondary paths.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

24.2 t391

t391

Syntax **t391** [*value*]
no t391

Context **[Tree]** (config>port>ethernet>elmi t391)

Full Context configure port ethernet elmi t391

Description This command configures the polling timer for UNI-C.

Parameters *value* — Specifies the polling timer for UNI-C.

Values 5 to 30

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.3 t391dte

t391dte

Syntax **t391dte** *keepalive*
no t391dte

Context **[Tree]** (config>port>ml-bundle>mlfr>frame-relay t391dte)

Full Context configure port multilink-bundle mlfr frame-relay t391dte

Description This command configures the DTE keepalive timer value for the LMI.

Parameters *keepalive* — Specifies the interval in seconds between status inquiries issued by the DTE.

Values 5 to 30

Platforms 7450 ESS, 7750 SR-7/12/12e

t391dte

Syntax **t391dte** *keepalive*
no t391dte

Context **[Tree]** (config>port>sonet-sdh>path>frame-relay t391dte)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay t391dte)
[Tree] (config>port>tdm>ds3>frame-relay t391dte)
[Tree] (config>port>tdm>e1>channel-group>frame-relay t391dte)
[Tree] (config>port>tdm>e3>frame-relay t391dte)

Full Context configure port sonet-sdh path frame-relay t391dte
configure port tdm ds1 channel-group frame-relay t391dte
configure port tdm ds3 frame-relay t391dte
configure port tdm e1 channel-group frame-relay t391dte
configure port tdm e3 frame-relay t391dte

Description This command sets the DTE keepalive timer for the Frame Relay Local Management Interface (LMI).

This number specifies the period at which the DTE sends out a keepalive response request to the DCE and updates status depending on the DTE error threshold value.

The **no** form of this command returns the **t391dte** keepalive timer to the default value.

Default t391dte 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *keepalive* — Specifies the interval in seconds between status inquiries issued by the DTE.

Values 5 to 30

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay t391dte

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 frame-relay t391dte
- configure port tdm e1 channel-group frame-relay t391dte
- configure port tdm e3 frame-relay t391dte
- configure port tdm ds1 channel-group frame-relay t391dte

24.4 t392

t392

Syntax **t392** [*value*]
no t392

Context **[Tree]** (config>port>ethernet>elmi t392)

Full Context configure port ethernet elmi t392

Description This command configures the polling verification timer for UNI-N.

Parameters *value* — Specifies the polling verification timer for UNI-N.

Values 5 to 30

Platforms All

24.5 t392dce

t392dce

Syntax **t392dce** *keepalive*
no t392dce

Context **[Tree]** (config>port>ml-bundle>mlfr>frame-relay t392dce)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port multilink-bundle mlfr frame-relay t392dce

Description This command configures the DCE keepalive timer value for the LMI.

Parameters *keepalive* — Specifies the expected interval in seconds between status inquiries issued by the DTE equipment.

Values 5 to 30

Platforms 7450 ESS, 7750 SR-7/12/12e

t392dce

Syntax **t392dce** *keepalive*
no t392dce

Context **[Tree]** (config>port>sonet-sdh>path>frame-relay t392dce)
[Tree] (config>port>tdm>ds1>channel-group>frame-relay t392dce)
[Tree] (config>port>tdm>ds3>frame-relay t392dce)
[Tree] (config>port>tdm>e1>channel-group>frame-relay t392dce)
[Tree] (config>port>tdm>e3>frame-relay t392dce)

Full Context configure port sonet-sdh path frame-relay t392dce
configure port tdm ds1 channel-group frame-relay t392dce
configure port tdm ds3 frame-relay t392dce
configure port tdm e1 channel-group frame-relay t392dce
configure port tdm e3 frame-relay t392dce

Description This command sets the DCE keepalive timer for the Frame Relay Local Management Interface (LMI).

This number specifies the period at which the DCE checks for keepalive responses from the DTE and updates status depending on the DCE error threshold value.

The **no** form of this command returns the **t392dce** keepalive timer to the default value.

Default t392dce 15

Parameters *keepalive* — Specifies the expected interval in seconds between status inquiries issued by the DTE equipment.

Values 5 to 30

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path frame-relay t392dce

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm e1 channel-group frame-relay t392dce
- configure port tdm ds1 channel-group frame-relay t392dce

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure port tdm e3 frame-relay t392dce
- configure port tdm ds3 frame-relay t392dce

24.6 tab

tab

Syntax [**no**] **tab**

Context **[Tree]**
(config>system>management-interface>cli>md-cli>environment>command-completion tab)

Full Context configure system management-interface cli md-cli environment command-completion tab

Description This command enables completion on the tab character.

The **no** form of this command reverts to the default value.

Default tab

Platforms All

24.7 table-size

table-size

Syntax **table-size** *table-size*

Context **[Tree]** (config>service>vpls>proxy-arp table-size)
[Tree] (config>service>vpls>proxy-nd table-size)

Full Context configure service vpls proxy-arp table-size
configure service vpls proxy-nd table-size

Description This command adds a table-size limit per service. By default, the table-size limit is 250; it can be set up to 16k entries per service. A non-configurable implicit high watermark of 95% and low watermark of 90% exists, per service and per system. When those watermarks are reached, a syslog/trap is triggered. When the system/service limit is reached, entries for a specified IP can be replaced (a different MAC can be learned and added) but no new IP entries will be added, regardless of the type (Static, evpn, dynamic). If the user attempts to change the **table-size** value to a value that cannot accommodate the number of existing entries, the attempt will fail.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default table-size 250

Parameters *table-size* — Specifies the table-size as number of entries for the service.

Values 1 to 16384

Platforms All

24.8 tacplus

tacplus

Syntax **no tacplus**
tacplus create

Context **[Tree]** (config>service>vprn>aaa>remote-servers tacplus)

Full Context configure service vprn aaa remote-servers tacplus

Description This command creates the context to configure TACACS+ authentication on the VPRN.

Configure multiple server addresses for each router for redundancy.

The **no** form of this command removes the TACACS+ configuration.

Platforms All

tacplus

Syntax [**no**] **tacplus**

Context **[Tree]** (config>system>security tacplus)

Full Context configure system security tacplus

Description This command creates the context to configure TACACS+ authentication on the router.

Configure multiple server addresses for each router for redundancy.

The **no** form of this command removes the TACACS+ configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.9 tacplus-map-to-priv-lvl

tacplus-map-to-priv-lvl

Syntax **tacplus-map-to-priv-lvl** [*admin-priv-lvl*]
no tacplus-map-to-priv-lvl

Context **[Tree]** (config>system>security>password>enable-admin-control tacplus-map-to-priv-lvl)

Full Context configure system security password enable-admin-control tacplus-map-to-priv-lvl

Description When **tacplus-map-to-priv-lvl** is enabled, and tacplus authorization is enabled with the *use-priv-lvl* option, typing **enable-admin** starts an interactive authentication exchange from the node to the TACACS+ server. The start message (service=enable) contains the user-id and the requested *admin-priv-lvl*. Successful authentication results in the use of a new profile (as configured under **config>system>security>tacplus>priv-lvl-map**).

Platforms All

24.10 tag

tag

Syntax **tag** *tag*
no tag [*tag*]

Context **[Tree]** (config>service>vprn>static-route-entry tag)

Full Context configure service vprn static-route-entry tag

Description This command associates a 4-byte route-tag with the static route. The tag value can be used in route policies to control distribution of the static route into other protocols.

The tag specified at this level of the static route causes tag values configured under the next-hop, black-hole, and indirect contexts of the static route to be ignored.

The **no** form of this command removes the tag association.

Default no tag

Parameters *tag* — Specifies an integer value.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tag

Syntax **tag** *tag-value*
no tag [*tag-value*]

Context **[Tree]** (config>service>vprn>static-route-entry>indirect tag)
[Tree] (config>service>vprn>static-route-entry>ipsec-tunnel tag)
[Tree] (config>service>vprn>static-route-entry>next-hop tag)

Full Context configure service vprn static-route-entry indirect tag
configure service vprn static-route-entry ipsec-tunnel tag
configure service vprn static-route-entry next-hop tag

Description This command adds a 32-bit integer tag to the associated static route.

The tag value can be used in route policies to control distribution of the route into other protocols.

Default no tag

Parameters *tag-value* — Specifies an integer tag value.

Values 32 bit integer

Platforms All

tag

Syntax **tag** *tag*
no tag

Context **[Tree]** (config>service>vprn>isis>if tag)

Full Context configure service vprn isis interface tag

Description This command configures a route tag to the specified IP address of an interface.

Parameters *tag* — Specifies the tag value.

Values 1 to 4294967295

Platforms All

tag

Syntax **tag** *tag*
no tag [*tag*]

Context **[Tree]** (config>router>static-route-entry tag)
[Tree] (config>router>static-route-entry>black-hole tag)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>static-route-entry>indirect tag)
[Tree] (config>router>static-route-entry>next-hop tag)

Full Context configure router static-route-entry black-hole tag
configure router static-route-entry indirect tag
configure router static-route-entry next-hop tag
configure router static-route-entry tag

Description This command associates a 4-byte route-tag with the static route. The tag value can be used in route policies to control distribution of the static route into other protocols.

The tag specified at this level of the static route causes tag values configured under the next-hop, black-hole and indirect contexts of the static route to be ignored.

The **no** form of this command removes the tag association.

Default no tag

Parameters *tag* — Specifies an integer tag value.

Values 1 to 4294967295

Platforms All

tag

Syntax **tag** *tag*
no tag

Context [Tree] (config>router>isis>interface tag)

Full Context configure router isis interface tag

Description This command configures a route tag to the specified IP address of an interface.

The **no** form of this command removes the tag value from the configuration.

Parameters *tag* — Specifies a route tag.

Values 1 to 4294967295

Platforms All

tag

Syntax **tag** *tag*
no tag

Context [Tree] (config>router>isis>interface tag)

Full Context configure router isis interface tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a route tag to the specified IP address of an interface.

The **no** form of this command removes the tag value from the configuration.

Default no tag

Parameters *tag* — Specifies a route tag.

Values 1 to 4294967295

Platforms All

tag

Syntax **tag** {**no-tag** | *tag*}
no tag

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from tag)

Full Context configure router policy-options policy-statement entry from tag

Description This command matches the tag value in static or IGP routes. A decimal or hexadecimal value of 4 octets can be entered. For IS-IS, OSPF, and static routes, all four octets can be used. For RIP and RIPng, only the two most significant octets are used if more than two octets are configured.

The **no** form of this command removes the tag field match criterion.

Default no tag

Parameters *tag* — Matches the configured tag value.

Values Accepts decimal or hexadecimal formats:

- IS-IS, OSPF and static routes: 0x0 – 0xFFFFFFFF or 1 – 4294967295
- RIP and RIPng: 0x0 – 0xFFFF or 1 – 65535

no-tag — Specifies that no tag value is set.

Platforms All

tag

Syntax **tag** *tag*
no tag

Context **[Tree]** (config>router>policy-options>policy-statement>default-action tag)
[Tree] (config>router>policy-options>policy-statement>entry>action tag)

Full Context configure router policy-options policy-statement default-action tag

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router policy-options policy-statement entry action tag

Description This command assigns a tag to routes matching the entry, which is then applied to IGP routes. A decimal or hexadecimal value of 4 octets can be entered.

For IS-IS and OSPF, all four octets can be used.

For RIP and RIPng, only the two most significant octets are used if more than two octets are configured.

The **no** form of this command removes the tag.

Default no tag

Parameters *tag* — Assigns an IS-IS, OSPF, RIP or RIPng tag to routes matching the entry.

Values Accepts decimal or hexadecimal formats:
IS-IS and OSPF: 0x0–0xFFFFFFFF or 1–4294967295
RIP and RIPng: 0x0–0xFFFF or 1–65535
name — The tag parameter variable name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

tag

Syntax **tag** *tag-id*
no tag

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry tag)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry tag)

Full Context configure qos sap-ingress ip-criteria entry tag
configure qos sap-ingress ipv6-criteria entry tag

Description This command associates a tag with the criteria entry.

Tag identifiers are not supported in SAP ingress QoS policies, MAC criteria statements, or in SAP egress QoS policies.

The **no** form of this command removes the tag.

Parameters *tag-id* — Specifies the tag ID.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tag

Syntax **tag** *tag*
no tag

Context **[Tree]** (config>router>isis>srv6>locator tag)

Full Context configure router isis segment-routing-v6 locator tag

Description This command configures a route tag to advertise in the locator TLV.

The **no** form of this command removes the tag value from the configuration.

Default no tag

Parameters *tag* — Specifies a route tag.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

24.11 tag-protocol-id

tag-protocol-id

Syntax **tag-protocol-id** *tag-protocol-id*
no tag-protocol-id

Context **[Tree]** (config>test-oam>build-packet>header>dot1q tag-protocol-id)
[Tree] (debug>oam>build-packet>packet>field-override>header>dot1q tag-protocol-id)

Full Context configure test-oam build-packet header dot1q tag-protocol-id
debug oam build-packet packet field-override header dot1q tag-protocol-id

Description This command defines the Dot1Q tag protocol ID to be used in the test Dot1Q header.

The **no** form of this command removes the tag protocol ID value.

Default tag-protocol-id 0x8100 (33024)

Parameters *tag-protocol-id* — Specifies the Dot1Q tag protocol ID to be used in the test Dot1Q header in either decimal or hexadecimal.

Values 1536 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tag-protocol-id

Syntax **tag-protocol-id** *tag-protocol-id*
no tag-protocol-id

Context **[Tree]** (config>test-oam>build-packet>header>pbb tag-protocol-id)

Full Context configure test-oam build-packet header pbb tag-protocol-id

Description This command defines the PBB Tag Protocol Identifier (TPID) to be used in the test PBB header.

The **no** form of this command reverts to the default.

Default tag-protocol-id 0x88E7 (35047)

Parameters *tag-protocol-id* — Specifies a tag Protocol Identifier (TPID) for a PBB packet header to be launched by the OAM **find-egress** tool.

Values 1536 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tag-protocol-id

Syntax **tag-protocol-id** *tag-protocol-id*
no tag-protocol-id

Context **[Tree]** (debug>oam>build-packet>packet>field-override>header>pbb tag-protocol-id)

Full Context debug oam build-packet packet field-override header pbb tag-protocol-id

Description This command defines the PBB TPID to be used in the PBB header.

The **no** form of this command reverts to the default.

Default tag-protocol-id 0

Parameters *tag-protocol-id* — Specifies a TPID for a PBB packet header to be launched by the OAM **find-egress** tool.

Values 1536 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.12 taii-type2

taii-type2

Syntax **taii-type2** *global-id:node-id:ac-id*
no taii-type2

Context **[Tree]** (config>service>apipe>spoke-sdp>pw-path-id taii-type2)
[Tree] (config>service>cpipe>spoke-sdp>pw-path-id taii-type2)
[Tree] (config>service>epipe>spoke-sdp>pw-path-id taii-type2)
[Tree] (config>service>vpls>spoke-sdp>pw-path-id taii-type2)

Full Context configure service apipe spoke-sdp pw-path-id taii-type2
configure service cpipe spoke-sdp pw-path-id taii-type2
configure service epipe spoke-sdp pw-path-id taii-type2
configure service vpls spoke-sdp pw-path-id taii-type2

Description This command configures the Target Individual Attachment Identifier (TAII) for an MPLS-TP spoke SDP. If this is configured on a spoke SDP for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the saii-type2 of the mate spoke SDP.

Parameters *global-id* — Specifies the global ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values 0 to 4294967295

node-id — Specifies the node ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values a.b.c.d or 0 to 4294967295

ac-id — Specifies the attachment circuit ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service cpipe spoke-sdp pw-path-id taii-type2
- configure service epipe spoke-sdp pw-path-id taii-type2
- configure service vpls spoke-sdp pw-path-id taii-type2

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp pw-path-id taii-type2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

taii-type2

Syntax **taii-type2** *global-id:prefix:ac-id*
no taii-type2

Context **[Tree]** (config>service>epipe>spoke-sdp-fec taii-type2)

Full Context configure service epipe spoke-sdp-fec taii-type2

Description taii-type2 configures the target attachment individual identifier for the SDP SDP. This is only applicable to FEC129 AII type 2.

This command is blocked in CLI if this end of the spoke SDP is configured for single-sided auto configuration (using the **auto-config** command).

Parameters *global-id* — Specifies a global ID of this router T-PE. This value must correspond to one of the global_id values configured for a local-prefix under **config>service>pw-routing>local-prefix** context.

Values 1 to 4294967295

prefix — Speecifies prefix on this router T-PE that the spoke SDP SDP is associated with. This value must correspond to one of the prefixes configured under **config>service>pw-routing>local-prefix** context.

Values an IPv4-formatted address a.b.c.d or 1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique identifier for the spoke SDP.

Values 1 to 4294967295

Platforms All

taii-type2

Syntax **taii-type2** *global-id:node-id:ac-id*
no taii-type2

Context **[Tree]** (config>service>ies>if>spoke-sdp>pw-path-id taii-type2)

Full Context configure service ies interface spoke-sdp pw-path-id taii-type2

Description This command configures the target individual attachment identifier (TAII) for an MPLS-TP spoke-sdp. If this is configured on a spoke-sdp for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the saii-type2 of the mate spoke-sdp.

Parameters *global-id* — Specifies the global ID at the target PE or T-PE for the MPLS-TP PW for a spoke-SDP.

Values 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

node-id — Specifies the node ID at the target PE or T-PE for the MPLS-TP PW for a spoke-SDP.

Values a.b.c.d or 0 to 4294967295

ac-id — Specifies the attachment circuit ID at the target PE or T-PE for the MPLS-TP PW for a spoke-SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

taii-type2

Syntax **taii-type2** *global-id:node-id:ac-id*
no taii-type2

Context **[Tree]** (config>service>vprn>red-if>spoke-sdp>pw-path-id taii-type2)

Full Context configure service vprn redundant-interface spoke-sdp pw-path-id taii-type2

Description This command configures the target individual attachment identifier (TAII) for an MPLS-TP spoke SDP. If this is configured on a spoke SDP for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the saii-type2 of the mate spoke SDP.

Parameters *global-id* — Specifies the global ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values 0 to 4294967295

node-id — Specifies the node ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values a.b.c.d or 1 to 4294967295

ac-id — Specifies the attachment circuit ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

taii-type2

Syntax **taii-type2** *global-id:node-id:ac-id*
no taii-type2

Context **[Tree]** (config>mirror>mirror-dest>remote-src>spoke-sdp>pw-path-id taii-type2)
[Tree] (config>mirror>mirror-dest>spoke-sdp>pw-path-id taii-type2)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure mirror mirror-dest remote-source spoke-sdp pw-path-id taii-type2
configure mirror mirror-dest spoke-sdp pw-path-id taii-type2

Description This command configures the target individual attachment identifier (TAII) for an MPLS-TP spoke SDP. If this is configured on a spoke SDP for which vc-switching is also configured (for example, it is at an S-PE), then the values must match those of the saii-type2 of the mate spoke SDP.

Parameters *global-id* — Specifies the global ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values 0 to 4294967295

node-id — Specifies the node ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP.

Values a.b.c.d or 0 to 4294967295

ac-id — Specifies the attachment circuit ID at the target PE or T-PE for the MPLS-TP PW for a spoke SDP. If this node is the source of the PW, then the AC ID must be set to a locally unique value.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.13 target-name

target-name

Syntax **target-name {node-name | user-agent | custom-string** *name***}**
no target-name

Context **[Tree]** (config>system>grpc-tunnel>tunnel target-name)

Full Context configure system grpc-tunnel tunnel target-name

Description This command assigns a target name that the node will register with.

The **no** form of this command removes the target name.

Default no target-name

Parameters **node-name** — Keyword to register the tunnel with the node name configured using the **configure system name** command.

user-agent — Keyword to register the tunnel with the user agent name string defined as *node-name:vendor:model:software-version*.

custom-string — Assigns an arbitrary string as the target name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name — Specifies a string, up to 64 characters, that defines the target name.

Platforms All

24.14 target-power

target-power

Syntax **target-power** *power*

Context **[Tree]** (config>port>dwdm>coherent target-power)

Full Context configure port dwdm coherent target-power

Description This command configures the target transmit optical power for the port.

Default target-power 1.00

Parameters *power* — Specifies the desired average output power in dBm.

Values -20.00 to 3.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.15 target-retry-wait

target-retry-wait

Syntax **target-retry-wait** *seconds*

Context **[Tree]** (config>li>x-interfaces>x3>timeouts target-retry-wait)

Full Context configure li x-interfaces x3 timeouts target-retry-wait

Description This command configures the retry interval for target tunnel set up.

Parameters *seconds* — Specifies the time that the system must wait before attempting another tunnel creation request to avoid overloading the LIC.

Values 300 to 1200

Default 300

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.16 target-type

target-type

Syntax **target-type {grpc-server | ssh-server | custom-type** *type***}**
no target-type

Context **[Tree]** (config>system>grpc-tunnel>tunnel>handler target-type)

Full Context configure system grpc-tunnel tunnel handler target-type

Description This command assigns a server as a handler for all tunnel sessions.

The **no** form of this command disables the tunnel handler server.

Default no target-type

Parameters **grpc-server** — Keyword that assigns the gRPC server as a handler for all tunnels sessions. The gRPC-tunnel protocol value corresponds to “GNMI_GNOI”.

ssh-server — Keyword that assigns the SSH server as a handler for all tunnels sessions. The gRPC-tunnel protocol value corresponds to “SSH”.

custom-type — Keyword that assigns an arbitrary string as the target type.

type — Specifies a string, up to 255 characters, defining the client to serve as a handler for all tunnel sessions. Values used by gRPC tunnel protocol, such as “GNMI_GNOI” or “SSH” can also be used.

Platforms All

24.17 targeted-session

targeted-session

Syntax **targeted-session**

Context **[Tree]** (config>router>ldp targeted-session)

Full Context configure router ldp targeted-session

Description This command configures targeted LDP sessions. Targeted sessions are LDP sessions between non-directly connected peers. Hello messages are sent directly to the peer platform instead of to all the routers on this subnet multicast address. The user can configure different default parameters for IPv4 and IPv6 LDP targeted hello adjacencies.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The discovery messages for an indirect LDP session are addressed to the specified peer and not to the multicast address.

Platforms All

24.18 task-scheduling-int

task-scheduling-int

Syntax **task-scheduling-int** *percent-of-default*
no task-scheduling-int

Context **[Tree]** (config>card>virt-sched-adj task-scheduling-int)

Full Context configure card virtual-scheduler-adjustment task-scheduling-int

Description This command overrides the system default time between scheduling the hierarchical virtual scheduling task. By default, the system "wakes" the virtual scheduler task every 50ms; this is equivalent to five 10ms timer ticks. The task-scheduling-int command uses a percent value parameter to modify the number of timer ticks.

While the system accepts a wide range of percent values, the result is rounded to the nearest 10ms tick value. The fastest wake interval is 10ms (1 timer tick).

The **no** form of this command restores the default task scheduling interval of the card's hierarchical virtual scheduler task.

Parameters *percent-of-default:* — Specifies that the percent-of-default parameter is required and is used to modify the default task scheduling interval for the hierarchical virtual scheduling task on the card. Defining 100.00 percent is equivalent to removing the override.

Values 0.01% to 1000.00%

Default 100.00%

Platforms All

24.19 tcp

tcp

Syntax **tcp**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>test-oam>build-packet>header tcp)
[Tree] (debug>oam>build-packet>packet>field-override>header tcp)

Full Context configure test-oam build-packet header tcp
debug oam build-packet packet field-override header tcp

Description This command creates a TCP header and enables the context to define the associated parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.20 tcp-ack

tcp-ack

Syntax **tcp-ack** {**true** | **false**}
no tcp-ack

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match tcp-ack)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match tcp-ack)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match tcp-ack)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match tcp-ack)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match tcp-ack
configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match tcp-ack
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match tcp-ack
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match tcp-ack

Description This command configures the TCP ACK match condition.

The **no** form of this command reverts to the default.

Parameters **true** — Enables checking for the ACK bit.

false — Disables checking for the ACK bit.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

tcp-ack

Syntax **tcp-ack** {**true** | **false**}
no tcp-ack

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>ip-filter>entry>match tcp-ack)
[Tree] (config>filter>ipv6-filter>entry>match tcp-ack)

Full Context configure filter ip-filter entry match tcp-ack
configure filter ipv6-filter entry match tcp-ack

Description This command configures an IP filter match criterion based on the Acknowledgment (ACK) TCP Flag bit, defined in RFC 793, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-ack

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

tcp-ack

Syntax **tcp-ack** {**true** | **false**}
no tcp-ack

Context [Tree] (cfg>sys>sec>cpm>ip-filter>entry>match tcp-ack)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match tcp-ack)

Full Context configure system security cpm-filter ip-filter entry match tcp-ack
configure system security cpm-filter ipv6-filter entry match tcp-ack

Description This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP or IPv6 packet as an IP filter match criterion.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

The **no** form of this command removes the criterion from the match entry.

Default no tcp-ack

Parameters **true** — Specifies matching on IP or IPv6 packets that have the ACK bit set in the control bits of the TCP header of an IP or IPv6 packet.

false — Specifies matching on IP or IPv6 packets that do not have the ACK bit set in the control bits of the TCP header of the IP or IPv6 packet.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.21 tcp-adv-func

tcp-adv-func

Syntax **tcp-adv-func** *size*

Context **[Tree]** (config>isa>aa-grp>shared-resources tcp-adv-func)

Full Context configure isa aa-group shared-resources tcp-adv-func

Description This command configures the allocation of shared resource pool for TCP advanced functions.

Default tcp-adv-func 100

Parameters *size* — Specifies the allocation of the shared resource pool.

Values 0 to 100

24.22 tcp-client-reset

tcp-client-reset

Syntax [**no**] **tcp-client-reset**

Context **[Tree]** (config>app-assure>group>http-redirect tcp-client-reset)

Full Context configure application-assurance group http-redirect tcp-client-reset

Description This command enables an HTTP-redirect policy to initiate a TCP reset towards the client if the AA policy results in a redirect with packet drop but the http redirect cannot be delivered. Scenarios for this include HTTPs (TLS) sessions, blocking of non-HTTP TCP traffic, and blocking of existing flows after a policy re-evaluate of an existing subscriber.

The **no** form of this command disables the command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.23 tcp-cwr

tcp-cwr

Syntax **tcp-cwr** {**true** | **false**}
no tcp-cwr

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-cwr)
[Tree] (config>filter>ipv6-filter>entry>match tcp-cwr)

Full Context configure filter ip-filter entry match tcp-cwr
configure filter ipv6-filter entry match tcp-cwr

Description This command configures an IP filter match criterion based on the Congestion Window Reduced (CWR) TCP Flag bit, defined in RFC 3168, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-cwr

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.24 tcp-ece

tcp-ece

Syntax **tcp-ece** {**true** | **false**}
no tcp-ece

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-ece)
[Tree] (config>filter>ipv6-filter>entry>match tcp-ece)

Full Context configure filter ip-filter entry match tcp-ece
configure filter ipv6-filter entry match tcp-ece

Description This command configures an IP filter match criterion based on the ECN-Echo (ECE) TCP Flag bit, defined in RFC 3168, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no tcp-ece

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.25 tcp-established

tcp-established

Syntax **tcp-established** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-established

Context **[Tree]** (config>service>nat>nat-policy>timeouts tcp-established)
[Tree] (config>service>nat>firewall-policy>timeouts tcp-established)
[Tree] (config>service>nat>up-nat-policy>timeouts tcp-established)

Full Context configure service nat firewall-policy timeouts tcp-established
configure service nat nat-policy timeouts tcp-established
configure service nat up-nat-policy timeouts tcp-established

Description This command configures the idle timeout applied to a TCP session in the established state.

Default tcp-established hrs 2 min 4

Parameters *hours* — Specifies the timeout hours field.

Values 1 to 24

minutes — Specifies the timeout minutes field.

Values 1 to 59

seconds — Specifies the timeout seconds field.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy timeouts tcp-established
- configure service nat up-nat-policy timeouts tcp-established

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts tcp-established

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.26 tcp-fin

tcp-fin

Syntax **tcp-fin** {**true** | **false**}
no tcp-fin

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-fin)
[Tree] (config>filter>ipv6-filter>entry>match tcp-fin)

Full Context configure filter ip-filter entry match tcp-fin
configure filter ipv6-filter entry match tcp-fin

Description This command configures an IP filter match criterion based on the FIN TCP Flag bit, defined in RFC 793, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-fin

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.27 tcp-keepalive

tcp-keepalive

Syntax **tcp-keepalive**

Context **[Tree]** (config>system>grpc tcp-keepalive)

Full Context configure system grpc tcp-keepalive

Description Commands in this context configure the sending of TCP keepalives by the router towards all gRPC clients.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Enabling TCP keepalive speeds up the detection of certain failures. The TCP keepalives sent by the router are controlled by three commands: **idle-time**, **interval**, and **retries**. The router starts sending TCP keepalives when the connection has been idle (no TCP segments sent or received) for more than **idle-time** seconds. At that point, the router sends a probe (TCP ACK with a sequence number = current sequence number - 1) and expects a TCP ACK. It repeats this probe every **interval** seconds for the configured number of **retries**. If no response is received to any of the probes, the connection is immediately closed, which starts the purge timer if the TCP connection is currently supporting the RibApi service.

Platforms All

tcp-keepalive

Syntax **tcp-keepalive**

Context **[Tree]** (config>bmp>station>connection tcp-keepalive)

Full Context configure bmp station connection tcp-keepalive

Description Commands in this context configure TCP keepalive parameters for the station.

Platforms All

tcp-keepalive

Syntax **tcp-keepalive**

Context **[Tree]** (config>system>grpc-tunnel>destination-group tcp-keepalive)
[Tree] (config>system>telemetry>destination-group tcp-keepalive)

Full Context configure system grpc-tunnel destination-group tcp-keepalive
configure system telemetry destination-group tcp-keepalive

Description Commands in this context configure TCP keepalive commands.

Platforms All

24.28 tcp-mss

tcp-mss

Syntax **tcp-mss** *mss-value*
no tcp-mss

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>ies>if tcp-mss)
[Tree] (config>service>ies>if>ipv6 tcp-mss)

Full Context configure service ies interface ipv6 tcp-mss
configure service ies interface tcp-mss

Description This command statically sets the TCP maximum segment size (MSS) for TCP connections originated from the associated IP interface to the specified value.

The **no** form of this command removes the static value and allows the TCP MSS value to be calculated based on the IP MTU value by subtracting the base IP and TCP header lengths from the IP MTU value (tcp_mss = ip_mtu – 40).

Default no tcp-mss

Parameters *mss-value* — The TCP MSS value that should be used in the TCP SYN packet during the three-way handshake negotiation of a TCP connection.

Note: 9158 = max-IP_MTU (9198)-40

Values 536 to 9746 (IPv4) 1220 to 9726 (IPv6)

Platforms All

tcp-mss

Syntax **tcp-mss** *mss-value*
no tcp-mss

Context [Tree] (config>service>vprn>if tcp-mss)
[Tree] (config>service>vprn>if>ipv6 tcp-mss)
[Tree] (config>service>vprn>nw-if tcp-mss)

Full Context configure service vprn interface ipv6 tcp-mss
configure service vprn interface tcp-mss
configure service vprn network-interface tcp-mss

Description This command statically sets the TCP maximum segment size (MSS) for TCP connections originated from the associated IP or network interface to the specified value.

The **no** form of this command removes the static value and allows the TCP MSS value to be calculated based on the IP MTU value by subtracting the base IP and TCP header lengths from the IP MTU value (tcp_mss = ip_mtu – 40).

Default no tcp-mss

Parameters *mss-value* — Specifies the TCP MSS value that should be used in the TCP SYN packet during the three-way handshake negotiation of a TCP connection.

Note: 9746 = max-IP_MTU (9786)-40

Values 384 to 9746 (IPv4 or network)
1220 to 9726(IPv6)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

tcp-mss

Syntax **tcp-mss** *mss-value*
no tcp-mss

Context **[Tree]** (config>router>if tcp-mss)
[Tree] (config>router>if>ipv6 tcp-mss)

Full Context configure router interface ipv6 tcp-mss
configure router interface tcp-mss

Description This command statically sets the TCP maximum segment size (MSS) for TCP connections originated from the associated IP interface to the specified value.

The **no** form of this command removes the static value and allows the TCP MSS value to be calculated based on the IP MTU value by subtracting the base IP and TCP header lengths from the IP MTU value (tcp_mss = ip_mtu – 40).

Default no tcp-mss

Parameters *mss-value* — Specifies the TCP MSS value that should be used in the TCP SYN packet during the three-way handshake negotiation of a TCP connection.

9158 = max-IP_MTU (9198)-40

Values 536 to 9746 (IPv4) 1220 to 9726 (IPv6)

Platforms All

tcp-mss

Syntax **tcp-mss** *mss-value*
no tcp-mss

Context **[Tree]** (config>router>bgp tcp-mss)
[Tree] (config>service>vprn>bgp tcp-mss)

Full Context configure router bgp tcp-mss
configure service vprn bgp tcp-mss

Description This command configures an override for the TCP maximum segment size to use with a specific peer or set of peers (depending on the scope of the command).

The configured value controls two properties of the TCP connection as follows:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- TCP MSS option — The router advertises the TCP MSS option value in the TCP SYN packet it sends as part of the 3-way handshake. The advertised value may be lower than the configured value, depending on the IP MTU of the first hop IP interface. The peers are asked to abide by this value when sending TCP segments to the local router.
- TCP maximum segment size — The actual transmitted size may be lower than the configured value, depending on the TCP MSS option value signaled by the peers, the effect of path MTU discovery, or other factors.

The **no** form of this command removes the TCP MSS override values from the configuration.

Default no tcp-mss

Parameters *mss-value* — Specifies the The router uses the TCP SYN to advertise the TCP MSS option value towards its peer. MSS value, in bytes, to use with the peers that fall within the scope of the command.

Values 384 to 9746

Platforms All

tcp-mss

Syntax **tcp-mss ip-stack**
tcp-mss *mss-value*
no tcp-mss

Context **[Tree]** (config>router>bgp>group tcp-mss)
[Tree] (config>router>bgp>group>neighbor tcp-mss)
[Tree] (config>service>vprn>bgp>group tcp-mss)
[Tree] (config>service>vprn>bgp>group>neighbor tcp-mss)

Full Context configure router bgp group neighbor tcp-mss
configure router bgp group tcp-mss
configure service vprn bgp group neighbor tcp-mss
configure service vprn bgp group tcp-mss

Description This command configures an override for the TCP maximum segment size to use with a specific peer or set of peers (depending on the scope of the command).

The configured value controls two properties of the TCP connection as follows:

- TCP MSS option — The router advertises the TCP MSS option value in the TCP SYN packet it sends as part of the 3-way handshake. The advertised value may be lower than the configured value, depending on the IP MTU of the first hop IP interface. The peers are asked to abide by this value when sending TCP segments to the local router.
- TCP maximum segment size — The actual transmitted size may be lower than the configured value, depending on the TCP MSS option value signaled by the peers, the effect of path MTU discovery, or other factors.

The **no** form of this command removes the TCP MSS override values from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no tcp-mss

Parameters *mss-value* — Specifies the TCP MSS value, in bytes, to use with the peers that fall within the scope of the command.

Values 384 to 9746

ip-stack — This keyword requests that TCP MSS be derived from mechanisms and configurations outside of BGP, including the configuration of **tcp-mss** at the IP interface level. It provides a method to override inheritance within the BGP configuration.

Platforms All

24.29 tcp-mss-adjust

tcp-mss-adjust

Syntax **tcp-mss-adjust** *segment-size*
no tcp-mss-adjust

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw tcp-mss-adjust)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw tcp-mss-adjust)

Full Context configure service ies subscriber-interface group-interface wlan-gw tcp-mss-adjust
configure service vprn subscriber-interface group-interface wlan-gw tcp-mss-adjust

Description This command configures the TCP Maximum Segment Size (MSS) adjustment for the wlan-gw gateway.

The **no** form of this command disables adjusting tcp-mss values.

For DSM, this only applies to packets sent in the downstream direction (TCP SYN towards UE). For the upstream direction, it is also required to configure MSS adjust under the applicable NAT-policy.

Parameters *segment-size* — Specifies the value to put into the TCP Maximum Segment Size (MSS) option if not already present, or if the present value is higher.

Values 160 to 10240

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tcp-mss-adjust

Syntax **tcp-mss-adjust** *segment-size*
no tcp-mss-adjust

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>aqp>entry>action tcp-mss-adjust)

Full Context configure application-assurance group app-qos-policy entry action tcp-mss-adjust

Description This command configures the value to adjust the TCP Maximum Segment Size (MSS) option. The no form of this command disables the segment size adjustment.

Default no tcp-mss-adjust

Parameters *segment-size* — Specifies the value to put into the TCP Maximum Segment Size (MSS) option if not already present, or if the present value is higher.

Values 160 to 10240

tcp-mss-adjust

Syntax **tcp-mss-adjust** *segment-size*
no tcp-mss-adjust

Context [Tree] (config>service>nat>nat-policy tcp-mss-adjust)
[Tree] (config>service>nat>firewall-policy tcp-mss-adjust)
[Tree] (config>service>nat>up-nat-policy tcp-mss-adjust)

Full Context configure service nat firewall-policy tcp-mss-adjust
configure service nat nat-policy tcp-mss-adjust
configure service nat up-nat-policy tcp-mss-adjust

Description This command configures the value to adjust the TCP Maximum Segment Size (MSS) option.

The **no** form of the command returns the segment size to the default.

Default no tcp-mss-adjust

Parameters *segment-size* — Specifies the value to put into the TCP Maximum Segment Size (MSS) option if not already present, or if the present value is higher.

Values 160 to 10240

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy tcp-mss-adjust
- configure service nat up-nat-policy tcp-mss-adjust

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy tcp-mss-adjust

tcp-mss-adjust

Syntax **tcp-mss-adjust**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>filter>ip-filter>entry>action tcp-mss-adjust)
[Tree] (config>filter>ipv6-filter>entry>action tcp-mss-adjust)

Full Context configure filter ip-filter entry action tcp-mss-adjust
configure filter ipv6-filter entry action tcp-mss-adjust

Description This command activates the adjustment of the TCP Maximum Segment Size (MSS) option of TCP packets matching the entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tcp-mss-adjust

Syntax **tcp-mss-adjust** *segment-size*
no tcp-mss-adjust

Context [Tree] (config>service>nat>map-domain tcp-mss-adjust)

Full Context configure service nat map-domain tcp-mss-adjust

Description This command enables the TCP maximum segment size (MSS) adjustments in a MAP domain. The TCP SYN and SYN-ACK packets are intercepted in both directions, and if their MSS value is larger than the one configured using this command, the MSS value in the packet is re-written (lowered) to the configured value. The end hosts use the lowest setting of the two hosts. The MSS value does not account for the IP or TCP header length.

If the MSS value in the SYN or SYN-ACK is not found, a new value is added and set to the configured value.

Default no tcp-mss-adjust

Parameters *segment-size* — Specifies the maximum size of the segment.

Values 160 to 8626

Platforms VSR

24.30 tcp-ns

tcp-ns

Syntax **tcp-ns** {**true** | **false**}
no tcp-ns

Context [Tree] (config>filter>ip-filter>entry>match tcp-ns)
[Tree] (config>filter>ipv6-filter>entry>match tcp-ns)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure filter ip-filter entry match tcp-ns
configure filter ipv6-filter entry match tcp-ns

Description This command configures an IP filter match criterion based on the Nonce Sum (NS) TCP Flag bit, defined in RFC 3540, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-ns

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.31 tcp-optimizer

tcp-optimizer

Syntax **tcp-optimizer** *tcp-optimizer-name* [**create**]
no tcp-optimizer *tcp-optimizer-name*

Context **[Tree]** (config>app-assure>group tcp-optimizer)

Full Context configure application-assurance group tcp-optimizer

Description This command configures the TCP optimizer policy. When a TCP optimizer policy is removed or deleted, the existing flows using this policy are abandoned, and optimization is stopped. If, however, the TCP optimizer action is removed from a session-filter entry (in the **config>app-assure>group>sess-fltr>entry action** context), the existing flows are not affected.

The **no** form of this command removes the specified TCP optimizer policy.

Parameters *tcp-optimizer-name* — Specifies the name of the TCP optimizer policy, up to 32characters.

create — This keyword is mandatory when creating a TCP optimizer policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.32 tcp-option-number

tcp-option-number

Syntax **tcp-option-number**

Context **[Tree]** (config>system>security>keychain tcp-option-number)

Full Context configure system security keychain tcp-option-number

Description Commands in this context configure the TCP option number to be placed in the TCP packet header.

Platforms All

24.33 tcp-performance

tcp-performance

Syntax **tcp-performance**

Context **[Tree]** (config>app-assure>group>cflowd tcp-performance)

Full Context configure application-assurance group cflowd tcp-performance

Description Commands in this context configure Cflowd TCP performance export parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.34 tcp-psh

tcp-psh

Syntax **tcp-psh** {**true** | **false**}
no tcp-psh

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-psh)
[Tree] (config>filter>ipv6-filter>entry>match tcp-psh)

Full Context configure filter ip-filter entry match tcp-psh
configure filter ipv6-filter entry match tcp-psh

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an IP filter match criterion based on the Push (PSH) TCP Flag bit, defined in RFC 793, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-psh

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.35 tcp-rst

tcp-rst

Syntax **tcp-rst [min** *minutes*] **[sec** *sec*]
no tcp-rst

Context [Tree] (config>service>nat>nat-policy>timeouts tcp-rst)
[Tree] (config>service>nat>firewall-policy>timeouts tcp-rst)
[Tree] (config>service>nat>up-nat-policy>timeouts tcp-rst)

Full Context configure service nat firewall-policy timeouts tcp-rst
configure service nat nat-policy timeouts tcp-rst
configure service nat up-nat-policy timeouts tcp-rst

Description This command suspends the use of the outside TCP ports that have been used in translations for TCP connections that are closed via TCP RST. Once this timer expires, the outside ports can be reused for new TCP translations.

The **no** form of the command reverts to the default.

Default no tcp-rst

Parameters *minutes* — Specifies the timeout, in minutes, after receiving a RST and closing the session before going to the LISTEN state again.

Values 1 to 4

sec — Specifies the timeout, in seconds, after receiving a RST and closing the session before going to the LISTEN state again.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service nat up-nat-policy timeouts tcp-rst
- configure service nat nat-policy timeouts tcp-rst

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts tcp-rst

tcp-rst

Syntax **tcp-rst** {**true** | **false**}
no tcp-rst

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-rst)
[Tree] (config>filter>ipv6-filter>entry>match tcp-rst)

Full Context configure filter ip-filter entry match tcp-rst
configure filter ipv6-filter entry match tcp-rst

Description This command configures an IP filter match criterion based on the Reset (RST) TCP Flag bit, defined in RFC 793, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-rst

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.36 tcp-session-parameters

tcp-session-parameters

Syntax **tcp-session-parameters**

Context **[Tree]** (config>router>ldp tcp-session-parameters)

Full Context configure router ldp tcp-session-parameters

Description Commands in this context configure parameters applicable to TCP transport session of an LDP session to remote peer.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.37 tcp-stack

tcp-stack

Syntax **tcp-stack** *tcp-stack-type*

Context [Tree] (config>app-assure>group>tcp-optimizer tcp-stack)

Full Context configure application-assurance group tcp-optimizer tcp-stack

Description This command configures the TCP stack used toward the subscriber.

- The TCP stack used toward the core network is new-reno, and it is not configurable.
- TCP BBR, TCP Illinois, and TCP Westwood implement a sender-side modification of the TCP congestion window algorithm that improves upon the performance of TCP Reno in wireless networks with lossy links.

The **no** form of this command reverts to the default.

Default tcp-westwood

Parameters *tcp-stack-type* — Specifies the TCP stack used toward the subscriber.

Values tcp-bbr | tcp-illinois | tcp-new-reno | tcp-westwood

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.38 tcp-syn

tcp-syn

Syntax **tcp-syn** {**true** | **false**}
no tcp-syn

Context [Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ip>entry>match tcp-syn)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>ingr-ipv6>entry>match tcp-syn)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ip>entry>match tcp-syn)
[Tree] (config>subscr-mgmt>cat-map>category>exh-lvl>egr-ipv6>entry>match tcp-syn)

Full Context configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ip-filter-entries entry match tcp-syn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt category-map category exhausted-credit-service-level egress-ipv6-filter-entries entry match tcp-syn
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry match tcp-syn
configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ipv6-filter-entries entry match tcp-syn

Description This command configures the TCP SYN match condition.

The **no** form of this command reverts to the default.

Parameters **true** — Enables checking for the SYN bit.

false — Disables checking for the SYN bit.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

tcp-syn

Syntax **tcp-syn** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-syn

Context **[Tree]** (config>service>nat>nat-policy>timeouts tcp-syn)
[Tree] (config>service>nat>firewall-policy>timeouts tcp-syn)
[Tree] (config>service>nat>up-nat-policy>timeouts tcp-syn)

Full Context configure service nat firewall-policy timeouts tcp-syn
configure service nat nat-policy timeouts tcp-syn
configure service nat up-nat-policy timeouts tcp-syn

Description This command configures the timeout applied to a TCP session in the SYN state.

Default tcp-syn sec 15

Parameters *hours* — Specifies the timeout hours field.

Values 1 to 24

minutes — Specifies the timeout minutes field.

Values 1 to 59

seconds — Specifies the timeout seconds field.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy timeouts tcp-syn
- configure service nat nat-policy timeouts tcp-syn

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service nat firewall-policy timeouts tcp-syn

tcp-syn

Syntax **tcp-syn** {**true** | **false**}
no tcp-syn

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-syn)
[Tree] (config>filter>ipv6-filter>entry>match tcp-syn)

Full Context configure filter ip-filter entry match tcp-syn
configure filter ipv6-filter entry match tcp-syn

Description This command configures an IP filter match criterion based on the Synchronize (SYN) TCP Flag bit, defined in RFC 793, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-syn

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

tcp-syn

Syntax **tcp-syn** {**true** | **false**}
no tcp-syn

Context **[Tree]** (cfg>sys>sec>cpm>ip-filter>entry>match tcp-syn)
[Tree] (cfg>sys>sec>cpm>ipv6-filter>entry>match tcp-syn)

Full Context configure system security cpm-filter ip-filter entry match tcp-syn
configure system security cpm-filter ipv6-filter entry match tcp-syn

Description This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP or IPv6 packet as an IP filter match criterion.

Note: An entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP or IPv6 address.

The **no** form of this command removes the criterion from the match entry.

Default no tcp-syn

Parameters **true** — Specifies matching on IP or IPv6 packets that have the SYN bit set in the control bits of the TCP header.

false — Specifies matching on IP or IPv6 packets that do not have the SYN bit set in the control bits of the TCP header.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.39 tcp-time-wait

tcp-time-wait

Syntax **tcp-time-wait** [**min** *minutes*] [**sec** *seconds*]
no tcp-time-wait

Context **[Tree]** (config>service>nat>nat-policy>timeouts tcp-time-wait)
[Tree] (config>service>nat>firewall-policy>timeouts tcp-time-wait)
[Tree] (config>service>nat>up-nat-policy>timeouts tcp-time-wait)

Full Context configure service nat firewall-policy timeouts tcp-time-wait
configure service nat nat-policy timeouts tcp-time-wait
configure service nat up-nat-policy timeouts tcp-time-wait

Description This command configures the timeout applied to a TCP session in a time-wait state.

Default no tcp-time-wait

Parameters *minutes* — Specifies the timeout minutes field.

Values 1 to 4

seconds — Specifies the timeout seconds field.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy timeouts tcp-time-wait
- configure service nat nat-policy timeouts tcp-time-wait

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service nat firewall-policy timeouts tcp-time-wait

24.40 tcp-transitory

tcp-transitory

Syntax **tcp-transitory** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-transitory

Context **[Tree]** (config>service>nat>nat-policy>timeouts tcp-transitory)
[Tree] (config>service>nat>firewall-policy>timeouts tcp-transitory)
[Tree] (config>service>nat>up-nat-policy>timeouts tcp-transitory)

Full Context configure service nat firewall-policy timeouts tcp-transitory
configure service nat nat-policy timeouts tcp-transitory
configure service nat up-nat-policy timeouts tcp-transitory

Description This command configures the idle timeout applied to a TCP session in a transitory state.

Default tcp-transitory min 4

Parameters *hours* — Specifies the timeout hours field.

Values 1 to 24

minutes — Specifies the timeout minutes field.

Values 1 to 59

seconds — Specifies the timeout seconds field.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy timeouts tcp-transitory
- configure service nat up-nat-policy timeouts tcp-transitory

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts tcp-transitory

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.41 tcp-urg

tcp-urg

Syntax **tcp-urg** {**true** | **false**}
no tcp-urg

Context **[Tree]** (config>filter>ip-filter>entry>match tcp-urg)
[Tree] (config>filter>ipv6-filter>entry>match tcp-urg)

Full Context configure filter ip-filter entry match tcp-urg
configure filter ipv6-filter entry match tcp-urg

Description This command configures an IP filter match criterion based on the Urgent (URG) TCP Flag bit, defined in RFC 793, as being set or not in the TCP header of an IP packet.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-urg

Parameters **true** — Specifies matching on IP packets that have the selected TCP flag bit set in the TCP header.

false — Specifies matching on IP packets that do not have the selected TCP flag bit set in the TCP header.

Platforms All

24.42 tcp-validate

tcp-validate

Syntax **tcp-validate** *tcp-validate-name*
no tcp-validate

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>action tcp-validate)

Full Context configure application-assurance group policy app-qos-policy entry action tcp-validate

Description This command assigns an existing TCP validation policy as an action on flows matching this AQP entry.

tcp-validate can only be called from AQP entries that:

- have no matching conditions that relate to information extracted from the incoming IP packets; for example, no application or IP address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- allow the following match conditions:
  - none
  - aa-sub
  - characteristic
  - traffic-direction (both only)

    traffic-direction cannot be unidirectional (from or to sub). It can either be set to both or left unspecified.

The **no** form of this command removes the TCP validation policy action from flows matching this AQP entry.

Default no tcp-validate

Parameters *tcp-validate-name* — Specifies the name of the TCP validation policy for this application assurance profile. The TCP validation policy is configured using the **config**>**app-assure**>**group**>**tcp-validate** *tcp-validate-name* command.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tcp-validate

Syntax **tcp-validate** *tcp-validate-name* **direction** *direction* [**create**]
no tcp-validate *tcp-validate-name* **direction** *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca tcp-validate)

Full Context configure application-assurance group statistics threshold-crossing-alert tcp-validate

Description This command configures TCA for the counter, and enables the capture of drop or admit events due to the specified TCP validation function.

Parameters *tcp-validate-name* — Specifies the name of the TCP validation policy up to 32 characters.

direction — Specifies the traffic direction in relation to the AA subscriber.

Values from-sub, to-sub

create — This keyword is mandatory when creating a TCA instance.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tcp-validate

Syntax **tcp-validate** *tcp-validate-name* [**create**]
no tcp-validate *tcp-validate-name*

Context **[Tree]** (config>app-assure>group tcp-validate)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group tcp-validate

Description This command configures a TCP validation policy.

The **no** form of this command removes the specified TCP validation policy.

Default no tcp-validate

Parameters *tcp-validate-name* — Specifies the name of the TCP validation policy up to 32 characters.

create — This keyword is mandatory when creating a TCP validation policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.43 tcp-validate-stats

tcp-validate-stats

Syntax [**no**] **tcp-validate-stats**

Context **[Tree]** (config>app-assure>group>statistics>aa-admit-deny tcp-validate-stats)

Full Context configure application-assurance group statistics aa-admit-deny tcp-validate-stats

Description This command configures whether to include or exclude TCP validation admit-deny statistics in accounting records.

Default no tcp-validate-stats

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.44 tdcm

tdcm

Syntax **tdcm**

Context **[Tree]** (config>port>dwdm tdcm)

Full Context configure port dwdm tdcm

Description This command configures the Tunable Dispersion Compensation Module parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.45 tdm

tdm

Syntax **tdm**

Context **[Tree]** (config>port tdm)

Full Context configure port tdm

Description Commands in this context configure DS-1/E-1 and DS-3/E-3 parameters for a port on a channelized MDA T1/E1. This context cannot be accessed on non-channelized MDAs.

TDM is a mechanism to divide the bandwidth of a stream into separate channels or time slots by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel. Each individual data stream is reassembled at the receiving end based on the timing.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

24.46 tdm-sat

tdm-sat

Syntax **tdm-sat** *sat-id* [**create**]
no tdm-sat *sat-id*

Context **[Tree]** (config>system>satellite tdm-sat)

Full Context configure system satellite tdm-sat

Description Commands in this context configure the specified TDM satellite.

The **no** form of the command deletes the specified TDM satellite.

Parameters *sat-id* — Specifies the satellite ID for the associated TDM satellite.

Values 1 to 20

create — The keyword used to create a new TDM satellite context. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.47 te

te

Syntax [**no**] **te**

Context **[Tree]** (debug>router>mpls>event te)

Full Context debug router mpls event te

Description This command debugs te events.

The **no** form of the command disables the debugging.

Platforms All

24.48 te-class

te-class

Syntax **te-class** *te-class-number* **class-type** *ct-number* **priority** *priority*
no te-class te-class-number

Context **[Tree]** (config>router>rsvp>diffserv-te te-class)

Full Context configure router rsvp diffserv-te te-class

Description This command configures a TE class. A TE class is defined as:

TE Class = {Class Type (CT), LSP priority}

Eight TE classes are supported. There is no default TE class once Diff-Serv is enabled. The user has to explicitly define each TE class.

When Diff-Serv is disabled, there will be an internal use of the default CT (CT0) and eight pre-emption priorities as shown in Table 184.

Table 184 **Default Class Type**

Class Type (CT internal)	LSP Priority
0	7
0	6

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 184 **Default Class Type**

Class Type (CT internal)	LSP Priority
0	5
0	4
0	3
0	2
0	1
0	0

The **no** form of this command deletes the TE class.

Parameters **te-class** *te-class-number* — Specifies the TE class number.

Values 0 to 7

class-type *ct-number* — Specifies the Diff-Serv Class Type number. One or more system forwarding classes can be mapped to a CT.

Values 0 to 7

priority *priority* — Specifies the LSP priority.

Values 0 to 7

Platforms All

24.49 te-down-threshold

te-down-threshold

Syntax **te-down-threshold** *threshold-level* [*threshold-level*]
no te-down-threshold

Context **[Tree]** (config>router>rsvp te-down-threshold)
[Tree] (config>router>rsvp>interface te-down-threshold)

Full Context configure router rsvp interface te-down-threshold
configure router rsvp te-down-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the specific threshold levels per node and per interface. Threshold levels are for reserved bandwidth per interface. The **te-threshold-update** command is used to enable or disable threshold-based IGP TE updates. Any reserved bandwidth change per interface is compared with all the threshold levels and trigger an IGP TE update if a defined threshold level is crossed in either direction (LSP setup or teardown). Threshold-based updates must be supported with both ISIS and OSPF. A minimum of one and a maximum of 16 threshold levels is supported.

Threshold levels configured per node is inherited by all configured RSVP interfaces. Threshold levels defined under the RSVP interface is used to trigger IGP updates if non-default threshold levels are configured.

The **no** form of this command resets te-down-threshold to its default value.

Default no te-down-threshold (equals following values 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0)

Parameters *threshold-level* — Specifies the threshold level.

Values 0 to 100

Platforms All

24.50 te-link

te-link

Syntax [**no**] **te-link** *te-link-id*

Context **[Tree]** (config>router>lmp>peer te-link)

Full Context configure router lmp peer te-link

Description This command assigns a Traffic Engineering (TE) Link to a given LMP peer. The TE Link with ID *te-link-id* must already have been created under **config>router>lmp>te-link**.

Default no te-link

Parameters *te-link-id* — Specifies the ID of the TE Link.

Values 1 to 4294967295 | *te-link-name te-link-name*: 32 character (max) name of the TE Link

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

te-link

Syntax [**no**] **te-link** *te-link-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>lmp te-link)

Full Context configure router lmp te-link

Description This command creates a Traffic Engineering (TE) Link in LMP across a GMPLS UNI. An unsigned integer TE link ID must be specified when the TE Link is first created. Once the link is created, the user can configure the link name (that is 'link-name te-link-name'). From here, the user can refer to this TE Link by either the unsigned integer or the ASCII name.

Default no te-link

Parameters *te-link-id* — Specifies the ID of the TE Link.

Values 1 to 4294967295 | *te-link-name te-link-name*: 32 character (max) name of the TE Link

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

te-link

Syntax [**no**] **te-link** *te-link-id*

Context [Tree] (config>router>gmpls te-link)

Full Context configure router gmpls te-link

Description This command enables the use of a Traffic Engineering (TE) Link (which has previously been configured under **config>router>lmp**) in GMPLS.

The **no** form of this command resets the configuration to the default value.

Default no te-link

Parameters *te-link-id* — Specifies the ID or name of the configured TE Link.

Values 1 to 4294967295 | *te-link-name te-link-name*: 32 character maximum name of the TE Link

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.51 te-metric

te-metric

Syntax **te-metric** *value*
no te-metric

Context [Tree] (config>router>mpls>interface te-metric)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router mpls interface te-metric

Description This command configures the TE metric used on the interface. This metric is in addition to the interface metric used by IGP for the shortest path computation.

This metric is flooded as part of the TE parameters for the interface using an opaque LSA or an LSP. The IS-IS TE metric is encoded as sub-TLV 18 as part of the extended IS reachability TLV. The metric value is encoded as a 24-bit unsigned integer. The OSPF TE metric is encoded as a sub-TLV Type 5 in the Link TLV. The metric value is encoded as a 32-bit unsigned integer.

When the use of the TE metric is enabled for an LSP, CSPF will first prune all links in the network topology which do not meet the constraints specified for the LSP path. Such constraints include bandwidth, admin-groups, and hop limit. Then, CSPF will run an SPF on the remaining links. The shortest path among the all SPF paths will be selected based on the TE metric instead of the IGP metric which is used by default.

The TE metric in CSPF LSP path computation can be configured by entering the command **config>router>mpls>lsp>metric-type te**.

Note that the TE metric is only used in CSPF computations for MPLS paths and not in the regular SPF computation for IP reachability.

The **no** form of this command reverts to the default value.

Default no te-metric

The value of the IGP metric is advertised in the TE metric sub-TLV by IS-IS and OSPF.

Parameters *value* — Specifies the metric value.

Values 1 to 16777215

Platforms All

24.52 te-threshold-update

te-threshold-update

Syntax [**no**] **te-threshold-update**

Context **[Tree]** (config>router>rsvp te-threshold-update)

Full Context configure router rsvp te-threshold-update

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command is used to control threshold-based IGP TE updates. The **te-threshold-update** command must enable IGP TE update based only on bandwidth reservation thresholds per interface and must block IGP TE update on bandwidth changes for each reservation. Threshold levels can be defined using the **te-up-threshold** and **te-down-threshold** commands at the global RSVP or per-interface level.

The **no** form of this command should reset te-threshold-update to the default value and disable threshold based update.

Default no te-threshold-update

Platforms All

te-threshold-update

Syntax **te-threshold-update**
no te-threshold-update

Context **[Tree]** (debug>router>rsvp>event te-threshold-update)
[Tree] (debug>router>rsvp>interface>event te-threshold-update)

Full Context debug router rsvp event te-threshold-update
debug router rsvp interface event te-threshold-update

Description This command debugs the TE threshold update and the dark bandwidth threshold events.

The **no** form of this command disables the debugging.

Platforms All

24.53 te-up-threshold

te-up-threshold

Syntax **te-up-threshold** *threshold-level* [*threshold-level*]
no te-up-threshold

Context **[Tree]** (config>router>rsvp te-up-threshold)
[Tree] (config>router>rsvp>interface te-up-threshold)

Full Context configure router rsvp interface te-up-threshold
configure router rsvp te-up-threshold

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the specific threshold levels per node and per interface. Threshold levels are for reserved bandwidth per interface. The **te-threshold-update** command is used to enable or disable threshold-based IGP TE updates. Any reserved bandwidth change per interface is compared with all the threshold levels and trigger an IGP TE update if a defined threshold level is crossed in either direction (LSP setup or teardown). Threshold-based updates must be supported with both ISIS and OSPF. A minimum of one and a maximum of 16 threshold levels must be supported.

Threshold levels configured per node is inherited by all configured RSVP interfaces. Threshold levels defined under the RSVP interface is used to trigger IGP updates if non-default threshold levels are configured.

The **no** form of this command resets te-up-threshold to its default value.

Default no te-up-threshold (equals values of 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100)

Parameters *threshold-level* — Specifies the threshold level.

Values 0 to 100

Platforms All

24.54 tech-support

tech-support

Syntax **tech-support** [*file-url*]

Context **[Tree]** (admin tech-support)
[Tree] (admin>satellite>eth-sat tech-support)

Full Context admin satellite eth-sat tech-support
admin tech-support

Description This command creates a system core dump. If the *file-url* is omitted, and a *ts-location* is defined, then the **tech support** file will have an automatic SR OS generated file name based on the system name and the date and time and will be saved to the directory indicated by the configured *ts-location*.

The format of the auto-generated filename is ts-XXXXX.YYYYMMDD.HHMMUTC.dat where:

- XXXXX: system name with special characters expanded to avoid problems with file systems (for example, a '.' is expanded to %2E.)
- YYYYMMDD: Date with leading zeros on year, month and day
- HHMM: Hours and Minutes in UTC time (24hr format, always 4 chars, with leading zeros on hours and minutes)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note: This command should only be used with authorized direction of Nokia support.

Parameters *file-url* — Specifies the file URL location to save the binary file.

Values

local-url | *remote-url*	
local-url	[*cflash-id*/][*file-path*] 200 chars max, including cflash-id directory length 99 chars max each
remote-url	[{ftp:// | tftp://}*login:pswd@remote-locn*/][*file-path*] 199 chars max
remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - 32 chars max, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- admin satellite eth-sat tech-support

All

- admin tech-support

24.55 tei-set

tei-set

Syntax [**no**] **tei-set**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms tei-set)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms tei-set)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms tei-set)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms tei-set
configure mcast-management multicast-info-policy bundle channel video analyzer alarms tei-set
configure mcast-management multicast-info-policy bundle video analyzer alarms tei-set

Description This command configures the analyzer to check for TEI set errors.

Default no tei-set

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

24.56 teid-load-balancing

teid-load-balancing

Syntax [**no**] **teid-load-balancing**

Context **[Tree]** (config>service>vpls>load-balancing teid-load-balancing)
[Tree] (config>service>template>vpls-template>load-balancing teid-load-balancing)

Full Context configure service template vpls-template load-balancing teid-load-balancing
configure service vpls load-balancing teid-load-balancing

Description This command enables inclusion of TEID in hashing for GTP-U/C encapsulates traffic for GTPv1/GTPv2. The **no** form of this command ignores TEID in hashing.

Default no teid-load-balancing

Platforms All

teid-load-balancing

Syntax [**no**] **teid-load-balancing**

Context **[Tree]** (config>service>ies>if>load-balancing teid-load-balancing)

Full Context configure service ies interface load-balancing teid-load-balancing

Description This command enables inclusion of TEID in hashing for GTP-U/C encapsulates traffic for GTPv1/GTPv2. The **no** form of this command ignores TEID in hashing.

Default no teid-load-balancing

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

teid-load-balancing

Syntax [**no**] **teid-load-balancing**

Context **[Tree]** (config>service>vprn>if>load-balancing teid-load-balancing)
[Tree] (config>service>vprn>nw-if>load-balancing teid-load-balancing)

Full Context configure service vprn interface load-balancing teid-load-balancing
configure service vprn network-interface load-balancing teid-load-balancing

Description This command enables inclusion of TEID in hashing for GTP-U/C encapsulates traffic for GTPv1/GTPv2.

The **no** form of this command ignores TEID in hashing.

Default no teid-load-balancing

Platforms All

teid-load-balancing

Syntax [**no**] **teid-load-balancing**

Context **[Tree]** (config>router>if>load-balancing teid-load-balancing)

Full Context configure router interface load-balancing teid-load-balancing

Description This command enables inclusion of TEID in hashing for GTP-U/C encapsulates traffic for GTPv1/GTPv2. The **no** form of this command ignores TEID in hashing.

Default no teid-load-balancing

Platforms All

24.57 telemetry

telemetry

Syntax **telemetry**

Context **[Tree]** (config>system telemetry)
[Tree] (admin>system telemetry)

Full Context admin system telemetry
configure system telemetry

Description Commands in this context configure the dial-out telemetry commands.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

24.58 telemetry-data

telemetry-data

Syntax [**no**] **telemetry-data**

Context **[Tree]** (config>system>security>management-interface>output-authorization telemetry-data)

Full Context configure system security management-interface output-authorization telemetry-data

Description This command controls output authorization of telemetry configuration and state data in gNMI Subscribe RPC responses.

When enabled, telemetry data output authorization is performed, which may significantly increase the system response time with command authorization requests, especially when remote AAA servers are used.

By default, authorization checks are not performed for telemetry data.

The **no** form of this command reverts to the default value.

Default no telemetry-data

Platforms All

24.59 telnet

telnet

Syntax **telnet** {*ip-address* | *dns-name*} [*port*] **service-name** *service-name* [**source** *ip-address*]
telnet {*ip-address* | *dns-name*} [*port*] [**router** *router-instance*] [**source** *ip-address*]

Context **[Tree]** (global telnet)

Full Context global telnet

Description This command opens a Telnet session to a remote host. In SR-series networks, the Telnet servers limit Telnet clients to three login attempts; if unsuccessful, the Telnet client session is disconnected. The number is not user configurable.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If a source address is specified, it is used for the source IP address in the originated IP packets for the Telnet session.

Parameters *ip-address* — Specifies the IP address or the DNS name (if DNS name resolution is configured).

Values

ipv4-address	*a.b.c.d*	
ipv6-address	*x:x:x:x:x:x:x:x*[-interface]	*x*: [0 to FFFF]H
	x:x:x:x:x:x:d.d.d.d[-interface]	*d*: [0 to 255]D *ipv6-address* interface: up to 32 characters, mandatory for link local addresses
dns-name	up to 128 characters	

Note: IPv6 applies to the 7750 SR and 7950 XRS.

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 128 characters.

port — Specifies the TCP port number to use Telnet to the remote host, expressed as a decimal integer.

Values 1 to 65535

Default 23

router-instance — Specifies the router name or service ID used to identify the router instance.

Values

router-instance: *router-name* or *vprn-svc-id*

router-name	“Base”, “management”, vpls-management”
vprn-svc-id	1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

source *ip-address* — Specifies the source IP address to use as the source of the Telnet packets.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x
	x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0 to FFFF]H
d: [0 to 255]

telnet

Syntax **telnet**

Context **[Tree]** (config>system>login-control telnet)

Full Context configure system login-control telnet

Description This command creates the context to configure the Telnet login control parameters.

Platforms All

24.60 telnet-max-sessions

telnet-max-sessions

Syntax **telnet-max-sessions** *number-of-sessions*
no telnet-max-sessions

Context **[Tree]** (config>system>security>cli-session-group telnet-max-sessions)
[Tree] (config>system>security>profile telnet-max-sessions)

Full Context configure system security cli-session-group telnet-max-sessions
configure system security profile telnet-max-sessions

Description This command is used to limit the number of Telnet-based CLI sessions available to all users that are part of a particular profile, or to all users of all profiles that are part of the same cli-session-group.

The **no** form of this command disables the command and the profile/group limit is not applied on the number of sessions.

Default no telnet-max-sessions

Parameters *number-of-sessions* — Specifies the maximum number of allowed Telnet-based CLI sessions.

Values 0 to 50

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.61 telnet-reply

telnet-reply

Syntax [**no**] **telnet-reply**

Context **[Tree]** (config>service>ies>if>ipv6>vrrp telnet-reply)

Full Context configure service ies interface ipv6 vrrp telnet-reply

Description This command enables the non-owner master to reply to TCP port 23 Telnet requests directed at the virtual router instances IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet requests regardless of the telnet-reply configuration.

The **telnet-reply** command is only available in non-owner VRRP nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

Default no telnet-reply

Platforms All

telnet-reply

Syntax [**no**] **telnet-reply**

Context **[Tree]** (config>service>ies>if>vrrp telnet-reply)

Full Context configure service ies interface vrrp telnet-reply

Description The telnet-reply command enables the non-owner master to reply to TCP port 23 Telnet Requests directed at the virtual router instances IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet Requests regardless of the telnet-reply configuration.

The telnet-reply command is only available in non-owner VRRP nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

Default no telnet-reply

Platforms All

telnet-reply

Syntax [**no**] **telnet-reply**

Context **[Tree]** (config>service>vprn>if>vrrp telnet-reply)
[Tree] (config>service>vprn>if>ipv6>vrrp telnet-reply)

Full Context configure service vprn interface ipv6 vrrp telnet-reply
configure service vprn interface vrrp telnet-reply

Description This command enables the non-owner master to reply to TCP port 23 Telnet Requests directed at the virtual router instance's IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet Requests regardless of the telnet-reply configuration.

The telnet-reply command is only available in non-owner **VRRP** nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

Default no telnet-reply

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

telnet-reply

Syntax [**no**] **telnet-reply**

Context **[Tree]** (config>router>if>vrrp telnet-reply)
[Tree] (config>router>if>ipv6>vrrp telnet-reply)

Full Context configure router interface ipv6 vrrp telnet-reply
configure router interface vrrp telnet-reply

Description This command enables the non-owner master to reply to TCP port 23 Telnet requests directed at the virtual router instances' IP addresses.

Non-owner virtual router instances are limited by the VRRP specifications to responding to ARP requests destined to the virtual router IP addresses and routing IP packets not addressed to the virtual router IP addresses. Many network administrators find this limitation frustrating when troubleshooting VRRP connectivity issues.

This limitation can be disregarded for certain applications. Ping, SSH and Telnet can each be individually enabled or disabled on a per-virtual-router-instance basis.

The **telnet-reply** command enables the non-owner master to reply to Telnet requests directed at the virtual router instances' IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Correct login and CLI command authentication is still enforced.

When **telnet-reply** is not enabled, Telnet requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet requests regardless of the **telnet-reply** setting.

The **telnet-reply** command is only available in non-owner **vrrp** nodal context.

By default, Telnet requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of the command configures discarding all Telnet request messages destined to the non-owner virtual router instance IP addresses.

Default no telnet-reply — Telnet requests to the virtual router instance IP addresses are discarded.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.62 telnet-server

telnet-server

Syntax [**no**] **telnet-server**

Context **[Tree]** (config>system>security telnet-server)

Full Context configure system security telnet-server

Description This command enables Telnet servers running on the system.

Telnet servers are shut down by default. At system startup, only SSH servers are enabled.

Telnet servers in networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries.

The **no** form of this command disables Telnet servers running on the system.

Platforms All

24.63 telnet6-server

telnet6-server

Syntax [**no**] **telnet6-server**

Context **[Tree]** (config>system>security telnet6-server)

Full Context configure system security telnet6-server

Description This command enables Telnet IPv6 servers running on the system and only applies to the 7750 SR and 7950 XRS.

Telnet servers are shut down by default. At system startup, only SSH servers are enabled.

The **no** form of this command disables Telnet IPv6 servers running on the system.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.64 temp-flooding

temp-flooding

Syntax **temp-flooding flood-time**
no temp-flooding

Context **[Tree]** (config>service>vpls temp-flooding)
[Tree] (config>service>template>vpls-template temp-flooding)

Full Context configure service template vpls-template temp-flooding
configure service vpls temp-flooding

Description The temporary flooding is designed to minimize failover times by eliminating the time it takes to flush the MAC tables and if MVRP is enabled the time it takes for MVRP registration. Temporary flooding is initiated only upon xSTP TCN reception. During this procedure while the MAC flush takes place the frames received on one of the VPLS SAPs/pseudowires are flooded in a VPLS context which for MVRP case includes also the unregistered MVRP trunk ports. The MAC Flush action is initiated by the STP TCN reception or if MVRP is enabled for the data VPLS, by the reception of a MVRP New message for the SVLAN ID associated with the data VPLS. As soon as the MAC Flush is done, regardless of whether the temp-flooding timer expired or not, traffic will be delivered according to the regular FDB content which may be built from MAC Learning or based on MVRP registrations. This command provides a flood-time value that configures a fixed amount of time, in seconds, during which all traffic is flooded (BUM or known unicast) as a safety mechanism. Once the flood-time expires, traffic will be delivered according to the regular FDB content which may be built from MAC Learning or based on MVRP registrations. The temporary flooding timer should be configured in such a way to allow auxiliary processes like MAC Flush, MMRP and/or MVRP to complete/converge. The temporary flooding behavior applies to regular VPLS, VPLS instantiated with VPLS-template, IVPLS and BVPLS when MMRP is disabled.

The **no** form of this command disables the temporary flooding behavior.

Default no temp-flooding

Parameters *flood-time* — Specifies the flood time, in seconds

Values 3 to 600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.65 template

template

Syntax **template**

Context **[Tree]** (config>service template)

Full Context configure service template

Description This is the node for service templates.

Platforms All

template

Syntax **template**

Context **[Tree]** (config>app-assure>group>cflowd>comp template)
[Tree] (config>app-assure>group>cflowd>tcp-perf template)
[Tree] (config>app-assure>group>cflowd>volume template)

Full Context configure application-assurance group cflowd comprehensive template
configure application-assurance group cflowd tcp-performance template
configure application-assurance group cflowd volume template

Description Commands in this context configure the template for cflowd comprehensive, TCP performance, or volume fields.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

template

Syntax **template** *template-id*
no template

Context **[Tree]** (config>app-assure>group template)
[Tree] (config>app-assure>group>http-error-redirect template)

Full Context configure application-assurance group http-error-redirect template
configure application-assurance group template

Description This command refers to the template of parameters passed from the AA-ISA to the redirect server via JavaScript in the redirect packet. The template is specific to the redirect server being used in the network.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Currently, two partners are used and tested with AA-ISA redirect solution, Barefruit and Xerocole.

The **no** form of this command reverts to the default.

Parameters *template-id* — Specifies an HTTP error redirect template.

1 = Barefruit specific template

2 = xerocole specific template.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

template

Syntax **template** *value*
no template

Context **[Tree]** (config>app-assure>group>http-notif template)

Full Context configure application-assurance group http-notification template

Description This command configures the template which defines the format and parameters included in the http notification message.

The **no** form of this command removes the template from the configuration.

Default no template

Parameters *value* — Specifies the template id of this HTTP Notification.

Values 1 — Javascript-url with SubID and optional Http-Url-Param

2 — Javascript-url and optional Http-Url-Param

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

template

Syntax **template** *template-id*
no template

Context **[Tree]** (config>app-assure>group>http-redirect template)

Full Context configure application-assurance group http-redirect template

Description This command configures the template that defines which parameters are appended to the HTTP host redirect field in the redirect message.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The HTTP redirect template provides HTTP 302 redirect containing only the URL specified in the redirect policy, with no other parameters.

The **no** form of this command removes the template from the configuration.

Default no template

Parameters *template-id* — Specifies the HTTP Policy Redirect template.

Values
1 — Javascript based redirect embedded in HTTP 200 OK response with a predefined number of arguments automatically appended to the redirect URL
2 — HTTP 302 Redirect with a predefined number of arguments automatically appended to the redirect URL.
3 — HTTP 302 Redirect with no parameters appended to the URL (empty).
4 — Empty Redirect format using Javascript.
5 — Redirect supporting macro substitution using HTTP 302.
6 — Redirect supporting macro substitution using Javascript.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

template

Syntax [**no**] **template** *template-name*

Context **[Tree]** (config>router>bier template)

Full Context configure router bier template

Description This command creates a BIER template to be assigned to IGP.

The **no** form of this command removes a specific template.

Parameters *template-name* — The name of the template to be created or removed, up to 32 characters.

Platforms All

template

Syntax [**no**] **template** *name*

Context **[Tree]** (config>router>route-next-hop-policy template)

Full Context configure router route-next-hop-policy template

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command creates a template to configure the attributes of a Loop-Free Alternate (LFA) Shortest Path First (SPF) policy. An LFA SPF policy allows the user to apply specific criteria, such as admin group and SRLG constraints, to the selection of an LFA backup next-hop for a subset of prefixes that resolve to a specific primary next-hop.

The user first creates a route next-hop policy template under the global router context and then applies it to a specific OSPF or IS-IS interface in the global routing instance or in a VPRN instance.

A policy template can be used in both IS-IS and OSPF to apply the specific criteria to prefixes protected by LFA. Each instance of IS-IS or OSPF can apply the same policy template to one or more interface.

The commands within the route next-hop policy template use the **begin-commit-abort** model. The following are the steps to create and modify the template:

To create a template, the user enters the name of the new template directly under the route-next-hop-policy context.

1. To delete a template that is not in use, the user enters the **no** form for the template name under the route-next-hop-policy context.
2. The user enters the editing mode by executing the begin command under the route-next-hop-policy context. The user can then edit and change any number of route next-hop policy templates. However, the parameter value will still be stored temporarily in the template module until the commit is executed under the route-next-hop-policy context. Any temporary parameter changes will be lost if the user enters the abort command before the commit command.
3. The user is allowed to create or delete a template instantly once in the editing mode without the need to enter the commit command. Furthermore, the abort command, if entered, will have no effect on the prior deletion or creation of a template.

Once the commit command is issued, IS-IS or OSPF will re-evaluate the templates and if there are any net changes, it will schedule a new LFA SPF to re-compute the LFA next-hop for the prefixes associated with these templates.

Parameters *name* — Specifies the name of the template, up to 32 characters.

Platforms All

template

Syntax **template** *template-name*
no template

Context **[Tree]** (config>router>isis>level>bier template)

Full Context configure router isis level bier template

Description This command assigns a BIER template to an IS-IS level.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes templates from the IS-IS level.

Parameters *template-name* — Specifies the BIER template name.

Platforms All

template

Syntax **template** *template-name*
no template

Context **[Tree]** (config>router>ospf>area>bier template)

Full Context configure router ospf area bier template

Description This command configures an OSPF BIER template at the OSPF area level.

The **no** form of this command removes templates from the OSPF area.

Parameters *template-name* — The name of the template, up to 32 characters.

Platforms All

24.66 template-format

template-format

Syntax **template-format** {**format1** | **format2**}
no template-format

Context **[Tree]** (config>service>ipfix>ipfix-export-policy template-format)

Full Context configure service ipfix ipfix-export-policy template-format

Description This command selects one of two template formats that contains a set of element IDs and their interpretation in IPFIX NAT flow logging. The difference between the two formats is related to the fields conveying information about the translated source IP addresses and ports (outside IP addresses and ports). Further, format 1 conveys information about the translated source port (post NAT) in the sourceTransportPort information element while format 2 conveys this information in the postNAPTsourceTrasportPort element.

Further, format1 conveys information about the translated source port (post NAT) in the information element sourceTransportPort while a new information element postNAPTsourceTrasportPort is introduced in format2 to carry this information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

For more information about template formats, refer to “Template Formats” in the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter and Extended Services Appliance Guide*, where the table lists supported information elements and their description for each format.

The **no** form of the command reverts to the default value.

Default template-format format1

Parameters **format1** — Specifies that template format 1 is used by the IPFIX collectors associated with this IPFIX Export policy.

format2 — Specifies that template format 2 is used by the IPFIX collectors associated with this IPFIX Export policy.

Platforms All

24.67 template-refresh-timeout

template-refresh-timeout

Syntax **template-refresh-timeout** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**days** *days*]
no template-refresh-timeout

Context **[Tree]** (config>service>ipfix>export-policy>collector template-refresh-timeout)

Full Context configure service ipfix ipfix-export-policy collector template-refresh-timeout

Description This command configures the time interval in which Template Set messages are sent to the collector node. Template sets is an IPFIX message that defines fields for subsequent IPFIX messages but contains no data of its own. In other words, IPFIX data is not passed as set of TLVs, but instead data is encoded with a scheme defined through the Template Set message.

Default template-refresh-timeout min 10

Parameters *hours* — Specifies the time interval, in hours, after which IPFIX templates are resent to this collector.

Values 1 to 24

minutes — Specifies the time interval, in minutes, after which IPFIX templates are resent to this collector.

Values 1 to 59

seconds — Specifies the time interval, in seconds, after which IPFIX templates are resent to this collector.

Values 1 to 59

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

days — Specifies the time interval, in days, after which IPFIX templates are resent to this collector.

Values 1

Platforms All

24.68 template-retransmit

template-retransmit

Syntax **template-retransmit** *seconds*
no template-retransmit

Context **[Tree]** (config>app-assure>group>cflowd template-retransmit)

Full Context configure application-assurance group cflowd template-retransmit

Description This command configures the period of time, in seconds, for the template to be retransmitted.

Default template-retransmit 600

Parameters *seconds* — Specifies the time period for the template to be retransmitted.

Values 10 to 600

Default 600

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

template-retransmit

Syntax **template-retransmit** *seconds*
no template-retransmit

Context **[Tree]** (config>cflowd template-retransmit)

Full Context configure cflowd template-retransmit

Description This command specifies the interval for sending template definitions.

Default template-retransmit 600

Parameters *seconds* — Specifies the value expressed in seconds before sending template definitions.

Values 10 to 600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.69 template-set

template-set

Syntax **template-set** {**basic** | **mpls-ip** | **l2-ip** | **mpls-transport**}

Context **[Tree]** (config>cflowd>collector template-set)

Full Context configure cflowd collector template-set

Description This command specifies the set of templates sent to the collector when using cflowd Version 9 or Version 10.

Default template-set basic

Parameters **basic** — Specifies that basic flow data is sent.

mpls-ip — Specifies that extended flow data is sent that includes IP and MPLS flow information.

If the sampled traffic is part of a locally configured service or IPv4 or IPv6 traffic is being forwarded with an MPLS shortcut, then the MPLS labels associated with that service encapsulation are included in the extended flow data for both network ingress and egress sampling.

l2-ip — Specifies that extended flow data is sent that includes Layer 2 (Ethernet) and IP flow information. This template is only applicable for V10 (IPFIX) collectors.

mpls-transport — Specifies that cflowd can collect flow statistics for MPLS traffic using only the outer transport label, EXP bit value, and ingress interface as the flow identifier. This template enables the collection of flow statistics on a core router to develop LSP usage statistics.

Platforms All

24.70 terminal

terminal

Syntax **terminal**
no terminal

Context **[Tree]** (environment terminal)

Full Context environment terminal

Description Commands in this context configure the terminal screen length for the current CLI session.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

24.71 terminate

terminate

Syntax [**no**] **terminate**

Context **[Tree]** (config>service>apipe>sap>atm>oam terminate)

Full Context configure service apipe sap atm oam terminate

Description This command specifies whether this SAP will act as an OAM termination point. ATM SAPs can be configured to tunnel or terminate OAM cells.

When configured to not terminate (the default is **no terminate**), the SAP will pass OAM cells through the VLL without inspecting them. The SAP will respond to OAM loopback requests that are directed to the local node by transmitting a loopback reply. Other loopback requests are transparently tunneled through the pseudowire. In this mode, it is possible to launch a loopback request toward the directly-attached ATM equipment and see the results of the reply.

When configured to terminate, the SAP will respond to AIS by transmitting RDI and will signal the change of operational status to the other endpoint (for example, through LDP status notifications). The SAP will respond to OAM loopback requests by transmitting a loopback reply. In this mode, it is possible to launch a loopback request toward the directly-attached ATM equipment and see the results of the reply.

For Apipe services, the user has the option of enabling or disabling this option for VC types atm-vcc and atm-sdu since these service types maintain the ATM layer and/or the AAL5 layer across the VLL. It is not supported on atm-vpc and atm-cell apipe vc types since the VLL must pass the VC level (F5) OAM cells.

The **terminate** option for OAM is the only and default mode of operation supported for an ATM SAP which is part of Epipe, Ipipe, VPLS, and IES/VPRN. This is because the ATM and AAL5 layers are terminated.

For Apipe services, the user has the option of enabling or disabling this option for vc types atm-vcc and atm-sdu since these service types maintain the ATM layer and/or the AAL5 layer across the VLL. It is not supported on atm-vpc and atm-cell Apipe vc types since the VLL must pass the VC level (F5).

The **terminate** option for OAM is the only and default mode of operation supported for an ATM SAP which is part of Epipe, Ipipe, VPLS, and IES/VPRN. This is because the ATM and AAL5 layers are terminated.

Default no terminate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

24.72 termination-fpe

termination-fpe

Syntax **termination-fpe** *termination-fpe*
no termination-fpe

Context **[Tree]** (config>router>segment-routing>srv6>locator termination-fpe)

Full Context configure router segment-routing segment-routing-v6 locator termination-fpe

Description This command associates the FPE ID to the locator for termination of SRv6 in local services. One or more FPEs can be configured for SRv6 termination, where a termination SRv6 FPE is assigned one or more configured locators.

The **no** form of this command removes the association.

Parameters *termination-fpe* — Specifies the FPE ID for SRv6 termination.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

24.73 tertiary

tertiary

Syntax **tertiary**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol tertiary)

Full Context configure subscriber-mgmt sub-ident-policy tertiary

Description Commands in this context configure tertiary identification script parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.74 tertiary-config

tertiary-config

Syntax **tertiary-config** *file-url*
no tertiary-config

Context **[Tree]** (bof tertiary-config)

Full Context bof tertiary-config

Description This command specifies the name and location of the tertiary configuration file.

The system attempts to use the configuration specified in **tertiary-config** if both the primary and secondary config files cannot be located. If this file cannot be located, the system boots with the factory default configuration.

Note that if an error in the configuration file is encountered, the boot process aborts.

The **no** form of this command removes the **tertiary-config** configuration.

Parameters *file-url* — Specifies the tertiary configuration file location, expressed as a file URL.

Values

file-url	{*local-url* | *remote-url*} (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

24.75 tertiary-dns

tertiary-dns

Syntax **tertiary-dns** *ip-address*
no tertiary-dns

Context **[Tree]** (config>service>vprn>dns tertiary-dns)

Full Context configure service vprn dns tertiary-dns

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the tertiary DNS server for DNS name resolution. The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of this command removes the tertiary DNS server from the configuration.

Default no tertiary-dns — No tertiary DNS server is configured.

Parameters *ip-address* — The IP or IPv6 address of the tertiary DNS server.

Values

ipv4-address -a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x: [0 to FFFF]H
d: [0 to 255]D
interface - 32 characters max, for link local addresses.

Platforms All

tertiary-dns

Syntax **tertiary-dns** *ip-address*
no tertiary-dns [*ip-address*]

Context **[Tree]** (bof tertiary-dns)

Full Context bof tertiary-dns

Description This command configures the tertiary DNS server for DNS name resolution. The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of this command removes the tertiary DNS server from the configuration.

Default no tertiary-dns

Parameters *ip-address* — Specifies the IP or IPv6 address of the tertiary DNS server.

Values

ipv4-address	a.b.c.d
ipv6-address	*x:x:x:x:x:x:x:x*[-interface]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	x:x:x:x:x:x:d.d.d.d[-interface] *x*: [0 to FFFF]H *d*: [0 to 255]D
interface	32 chars max, for link local addresses

Note: IPv6 is applicable to the 7750 SR and 7950 XRS only.

Platforms All

24.76 tertiary-image

tertiary-image

Syntax **tertiary-image** *file-url*
no tertiary-image

Context **[Tree]** (bof tertiary-image)

Full Context bof tertiary-image

Description This command specifies the tertiary directory location for runtime image file loading.

The system attempts to load all runtime image files configured in the **primary-image** first. If this fails, the system attempts to load the runtime images from the location configured in the **secondary-image**. If the secondary image load fails, the tertiary image specified in **tertiary-image** is used.

All runtime image files (*.tim files) must be located in the same directory.

The **no** form of this command removes the **tertiary-image** configuration.

Parameters *file-url* — Specifies the file URL; can be either local (this CPM) or a remote FTP server.

Values

file-url	{*local-url* | *remote-url*} (up to 180 characters)
local-url	[*cflash-id*/][*file-path*]
remote-url	[{ftp://| tftp://} *login:pswd@remote-locn*/][*file-path*]
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.77 tertiary-ip-address

tertiary-ip-address

Syntax **tertiary-ip-address** *ipv4-address*
no tertiary-ip-address

Context **[Tree]** (config>router>bgp>orr>location tertiary-ip-address)

Full Context configure router bgp optimal-route-reflection location tertiary-ip-address

Description This command specifies the tertiary IP address of a reference location used for BGP optimal route reflection. Up to three IPv4 addresses and three IPv6 addresses can be specified per location.

If the TE DB is unable to find a node in its topology database that matches the primary address, then the TE DB tries to find a node with the matching secondary address. If this attempt also fails, the TE DB then tries to find a node with the matching tertiary address.

The IP addresses specified for a location should be topologically “close” to a set of clients that should all receive the same optimal path for that location.

The **no** form of this command removes the tertiary IP address information.

Default no tertiary-ip-address

Parameters *ipv4-address* — Specifies the tertiary IPv4 address of a location, expressed in dotted decimal notation.

Values a.b.c.d

Platforms All

24.78 tertiary-ipv6-address

tertiary-ipv6-address

Syntax **tertiary-ipv6-address** *ipv6-address*
no tertiary-ipv6-address

Context **[Tree]** (config>router>bgp>orr>location tertiary-ipv6-address)

Full Context configure router bgp optimal-route-reflection location tertiary-ipv6-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the tertiary IPv6 address of a reference location used for BGP optimal route reflection. Up to three IPv4 addresses and three IPv6 addresses can be specified per location.

If the TE DB is unable find a node in its topology database that matches a primary address of the location, then it tries to find a node matching a secondary address. If this attempt also fails, the TE DB tries to find a node matching a tertiary address.

The IP addresses specified for a location should be topologically “close” to a set of clients that should all receive the same optimal path for that location.

The **no** form of this command removes the tertiary IPv6 address information.

Default no tertiary-ipv6-address

Parameters *ipv6-address* — Specifies the tertiary IPv6 address of a location.

Values ipv6-address:

- x:x:x:x:x:x:x:x (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d
- x: [0 to FFFF]H
- d: [0 to 255]D

Platforms All

24.79 tertiary-location

tertiary-location

Syntax **tertiary-location** *file-url*
no tertiary-location

Context **[Tree]** (config>system>software-repository tertiary-location)

Full Context configure system software-repository tertiary-location

Description This command configures the tertiary location for the files in the software repository. See the **software-repository** command description for more information.

The **no** form of the command removes the tertiary location.

Parameters *file-url* — Specifies the tertiary location to be used to access the files in the software repository.

Values

file url	*local-url* | *remote-url*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

local-url	[*cflash-id/*][*file-path*]	up to 200 characters, including cflash-id directory length 99 characters each
remote-url	[{ftp://} *login:pswd@remote-locn/*][*file-path*] 243 characters maximum directory length, up to 99 characters each	
	remote-locn	[*hostname* | *ipv4-address* | [*ipv6-address*]]
	ipv4-address	*a.b.c.d*
	ipv6-address	*x:x:x:x:x:x:x:x*[*-interface*] *x:x:x:x:x:x:d.d.d.d*[*-interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D *interface* - up to 32 characters, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:	

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.80 tertiary-url

tertiary-url

Syntax **tertiary-url** *url*
no tertiary-url

Context **[Tree]** (config>python>py-script tertiary-url)

Full Context configure python python-script tertiary-url

Description This command specifies the location of tertiary Python script. The system supports three locations for each Python-script. Users can store scripts file on either a local CF card or a FTP server.

The **no** form of this command removes the URL.

Parameters **url** — Specifies the tertiary URL of the Python script up to 180 characters, either a local CF card URL or a FTP server URL.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.81 test

test

Syntax [**no**] **test** *test-name* [**owner** *test-owner*]

Context **[Tree]** (config>saa test)

Full Context configure saa test

Description This command identifies a test and enables the context to provide the test parameters for the named test. After the creation of the test instance, the test can be started in the OAM context.

A test can only be modified while it is shut down.

The **no** form of this command removes the test from the configuration. To remove a test, it cannot be active at the time.

Parameters *test-name* — Identifies the SAA test name, up to 32 characters.

test-owner — Specifies the owner, up to 32 characters, of an SAA operation. If a value is not specified, the default owner is used.

Default "TiMOS CLI"

Platforms All

24.82 test-account

test-account

Syntax **test-account**

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>health-check test-account)

Full Context configure aaa radius-server-policy servers health-check test-account

Description This command sets up a test account as a probing mechanism to check the connectivity of all configured RADIUS authentication servers within the RADIUS server policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.83 test-completion-enable

test-completion-enable

Syntax [**no**] **test-completion-enable**

Context **[Tree]** (config>saa>test>trap-gen test-completion-enable)

Full Context configure saa test trap-gen test-completion-enable

Description This command enables the generation of a trap when an SAA test completes.

The **no** form of this command disables the trap generation.

Platforms All

24.84 test-duration

test-duration

Syntax **test-duration** *seconds*
no test-duration

Context **[Tree]** (config>oam-pm>session>ethernet>slm test-duration)
[Tree] (config>oam-pm>session>ethernet>dmm test-duration)
[Tree] (config>oam-pm>session>ethernet>lmm test-duration)

Full Context configure oam-pm session ethernet dmm test-duration
configure oam-pm session ethernet lmm test-duration
configure oam-pm session ethernet slm test-duration

Description This optional command defines the length of time the test runs before stopping automatically. This command is only a valid option when a session has been configured with a **session-type** of **on-demand**. This is not an option when the **session-type** is configured as **proactive**. On-demand tests do not start until the **config>oam-pm>session>start** command has been issued and they stop when the **config>oam-pm>session>stop** command is issued.

The **no** form of this command removes a previously configured test-duration and allow the test to run until manually stopped.

Parameters *seconds* — Specifies the number of seconds the test runs from its start time.

Values 1 to 86400

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

test-duration

Syntax **test-duration** *seconds*
no test-duration

Context **[Tree]** (config>oam-pm>session>ip>twamp-light test-duration)

Full Context configure oam-pm session ip twamp-light test-duration

Description This command defines the length of time the test runs before stopping automatically. This optional command is only valid when a session has been configured with a **session-type** of **on-demand**. This is not an option when the **session-type** is configured as **proactive**. On-demand tests do not start until the **config>oam-pm>session>start** command has been issued and they stop when the **config>oam-pm>session>stop** command is issued.

The **no** form of this command removes a previously configured test-duration value and allows the TWAMP Light test to execute until it is stopped manually.

Parameters *seconds* — Specifies the length of time, in seconds, that the TWAMP Light test runs.

Values 1 to 86400

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-duration

Syntax **test-duration** *seconds*
no test-duration

Context **[Tree]** (config>oam-pm>session>mpls>dm test-duration)

Full Context configure oam-pm session mpls dm test-duration

Description This command defines the length of time the test runs before stopping automatically. This command is only valid when a session has been configured with a **session-type** of **on-demand**. This is not an option when the **session-type** is configured as **proactive**.

On-demand tests do not start until the **oam-pm>session>start** command has been issued and they stops when scheduled or the **oam-pm>session>stop** command is issued.

The **no** form of this command removes a previously configured test-duration and allow the test to run until manually stopped.

Parameters *seconds* — Specifies the number of seconds the test runs from its start time.

Values 1 to 8640

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.85 test-fail-enable

test-fail-enable

Syntax [**no**] **test-fail-enable**

Context **[Tree]** (config>saa>test>trap-gen test-fail-enable)

Full Context configure saa test trap-gen test-fail-enable

Description This command enables the generation of a trap when a test fails. In the case of a ping test, the test is considered failed (for trap generation) if the number of failed probes is at least the value of the **test-fail-threshold** parameter.

The **no** form of this command disables the trap generation.

Platforms All

24.86 test-fail-threshold

test-fail-threshold

Syntax **test-fail-threshold** *threshold*
no test-fail-threshold

Context **[Tree]** (config>saa>test>trap-gen test-fail-threshold)

Full Context configure saa test trap-gen test-fail-threshold

Description This command configures the threshold for trap generation on test failure.

This command has no effect when **test-fail-enable** is disabled. This command is not applicable to SAA trace route tests.

The **no** form of this command returns the threshold value to the default.

Default test-fail-threshold 1

Parameters *threshold* — Specifies the number of consecutive test failures required to generate a trap.

Values 0 to 15

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.87 test-link

test-link

Syntax **test-link** *port-id*
no test-link

Context **[Tree]** (config>port>ml-bundle>ima>test-pattern-procedure test-link)

Full Context configure port multilink-bundle ima test-pattern-procedure test-link

Description This command specifies IMA members on which an IMA test pattern procedure is to be performed.

The **no** form of this command deletes the link from test-pattern procedure. The test-pattern procedure must be shutdown first.

Default no test-link

Parameters *port-id* — Specifies the port ID that verifies link connectivity within an IMA group.

Values

port-id	*slot*/*mda*/*port* [.*channel*]		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b
	aps-id	aps-*group-id*[.*channel*]	
		aps	keyword
		group-id	1 to 128

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.88 test-oam

test-oam

Syntax **test-oam**

Context **[Tree]** (config test-oam)

Full Context configure test-oam

Description Commands in this context configure Operations, Administration, and Maintenance (OAM) test parameters.

Platforms All

24.89 test-pattern

test-pattern

Syntax **test-pattern** *pattern*
no test-pattern

Context **[Tree]** (config>port>ml-bundle>ima>test-pattern-procedure test-pattern)

Full Context configure port multilink-bundle ima test-pattern-procedure test-pattern

Description This command specifies the transmit test pattern in an IMA group loopback operation. This value can only be changed when the **test-pattern-procedure** command is shut down.

The **no** form of this command restores the test-pattern to the default.

Default test-pattern 0

Parameters *pattern* — Specifies an integer taking the following values:

Values 0 to 255

Platforms 7450 ESS, 7750 SR-7/12/12e

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>eth-tunnel>path>eth-cfm>mep>eth-test-enable test-pattern)

Full Context configure eth-tunnel path eth-cfm mep eth-test-enable test-pattern

Description This command configures the test pattern for eth-test frames.

The **no** form of this command removes the values from the configuration.

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Default all-zeros

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context [Tree] (config>lag>eth-cfm>mep>eth-test test-pattern)
[Tree] (config>port>ethernet>eth-cfm>mep>eth-test test-pattern)
[Tree] (config>router>if>eth-cfm>mep>eth-test test-pattern)

Full Context configure lag eth-cfm mep eth-test-enable test-pattern
configure port ethernet eth-cfm mep eth-test-enable test-pattern
configure router interface eth-cfm mep eth-test-enable test-pattern

Description This command specifies the test pattern of the ETH-TEST frames. This does not have to be configured the same on the sender and the receiver.

The **no** form of this command reverts to the default values.

Default test-pattern all-zeros

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context [Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>eth-test-enable test-pattern)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>epipe>sap>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>eth-test-enable test-pattern)

Full Context configure service epipe sap eth-cfm mep eth-test-enable test-pattern
configure service epipe spoke-sdp eth-cfm mep eth-test-enable test-pattern
configure service ipipe sap eth-cfm mep eth-test-enable test-pattern

Description This command configures the test pattern for eth-test frames.

The **no** form of this command removes the values from the configuration.

Default test-pattern all-zeros

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context [Tree] (config>service>vpls>sap>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>eth-test-enable test-pattern)

Full Context configure service vpls mesh-sdp eth-cfm mep eth-test-enable test-pattern
configure service vpls sap eth-cfm mep eth-test-enable test-pattern
configure service vpls spoke-sdp eth-cfm mep eth-test-enable test-pattern

Description This command configures the test pattern for eth-test frames.

The **no** form of this command removes the values from the configuration.

Parameters **all-zeros** — Specifies to use all zeros in the test pattern

all-ones — Specifies to use all ones in the test pattern

crc-enable — Generates a CRC checksum

Default all-zeros

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no test-pattern

Context [Tree] (config>service>ies>if>sap>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>eth-test-enable test-pattern)

Full Context configure service ies interface sap eth-cfm mep eth-test-enable test-pattern
configure service ies interface spoke-sdp eth-cfm mep eth-test-enable test-pattern
configure service ies subscriber-interface group-interface sap eth-cfm mep eth-test-enable test-pattern

Description This command configures the test pattern for eth-test frames.

The **no** form of this command removes the values from the configuration.

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Default all-zeros

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep eth-test-enable test-pattern

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep eth-test-enable test-pattern
- configure service ies interface sap eth-cfm mep eth-test-enable test-pattern

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context [Tree] (config>service>vprn>if>sap>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>eth-test-enable test-pattern)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>eth-test-enable test-pattern)

Full Context configure service vprn interface sap eth-cfm mep eth-test-enable test-pattern
configure service vprn interface spoke-sdp eth-cfm mep eth-test-enable test-pattern
configure service vprn subscriber-interface group-interface sap eth-cfm eth-test-enable test-pattern

Description This command configures the test pattern for eth-test frames.

The **no** form of this command removes the values from the configuration.

Default test-pattern all-zeros

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — generates a CRC checksum.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context **[Tree]** (config>router>if>eth-cfm>mep>eth-test-enable test-pattern)

Full Context configure router interface eth-cfm mep eth-test-enable test-pattern

Description This command specifies the test pattern of the eth-test frames. The test pattern does not need to be configured the same on the transmitter and the receiver.

The **no** form of this command reverts to the default value.

Default test-pattern all-zeros

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>eth-test-enable test-pattern)

Full Context configure eth-ring path eth-cfm mep eth-test-enable test-pattern

Description This command configures the test pattern for eth-test frames.

The **no** form of the command removes the values from the configuration.

Default test-pattern all-zeros

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.90 test-pattern-procedure

test-pattern-procedure

Syntax **test-pattern-procedure**

Context **[Tree]** (config>port>ml-bundle>ima test-pattern-procedure)

Full Context configure port multilink-bundle ima test-pattern-procedure

Description Commands in this context configure IMA test pattern procedures. Note that this command and sub-commands are not saved in the router configuration between reboots.

Platforms 7450 ESS, 7750 SR-7/12/12e

24.91 tethering-detection

tethering-detection

Syntax **tethering-detection**

Context **[Tree]** (config>app-assure>group tethering-detection)

Full Context configure application-assurance group tethering-detection

Description Commands in this context configure tethering detection for the group. The **shutdown** and **no shutdown** commands are used in this context to enable or disable tethering detection.

Default tethering-detection shutdown

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.92 tethering-summary

tethering-summary

Syntax [**no**] **tethering-summary**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>statistics>aa-partition tethering-summary)

Full Context configure application-assurance group statistics aa-partition tethering-summary

Description This command enables tethering summary statistics collection within an aa-partition.

The **no** form of this command disables tethering summary statistics collection.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.93 third-party

third-party

Syntax [**no**] **third-party**

Context [Tree] (config>service>nat>pcp-server-policy>option third-party)

Full Context configure service nat pcp-server-policy option third-party

Description This command enables/disables support for the **third-party** option.

Default no third-party

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.94 third-party-nexthop

third-party-nexthop

Syntax **third-party-nexthop**
no third-party-nexthop

Context [Tree] (config>service>vprn>bgp third-party-nexthop)
[Tree] (config>service>vprn>bgp>group third-party-nexthop)
[Tree] (config>service>vprn>bgp>group>neighbor third-party-nexthop)

Full Context configure service vprn bgp group neighbor third-party-nexthop
configure service vprn bgp group third-party-nexthop
configure service vprn bgp third-party-nexthop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Use this command to enable the router to send third-party next-hop to EBGP peers in the same subnet as the source peer, as described in RFC 4271. If enabled when an IPv4 or IPv6 route is received from one EBGP peer and advertised to another EBGP peer in the same IP subnet, the BGP next-hop is left unchanged. Third-party next-hop is not done if the address family of the transport does not match the address family of the route.

The **no** form of this command prevents BGP from performing any third party next-hop processing toward any single-hop EBGP peers within the scope of the command. No third-party next-hop means the next-hop will always carry the IP address of the interface used to establish the TCP connection to the peer.

Default no third-party-nexthop

Platforms All

third-party-nexthop

Syntax **third-party-nexthop**
no third-party-nexthop

Context **[Tree]** (config>router>bgp third-party-nexthop)
[Tree] (config>router>bgp>group>neighbor third-party-nexthop)

Full Context configure router bgp group neighbor third-party-nexthop
configure router bgp third-party-nexthop

Description Use this command to enable the router to send third-party next-hop to EBGP peers in the same subnet as the source peer, as described in RFC 4271. If enabled when an IPv4 or IPv6 route is received from one EBGP peer and advertised to another EBGP peer in the same IP subnet, the BGP next-hop is left unchanged. Third-party next-hop is not done if the address family of the transport does not match the address family of the route.

The **no** form of this command prevents BGP from performing any third party next-hop processing toward any single-hop EBGP peers within the scope of the command. No third-party next-hop means the next-hop will always carry the IP address of the interface used to establish the TCP connection to the peer.

Default no third-party-nexthop

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.95 three-way-hello

three-way-hello

Syntax [**no**] **three-way-hello**

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>pim three-way-hello)

Full Context configure service vprn mvpn provider-tunnel inclusive pim three-way-hello

Description This command enables PIM three-way hello on the inclusive provider tunnel.

The **no** form of this command disables the PIM three-way hello.

Default disabled

Platforms All

three-way-hello

Syntax [**no**] **three-way-hello**

Context **[Tree]** (config>service>vprn>pim>if three-way-hello)

Full Context configure service vprn pim interface three-way-hello

Description This command configures the compatibility mode for enabling the three way hello.

Platforms All

three-way-hello

Syntax **three-way-hello** [**compatibility-mode**]
no three-way-hello

Context **[Tree]** (config>router>pim>interface three-way-hello)

Full Context configure router pim interface three-way-hello

Description This command sets the compatibility mode to enable three-way hello. By default, the value is disabled on all interface which specifies that the standard two-way hello is supported. When enabled, the three-way hello is supported.

The **no** form of this command disables three-way hello.

Default no three-way-hello

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

24.96 threshold

threshold

Syntax **threshold** *xpl-errors*

Context **[Tree]** (config>card>mda>egress-xpl threshold)

Full Context configure card mda egress-xpl threshold

Description This command configures the Egress XPL Error Threshold value used by the **fail-on-error** feature.

Default threshold 1000

Parameters *xpl-errors* — Specifies an upper limit on the frequency of Egress XPL Errors that can occur on the MDA. When **fail-on-error** is enabled, if the MDA experiences more than *xpl-errors* errors per minute for the specified number of minutes from the **window** *minutes* command, the MDA will be put in the failed state.

The threshold value cannot be changed while **fail-on-error** is enabled for this MDA.

Values 1 to 1000000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

threshold

Syntax **threshold** *xpl-errors*

Context **[Tree]** (config>card>mda>ingress-xpl threshold)

Full Context configure card mda ingress-xpl threshold

Description This command configures the Ingress XPL Error Threshold value used by the **fail-on-error** feature.

Default threshold 1000

Parameters *xpl-errors* — Specifies an upper limit on the frequency of Ingress XPL Errors that can occur on the MDA. When **fail-on-error** is enabled, if the MDA experiences more than *xpl-errors* errors per minute for the specified number of minutes from the **window** *minutes* command, the MDA will be put in the failed state.

The threshold value cannot be changed while **fail-on-error** is enabled for this MDA.

Values 1 to 1000000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

threshold

Syntax **threshold** *num-members*
no threshold

Context **[Tree]** (config>interface-group-handler threshold)

Full Context configure interface-group-handler threshold

Description This command identifies the minimum number of active links that must be present for the interface group handler to be active. A threshold of 1 effectively disables the effect of the interface group handler.

The **no** form of this command resets the threshold to 1.

Note that for APS configurations, if the ber-sd or ber-sf threshold rates must be modified, the changes must be performed at the line level on both the working and protect APS port member.

Default threshold 1

Parameters *num-members* — Specifies the minimum number of active links that must be present for the interface group handler to be active.

Values 1 to 8

Platforms All

threshold

Syntax **threshold** {**ber-sd** | **ber-sf**} **rate** *threshold-rate*
no threshold {**ber-sd** | **ber-sf**}

Context **[Tree]** (config>port>sonet-sdh threshold)

Full Context configure port sonet-sdh threshold

Description This command configures the line signal degradation bit error rate (BER) and line signal failure thresholds.

Line signal (b2) bit interleaved parity error rates are measured and when they cross either the degradation or failure thresholds alarms are raised (see the **report-alarm** command), furthermore if the failure threshold is crossed the link will be set to operationally down.

For APS configurations, if the **ber-sd** or **ber-sf** threshold rates must be modified, the changes must be performed at the line level on both the working and protect APS port member.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default threshold ber-sd rate 6 — Signal degrade BER threshold of 10-6.

threshold ber-sf rate 3 — Signal failure BER threshold of 10-3.

Parameters **ber-sd** — Specifies the BER that specifies signal degradation.

ber-sf — Specifies the BER that specifies signal failure.

threshold-rate — The BER negative exponent (n in 10-n), expressed as a decimal integer.

Values 3 to 9 (10-3 to 10-9) for ber-sd, 3 to 6 for ber-sf

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

threshold

Syntax **threshold** {**ber-sd** | **ber-sf**} **rate** {**1** | **5** | **10** | **50** | **100**}
no threshold {**ber-sd** | **ber-sf**}

Context **[Tree]** (config>port>tdm>ds1 threshold)
[Tree] (config>port>tdm>e1 threshold)

Full Context configure port tdm ds1 threshold
configure port tdm e1 threshold

Description This command configures the line signal degradation bit error rate (BER) and line signal failure thresholds.

Line signal (b2) bit interleaved parity error rates are measured and when they cross either the degradation or failure thresholds alarms are raised (see the **report-alarm** command), furthermore if the failure threshold is crossed the link will be set to operationally down.

The **no** form of this command reverts to the default value.

Default threshold ber-sd rate 5 threshold ber-sf rate 50

Parameters **ber-sd** — Specifies the BER that specifies signal degradation.

ber-sf — Specifies the BER that specifies signal failure.

rate — Specifies the number of errors, in millions.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

threshold

Syntax **threshold** *threshold*
no threshold

Context **[Tree]** (config>router>segment-routing>maintenance-policy threshold)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router segment-routing maintenance-policy threshold

Description This command configures the minimum number of S-BFD sessions that must be up in order to consider the SR policy candidate path to which the maintenance template is bound to be up. If it is below this number, then the policy candidate path is marked as BFD degraded by the system. This command is only valid in the **ecmp-protected** mode.

The **no** form of this command reverts to the default.

Default threshold 1

Parameters *threshold* — Specifies the minimum number of S-BFD sessions that must be up.

Values 1 to 32

Platforms All

threshold

Syntax **threshold**

Context **[Tree]** (config>test-oam>link-meas>template>asw threshold)
[Tree] (config>test-oam>link-meas>template>sw threshold)

Full Context configure test-oam link-measurement measurement-template aggregate-sample-window threshold
configure test-oam link-measurement measurement-template sample-window threshold

Description Commands in this context configure the applicable thresholds for the sample windows.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.97 threshold-crossing-alert

threshold-crossing-alert

Syntax **threshold-crossing-alert**

Context **[Tree]** (config>app-assure>group>statistics threshold-crossing-alert)

Full Context configure application-assurance group statistics threshold-crossing-alert

Description Commands in this context configure the generation of threshold crossing alerts (TCAs).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.98 thresholds

thresholds

Syntax **thresholds**

Context **[Tree]** (config>router>dhcp6>server>pool thresholds)
[Tree] (config>router>dhcp6>server>pool>prefix thresholds)
[Tree] (config>service>vprn>dhcp6>server>pool thresholds)
[Tree] (config>service>vprn>dhcp6>server>pool>prefix thresholds)

Full Context configure router dhcp6 local-dhcp-server pool prefix thresholds
configure router dhcp6 local-dhcp-server pool thresholds
configure service vprn dhcp6 local-dhcp-server pool prefix thresholds
configure service vprn dhcp6 local-dhcp-server pool thresholds

Description Commands in this context configure pool level thresholds.

Default thresholds

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

thresholds

Syntax **thresholds**

Context **[Tree]** (config>system thresholds)

Full Context configure system thresholds

Description Commands in this context configure monitoring thresholds.

Platforms All

24.99 throttle-rate

throttle-rate

Syntax **throttle-rate** *events* [**interval** *seconds*]
no throttle-rate

Context **[Tree]** (config>log throttle-rate)

Full Context configure log throttle-rate

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the number of events and interval length to be applied to all event types that have throttling enabled by the **event-control** command and do not have a **specific-throttle-rate** configured.

The **no** form of this command reverts to the default values.

Default throttle-rate 2000 interval 1

Parameters *events* — Specifies the number of log events that can be logged within the specified interval for a specific event. Once the limit has been reached, any additional events of that type will be dropped, for example, the event drop count will be incremented. At the end of the throttle interval if any events have been dropped a trap notification will be sent.

Values 1 to 20000

Default 2000

seconds — Specifies the number of seconds that an event throttling interval lasts.

Values 1 to 1200

Default 1

Platforms All

24.100 throughput-alarm

throughput-alarm

Syntax **throughput-alarm high-threshold** *Mbps* **low-threshold** *Mbps*
no throughput-alarm

Context **[Tree]** (config>li>x-interfaces>x3>alarms throughput-alarm)

Full Context configure li x-interfaces x3 alarms throughput-alarm

Description This command configures the thresholds for raising the throughput alarm. The throughput is shared with other ISA BB applications. The low threshold value must be configured with a smaller value than the high threshold.

The **no** form of this command reverts to the default values.

Parameters **high-threshold** *Mbps* — Specifies the high threshold value.

Values 1 to 4294967295

low-threshold *Mbps* — Specifies the low threshold value.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.101 ti-lfa

ti-lfa

Syntax **ti-lfa** [**max-sr-frr-labels** *value*]
no ti-lfa

Context **[Tree]** (config>router>isis>loopfree-alternates ti-lfa)

Full Context configure router isis loopfree-alternates ti-lfa

Description This command enables the use of the Topology-Independent LFA algorithm in the LFA SPF calculation for this ISIS instance.

The **no** form of this command disables the use of the Topology-Independent LFA algorithm in the LFA SPF calculation for this ISIS instance.

Default no ti-lfa

Parameters *value* — Specifies the maximum number of labels that the TI-LFA backup next-hop can use. The TI-LFA algorithm uses this value to limit the search for the Q node from the P node on the post-convergence path.

Values 0 to 3

Default 2

Platforms All

ti-lfa

Syntax **ti-lfa** [**max-sr-frr-labels** *value*]
no ti-lfa

Context **[Tree]** (config>router>ospf>loopfree-alternates ti-lfa)
[Tree] (config>router>ospf3>loopfree-alternates ti-lfa)

Full Context configure router ospf loopfree-alternates ti-lfa
configure router ospf3 loopfree-alternates ti-lfa

Description This command enables the use of the Topology-Independent LFA algorithm in the LFA SPF calculation in this OSPF or OSPF3 instance.

The **no** form of this command disables the use of the Topology-Independent LFA algorithm in the LFA SPF calculation in this OSPF or OSPF3 instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no ti-lfa

Parameters **max-sr-frr-labels [***value***]]** — Specifies the maximum number of labels that the TI-LFA backup next hop can use. The TI-LFA algorithm uses this value to limit the search for the Q node from the P node on the post-convergence path.

Values 0 to 3

Default 2

Platforms All

24.102 tier

tier

Syntax **tier** {**1** | **2**}

Context **[Tree]** (config>qos>policer-control-policy tier)

Full Context configure qos policer-control-policy tier

Description This command is used to create, configure, and delete tiered arbiters. Two tiers are supported that always exist, specified as tier 1 and tier 2. Tiered arbiters enable the creation of a bandwidth control hierarchy for managing child policers in an arbitrary fashion. Each arbiter enables parenting of child policers within eight strict levels of priority and a maximum aggregate rate may be defined for the children that the arbiter will enforce. Arbiters created on tier 1 are automatically parented to the root arbiter that is always present. Arbiters created on tier 2 default to the root arbiter as parent but can also be explicitly parented to a tier 2 arbiter. Child policers associated with an instance of the **policer-control-policy** can be parented to any tiered arbiter or to the root arbiter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

tier

Syntax [**no**] **tier** *tier*

Context **[Tree]** (config>qos>scheduler-policy tier)

Full Context configure qos scheduler-policy tier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command identifies the level of hierarchy that a group of schedulers are associated with. Within a tier level, a scheduler can be created or edited. Schedulers created within a tier can only be a child (take bandwidth from a scheduler in a higher tier). Tier levels increase sequentially with 1 being the highest tier. All tier 1 schedulers are considered to be root and cannot be a child of another scheduler. Schedulers defined in tiers other than 1 can also be root (parentless).

3 tiers (levels 1, 2, and 3) are supported.

The **save config** and **show config** commands only display information on scheduler tiers that contain defined schedulers. When all schedulers have been removed from a level, that level ceases to be included in output from these commands.

Parameters *tier* — This parameter is required to indicate the group of schedulers to create or be edited. Tier levels cannot be created or deleted. If a value for level is given that is out-of-range, an error will occur and the current context of the CLI session will not change.

Values 1 to 3

Platforms All

24.103 time

time

Syntax **time**

Context **[Tree]** (config>system time)

Full Context configure system time

Description Commands in this context configure the system time zone and time synchronization parameters.

Platforms All

24.104 time-average-factor

time-average-factor

Syntax **time-average-factor** *taf-value* [**dec-only**]
no time-average-factor

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>adv-config-policy>child-control>offered-measurement time-average-factor)

Full Context configure qos adv-config-policy child-control offered-measurement time-average-factor

Description This command is used to weight the new offered rate with a portion of the previous offered rate. It would be expected that this command would mainly be used with the dec-only option enabled.

The adjustment to the offered rate is performed using the following formula when taf-value is not set to '0':

Adjusted_Rate = ((Prev_Offered_Rate x (taf-value – 1)) + New_Offered_Rate) / taf-value

If the dec-only option is specified, the adjustment is only applied when New_Offered_Rate is less than the Prev_Offered_Rate. When taf-value is set to '0', the adjustment is never applied.

The **no** form of this command is used to remove the time average factor adjustments to new offered rate measurements.

Parameters *taf-value* — The taf-value is specified as a whole number between 0 and 64. The value '0' has special meaning in that it disables the time average factor adjustment and has the same effect as no time-average-factor.

Default 0

Values 0 to 64

dec-only — This keyword is an optional parameter. When enabled, the time average factor adjustment is only applied if the new offered rate is decreasing compared to the previous offered rate. If the new offered rate is greater than the previous offered rate, the adjustment is not applied.

Platforms All

time-average-factor

Syntax **time-average-factor** *value*
no time-average-factor

Context [Tree] (config>qos>slope-policy time-average-factor)

Full Context configure qos slope-policy time-average-factor

Description This command sets a weighting factor to calculate the new shared buffer average utilization after assigning buffers for a packet entering a queue. To derive the new shared buffer average utilization, the buffer pool takes a portion of the previous shared buffer average and adds it to the inverse portion of the instantaneous shared buffer utilization.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **time-average-factor** command sets the weighting factor between the old shared buffer average utilization and the current shared buffer instantaneous utilization when calculating the new shared buffer average utilization

The TAF value applies to all high- and low-priority RED slopes for ingress and egress access buffer pools controlled by the slope policy.

The **no** form of this command restores the default setting.

Default time-average-factor 7

Parameters *value* — Represents the Time Average Factor (TAF), expressed as a decimal integer. The value specified for TAF affects the speed at which the shared buffer average utilization tracks the instantaneous shared buffer utilization. A low value weights the new shared buffer average utilization calculation more to the shared buffer instantaneous utilization; zero using it exclusively. A high value weights the new shared buffer average utilization calculation more to the previous shared buffer average utilization value.

Values 0 to 15

Platforms All

24.105 time-display

time-display

Syntax **time-display** {**local** | **utc**}

Context **[Tree]** (environment time-display)

Full Context environment time-display

Description This command displays time stamps in the CLI session based on local time or Coordinated Universal Time (UTC).

The system keeps time internally in UTC and is capable of displaying the time in either UTC or local time based on the time zone configured.

This environment command only applies to times displayed in the current CLI session. This includes displays of event logs, traps and all other places where a time stamp is displayed.

In general all time stamps are shown in the time selected. This includes log entries destined for console/session, memory, or SNMP logs. Log files on compact flash are maintained and displayed in UTC format.

Default time-display local

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters **local** — Indicates that local time should be used.

utc — Indicates that UTC time should be used.

Platforms All

time-display

Syntax **time-display** {**local** | **utc**}

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment time-display)

Full Context configure system management-interface cli md-cli environment time-display

Description This command configures whether the time is displayed in coordinated Universal Time (UTC) or local time (as configured in **config**>**system**>**time**).

Default time-display local

Parameters **local** — Specifies that the local time zone is used.

utc — Specifies that UTC is used.

Platforms All

24.106 time-exceeded

time-exceeded

Syntax **time-exceeded** [*number seconds*]
no time-exceeded

Context **[Tree]** (config>service>ies>if>ipv6>icmp6 time-exceeded)

Full Context configure service ies interface ipv6 icmp6 time-exceeded

Description This command specifies whether time-exceeded ICMP messages should be sent. When enabled, ICMPv6 time-exceeded messages are generated by this interface.

When disabled, ICMPv6 time-exceeded messages are not sent.

The **no** form of this command reverts to the default.

Default time-exceeded 100 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the number of time-exceeded ICMP messages are to be issued in the time frame specified by the *seconds* parameter.

Values 10 to 2000

seconds — Specifies the time frame, in seconds, that is used to limit the number of time-exceeded ICMP message to be issued.

Values 1 to 60

Platforms All

time-exceeded

Syntax **time-exceeded** [*number seconds*]
no time-exceeded

Context **[Tree]** (config>router>if>ipv6>icmp6 time-exceeded)
[Tree] (config>service>vprn>if>ipv6>icmp6 time-exceeded)

Full Context configure router interface ipv6 icmp6 time-exceeded
configure service vprn interface ipv6 icmp6 time-exceeded

Description This command configures rate for ICMPv6 time-exceeded messages.

Parameters *number* — Limits the number of time-exceeded messages issued per the time frame specified in *seconds* parameter.

Values 10 to 2000

seconds — Determines the time frame, in seconds, that is used to limit the number of time-exceeded messages issued per time frame.

Values 1 to 60

Platforms All

24.107 time-format

time-format

Syntax **time-format** {**local** | **utc**}

Context **[Tree]** (config>service>vprn>log>log-id time-format)

Full Context configure service vprn log log-id time-format

Description This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default time-format utc

Parameters **local** — Specifies that timestamps are written in the system's local time.

utc — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

Platforms All

time-format

Syntax **time-format** {**local** | **utc**}

Context **[Tree]** (config>li>log>log-id time-format)

Full Context configure li log log-id time-format

Description This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

Default time-format utc

Parameters **local** — Specifies that timestamps are written in the system's local time.

utc — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

Platforms All

time-format

Syntax **time-format** {**local** | **utc**}

Context **[Tree]** (config>log>log-id time-format)

Full Context configure log log-id time-format

Description This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

Default time-format utc

Parameters **local** — Specifies that timestamps are written in the system's local time.

utc — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.108 time-limit

time-limit

Syntax **time-limit** *limit-value*

Context **[Tree]** (config>call-trace>trace-profile time-limit)

Full Context configure call-trace trace-profile time-limit

Description This command specifies how long a trace may run before it is stopped.

Default time-limit 86400

Parameters *limit-value* — Specifies the maximum duration of a single call trace job in seconds. After reaching the limit the call trace job for a given host is automatically terminated.

Values 1 to 604800

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.109 time-range

time-range

Syntax **time-range daily start** *start-time* **end** *end-time* [**on** *day* [*day*]]
time-range weekly start *start-time* **end** *end-time*
no time-range

Context **[Tree]** (config>app-assure>group>tod-override time-range)

Full Context configure application-assurance group policer tod-override time-range

Description This command configures up to seven time-ranges applicable to a particular override-id. The time-range can be configured as daily or weekly policies.

When using a daily override the operator can select which days during the week from Sunday to Saturday it is applicable along with the start/end hour/min time range repeated over these days.

When using a weekly override the operator can select between which days in the week the policy start up to the hours/min for both start day and end day.

Default no time-range

Parameters **daily** — Schedule the override as a daily occurrence.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

weekly — Schedule the override as a weekly occurrence.

Values

start-time	daily	<hh>:<mm>
	weekly	<day>,<hh>:<mm>
		<hh> : 0..23
		<mm> : 0 | 15 | 30 | 45
end-time	daily	<hh>:<mm>
	weekly	<day>,<hh>:<mm>
		<hh> 0..23
		<mm> 0 | 15 | 30 | 45
day	sunday | monday | tuesday | wednesday | thursday | friday | saturday	

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.110 time-stamp

time-stamp

Syntax [**no**] **time-stamp**

Context **[Tree]** (environment time-stamp)

Full Context environment time-stamp

Description This command specifies whether the time-stamp should be displayed before the prompt.

Platforms All

24.111 timeout

timeout

Syntax **timeout** [**sec** *seconds*] [**min** *minutes*]

Context **[Tree]** (config>aaa>l2tp-acct-plcy>radius-acct-server timeout)

Full Context configure aaa l2tp-accounting-policy radius-accounting-server timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the time that the router waits for a response from a RADIUS server.

The **no** form of this command reverts to the default value.

Default timeout sec 5

Parameters *seconds* — Specifies the time, in seconds, that the router waits for a response from a RADIUS server.

Values 1 to 59

minutes — Specifies the time, in minutes, that the router waits for a response from a RADIUS server.

Values 1 to 1

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*

Context **[Tree]** (config>app-assure>rad-acct-plcy>server timeout)

Full Context configure application-assurance radius-accounting-policy radius-accounting-server timeout

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of this command reverts to the default value.

Default timeout 5

Parameters *seconds* — Specifies the time the router waits for a response from a RADIUS server.

Values 1 to 90

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>subscr-mgmt>auth-plcy>radius-auth-server timeout)
[Tree] (config>subscr-mgmt>acct-plcy>server timeout)

Full Context configure subscriber-mgmt radius-accounting-policy radius-accounting-server timeout
configure subscriber-mgmt authentication-policy radius-authentication-server timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *seconds* — Specifies the time, in seconds, that the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 to 90

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>subscr-mgmt>shcv-policy>periodic timeout)

Full Context configure subscriber-mgmt shcv-policy periodic timeout

Description This command configures the timeout before a retransmission in triggered connectivity verification.

The **no** form of this command reverts to the default.

Default timeout 10

Parameters *seconds* — Specifies the timeout, in seconds, before a retransmission in triggered connectivity verification.

Values 10 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>subscr-mgmt>shcv-policy>trigger timeout)

Full Context configure subscriber-mgmt shcv-policy trigger timeout

Description This command configures the timeout before a retransmission.

The **no** form of this command reverts to the default.

Default timeout 1 — trigger-type ip-conflict, host-limit-exceeded and mobility

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout 2 — trigger-type inactivity and mac-learning

Parameters *seconds* — Specifies the retry timeout in seconds.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** [**sec** *seconds*] [**min** *minutes*]
no timeout

Context **[Tree]** (config>aaa>radius-srv-plcy>servers timeout)

Full Context configure aaa radius-server-policy servers timeout

Description This command configures the time the router waits for a response from a RADIUS server.

The no form of this command reverts to the default value.

Default timeout sec 5

Parameters *seconds* — Specifies the number of seconds for the timeout.

Values 1 to 59

minutes — Specifies the number of minutes for the timeout.

Values 1 to 5

Values Max. value = 5 min 40 sec

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no timeout

Context **[Tree]** (config>router>radius-proxy>server>cache timeout)
[Tree] (config>service>vprn>radius-proxy>server>cache timeout)

Full Context configure router radius-proxy server cache timeout
configure service vprn radius-proxy server cache timeout

Description This command configures the time for which the cache entry is kept if there is no corresponding DHCP DISCOVER. At the expiry of this time, the cache entry is deleted.

The **no** form of this command reverts to the default value.

Default timeout min 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hours* — Specifies, in hours, the timeout after which an entry in the cache will expire.

Values 1

minutes — Specifies, in minutes, the timeout after which an entry in the cache will expire.

Values 1 to 59

seconds — Specifies, in seconds, the timeout after which an entry in the cache will expire.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*

Context **[Tree]** (config>subscr-mgmt>pfcp-association>heartbeat timeout)

Full Context configure subscriber-mgmt pfcp-association heartbeat timeout

Description This command configures the timeout period, after which, a Heartbeat Request message is considered unanswered.

Default timeout 5

Parameters *seconds* — Specifies the timeout value, in seconds. This interval should be identical on both the BNG UPF and CPF. For information about the BNG CUPS CPF configuration, refer to the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide*.

Values 1 to 20

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*

Context **[Tree]** (config>subscr-mgmt>pfcp-association>tx timeout)

Full Context configure subscriber-mgmt pfcp-association tx timeout

Description This command configures the timeout period, after which, a message is considered unanswered. This timeout value is also known as T1.

Default timeout 5

Parameters *seconds* — Specifies the timeout value, in seconds.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This value must be identical on both the BNG UPF and CPF. For information about the BNG CUPS CPF configuration, refer to the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide*.

Values 1 to 30

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius timeout)

Full Context configure service vprn aaa remote-servers radius timeout

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *seconds* — Specifies the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 to 90

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>service>vprn>aaa>remote-servers>tacplus timeout)

Full Context configure service vprn aaa remote-servers tacplus timeout

Description This command configures the number of seconds the router waits for a response from a TACACS+ server.

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *seconds* — Specifies the number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer.

Values 1 to 90

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>router>mpls>lsp-self-ping timeout)

Full Context configure router mpls lsp-self-ping timeout

Description This command configures a timeout value for LSP Self Ping. The LSP Self Ping timer is started when the RESV message is received for an LSP. The system then periodically sends LSP Self Ping packets until the timer expiry or the receipt of the first LSP Self Ping reply, whichever comes first. If the timeout expires before an LSP Self Ping packet is received, then the configured **timeout-action** is performed.

The **no** form of this command reverts to the default value.

Default timeout 300

Parameters *seconds* — Specifies the value, in seconds, of the fast retry timer for a secondary path.

Values 3 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

timeout

Syntax **timeout** *seconds*

Context **[Tree]** (config>system>file-trans-prof timeout)

Full Context configure system file-transmission-profile timeout

Description This command specifies timeout value in seconds for transport protocol. The timeout is the maximum waiting time to receive any data from the server (e.g., FTP or HTTP server).

Default timeout 60

Parameters *seconds* — Specifies the connection timeout (in seconds) for the file transmission.

Values 1 to 3600

Platforms All

timeout

Syntax **timeout** [**sec** *seconds*] [**min** *minutes*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no timeout

Context **[Tree]** (config>aaa>isa-radius-plcy>servers timeout)

Full Context configure aaa isa-radius-policy servers timeout

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of the command reverts to the default value.

Default timeout sec 5

Parameters *seconds* — Specifies the wait for a response from a RADIUS server, in seconds.

minutes — Specifies the wait for a response from a RADIUS server, in minutes.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

timeout

Syntax **timeout** *timeout*
no timeout

Context **[Tree]** (config>test-oam>ldp-treetrace>path-discovery timeout)

Full Context configure test-oam ldp-treetrace path-discovery timeout

Description This command configures the time the node waits for the response to an LSP Trace message discovering the path of an LDP FEC before it declares failure. After consecutive failures equal to the **retry-count** parameter, the node gives up.

The **no** form of this command resets the timeout to its default value.

Default timeout 30

Parameters *timeout* — Specifies the *timeout* parameter, in seconds, within a range of 1 to 60, expressed as a decimal integer.

Values 1 to 60

Platforms All

timeout

Syntax **timeout** *timeout*
no timeout

Context **[Tree]** (config>test-oam>ldp-treetrace>path-probing timeout)

Full Context configure test-oam ldp-treetrace path-probing timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the time the node waits for the response to an LSP Ping message probing the path of an LDP FEC before it declares failure. After consecutive failures equal to the **retry-count** parameter, the node gives up.

The **no** form of this command resets the time out to its default value.

Default timeout 1

Parameters *timeout* — Specifies the timeout parameter, in minutes, expressed as a decimal integer.

Values 1 to 3

Platforms All

timeout

Syntax **timeout** *timeout*
no timeout

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy timeout)

Full Context configure saa test type-multi-line lsp-ping sr-policy timeout

Description This command configures the number, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the last probe for a specific test. Upon the expiration of the time out, the test is marked complete and no more packets are processed for any of the request probes.

The **no** form of this command reverts to the default value.

Default timeout 5

Parameters *timeout* — Specifies the timeout value in seconds.

Values 1 to 10

Default 5

Platforms All

timeout

Syntax **timeout** *timeout*
no timeout

Context **[Tree]** (config>saa>test>type-multi-line>lsp-trace>sr-policy timeout)

Full Context configure saa test type-multi-line lsp-trace sr-policy timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response is not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *timeout* — Specifies the timeout value in seconds.

Values 1 to 60

Default 3

Platforms All

timeout

Syntax **timeout** [*seconds*]
no timeout

Context **[Tree]** (config>filter>redirect-policy>dest>ping-test timeout)

Full Context configure filter redirect-policy destination ping-test timeout

Description Specifies the amount of time, in seconds, that is allowed for receiving a response from the far-end host. If a reply is not received within this time the far-end host is considered unresponsive.

Default timeout 1

Parameters *seconds* — Specifies the amount of time, in seconds, that is allowed for receiving a response from the far end host.

Values 1 to 60

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>vrrp>vrrp-policy-id>priority-event>host-unreachable timeout)

Full Context configure vrrp vrrp-policy-id priority-event host-unreachable timeout

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command defines the time, in seconds, that must pass before considering the far-end IP host unresponsive to an outstanding ICMP echo request message.

The **timeout** value is not directly related to the configured **interval** parameter. The **timeout** value may be larger, equal, or smaller, relative to the **interval** value.

If the **timeout** value is larger than the **interval** value, multiple ICMP echo request messages may be outstanding. Every ICMP echo request message transmitted to the far end host is tracked individually according to the message identifier and sequence number.

With each consecutive attempt to send an ICMP echo request message, the timeout timer is loaded with the **timeout** value. The timer decrements until:

- an internal error occurs preventing message sending (request unsuccessful)
- an internal error occurs preventing message reply receiving (request unsuccessful)
- a required route table entry does not exist to reach the IP address (request unsuccessful)
- a required ARP entry does not exist and ARP request timed out (request unsuccessful)
- a valid reply is received (request successful)

It is possible for a required ARP request to succeed or timeout after the message timeout timer expires. In this case, the message request is unsuccessful.

If an ICMP echo reply message is not received prior to the **timeout** period for a given ICMP echo request, that request is considered to be dropped and increments the consecutive message drop counter for the priority event.

If an ICMP echo reply message with the same sequence number as an outstanding ICMP echo request message is received prior to that message timing out, the request is considered successful. The consecutive message drop counter is cleared and the request message no longer is outstanding.

If an ICMP Echo Reply message with a sequence number equal to an ICMP echo request sequence number that had previously timed out is received, that reply is silently discarded while incrementing the priority event reply discard counter.

The **no** form of the command reverts to the default value.

Default timeout 1

Parameters *seconds* — The number of seconds before an ICMP echo request message is timed out. Once a message is timed out, a reply with the same identifier and sequence number is discarded.

Values 1 to 60

timeout

Syntax **timeout** *timeout*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no timeout

Context **[Tree]** (config>service>sdp>keep-alive timeout)

Full Context configure service sdp keep-alive timeout

Description This command configures the time interval that the SDP waits before tearing down the session.

Default timeout 5

Parameters **timeout** — Specifies the timeout time, in seconds.

Values 1 to 10

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>system>security>radius timeout)

Full Context configure system security radius timeout

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *seconds* — Specifies the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 to 90

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>system>security>tacplus timeout)

Full Context configure system security tacplus timeout

Description This command configures the number of seconds the router waits for a response from a TACACS+ server.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *seconds* — The number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer.

Values 1 to 90

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>system>security>ldap timeout)

Full Context configure system security ldap timeout

Description The **timeout** value is the number of seconds that the SR OS will wait for a response from the current server that it is trying to establish a connection with. If the server does not reply within the configured **timeout** value, the SR OS will increment the retry counter by 1. The SR OS attempts to establish the connection to the current server up to the configured **retry** value before it moves to the next configured server.

The **no** form of this command reverts to the default value.

Default timeout 3

Parameters *seconds* — The length of time that the SR OS waits for a response from the server.

Values 1 to 90

Default 3

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>system>security>dot1x>radius-plcy timeout)

Full Context configure system security dot1x radius-plcy timeout

Description This command configures the number of seconds the router waits for a response from a RADIUS server.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default timeout 3

Parameters *seconds* — Specifies the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values 1 to 90

Platforms All

timeout

Syntax **timeout** *seconds*
no timeout

Context **[Tree]** (config>test-oam>icmp>ping-template timeout)

Full Context configure test-oam icmp ping-template timeout

Description This command configures the time the function waits before declaring an ICMP echo request packet is lost. This is the timer used to time out the interval transmitted packets. The timeout can be equal to or lower than the interval but not higher.

The **no** form of this command reinstates the default value for timeout.

Default timeout 5

Parameters *seconds* — Specifies the time, in seconds, before declaring an ICMP echo request being lost.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.112 timeout-action

timeout-action

Syntax **timeout-action** *action*
no timeout-action

Context **[Tree]** (config>router>l2tp>tunnel-selection-blacklist timeout-action)
[Tree] (config>service>vprn>l2tp>tunnel-selection-blacklist timeout-action)

Full Context configure router l2tp tunnel-selection-blacklist timeout-action
configure service vprn l2tp tunnel-selection-blacklist timeout-action

Description This command defines an action that is executed on the entity (peer/tunnel) in the denylist once the entity becomes eligible for selection again.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Default timeout-action remove-from-blacklist

Parameters *action* — Specifies the Action to be taken when a tunnel or peer has been in the denylist for the max-period of time.

Values **remove-from-blacklist** — The peer or tunnel in the denylist is removed completely from the denylist and made eligible for the selection process once the max-time expires. In this mode of operation, multiple new sessions can be mapped into the same, newly released tunnel from the denylist. The first such session will try to setup the tunnel, while the other is buffered until the tunnel establishment process is completed. In case that the tunnel remains unavailable, it is placed in the denylist again. Consequently, all new sessions are re-negotiated over an alternate tunnel.

try-one-session — Once the max-time expired, the peer or tunnel in the denylist is made available for selection only to a single new session request. Only upon successful tunnel establishment will the incoming new sessions be eligible to be mapped into this tunnel. This behavior will avoid session establishment delays in case that the tunnel just removed from the denylist is still unavailable.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timeout-action

Syntax **timeout-action** {**retry** | **switch**}
no timeout-action

Context **[Tree]** (config>router>mpls>lsp-self-ping timeout-action)

Full Context configure router mpls lsp-self-ping timeout-action

Description This command configures an action that the router takes when the timeout LSP self ping timeout timer expires. The lsp-self-ping timer is started when the RESV is received for an LSP. If the retry is configured and the timeout expires before an LSP self ping packet is received, then the system tears down the candidate path and goes back to CSPF for a new path. If the switch is configured and the timeout expires before an LSP self ping packet is received, then the system switches to the candidate path.

The **no** form of this command reverts to the default value.

Default timeout-action retry

Parameters **retry** — Specifies to retry the candidate path when the timeout expires.

switch — Specifies to switch to the candidate path when the timeout expires.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.113 timeouts

timeouts

Syntax [**no**] **timeouts**

Context **[Tree]** (config>service>nat>nat-policy timeouts)
[Tree] (config>service>nat>firewall-policy timeouts)
[Tree] (config>service>nat>up-nat-policy timeouts)

Full Context configure service nat firewall-policy timeouts
configure service nat nat-policy timeouts
configure service nat up-nat-policy timeouts

Description This command configures session idle timeouts for this policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy timeouts
- configure service nat nat-policy timeouts

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts

timeouts

Syntax **timeouts**

Context **[Tree]** (config>li>x-interfaces>x1 timeouts)
[Tree] (config>li>x-interfaces>x2 timeouts)
[Tree] (config>li>x-interfaces>x3 timeouts)

Full Context configure li x-interfaces x1 timeouts
configure li x-interfaces x2 timeouts
configure li x-interfaces x3 timeouts

Description This command configures the X1, X2, and X3 messages timeout.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.114 timers

timers

Syntax **timers**

Context **[Tree]** (config>service>dynsvc timers)

Full Context configure service dynamic-services timers

Description Commands in this context configure dynamic data services related timers.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

timers

Syntax **timers**

Context **[Tree]** (config>service>vpls>spb timers)

Full Context configure service vpls spb timers

Description Commands in this context configure SPB timers.

Platforms All

timers

Syntax [**no**] **timers**

Context **[Tree]** (config>service>vprn>isis timers)

Full Context configure service vprn isis timers

Description This command configures the IS-IS timer values.

Default n/a

Platforms All

timers

Syntax **timers**

Context **[Tree]** (config>service>vprn>ospf timers)
[Tree] (config>service>vprn>ospf3 timers)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vprn ospf timers
configure service vprn ospf3 timers

Description Commands in this context configure OSPF timers. Timers control the delay between receipt of a LSA requiring a Dijkstra (Shortest Path First (SPF)) calculation and the minimum time between successive SPF calculations.

Changing the timers affect CPU utilization and network reconvergence times. Lower values reduce convergence time but increase CPU utilization. Higher values reduce CPU utilization but increase reconvergence time.

Platforms All

timers

Syntax **timers** *update timeout flush*
no timers

Context **[Tree]** (config>service>vprn>rip timers)
[Tree] (config>service>vprn>rip>group timers)
[Tree] (config>service>vprn>rip>group>neighbor timers)
[Tree] (config>service>vprn>ripng timers)
[Tree] (config>service>vprn>ripng>group timers)
[Tree] (config>service>vprn>ripng>group>neighbor timers)

Full Context configure service vprn rip group neighbor timers
configure service vprn rip group timers
configure service vprn rip timers
configure service vprn ripng group neighbor timers
configure service vprn ripng group timers
configure service vprn ripng timers

Description This command configures the values for the update, timeout, and flush timers:

- **update timer**
  Determines how often RIP updates are sent.
- **timeout timer**
  If a router is not updated by the time the timer expires, the route is declared invalid, but maintained in the RIP database.
- **flush timer**
  Determines how long a route is maintained in the RIP database, after it has been declared invalid. Once this timer expires it is flushed from the RIP database completely.

The **no** form of this command resets all timers to their default values of 30, 180, and 120 seconds respectively.

Default no timers

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *update* — The RIP update timer value in seconds.

Values 1 to 600

Default 30

timeout — The RIP timeout timer value in seconds.

Values 1 to 1200

Default 180

flush — The RIP flush timer value in seconds.

Values 1 to 1200

Default 120

Platforms All

timers

Syntax **timers** [**neighbor** *ip-address* | **group** *name*]
no timers

Context **[Tree]** (debug>router>bgp timers)

Full Context debug router bgp timers

Description This command logs all BGP timer events to the debug log.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:

- a.b.c.d (host bits must be 0)

ipv6-address:

- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timers

Syntax [**no**] **timers**

Context **[Tree]** (config>router>isis timers)

Full Context configure router isis timers

Description This command configures the IS-IS timer values.

Platforms All

timers

Syntax **timers**

Context **[Tree]** (config>router>ospf timers)
[Tree] (config>router>ospf3 timers)

Full Context configure router ospf timers
configure router ospf3 timers

Description Commands in this context configure OSPF timers. Timers control the delay between receipt of a link state advertisement (LSA) requiring a Dijkstra (Shortest Path First (SPF)) calculation and the minimum time between successive SPF calculations.

Changing the timers affects CPU utilization and network re-convergence times. Lower values reduce convergence time but increase CPU utilization. Higher values reduce CPU utilization but increase re-convergence time.

Platforms All

timers

Syntax **timers** *update timeout flush*
no timers

Context **[Tree]** (config>router>rip timers)
[Tree] (config>router>rip>group timers)
[Tree] (config>router>rip>group>neighbor timers)
[Tree] (config>router>ripng timers)
[Tree] (config>router>ripng>group timers)
[Tree] (config>router>ripng>group>neighbor timers)

Full Context configure router rip group neighbor timers
configure router rip group timers
configure router rip timers
configure router ripng group neighbor timers
configure router ripng group timers

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure router ripng timers

Description This command configures values for the update, timeout and flush RIP timers.

The RIP update timer determines how often RIP updates are sent.

If the route is not updated by the time the RIP timeout timer expires, the route is declared invalid but is maintained in the RIP database.

The RIP flush timer determines how long a route is maintained in the RIP database after it has been declared invalid. After the flush timer expires, the route is removed from the RIP database.

The **no** form of the command reverts to the default values.

Default timers 30 180 120

Parameters *update* — Specifies the RIP update timer value in seconds expressed as a decimal integer.

Values 1 to 600

timeout — Specifies the RIP timeout timer value in seconds expressed as a decimal integer.

Values 1 to 1200

flush — Specifies the RIP flush timer value in seconds expressed as a decimal integer.

Values 1 to 1200

Platforms All

24.115 timeslots

timeslots

Syntax **timeslots** *timeslots*
no timeslots

Context **[Tree]** (config>port>tdm>ds1>channel-group timeslots)
[Tree] (config>port>tdm>e1>channel-group timeslots)

Full Context configure port tdm ds1 channel-group timeslots
configure port tdm e1 channel-group timeslots

Description This command defines the list of DS-0 timeslots to be used in the DS-1 or E-1 channel-group. The timeslots are defaulted as defined below when encap-type is set **to/from atm**. ATM channel groups do not allow timeslots to change.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes DS-0 timeslots from a channel group.

Parameters *timeslots* — Specifies the timeslot(s) to be associated with the channel group. The value can consist of a list of timeslots. Each member of the list can either be a single timeslot or a range of timeslots.

Values 1 to 24 for DS-1 interfaces (the full range is auto-configured for ATM channel groups and cannot be changed) 2 to 32 for E-1 interfaces (the 2 to 16,18 to 32 ranges are auto-configured for ATM channel groups and cannot be changed)

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

24.116 timestamp

timestamp

Syntax [**no**] **timestamp**

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment>prompt timestamp)

Full Context configure system management-interface cli md-cli environment prompt timestamp

Description This command displays the timestamp before the first prompt line.

The **no** form of this command suppresses the timestamp before the first prompt line.

Default timestamp

Platforms All

24.117 timestamp-format

timestamp-format

Syntax **timestamp-format** *timestamp-format*

Context **[Tree]** (config>test-oam>link-meas>template>twl timestamp-format)

Full Context configure test-oam link-measurement measurement-template twamp-light timestamp-format

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the format of the timestamp used in the TWAMP Light PDU.This configuration places the requested timestamp format in the packet using the appropriate epoch. This is unrelated to any time distribution protocol being used to synchronize time between clocks.

Default timestamp-format ntp

Parameters *parameter* — Specifies the timestamp format to be used in the TWAMP Light PDU.

Values ntp, ptp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.118 timing

timing

Syntax **timing frames-per-delta-t** *frames* **consec-delta-t** *deltas* **chli-threshold** *threshold*
no timing

Context **[Tree]** (config>oam-pm>session>ethernet>lmm>availability timing)

Full Context configure oam-pm session ethernet lmm availability timing

Description This command defines various availability parameters for LMM availability testing. This command does not define the probe interval. Validation occurs when the LMM test is activated using the **no shutdown** command. The maximum size of the availability window cannot exceed 100 seconds (100 000 milliseconds). LMM test activation fails if the availability window exceeds the maximum value.

The **no** form of this command restores the default values for all timing parameters, and uses those values to compute availability and set the loss frequency.

Parameters *frames* — Specifies the number of SLM frames that define the size of the small measurement window. Each delta-t is marked as a high-loss interval or non-high-loss interval based on the **flr-threshold**. The size of the delta-t measurement is the product of the number of frames and the interval.

Values 1 to 50

Default 10

deltas — Specifies the number of consecutive delta-t measurement intervals that make up the sliding window over which availability and unavailability determined. Transitions from one state to another occurs when the **consec-delta-t** are in a new state. The sliding window cannot exceed 100 seconds.

Values 2 to 10

Default 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

threshold — Specifies the number of consecutive unavailable delta-t intervals that, when reached or exceeded, increments the CHLI counter. A CHLI counter is an indication that the sliding window is available but has crossed a threshold of consecutive unavailable delta-t intervals. A CHLI can only be incremented once during a sliding window and, by default, is incremented during times of availability.

Values 1 to 9

Default 5

Platforms All

timing

Syntax **timing frames-per-delta-t** *frames* **consec-delta-t** *deltas* **interval** *milliseconds* **chli-threshold** *threshold*
no timing

Context **[Tree]** (config>oam-pm>session>ethernet>slm timing)

Full Context configure oam-pm session ethernet slm timing

Description This command defines various availability parameters and the probe spacing (interval) for the SLM frames. The maximum size of the availability window cannot exceed 10 s (10 000 ms).

The **no** form of this command installs the default values for all timing parameters and use those values to compute availability and set the SLM frequency. If an SLM test is in the **no shutdown** state, it always has timing parameters, default or operator configured.

Parameters *frames* — Specifies the of SLM frames that define the size of the delta-t (small measurement window). Each delta-t is marked as available or unavailable based on the flr-threshold. The size of the delta-t measurement is the product of the number of frames and the interval.

Values 1 to 50

Default 10

deltas — Specifies the number of consecutive delta-t small measurement intervals that make up the sliding window over which availability and unavailability is determined. Transitions from one state to another occurs when the consec-delta-t is in a new state.

Values 2 to 10

Default 10

milliseconds — Specifies the number of milliseconds between the transmission of the SLM frames. By design, the default value for the SLM interval is different than the default interval for DMM.

Values 100, 1000

Default 100

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

threshold — Specifies the number of consecutive high loss intervals (unavailable delta-t) that when equal to or exceeded increments the CHLI counter. A CHLI counter is an indication that the sliding window is available but has crossed a threshold consecutive of unavailable delta-t intervals. A CHLI can only be incremented once during a sliding window and, by default, it is only incremented during times of availability.

Values 1 to 9

Default 5

Platforms All

timing

Syntax **timing frames-per-delta-t** *frames* **consec-delta-t** *deltas* **chli-threshold** *threshold*
no timing

Context **[Tree]** (config>oam-pm>session>ip>twamp-light>loss timing)

Full Context configure oam-pm session ip twamp-light loss timing

Description This command defines various availability parameters but not the probe interval. A single TWAMP-Light frame is used to collect both delay and loss metrics; the interval is common to both and as such not unique per metric type. Any TWAMP light test that is attempting to become active validates the configuration of the timing parameter regardless of which statistics are being recorded.

The **no** form of this command restores the default values for all timing parameters and use those values to compute availability and set the loss frequency.

Default timing frames-per-delta-t 1 consec-delta-t 10 chli-threshold 5

Parameters *frames* — Defines the size of the small measurement window. Each delta-t is marked as available of unavailable based on the flr-threshold. The size of the delta-t measurement is the product of the number of frames and the interval. This value defaults to a different value thank single probe per metric approaches.

Values 1 to 50

Default 1

deltas — Specifies the number of consecutive delta-t small measurement intervals that make up the sliding window over which availability and unavailability are determined. Transitions from one state to another occurs when the consec-delta-t are now in a new state. The sliding window cannot exceed 100 seconds.

Values 2 to 10

Default 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

threshold — Specifies the number of consecutive high loss intervals (unavailable delta-t) that when equal to or exceeded increments the CHLI counter. A CHLI counter is an indication that the sliding window is available but has crossed a threshold consecutive of unavailable delta-t intervals. A CHLI can only be incremented once during a sliding window and, by default, is only incremented during times of availability.

Values 1 to 9

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.119 tls

tls

Syntax **tls**

Context **[Tree]** (config>system>security tls)

Full Context configure system security tls

Description This command configures TLS parameters.

Platforms All

24.120 tls-client-profile

tls-client-profile

Syntax **tls-client-profile** *profile-name*
no tls-client-profile

Context **[Tree]** (config>open-flow>of-switch>of-controller tls-client-profile)

Full Context configure open-flow of-switch of-controller tls-client-profile

Description This command configures the use of Transport Layer Security (TLS) on the control channel to a given OpenFlow controller for this OpenFlow switch.

The **no** form of this command deletes removed TLS from the control channel.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *profile-name* — Specifies the use of TLS for the control channel. A named TLS profile must also be specified, referring to a TLS profile configured under **config**>**system**>**security**>**tls**.

Platforms All

tls-client-profile

Syntax **tls-client-profile** *name*
no tls-client-profile

Context **[Tree]** (config>system>grpc-tunnel>destination-group tls-client-profile)
[Tree] (config>system>telemetry>destination-group tls-client-profile)

Full Context configure system telemetry destination-group tls-client-profile
configure system telemetry destination-group tls-client-profile

Description This command configures a TLS client profile to a destination group.

This command is mutually exclusive with the **allow-unsecured-connection** command.

The **no** form of this command removes the TLS client profile.

Default no tls-client-profile

Parameters *name* — Specifies the TLS client profile name, up to 32 characters.

Platforms All

tls-client-profile

Syntax **tls-client-profile** *tls-client-profile*
no tls-client-profile

Context **[Tree]** (config>log>syslog tls-client-profile)
[Tree] (config>service>vprn>log>syslog tls-client-profile)

Full Context configure log syslog tls-client-profile
configure service vprn log syslog tls-client-profile

Description This command specifies the Transport Layer Security (TLS) client profile used to encrypt syslog communications. When configured, syslog messages are sent using TLS.

Any change to this command results in a brief interruption of the event log, which may cause the loss of a few syslog messages.

The **no** form of this command removes TLS encryption of syslog communications and sends syslog messages over UDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *tls-client-profile* — Specifies the name of a TLS profile configured in the **config**>**system**>**security**>**tls** context, up to 32 characters.

Platforms All

tls-client-profile

Syntax **tls-client-profile** *profile-name*
no tls-client-profile

Context **[Tree]** (config>router>pcep>pcc>peer tls-client-profile)

Full Context configure router pcep pcc peer tls-client-profile

Description This command configures a TLS client profile on the PCC. When the TLS profile is configured, the PCC tries to establish a PCEP connection with the PCE over TLS. Because SR OS supports a strict TLS-only mode, both the PCE and PCC must support TLS. If a TLS failure occurs, the connection over TLS is closed and a new connection is retried within 60 seconds.

The **no** form of this command removes TLS encryption from the communication between this PCC and the PCE.

Default no tls-client-profile

Parameters *profile-name* — Specifies the TLS client profile name, up to 32 characters.

Platforms All

24.121 tls-extension

tls-extension

Syntax **tls-extension**

Context **[Tree]** (config>app-assure>group>http-enrich tls-extension)

Full Context configure application-assurance group http-enrich tls-extension

Description Commands in this context configure the TLS extension field name.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.122 tls-profile

tls-profile

Syntax **tls-profile** *tls-profile-name*
no tls-profile

Context **[Tree]** (config>system>security>ldap>server tls-profile)

Full Context configure system security ldap server tls-profile

Description This command attaches a TLS client profile to the LDAP client. The parameter in the TLS profile is used to encrypt the LDAP connection to the server. Each LDAP server can use its own TLS profile.

When a TLS profile is assigned, the LDAP application will send encrypted PDUs from the client to the LDAP server. If TLS is operationally down, the LDAP application should not send any PDUs.

The **no** form of this command removes the TLS profile from LDAP and disables the TLS encryption from LDAP.

Parameters *tls-profile-name* — Specifies the TLD profile for encryption.

Platforms All

24.123 tls-re-negotiate-timer

tls-re-negotiate-timer

Syntax **tls-re-negotiate-timer** *timer-min*
no tls-re-negotiate-timer

Context **[Tree]** (config>system>security>tls>server-tls-profile tls-re-negotiate-timer)

Full Context configure system security tls server-tls-profile tls-re-negotiate-timer

Description This command configures the timed interval after which the server is triggered to send a Hello request message to all clients and force a renegotiation of the symmetric encryption key. When an interval of 0 is configured, the server will never send a hello request message.

Default tls-re-negotiate-timer 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *timer-min* — Specifies the interval, in minutes, after which the server is triggered to send a Hello request message.

Values 0 to 65000

Platforms All

24.124 tls-server-profile

tls-server-profile

Syntax **tls-server-profile** *name*
no tls-server-profile

Context **[Tree]** (config>system>grpc tls-server-profile)

Full Context configure system grpc tls-server-profile

Description This command adds a configured TLS server profile to the gRPC session. The TLS server is used for encryption of the gRPC session. gRPC will not transmit any PDUs if there is a TLS server profile assigned to it and the TLS connection is down.

The **no** form of this command removes the specified TLS server profile from the gRPC session.

Parameters *name* — Specifies the name of the TLS server profile configured under the **config**>**system**>**security**>**tls** context.

Platforms All

tls-server-profile

Syntax **tls-server-profile** *name*
no tls-server-profile

Context **[Tree]** (config>router>pcep>pce tls-server-profile)

Full Context configure router pcep pce tls-server-profile

Description This command configures a TLS server profile on the PCE. When a TLS server profile is configured, the PCE accepts TLS handshakes from the PCC. Because SR OS supports a strict TLS mode only, both the PCE and the PCC must support TLS. If a TLS failure occurs, the connection over TLS is closed and a new connection is retried within 60 seconds.

The **no** form of this command removes the specified TLS server profile.

Default no tls-server-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *name* — Specifies the name of the TLS server profile, up to 32 characters.

24.125 tls-wait-timer

tls-wait-timer

Syntax **tls-wait-timer** *tls-wait-timer*
no tls-wait-timer

Context **[Tree]** (config>router>pcep>pcc>peer tls-wait-timer)

Full Context configure router pcep pcc peer tls-wait-timer

Description This command configures the time that the PCC waits before declaring a TLS handshake failure if the handshake is not established.

The **no** form of this command reverts to the default.

Default tls-wait-timer 60

Parameters *tls-wait-timer* — Specifies the time, in seconds.

Values 60 to 255

Platforms All

24.126 to

to

Syntax **to** *ip-address*

Context **[Tree]** (config>router>gmpls>lsp to)

Full Context configure router gmpls lsp to

Description This command specifies the GMPLS loopback address of the far-end UNI-C router for a GMPLS LSP. When creating a GMPLS LSP, this command is mandatory.

Parameters *ip-address* — Specifies the system IP address of the far-end UNI-C router.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

to

Syntax **to** [*ip-address* | **node-id** [*a.b.c.d* | *1...4294967295*]]

Context **[Tree]** (config>router>mpls>lsp to)

Full Context configure router mpls lsp to

Description This command specifies the IP address or MPLS-TP node-id of the egress router for the LSP. This command is mandatory to create an LSP.

An IP address for which a route does not exist is allowed in the configuration. If the LSP signaling fails because the destination is not reachable, an error is logged and the LSP operational status is set to down.

For a non MPLS-TP LSP, the **to** *ip-address* can be an IP address of a network IP interface, the system interface, or a loopback interface of the egress router. When used in a SDP, if the LSP **to** address does not match the SDP address, the LSP is not included in the SDP definition.

For an MPLS-TP LSP, the **to node-id** may be either in 4-octet IPv4 address format, or a 32-bit unsigned integer. This command is mandatory to create an MPLS-TP LSP. A value of zero is invalid. This **to** address is used in the MPLS-TP LSP ID, and the MPLS-TP MEP ID for the LSP.

Default no default

Parameters *ip-address* — Specifies the IP address of the egress router. When the LSP type is **sr-te**, then an IPv6 address can be used.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — 0 to FFFF (hexadecimal)
d — 0 to 255 (decimal)

node-id *a.b.c.d.* | *1...4294967295* — 4-octet IPv4 formatted or unsigned 32-bit integer MPLS-TP node-id of the egress router.

Platforms All

to

Syntax **to** *ip-address*

Context **[Tree]** (config>router>mpls>static-lsp to)

Full Context configure router mpls static-lsp to

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the IP address of the egress router for the static LSP. When creating an LSP this command is required. The **to** IP address may be the address of a local interface, the system IP interface, or of a loopback interface of the egress router. When used in a SDP and the **to** address does not match the far-end SDP address, the LSP is not included in the SDP definition.

Parameters *ip-address* — Specifies the system IP address of the egress router.

Platforms All

to

Syntax **to memory** [*size*]
to netconf [*size*]
to session
to snmp [*size*]

Context **[Tree]** (config>li>log>log-id to)

Full Context configure li log log-id to

Description Commands in this context configure the destination type for the event log.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of a memory log, NETCONF log, or SNMP log needs to be modified, the log ID must be removed and then re-created.

Parameters *size* — The size parameter indicates the number of events that can be stored into memory.

Default 100

Values 50 to 1024

Platforms All

to

Syntax **to** *ipv4-address*
no to

Context **[Tree]** (config>oam-pm>session>mpls>lsp>rsvp-auto to)

Full Context configure oam-pm session mpls lsp rsvp-auto to

Description This command specifies an IPv4 address used (with the LSP template) to identify the LSP to be tested.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

One of three mandatory configuration statements that are required to identify automatically created RSVP LSPs, using **config>router>mpls>lsp-template**. The **config>router>mpls>auto-lsp>lsp-template** links three distinct functions, the **config>router>policy-options>prefix-list**, **config>router>policy-options>policy-statement>entry>from** and the **config>router>mpls> lsp-template**. The **to** address is the same address configured as the **from** address for the **config>router>policy-options>policy-statement>entry>from**. The required identifiers are **from**, **lsp-template** and **to**, all under this node.

Parameters *ipv4-address* — Specifies the IPv4 address.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

to

Syntax **to file** *file-id*

Context **[Tree]** (config>log>accounting-policy to)

Full Context configure log accounting-policy to

Description This command specifies the destination for the accounting records selected for the accounting policy.

Parameters *file-id* — Specifies the destination for the accounting records selected for this destination. The characteristics of the file ID must have already been defined in the **config>log>file** context. A file ID can only be used once.

The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics.

If the **to** command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.

Values 1 to 99

Platforms All

to

Syntax [**no**] **to**

Context **[Tree]** (config>router>policy-options>policy-statement>entry to)

Full Context configure router policy-options policy-statement entry to

Description This command creates the context to configure export policy match criteria based on a route's destination or the protocol into which the route is being advertised.

If no condition is specified, all route destinations are considered to match.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **to** command context only applies to export policies. If it is used for an import policy, match criteria is ignored.

The **no** form of this command deletes export match criteria for the route policy statement entry.

Platforms All

to

Syntax **to cli** [*size*]
to console
to file *log-file-id*
to memory [*size*]
to netconf [*size*]
to session
to snmp [*size*]
to syslog *syslog-id*

Context **[Tree]** (config>log>log-id to)

Full Context configure log log-id to

Description This command specifies a destination for the log data.

The source of the data stream must be specified in the **from** command before configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then recreated.

Parameters **cli** — Specifies that events selected for the log are directed to any subscribed CLI session. Subscribe to a CLI log from within a CLI session using the **tools**>**perform**>**log**>**subscribe-to log-id** *log-id* command. Events are sent to the CLI session for the duration of that CLI session, or until an **unsubscribe-from** command is issued. A local circular memory log is maintained for CLI logs.

console — Specifies that events selected for the log are directed to the console. If the console is not connected, all the entries are dropped.

file *log-file-id* — Specifies that events selected for the log are directed to a file with the specified *log-file-id*. The characteristics of the *log-file-id* referenced in this parameter must have already been defined in the **config**>**log**>**file** *file-id* context. When the *file-id* location parameter is modified, log files are not written to the new location until a rollover occurs or the log is manually cleared. A rollover can be forced by using the **clear**>**log** command. Subsequent log entries are then written to the new location. If a rollover does not occur or the log is not cleared, the old location continues to be used.

Values 1 to 99, *name* (up to 64 characters max)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

memory — Specifies that events selected for the log are directed to a memory file. A memory file is a circular buffer; when the file is full, each new entry replaces the oldest entry in the log. If the optional size parameter is not configured, the default value is used.

Default 100

netconf — Specifies that events selected for the log are directed to a NETCONF session as notifications. A NETCONF client can subscribe to a NETCONF log using the configured **netconf-stream** *stream-name* for the log in a subscription request. One or more NETCONF sessions can subscribe to a NETCONF log or stream.

session — Specifies that events selected for the log are directed to the current console or telnet session. This command is only valid for the duration of the session. When the session is terminated, the **to session** configuration is removed. A log ID with a **session** destination is saved in the configuration file but the **to session** part is not stored.

size — Specifies the maximum size of the log data destination, in bytes.

Values 50 to 3000

snmp — Specifies that events selected for the log are directed to the **snmp-trap-group** associated with the log ID. A local circular memory log is maintained for SNMP logs.

syslog *syslog-id* — Specifies that events selected for the log are directed to the specified syslog collector. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1024 bytes. The characteristics of the *syslog-id* referenced in this parameter must have already been defined in the **config**>**log**>**syslog** *syslog-id* context.

Values 1 to 10

Platforms All

24.127 to-aa-sub-counters

to-aa-sub-counters

Syntax **to-aa-sub-counters**
no to-aa-sub-counters

Context **[Tree]** (config>log>acct-policy>cr>aa to-aa-sub-counters)

Full Context configure log accounting-policy custom-record aa-specific to-aa-sub-counters

Description Commands in this context configure Application Assurance “to subscriber” counter parameters and only applies to the 7750 SR.

The **no** form of this command excludes the “to subscriber” count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.128 to-client-options

to-client-options

Syntax **to-client-options**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host to-client-options)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host to-client-options)

Full Context configure subscriber-mgmt local-user-db ipoe host to-client-options
configure subscriber-mgmt local-user-db ppp host to-client-options

Description Commands in this context configure DHCP options to send to the client.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.129 to-sap

to-sap

Syntax **to-sap** *sap-id*
no to-sap

Context **[Tree]** (config>service>vpls>sap>snooping>mvr to-sap)

Full Context configure service vpls sap snooping mvr to-sap

Description In some situations, the multicast traffic should not be copied from the MVR VPLS to the SAP on which the IGMP message was received (standard MVR behavior) but to another SAP.

This command configures the SAP to which the multicast data needs to be copied.

The **no** form of this command reverts to the default value.

Parameters *sap-id* — Specifies the SAP to which multicast channels should be copied.

to-sap

Syntax **to-sap** *sap-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no to-sap

Context [Tree] (config>service>vpls>sap>igmp-snooping>mvr to-sap)

Full Context configure service vpls sap igmp-snooping mvr to-sap

Description In some situations, the multicast traffic should not be copied from the MVR VPLS to the SAP on which the IGMP message was received (standard MVR behavior) but to another SAP.

This command configures the SAP to which the multicast data needs to be copied.

Default no to-sap

Parameters *sap-id* — Specifies the SAP to which multicast channels should be copied

Platforms All

24.130 to-server-options

to-server-options

Syntax [**no**] **to-server-options**

Context [Tree] (config>subscr-mgmt>loc-user-db>ipoe>host to-server-options)

Full Context configure subscriber-mgmt local-user-db ipoe host to-server-options

Description Commands in this context configure DHCP options to send to the server.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.131 to-subscriber

to-subscriber

Syntax **to-subscriber**

Context [Tree] (config>isa>aa-grp>qos>egress to-subscriber)

Full Context configure isa application-assurance-group qos egress to-subscriber

Description Commands in this context configure Quality of Service for this application assurance group to-subscriber logical port, traffic destined to AA subscribers and entering an application assurance engine.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.132 tod-override

tod-override

Syntax **tod-override** *tod-override-id* [**create**]
no tod-override *tod-override-id*

Context **[Tree]** (config>app-assure>group>policer tod-override)

Full Context configure application-assurance group policer tod-override

Description This commands creates a time of day override policy for a given policer. Up to 8 overrides can be configured per policer. Rate/mbs/cbs/flow-rate/flow-count configured in each override-id will override the default policer values at the specified time of day configured in the override.

Parameters *tod-override-id* — Specifies the time of day override ID.

Values 1 to 255

create — Keyword used to create the time of day override policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.133 tolerance

tolerance

Syntax **tolerance** [*seconds* | **forever**]
no tolerance

Context **[Tree]** (config>system>security>keychain>direction>bi>entry tolerance)
[Tree] (config>system>security>keychain>direction>uni>receive>entry tolerance)

Full Context configure system security keychain direction bi entry tolerance
configure system security keychain direction uni receive entry tolerance

Description This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the duration that an eligible receive key overlaps with the active send key.

Values 0 to 4294967294 seconds

forever — Specifies that an eligible receive key overlap with the active send key forever.

Platforms All

24.134 tos-marking-state

tos-marking-state

Syntax **tos-marking-state** {**trusted** | **untrusted**}
no tos-marking-state

Context **[Tree]** (config>service>ies>if tos-marking-state)
[Tree] (config>service>ies>sub-if>grp-if tos-marking-state)
[Tree] (config>service>vprn>interface tos-marking-state)
[Tree] (config>service>vprn>sub-if>grp-if tos-marking-state)

Full Context configure service ies interface tos-marking-state
configure service ies subscriber-interface group-interface tos-marking-state
configure service vprn interface tos-marking-state
configure service vprn subscriber-interface group-interface tos-marking-state

Description This command is used to alter the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field are not remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all VPRN and network IP interface as untrusted.

When the ingress interface is set to untrusted, all egress network IP interfaces remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived from the egress network QoS definitions.

Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing.

The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The **save config** command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command restores the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

Default tos-marking-state trusted

Parameters **trusted** — The default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set.

untrusted — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface tos-marking-state
- configure service ies subscriber-interface group-interface tos-marking-state

All

- configure service vprn interface tos-marking-state
- configure service ies interface tos-marking-state

tos-marking-state

Syntax **tos-marking-state** {**trusted** | **untrusted**}
no tos-marking-state

Context **[Tree]** (config>service>vprn>nw-if tos-marking-state)

Full Context configure service vprn network-interface tos-marking-state

Description This command is used to alter the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field will not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all VPRN and network IP interface as untrusted.

When the ingress interface is set to untrusted, all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived from the egress network QoS definitions. Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The **save config** command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

The **no** tos-marking-state command is used to restore the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

Default tos-marking-state trusted

Parameters **trusted** — The default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set.

untrusted — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.

Platforms All

tos-marking-state

Syntax **tos-marking-state** {**trusted** | **untrusted**}
no tos-marking-state

Context **[Tree]** (config>router>if tos-marking-state)

Full Context configure router interface tos-marking-state

Description This command is used on a network IP interface to alter the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field will not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all IES and network IP interface as untrusted. When the ingress network IP interface is set to untrusted, all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived from the egress network QoS definitions. Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing. The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The **save config** command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command is used to restore the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

Default tos-marking-state trusted

Parameters **trusted** — Specifies that the default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set

untrusted — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.

Platforms All

24.135 total

total

Syntax **total** *percent*

Context **[Tree]** (config>isa>video-group>watermark>bandwidth total)
[Tree] (config>isa>video-group>watermark>session total)

Full Context configure isa video-group watermark bandwidth total
configure isa video-group watermark session total

Description This command sets the watermark to trigger the SNMP trap if the combined FCC and RET bandwidth or session exceeds the configured percentage. The bandwidth is the available egress bandwidth of the ISA. The SNMP trap is cleared when the consumption is lowered by 10%. For example, if the system resource of the bandwidth available is 10 Gb/s and the watermark is configured to be 90%, the SNMP trap is raised as the bandwidth exceeds 9 Gb/s (90% of 10 Gb/s). The SNMP trap is cleared when the bandwidth drops below 8.1 Gb/s (10% of 9 Gb/s = 0.9 Gb/s, and 9 Gb/s - 0.9 Gb/s = 8.1 Gb/s). The default value of the watermark is set at 90% of the system resources for both bandwidth and session.

Default total 90

Parameters *percent* — Specifies the percentage of the system resources per ISA.

Values 1 to 99

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.136 total-capacity

total-capacity

Syntax **total-capacity** *capacity*
no total-capacity

Context **[Tree]** (config>mcast-mgmt>chassis-level>plane-capacity total-capacity)

Full Context configure mcast-management chassis-level per-mcast-plane-capacity total-capacity

Description This command configures the total multicast plane capacity supported individually by all switch fabric multicast planes.

The multicast plane capacity is determined based on the provisioned line cards and switch fabrics in the chassis.

The **no** form of this command reverts to the default.

Parameters *capacity* — Specifies the multicast plane capacity in Mb/s.

Values 2000, 4000, 5250, 8250, 15000, 19000, dynamic (Specifies that multicast plane capacity is determined based on provisioned line cards and switch fabrics in the chassis.)

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-s, 7950 XRS, VSR

24.137 total-flow-duration

total-flow-duration

Syntax [**no**] **total-flow-duration**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-cntr total-flow-duration)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-counters total-flow-duration

Description This command includes the total flow duration flow count in the AA subscriber's custom record. This command only applies to the 7750 SR.

The **no** form of this command excludes the total flow duration flow count.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.138 total-flows-completed-count

total-flows-completed-count

Syntax [**no**] **total-flows-completed-count**

Context **[Tree]** (config>log>acct-policy>cr>aa>aa-sub-cntr total-flows-completed-count)

Full Context configure log accounting-policy custom-record aa-specific aa-sub-counters total-flows-completed-count

Description This command includes the total flows completed count in the AA subscriber's custom record. This command only applies to the 7750 SR.

The **no** form of this command excludes the total flow duration flow count.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.139 tp-tunnel-id-range

tp-tunnel-id-range

Syntax **tp-tunnel-id-range** *start-id end-id*
no tp-tunnel-id-range

Context **[Tree]** (config>router>mpls>mpls-tp tp-tunnel-id-range)

Full Context configure router mpls mpls-tp tp-tunnel-id-range

Description This command configures the range of MPLS tunnel IDs reserved for MPLS-TP LSPs. The maximum difference between the start-id and end-id is 4K.

The tunnel ID referred to here is the RSVP-TE tunnel ID. This maps to the MPLS-TP Tunnel Number. There are some cases where the dynamic LSPs may have caused fragmentation to the number space such that contiguous range [*end-id* – *start-id*] is not available. In these cases, the command will fail.

There are no default values for the *start-id* and *end-id* of the tunnel id range, and they must be configured to enable MPLS-TP.

Default no tp-tunnel-id-range

Parameters *start-id* — Specifies the start ID.

Values 1 to 61440

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

end-id — Specifies the end ID.

Values 1 to 61440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.140 trace

trace

Syntax **trace sap** *sap-id* [**mac** *ieee-address*] [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]
trace mac *ieee-address* [**sap** *sap-id*] [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]
trace circuit-id *circuit-id* [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]
trace remote-id *remote-id* [**profile** *trace-profile-name*] [**trace-existing-sessions**] [**max-jobs** *num*] [**name** *trace-name*]
no trace [**sap** *sap-id*] [**mac** *ieee-address*] [{**circuit-id** *circuit-id* | **remote-id** *remoteid*}]
no trace name *trace-name*

Context **[Tree]** (debug>call-trace>ipoe trace)

Full Context debug call-trace ipoe trace

Description This command enables tracing for IPoE sessions specified by the configured parameters. This command can trace a single session or multiple sessions, and can use wildcard characters.

This command can be executed multiple times to start multiple traces. When rules overlap, such as for a wildcard SAP and a specific SAP, the rule that a specific trace is associated with cannot be guaranteed.

The **no** form of this command prevents new traces from being configured and terminates all trace jobs that were previously started using the **trace** command.

Parameters *circuit-id* — Specifies a circuit ID that is used to filter sessions to trace. The *circuit-id* and *remote-id* parameters are mutually exclusive.

ieee-address — Specifies a MAC address that is used to identify a session to trace, in the format “ab:cd:ef:01:23:45”. A wildcard character can be used to match all remaining octets; for example, the format “ab:cd:ef:*” can be used to filter by OUI.

num — Specifies the maximum number of jobs that may be started with this rule.

Values 1 to 50

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

remote-id — Specifies a remote ID that is used to filter sessions to trace. The *remote-id* and *circuit-id* parameters are mutually exclusive.

sap-id — Specifies a SAP to trace. The following formats are accepted:

- *port*/*lag*/*pw-port*:*svlan.cvlan*
- *port*/*lag*/*pw-port*:*vlan*
- *port*/*lag*/*pw-port*
- *port*/*lag*/*pw-port*:*vlan*.*
- *port*/*lag*/*pw-port*:* (also matches *.*)

trace-existing-sessions — Specifies that existing IPoE sessions is traced. If this parameter is not included, only new IPoE sessions is traced.

trace-name — Specifies the name by which the trace is referenced, up to 16 characters.

trace-profile-name — Specifies the name of the trace profile to be applied. The default parameters is used if a trace profile is not specified.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.141 trace-profile

trace-profile

Syntax **trace-profile** *profile-name* [**create**]
no trace-profile *profile-name*

Context **[Tree]** (config>call-trace trace-profile)

Full Context configure call-trace trace-profile

Description This command creates a profile that can be applied to a specific trace job.

Parameters *profile-name* — Specifies the unique name of the call trace profile.

create — Keyword used to create the trace profile instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.142 trace-string

trace-string

Syntax **trace-string** [*trace-string*]
no trace-string

Context **[Tree]** (config>port>sonet-sdh>path trace-string)

Full Context configure port sonet-sdh path trace-string

Description This command specifies that a J1-path-trace that identifies the circuit is inserted continuously at source. This can be checked against the expected value by the receiver. If no trace string is entered then a null string is used.

The **no** form of this command resets the string to its default.

This command is supported on TDM satellite.

Default The default J1 value is *Alcatel XXX YYY* where XXX is the platform number, such as “7750” or “7450”, and YYY is the platform acronym, such as “SR” or “ESS”. The value does not change when the encap-type changes. The J1 string contains all zeros for a non-provisioned path.

Parameters *trace-string* — Specifies either a string up to 62 bytes for SONET or 15 bytes for SDH. If the string contains spaces, enclose it in quotation marks. String ‘zeros’ will send all zeros in the J1 bytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.143 traceroute

traceroute

Syntax **traceroute** *ip-address* | *dns-name* [**probe-count** *probes-per-hop*] [**detail**] [**dest-port** *port-number*] [**dest-port-udp-fixed**] [**min-ttl** *min-ttl*] [**no-dns**] [**protocol udp | tcp**] [{**router** *router-or-service*} | {**router-instance** *router-instance*} | {**service-name** *service-name*}] [**size** *pad-size*] [**source** *ip-address*] [**tos** *type-of-service*] [**ttl** *max-ttl*] [**wait** *milliseconds*]

Context **[Tree]** (global traceroute)

Full Context global traceroute

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description The IP traceroute utility determines the route to a destination address. DNS lookups of the responding hosts are enabled by default.

The following shows a traceroute example.

```
*A:ALA-1# traceroute 192.168.xx.xx4
traceroute to 192.168.xx.xx4, 30 hops max, 40 byte packets
 1  192.168.xx.xx4 0.000 ms  0.000 ms  0.000 ms
*A:ALA-1#
```

Parameters **dest-port-udp-fixed** — Specifies that the destination UDP port number should not increment with each packet transmitted. By default, the UDP traceroute starts with destination UDP port 33434 and each subsequent packet sent to this destination UDP port increases by 1. The next packet uses UDP seat port 33435, the next 33436, and so on.

For a UDP test, this parameter prevents the per-transmitted packet increment of the destination UDP port number. The TCP protocol does not increment the destination TCP port, using a single destination TCP port for all traceroute packets for the test.

dns-name — Specifies the DNS name, up to 63 characters, of the far-end device to which to send the traceroute request message.

detail — Displays additional information about the resulting packet.

ip-address — Specifies the far-end IP address to which to send the traceroute request message in dotted decimal notation.

Values

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]

max-ttl — Specifies the maximum Time-To-Live (TTL) value to include in the traceroute request, expressed as a decimal integer.

Values 1 to 255

Default 30

milliseconds — Specifies the time in milliseconds to wait for a response to a probe, expressed as a decimal integer.

Values 1 to 60000

Default 5000

min-ttl — Specifies the IP TTL in the initial traceoute packet to target a specific node or starting node along the path.

Values 1 to 255

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no-dns — Specifies that, when the **no-dns** keyword is specified, DNS lookups of the responding hosts are not performed, and only the IP addresses are printed.

pad-size — Specifies the number of bytes added to the UDP or TCP payload.

Values 0 to 9786

Default 0

port-number — Specifies the transport protocol destination port number.

Values 1 to 65535

Default 33434

probes-per-hop — Specifies the number of probes per hop.

Values 1 to 10

Default 3

protocol udp | tcp — Sets the transport protocol for the traceroute packet. The TCP protocol is silently discarded on a targeted VRPN service. VPRN services only respond to UDP traceroutes.

Default udp

router-or-service — Specifies the routing instance or service, by number. The *router-instance* parameter is the preferred parameter to specify the router or service.

Values router-name: Base, management, vpls-management
vprn-svc-id: 1 to 2147483647

Default Base

router-instance — Specifies the preferred method for entering a service name. Stored as the service name. This is the only service-linking function allowed for both mixed-mode and model-driven configuration modes.

Values router-name: Base, management, *cpm-vr-name*, vpls-management
vprn-svc-name: up to 64 characters
cpm-vr-name: up to 32 characters

service-name — Specifies the alias function that allows the service-name to be used, converted and stored as service ID.

source *ip-address* — Specifies the source IP address to use as the source of the probe packets, in dotted decimal notation. If the IP address is not one of the device's interfaces, an error is returned.

Values

ipv4-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type-of-service — Specifies the Type-of-Service (ToS) bits in the IP header of the probe packets, expressed as a decimal integer.

Values 0 to 255

Default 0

Output The following are examples of traceroute information.

traceroute for IPv4 SR policy with icmp-tunneling

```
*A:Dut-A# traceroute 11.21.1.6 detail no-dns traceroute to 11.21.1.6, 30 hops max, 4
0 byte packets
  1   1  10.10.11.3  3.36 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28303, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =   28306, Exp = 7, TTL =   1, S = 0
             entry  3:  MPLS Label =  524283, Exp = 7, TTL =   1, S = 1
  1   2  10.10.11.3  3.68 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28303, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =   28306, Exp = 7, TTL =   1, S = 0
             entry  3:  MPLS Label =  524283, Exp = 7, TTL =   1, S = 1
  1   3  10.10.11.3  4.18 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28303, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =   28306, Exp = 7, TTL =   1, S = 0
             entry  3:  MPLS Label =  524283, Exp = 7, TTL =   1, S = 1
  2   1  10.10.10.5  3.77 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28506, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =  524283, Exp = 7, TTL =   2, S = 1
  2   2  10.10.10.5  8.02 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28506, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =  524283, Exp = 7, TTL =   2, S = 1
  2   3  10.10.10.5  4.72 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28506, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =  524283, Exp = 7, TTL =   2, S = 1
  3   1  11.21.1.6  5.33 ms
  3   2  11.21.1.6  4.77 ms
  3   3  11.21.1.6  4.07 ms
```

traceroute for IPv6 SR policy with icmp-tunneling

```
*A:Dut-A# traceroute fc00::b15:106 detail no-dns traceroute to fc00::b15:106, 30 hop
s max, 60 byte packets
  1   1  fc00::a0a:b03  3.41 ms
         returned MPLS Label Stack Object
             entry  1:  MPLS Label =   28303, Exp = 7, TTL =   1, S = 0
             entry  2:  MPLS Label =   28306, Exp = 7, TTL =   1, S = 0
             entry  3:  MPLS Label =       2, Exp = 7, TTL =   1, S = 1
  1   2  fc00::a0a:b03  2.58 ms
         returned MPLS Label Stack Object
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
            entry  1:  MPLS Label =   28303, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28306, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =       2, Exp = 7, TTL =   1, S = 1
  1   3  fc00::a0a:b03  3.90 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28303, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28306, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =       2, Exp = 7, TTL =   1, S = 1
  2   1  fc00::a0a:a05  4.65 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28506, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =       2, Exp = 7, TTL =   2, S = 1
  2   2  fc00::a0a:a05  4.85 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28506, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =       2, Exp = 7, TTL =   2, S = 1
  2   3  fc00::a0a:a05  4.78 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28506, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =       2, Exp = 7, TTL =   2, S = 1
  3   1  fc00::b15:106  2.89 ms
  3   2  fc00::b15:106  3.58 ms
  3   3  fc00::b15:106  4.15 ms
```

traceroute for SR-OSPF3 with icmp-tunneling

```
A:Dut-A# traceroute fc00::b14:106 detail traceroute to fc00::b14:106, 30 hops max, 6
0 byte packets
  1   1  fc00::a0a:402  (fc00::a0a:402)  4.38 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   29266, Exp = 7, TTL =   1, S = 1
  1   2  fc00::a0a:402  (fc00::a0a:402)  3.42 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   29266, Exp = 7, TTL =   1, S = 1
  1   3  fc00::a0a:402  (fc00::a0a:402)  4.19 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   29266, Exp = 7, TTL =   1, S = 1
  2   1  fc00::a0a:904  (fc00::a0a:904)  4.05 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   29466, Exp = 7, TTL =   1, S = 1
  2   2  fc00::a0a:904  (fc00::a0a:904)  3.62 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   29466, Exp = 7, TTL =   1, S = 1
  2   3  fc00::a0a:904  (fc00::a0a:904)  4.64 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   29466, Exp = 7, TTL =   1, S = 1
  3   1  fc00::b14:106  (fc00::b14:106)  3.35 ms
  3   2  fc00::b14:106  (fc00::b14:106)  4.02 ms
  3   3  fc00::b14:106  (fc00::b14:106)  3.30 ms
```

traceroute for a label-ipv4 with icmp-tunneling over IPv6 SR-TE LSP (requires IPv4 system address)

```
*A:Dut-F# traceroute 11.21.1.1 source 11.21.1.6 detail
traceroute to 11.21.1.1 from 11.21.1.6, 30 hops max, 40 byte packets
  1   1  10.20.1.4  (10.20.1.4)  4.96 ms
        returned MPLS Label Stack Object
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
            entry  1:  MPLS Label =  524270, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524236, Exp = 7, TTL =   1, S = 1
  1   2  10.20.1.4  (10.20.1.4)  5.35 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524270, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524236, Exp = 7, TTL =   1, S = 1
  1   3  10.20.1.4  (10.20.1.4)  5.43 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524270, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524236, Exp = 7, TTL =   1, S = 1
  2   1  10.20.1.2  (10.20.1.2)  4.72 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524236, Exp = 7, TTL =   2, S = 1
  2   2  10.20.1.2  (10.20.1.2)  5.71 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524236, Exp = 7, TTL =   2, S = 1
  2   3  10.20.1.2  (10.20.1.2)  5.03 ms
        returned MPLS Label Stack Object
           entry  1:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524236, Exp = 7, TTL =   2, S = 1
  3   1  11.21.1.1  (11.21.1.1)  3.51 ms
  3   2  11.21.1.1  (11.21.1.1)  3.91 ms
  3   3  11.21.1.1  (11.21.1.1)  3.09 ms
```

traceroute for a label-ipv6 with icmp-tunneling over IPv6 SR-TE LSP

```
*A:Dut-F# traceroute fc00::b15:101 detail
traceroute to fc00::b15:101, 30 hops max, 60 byte packets
  1   1  fc00::a0a:404  (fc00::a0a:404)  3.36 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524270, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =       2, Exp = 7, TTL =   1, S = 1
  1   2  fc00::a0a:404  (fc00::a0a:404)  3.46 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524270, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =       2, Exp = 7, TTL =   1, S = 1
  1   3  fc00::a0a:404  (fc00::a0a:404)  3.77 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524270, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =       2, Exp = 7, TTL =   1, S = 1
  2   1  fc00::a0a:102  (fc00::a0a:102)  4.54 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =       2, Exp = 7, TTL =   2, S = 1
  2   2  fc00::a0a:102  (fc00::a0a:102)  4.70 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =       2, Exp = 7, TTL =   2, S = 1
  2   3  fc00::a0a:102  (fc00::a0a:102)  3.63 ms
        returned MPLS Label Stack Object
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
            entry  1:  MPLS Label =  524285, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =       2, Exp = 7, TTL =   2, S = 1
  3   1  fc00::b15:101  (fc00::b15:101)  3.40 ms
  3   2  fc00::b15:101  (fc00::b15:101)  3.15 ms
  3   3  fc00::b15:101  (fc00::b15:101)  3.23 ms
```

traceroute for a VPN IPv4 with icmp-tunneling over IPv6 SR-TE LSP (requires IPv4 system address)

```
*A:Dut-F# traceroute router-instance "vprn.sr-te.4" 1.0.4.1 source 6.0.4.1 detail
traceroute to 1.0.4.1 from 6.0.4.1, 30 hops max, 40 byte packets
  1   1  10.20.1.4  (10.20.1.4)  5.03 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28462, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   1, S = 1
  1   2  10.20.1.4  (10.20.1.4)  4.52 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28462, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   1, S = 1
  1   3  10.20.1.4  (10.20.1.4)  5.61 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28462, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   1, S = 1
  2   1  10.20.1.2  (10.20.1.2)  5.38 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28262, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   2, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   2, S = 1
  2   2  10.20.1.2  (10.20.1.2)  5.39 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28262, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   2, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   2, S = 1
  2   3  10.20.1.2  (10.20.1.2)  5.27 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28262, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   2, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   2, S = 1
  3   1  1.0.4.1  (1.0.4.1)  4.09 ms
  3   2  1.0.4.1  (1.0.4.1)  4.47 ms
  3   3  1.0.4.1  (1.0.4.1)  4.13 ms
```

traceroute for a VPN IPv6 with icmp-tunneling over IPv6 SR-TE LSP

```
*A:Dut-F # traceroute router 5004 fc00::100:401 detail
traceroute to fc00::100:401, 30 hops max, 60 byte packets
  1   1  fc00::a0a:404  (fc00::a0a:404)  5.45 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28462, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   1, S = 1
  1   2  fc00::a0a:404  (fc00::a0a:404)  5.14 ms
         returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28462, Exp = 7, TTL =   1, S = 0
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   1, S = 1
  1   3  fc00::a0a:404  (fc00::a0a:404)  5.31 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28462, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   1, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   1, S = 1
  2   1  fc00::a0a:102  (fc00::a0a:102)  4.70 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28262, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   2, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   2, S = 1
  2   2  fc00::a0a:102  (fc00::a0a:102)  5.20 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28262, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   2, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   2, S = 1
  2   3  fc00::a0a:102  (fc00::a0a:102)  5.16 ms
        returned MPLS Label Stack Object
            entry  1:  MPLS Label =   28262, Exp = 7, TTL =   1, S = 0
            entry  2:  MPLS Label =   28261, Exp = 7, TTL =   2, S = 0
            entry  3:  MPLS Label =  524241, Exp = 7, TTL =   2, S = 1
  3   1  fc00::100:401  (fc00::100:401)  5.38 ms
  3   2  fc00::100:401  (fc00::100:401)  4.48 ms
  3   3  fc00::100:401  (fc00::100:401)  4.39 ms
```

traceroute for IPv4 using tcp and the detail option. Reaching the destination and the port is closed on the destination.

```
traceroute 192.168.34.2 protocol tcp detail
traceroute to 192.168.34.2, 30 hops max, 40 byte packets
  1   1  192.168.13.2  (192.168.13.2)  0.755 ms
  1   2  192.168.13.2  (192.168.13.2)  0.913 ms
  1   3  192.168.13.2  (192.168.13.2)  0.928 ms
  2   1  192.168.34.2  (192.168.34.2)  1.19 ms (port closed)
  2   2  192.168.34.2  (192.168.34.2)  1.29 ms (port closed)
  2   3  192.168.34.2  (192.168.34.2)  1.59 ms (port closed)
```

traceroute for IPv4 using tcp and the detail option. Reaching the destination and the port is open on the destination.

```
traceroute 192.168.34.2 protocol tcp dest-port 862 detail
traceroute to 192.168.34.2, 30 hops max, 40 byte packets
  1   1  192.168.13.2  (192.168.13.2)  0.915 ms
  1   2  192.168.13.2  (192.168.13.2)  0.861 ms
  1   3  192.168.13.2  (192.168.13.2)  0.825 ms
  2   1  192.168.34.2  (192.168.34.2)  1.42 ms (port open)
  2   2  192.168.34.2  (192.168.34.2)  1.27 ms (port open)
  2   3  192.168.34.2  (192.168.34.2)  1.52 ms (port open)
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.144 traceroute-reply

traceroute-reply

Syntax [**no**] **traceroute-reply**

Context **[Tree]** (config>service>ies>if>ipv6>vrrp traceroute-reply)

Full Context configure service ies interface ipv6 vrrp traceroute-reply

Description This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **trace-route-reply** status.

Default no traceroute-reply

Platforms All

traceroute-reply

Syntax [**no**] **traceroute-reply**

Context **[Tree]** (config>service>ies>if>vrrp traceroute-reply)

Full Context configure service ies interface vrrp traceroute-reply

Description This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **trace-route-reply** status.

Default no traceroute-reply

Platforms All

traceroute-reply

Syntax [**no**] **traceroute-reply**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>if>vrrp traceroute-reply)
[Tree] (config>service>vprn>if>ipv6>vrrp traceroute-reply)

Full Context configure service vprn interface ipv6 vrrp traceroute-reply
configure service vprn interface vrrp traceroute-reply

Description This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **trace-route-reply** status.

Default no traceroute-reply

Platforms All

traceroute-reply

Syntax [**no**] **traceroute-reply**

Context [Tree] (config>router>if>vrrp traceroute-reply)
[Tree] (config>router>if>ipv6>vrrp traceroute-reply)

Full Context configure router interface ipv6 vrrp traceroute-reply
configure router interface vrrp traceroute-reply

Description This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **trace-route-reply** status.

Default no traceroute-reply

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.145 track-accounting

track-accounting

Syntax **track-accounting** [**start**] [**stop**][**interim-update**][**accounting-on**] [**accounting-off**]
no track-accounting

Context **[Tree]** (config>router>radius-proxy>server>cache track-accounting)
[Tree] (config>service>vprn>radius-proxy>server>cache track-accounting)

Full Context configure router radius-proxy server cache track-accounting
configure service vprn radius-proxy server cache track-accounting

Description This command specifies the type of RADIUS accounting packets from RADIUS client (a WIFI AP) that the router should track.

The **no** form of this command removes the parameters from the configuration.

Parameters **start** — Specifies that the router will update the associated ESM-host with the RADIUS client (for example, a WIFI AP) that generated the accounting-start. This is required in cases where a UE roams to a new AP that does not re-authenticate due to key caching.

stop — Specifies that the router will remove the corresponding ESM host and forward the accounting-stop packet to the external RADIUS server.

accounting-on | accounting-off — Specifies that the router will remove all ESM hosts associated with the RADIUS client (a WIFI AP), and forward the accounting-on packet to the external RADIUS server.

interim-update — Specifies that the router will update the associated ESM-host with the RADIUS client (a WIFI AP) that generated the interim-update. The interim-updates with the updated information are sent to the RADIUS server as scheduled.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.146 track-authentication

track-authentication

Syntax **track-authentication** [**accept**]
no track-authentication

Context **[Tree]** (config>router>radius-proxy>server>cache track-authentication)
[Tree] (config>service>vprn>radius-proxy>server>cache track-authentication)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router radius-proxy server cache track-authentication
configure service vprn radius-proxy server cache track-authentication

Description This command specifies if RADIUS authentication (from the AP) should be tracked in order to update the ESM host with the RADIUS client (for example, WIFI AP) on UE mobility. It also specifies the authentication packet from RADIUS client (for example, a WIFI AP) that the router should track for mobility.

The **no** form of this command stops tracking authentication for UE mobility.

Default track-authentication accept

Parameters **accept** — Indicates access-accept is tracked for mobility.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.147 track-delete-hold-time

track-delete-hold-time

Syntax **track-delete-hold-time** *seconds*
no track-delete-hold-time

Context **[Tree]** (config>router>radius-proxy>server>cache track-delete-hold-time)

Full Context configure router radius-proxy server cache track-delete-hold-time

Description This command specifies the delete hold-time in case the DHCP host gets a trigger to delete from the matched RADIUS Proxy server.

The **no** form of this command reverts to the default.

Default track-delete-hold-time 0

Parameters *seconds* — Specifies the delete hold time, in seconds.

Values 0 to 600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.148 track-mobility

track-mobility

Syntax **track-mobility**

Context **[Tree]** (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range track-mobility)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range track-mobility)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range track-mobility
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range track-mobility

Description Commands in this context configure RADIUS-proxy cache information required for subscribers that are created via data-triggered authentication. The RADIUS proxy cache enables efficient handling of UE mobility.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.149 track-password-change

track-password-change

Syntax [**no**] **track-password-change**

Context **[Tree]** (config>service>vprn>l2tp>group>l2tpv3 track-password-change)

Full Context configure service vprn l2tp group l2tpv3 track-password-change

Description This command enables tracking of password changes, allowing password tunnel passwords to be changed without bringing down active tunnels or sessions. This is only supported with L2TPv3.

The **no** form of this command disables password change tracking.

Default no track-password-change

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.150 track-srrp

track-srrp

Syntax **track-srrp** *srrp-instance* **peer** *ip-address* **sync-tag** *sync-tag*
no track-srrp *srrp-instance*

Context **[Tree]** (config>router>l2tp>failover track-srrp)
[Tree] (config>service>vprn>l2tp>failover track-srrp)

Full Context configure router l2tp failover track-srrp
configure service vprn l2tp failover track-srrp

Description This command sets the sync-tag to be used to synchronize the tunnels with track-srrp *srrp-id* to MCS *peer IP-@*. The same sync-tag should be configured on the MCS peer.

The **no** form of this command reverts to the default.

Default Removes the sync-tag for the indicated track-srrp.

Parameters *srrp-instance* — Specifies the Simple Router Redundancy Protocol (SRRP) instance used for Multi-Chassis redundancy failover that is associated with this Layer Two Tunneling Protocol Tunnel.

sync-tag — Specifies a synchronization tag to be used while synchronizing with the peer.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

track-srrp

Syntax [**no**] **track-srrp** [*srrp-instance*]

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync>track-srrp-instances track-srrp)

Full Context configure redundancy multi-chassis peer sync track-srrp-instances track-srrp

Description This command configures a tracked SRRP instance.

The **no** form of this command removes the SRRP instance identifier from the configuration.

Parameters *srrp-instance* — Indicates the unique identifier of the tracked SRRP instance.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

track-srrp

Syntax **track-srrp** *srrp-id*
no track-srrp

Context **[Tree]** (config>service>vpls>sap track-srrp)

Full Context configure service vpls sap track-srrp

Description This command configures the SRRP instance this capture SAP will track. This is a capture SAP level command. This command is important in PPPoE deployments with MSAPs. PPPoE operation requires that the MAC address learned by the client at the very beginning of the session negotiation phase remains unchanged for the lifetime of the session (RFC 2516). This command ensures that the virtual MAC address used during the PPPoE session negotiation phase on the capture SAP is the same virtual MAC address that is used by the SRRP on the group interface on which the session is established. Therefore, it is mandated that the SRRP instance (and implicitly the group-interface) where the session belongs to is known in advance. If the group interface name for the session is returned by the RADIUS, it must be ensured that this group interface is the one on which the tracked SRRP instance is configured. PPPoE sessions on the same capture SAP cannot be shared across multiple group interfaces, but instead they all must belong to a single group interface that is known in advance.

The same restrictions apply to IPoE clients in MC Redundancy scenario if they are to be supported concurrently on the same capture SAP as PPPoE.

The supported capture SAP syntax is this:

sap <port-id>:X.* capture-sap

The capture SAP syntax that is not supported is this:

sap <port-id>:*.* capture-sap

The **no** form of this command removes the SRRP ID from this configuration.

Parameters *srrp-id* — Specifies the SRRP instance number.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.151 track-srrp-instances

track-srrp-instances

Syntax **track-srrp-instances**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>redundancy>multi-chassis>peer>sync track-srrp-instances)

Full Context configure redundancy multi-chassis peer sync track-srrp-instances

Description Commands in this context configure tracked SRRP instances.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.152 tracking-support

tracking-support

Syntax [**no**] **tracking-support**

Context [Tree] (config>service>vprn>mvpn>pt>inclusive>pim tracking-support)

Full Context configure service vprn mvpn provider-tunnel inclusive pim tracking-support

Description This command enables the setting of the T bit in the LAN Prune Delay option of the Hello message. This indicates the router's capability to disable Join message suppression.

The **no** form of this command disables the setting.

Default no tracking-support

Platforms All

tracking-support

Syntax [**no**] **tracking-support**

Context [Tree] (config>service>vprn>pim>if tracking-support)

Full Context configure service vprn pim interface tracking-support

Description This command sets the T bit in the LAN Prune Delay option of the Hello Message. This indicates the router's capability to disable Join message suppression.

Default no tracking-support

Platforms All

tracking-support

Syntax [**no**] **tracking-support**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>pim>interface tracking-support)

Full Context configure router pim interface tracking-support

Description This command sets the T bit in the LAN Prune Delay option of the Hello Message. This indicates the router's capability to enable join message suppression. This capability allows for upstream routers to explicitly track join membership.

The **no** form of this command disables tracking support.

Default no tracking-support

Platforms All

24.153 traffic

traffic

Syntax **traffic** [**sir** *sir-val*] [**pir** *pir-val*] [**mir** *mir-val*] [**mbs** *mbs-val*] [**cdvt** *cdvt-val*]
no traffic

Context [Tree] (config>qos>atm-td-profile traffic)

Full Context configure qos atm-td-profile traffic

Description This command is used to configure traffic attributes of an ATM traffic profile as per ATM Forum Traffic Management Specification Version 4.1.

The traffic parameters of a traffic descriptor that are configurable depends on the service category of this traffic descriptor profile (see the **config>qos>atm-td-profile service-category** command).

Table 185 lists which traffic descriptor parameters are applicable for what service category and what are configuration rules between the parameters. **Y** indicates the parameter can be configured for a given service category and will be defaulted if not provided, an **N/A** indicates the parameter cannot be configured for a given service category (an error will be returned). If an applicable parameter is not specified, the current value will be preserved.

Table 185 **Traffic Descriptor Parameter Support by Service Category**

Service Category	SIR	PIR	MBS	MIR	CDVT
CBR		✓			✓
rt-VBR	✓	✓ (must be >= SIR)	✓		✓

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 185 **Traffic Descriptor Parameter Support by Service Category**

Service Category	SIR	PIR	MBS	MIR	CDVT
Nrt-VBR	✓	✓ (must be >= SIR)	✓		✓
UBR		✓			
UBR with MIR		✓ (must be >= MIR		✓ (non-zero MIR specified)	

When a traffic descriptor profile is used to define egress scheduling, the following describes how traffic rates are used to derive scheduling weight:

1. UBR PVCCs (i.e., MIR = 0) are assigned weight value of 1
2. UBR with MIR PVCCs are assigned weight value in the inclusive range from 1 to 255 based on the MIR rate
3. rt-VBR and nrt-VBR PVCCs are assigned weight value in the inclusive range from 1 to 255 based on the SCR rate
4. CBR PVCCs are assigned weight value in the inclusive range from 1 to 255 based on the PIR rate

The scheduling weight is derived from the traffic rate based on the following formula:

If traffic rate <= 32 kb/s, then weight = 1

If 32 kb/s < traffic rate < 8160 kb/s, then weight = floor (traffic rate / 32)

If traffic rate >= 8160 kb/s, then weight = 255

The configuration of weight unit (32 kb/s) is left for future releases.

Since the SAR operates in cells/second with 1 cell granularity, PIR and SCR values programmed need to be converted to cells per second. When converting values to be used for scheduler, the result is rounded up to the next cell when required by conversion.

When any of SIR, PIR, or MIR is greater than the physical maximum port/channel capacity for a given PVCC, then the maximum physical port/channel capacity is used in BW accumulation and when configuring the H/W for that PVCC.

Hardware- enforceable mbs is in the inclusive range from 3 to 256 000 cells. Any value outside of that range will be accepted and rounded up/down to the minimum/maximum enforceable value.

The **no** form of this command restores traffic parameters to their defaults for a given service category.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ATM traffic parameter default values are listed in Table 186 in kb/s.

Table 186 **ATM Traffic Parameter Defaults**

Service Category	Traffic Parameter Defaults
CBR:	
PIR	0
rt-VBR and nrt-VBR	
PIR	0
SCR	0
MBS	32
UBR (by default UBR is without MIR)	
PIR	0
MIR	0

Parameters **sir** *sir-val* — Sustained Information Rate (including cell overhead) in kilobits per second.

Values 0 to 4294967295

pir *pir-val* — Peak Information Rate (including cell overhead) in kilobits per second.

Values 0 to 4294967295

mir *mir-val* — Minimum Desired Information Rate (including cell overhead) in kilobits per second.

Values 0 to 4294967295

mbs *mbs-val* — Maximum Burst Size in cells.

Values 0 to 4294967295

cdvt *cdvt-val* — The Cell Delay Variation Tolerance (CDVT), in microseconds.

Default Depending upon a given service category:
CBR/RT-VBR/NRT-VBR 250

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.154 traffic-capture

traffic-capture

Syntax [**no**] **traffic-capture**

Context **[Tree]** (debug>app-assure>group traffic-capture)

Full Context debug application-assurance group traffic-capture

Description This command configures debugging for traffic capture.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.155 traffic-class

traffic-class

Syntax **traffic-class** *traffic-class*
no traffic-class

Context **[Tree]** (config>test-oam>build-packet>header>mpls traffic-class)
[Tree] (debug>oam>build-packet>packet>field-override>header>mpls traffic-class)

Full Context configure test-oam build-packet header mpls traffic-class
debug oam build-packet packet field-override header mpls traffic-class

Description This command defines the traffic class value to be used in the MPLS header.

The **no** form of this command removes the traffic class value.

Default traffic-class 0 (BE)

Parameters *traffic-class* — Specifies the MPLS traffic class to be used in the MPLS header.

Values 0 to 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.156 traffic-desc

traffic-desc

Syntax **traffic-desc** *traffic-desc-profile-id*
no traffic-desc

Context **[Tree]** (config>service>ies>sub-if>grp-if>sap>atm>egress traffic-desc)
[Tree] (config>service>ies>sub-if>grp-if>sap>atm>ingress traffic-desc)
[Tree] (config>service>vprn>sub-if>grp-if>sap>atm>egress traffic-desc)
[Tree] (config>service>vprn>sub-if>grp-if>sap>atm>ingress traffic-desc)
[Tree] (config>subscr-mgmt>msap-policy>atm>egress traffic-desc)
[Tree] (config>subscr-mgmt>msap-policy>atm>ingress traffic-desc)

Full Context configure service ies subscriber-interface group-interface sap atm egress traffic-desc
configure service ies subscriber-interface group-interface sap atm ingress traffic-desc
configure service vprn subscriber-interface group-interface sap atm egress traffic-desc
configure service vprn subscriber-interface group-interface sap atm ingress traffic-desc
configure subscriber-mgmt msap-policy atm egress traffic-desc
configure subscriber-mgmt msap-policy atm ingress traffic-desc

Description This command assigns an ATM traffic descriptor profile to a SAP.

When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract for ATM cells received from the SAP. When configured under the egress context, the specified traffic descriptor profile defines the traffic contract for ATM cells transmitted into the SAP.

The **no** form of this command reverts the traffic descriptor to the default traffic descriptor profile.

Default traffic-desc 1

Parameters *traffic-desc-profile-id* — Specifies an existing ATM traffic descriptor profile. Traffic descriptor profiles are configured in the **config>qos>atm-td-profile** context.

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

traffic-desc

Syntax **traffic-desc** *traffic-desc-profile-id*
no traffic-desc

Context **[Tree]** (config>port>sonet-sdh>path>atm>ilmi>egress traffic-desc)
[Tree] (config>port>sonet-sdh>path>atm>ilmi>ingress traffic-desc)

Full Context configure port sonet-sdh path atm ilmi egress traffic-desc

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure port sonet-sdh path atm ilmi ingress traffic-desc

Description This command associates an ATM traffic descriptor profile to an ILMI link. It is recommended to configure the traffic descriptors of this profile in accordance with the ILMI Traffic Requirements in the ILMI specification.

Default traffic-desc 1

Parameters *traffic-desc-profile-id* — Specifies an existing ATM traffic descriptor profile. Traffic descriptor profiles are configured in the **config>qos>atm-td-profile** context.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

traffic-desc

Syntax **traffic-desc** *traffic-desc-profile-id*
no traffic-desc

Context **[Tree]** (config>service>apipe>sap>atm>egress traffic-desc)
[Tree] (config>service>apipe>sap>atm>ingress traffic-desc)
[Tree] (config>service>epipe>sap>atm>egress traffic-desc)
[Tree] (config>service>epipe>sap>atm>ingress traffic-desc)
[Tree] (config>service>ies>if>sap>atm>egress traffic-desc)
[Tree] (config>service>ies>if>sap>atm>ingress traffic-desc)
[Tree] (config>service>vpls>sap>atm>ingress traffic-desc)
[Tree] (config>service>vpls>sap>atm>egress traffic-desc)
[Tree] (config>service>vprn>if>sap>atm>egress traffic-desc)
[Tree] (config>service>vprn>if>sap>atm>ingress traffic-desc)

Full Context configure service apipe sap atm egress traffic-desc
configure service apipe sap atm ingress traffic-desc
configure service epipe sap atm egress traffic-desc
configure service epipe sap atm ingress traffic-desc
configure service ies interface sap atm egress traffic-desc
configure service ies interface sap atm ingress traffic-desc
configure service vpls sap atm egress traffic-desc
configure service vpls sap atm ingress traffic-desc
configure service vprn interface sap atm egress traffic-desc
configure service vprn interface sap atm ingress traffic-desc

Description This command assigns an ATM traffic descriptor profile to a SAP or to an IES or VPRN interface.

When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract for ATM cells received from the SAP or interface. When configured under the egress context, the specified traffic descriptor profile defines the traffic contract for ATM cells transmitted into the SAP or interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts the traffic descriptor to the default traffic descriptor profile.

Default traffic-desc 1

Parameters *traffic-desc-profile-id* — Specifies an existing ATM traffic descriptor profile. Traffic descriptor profiles are configured in the **config>qos>atm-td-profile** context.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

24.157 traffic-direction

traffic-direction

Syntax **traffic-direction** {**subscriber-to-network** | **network-to-subscriber** | **both**}

Context **[Tree]** (config>app-assure>group>policy>aqp>entry>match traffic-direction)

Full Context configure application-assurance group policy app-qos-policy entry match traffic-direction

Description This command specifies the direction of traffic where the AQP match entry will be applied.

To use a policer action with the AQP entry the match criteria must specify a traffic-direction of either subscriber-to-network or network-to-subscriber.

Default traffic-direction both

Parameters **subscriber-to-network** — Traffic from a local subscriber will match this AQP entry.

network-to-subscriber — Traffic to a local subscriber will match this AQP entry.

both — Combines subscriber-to-network and network-to-subscriber.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.158 traffic-engineering

traffic-engineering

Syntax [**no**] **traffic-engineering**

Context **[Tree]** (config>router>isis traffic-engineering)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router isis traffic-engineering

Description This command enables this IS-IS instance to advertise TE link attributes for RSVP-TE and SR-TE enabled interfaces.

Default no traffic-engineering

Platforms All

traffic-engineering

Syntax [**no**] **traffic-engineering**

Context **[Tree]** (config>router>ospf traffic-engineering)

Full Context configure router ospf traffic-engineering

Description This command enables the advertisement of the traffic engineering information for the router and its links.

Traffic engineering enables the router to perform route calculations constrained by nodes or links. The traffic engineering of this router are limited to calculations based on link and nodal constraints.

The **no** form of this command disables the advertisement of the traffic engineering information.

Default no traffic-engineering

Platforms All

24.159 traffic-engineering-options

traffic-engineering-options

Syntax [**no**] **traffic-engineering-options**

Context **[Tree]** (config>router>isis traffic-engineering-options)

Full Context configure router isis traffic-engineering-options

Description Commands in this context configure advanced traffic-engineering options.

The **no** form of this command deletes the context.

Default no traffic-engineering-options

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

traffic-engineering-options

Syntax [**no**] **traffic-engineering-options**

Context **[Tree]** (config>router>ospf traffic-engineering-options)

Full Context configure router ospf traffic-engineering-options

Description Commands in this context configure the advanced traffic-engineering options.

The **no** form of this command removes the context to configure the advanced traffic-engineering options.

Default no traffic-engineering-options

Platforms All

24.160 traffic-rate-delta

traffic-rate-delta

Syntax **traffic-rate-delta** *rate*
no traffic-rate-delta

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive>umh-rm traffic-rate-delta)
[Tree] (config>service>vprn>mvpn>pt>selective>umh-rm>group>source traffic-rate-delta)

Full Context configure service vprn mvpn provider-tunnel inclusive umh-rate-monitoring traffic-rate-delta
configure service vprn mvpn provider-tunnel selective umh-rate-monitoring group source traffic-rate-delta

Description This command configures the bandwidth delta upwards of which the traffic is switched from the primary UMH to the backup UMH.

The **no** form of this command removes UMH redundancy with bandwidth monitoring.

Default 1

Parameters *rate* — Specifies the bandwidth delta, in kbps.

Values 1 to 4294967294

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.161 traffic-type

traffic-type

Syntax [**no**] **traffic-type**

Context **[Tree]** (config>app-assure>group>statistics>aa-partition traffic-type)

Full Context configure application-assurance group statistics aa-partition traffic-type

Description This command enables traffic type statistics collection within an aa-partition.

The no form of this command disables traffic type statistics collection.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.162 transaction-timer

transaction-timer

Syntax **transaction-timer** *seconds*
no transaction-timer

Context **[Tree]** (config>aaa>diam-peer-plcy transaction-timer)
[Tree] (config>aaa>diam-peer-plcy>peer transaction-timer)

Full Context configure aaa diameter-peer-policy peer transaction-timer
configure aaa diameter-peer-policy transaction-timer

Description This command defines the time-out value for the Base Diameter messages (CER, DPR). When the transaction-timer expires, an appropriate action is taken for each message type.

This timer is used in the following cases:

- Opening the TCP connection (and completing the 3-way handshake) - if the TCP ACK is not received within the time specified by the transaction-timer, the TCP connection is closed and the connection-timer is started waiting for the new connection to be initiated
- Capability Exchange — If the response to the CER message (CEA) is not received within the time specified by the transaction-timer, the peer connection is closed and the connection-timer is started waiting for the new connection to be initiated.
- Peer disconnect Request — If the response to the DPR message is not received (DPA) within the time specified by the **transaction-timer**, the peer connection is closed.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command reverts to the default.

Parameters *seconds* — Specifies the policy peer transaction timer, in seconds.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.163 transceiver

transceiver

Syntax **transceiver**

Context **[Tree]** (config>port transceiver)

Full Context configure port transceiver

Description Commands in this context configure transceiver parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.164 transform

transform

Syntax **transform** *transform-id* [*transform-id*]
no transform

Context **[Tree]** (config>ipsec>tnl-temp transform)
[Tree] (config>ipsec>trans-mode-prof>dyn transform)
[Tree] (config>service>ies>if>ipsec>ipsec-tunnel>dyn transform)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn transform)
[Tree] (config>service>ies>if>sap>ipsec-gw transform)
[Tree] (config>service>vprn>if>sap>ipsec-gw transform)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel transform)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn transform)

Full Context configure ipsec tunnel-template transform
configure ipsec ipsec-transport-mode-profile dynamic-keying transform
configure router interface ipsec ipsec-tunnel dynamic-keying transform
configure service ies interface ipsec ipsec-tunnel dynamic-keying transform
configure service ies interface sap ipsec-gw transform

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface ipsec ipsec-tunnel dynamic-keying transform
configure service vprn interface sap ipsec-gw transform
configure service vprn interface sap ipsec-tunnel transform

Description This command associates the IPsec transform sets allowed for this the CHILD_SA. A maximum of four transforms can be specified. The transforms are listed in decreasing order of preference (the first one specified is the most preferred).

The **no** form of this command removes the transform ID from the configuration.

Default no transform

Parameters *transform-id* — Specifies a number to identify a tranform used for CHILD_SA negotiation. Up to four transform ID can be specified.

Values 1 to 2048

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure ipsec ipsec-transport-mode-profile dynamic-keying transform
- configure ipsec tunnel-template transform

VSR

- configure service vprn interface ipsec ipsec-tunnel dynamic-keying transform
- configure service ies interface ipsec ipsec-tunnel dynamic-keying transform
- configure router interface ipsec ipsec-tunnel dynamic-keying transform

transform

Syntax **transform** *transform-id* [*transform-id*]
no transform

Context **[Tree]** (config>service>vprn>if>sap>ipsec-tun>dyn transform)

Full Context configure service vprn interface sap ipsec-tunnel dynamic-keying transform

Description This command associates the IPsec transform sets allowed for this tunnel. A maximum of four transforms can be specified. The transforms are listed in decreasing order of preference (the first one specified is the most preferred).

Default no transform

Parameters *transform-id* — Specifies the value used for transforms for dynamic keying.

Values 1 to 2048

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.165 transit

transit

Syntax **transit** [**inherit** | **all** | **vc-only** | **none**]

Context **[Tree]** (config>service>vprn>ttl-propagate transit)

Full Context configure service vprn ttl-propagate transit

Description This command overrides the global configuration of the TTL propagation for in transit packets which are forwarded over a MPLS LSPs in a given VPRN service context.

The global configuration is performed under config>router>ttl-propagate>vprn-transit.

The default behavior for a given VPRN instance is to inherit the global configuration for the same command. The user can explicitly set the default behavior by configuring the inherit value.

Default transit inherit

Parameters *inherit* — specifies the TTL propagation behavior is inherited from the global configuration under config>router>ttl-propagate>vprn-transit.

none — specifies the TTL of the IP packet is not propagated into the VC label or labels in the transport label stack.

vc-only — specifies the TTL of the IP packet is propagated into the VC label and not into the labels. in the transport label stack

all — specifies the TTL of the IP packet is propagated into the VC label and all labels in the transport label stack.

Platforms All

24.166 transit-auto-create

transit-auto-create

Syntax **transit-auto-create**

Context **[Tree]** (config>app-assure>group>transit-ip-policy transit-auto-create)

Full Context configure application-assurance group transit-ip-policy transit-auto-create

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables seen-IP auto creation of transit subscribers using the transit-IP-policy name and subscriber IP address as the AA-sub name. The default app-profile configured against the transit-ip-policy is applied to these subscribers.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.167 transit-delay

transit-delay

Syntax **transit-delay** *seconds*
no transit-delay

Context **[Tree]** (config>service>vprn>ospf>area>if transit-delay)
[Tree] (config>service>vprn>ospf3>area>if transit-delay)
[Tree] (config>service>vprn>ospf>area>virtual-link transit-delay)
[Tree] (config>service>vprn>ospf3>area>virtual-link transit-delay)
[Tree] (config>service>vprn>ospf>area>sham-link transit-delay)

Full Context configure service vprn ospf area interface transit-delay
configure service vprn ospf area sham-link transit-delay
configure service vprn ospf area virtual-link transit-delay
configure service vprn ospf3 area interface transit-delay
configure service vprn ospf3 area virtual-link transit-delay

Description This command configures the estimated time, in seconds, that it takes to transmit a LSA on the interface or virtual link or sham-link.

The **no** form of this command reverts to the default delay time.

Default transit-delay 1

Parameters *seconds* — The transit delay in seconds expressed as a decimal integer.

Values 0 to 3600

Platforms All

transit-delay

Syntax **transit-delay** *seconds*
no transit-delay

Context **[Tree]** (config>router>ospf>area>interface transit-delay)
[Tree] (config>router>ospf>area>virtual-link transit-delay)
[Tree] (config>router>ospf3>area>interface transit-delay)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>ospf3>area>virtual-link transit-delay)

Full Context configure router ospf area interface transit-delay
configure router ospf area virtual-link transit-delay
configure router ospf3 area interface transit-delay
configure router ospf3 area virtual-link transit-delay

Description This command configures the estimated time, in seconds, that it takes to transmit a link state advertisement (LSA) on the interface or virtual link.

The **no** form of this command reverts to the default delay time.

Default transit-delay 1

Parameters *seconds* — Specifies the transit delay in seconds expressed as a decimal integer.

Values 1 to 1800

Platforms All

24.168 transit-ip-policy

transit-ip-policy

Syntax **transit-ip-policy** *ip-policy-id* [**create**]
no transit-ip-policy *ip-policy-id*

Context [Tree] (config>app-assure>group transit-ip-policy)

Full Context configure application-assurance group transit-ip-policy

Description This command defines a transit AA subscriber IP policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of this command deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Parameters *ip-policy-id* — An integer that identifies a transit IP profile entry.

Values 1 to 65535

create — Keyword used to create the entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.169 transit-path

transit-path

Syntax **transit-path** *path-name*
no transit-path

Context **[Tree]** (config>router>mpls>mpls-tp transit-path)

Full Context configure router mpls mpls-tp transit-path

Description This command enables the configuration or editing of an MPLS-TP transit path at an LSR.

Default no transit-path

Parameters *path-name* — Specifies the template of up to 32 characters in printable 7-bit ASCII, enclosed in double quotes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.170 transit-policy

transit-policy

Syntax **transit-policy ip** *ip-aasub-policy-id*
transit-policy prefix *prefix-aasub-policy-id*
no transit-policy

Context **[Tree]** (config>service>ies>if>sap transit-policy)
[Tree] (config>service>ies>if>spoke-sdp transit-policy)
[Tree] (config>service>vprn>if>sap transit-policy)
[Tree] (config>service>vprn>if>spoke-sdp transit-policy)
[Tree] (config>service>epipe>sap transit-policy)
[Tree] (config>service>epipe>spoke-sdp transit-policy)
[Tree] (config>service>vpls>sap transit-policy)
[Tree] (config>service>vpls>spoke-sdp transit-policy)

Full Context configure service epipe sap transit-policy
configure service epipe spoke-sdp transit-policy
configure service ies interface sap transit-policy
configure service ies interface spoke-sdp transit-policy
configure service vpls sap transit-policy
configure service vpls spoke-sdp transit-policy
configure service vprn interface sap transit-policy

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface spoke-sdp transit-policy

Description This command associates a transit AA subscriber IP or prefix policy to the service. The transit policy must be defined prior to associating the policy with a SAP in the **config**>**app-assure**>**group**>**transit-ip-policy** or **transit-prefix-policy** context.

The **no** form of this command removes the association of the policy to the service.

Default no transit-policy

Parameters *ip-aasub-policy-id* — Specifies a transit IP policy ID.

Values 1 to 65535

prefix-aasub-policy-id — Specifies a transit prefix policy ID.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

transit-policy

Syntax **transit-policy prefix** *prefix-aasub-policy-id*
no transit-policy

Context **[Tree]** (config>service>ipipe>sap transit-policy)
[Tree] (config>service>ipipe>spoke-sdp transit-policy)

Full Context configure service ipipe sap transit-policy
configure service ipipe spoke-sdp transit-policy

Description This command associates an AA transit policy to the service. The transit IP policy must be defined prior to associating the policy with a SAP in the **config>application assurance>group>policy>transit-ip-policy** context.

Transit AA subscribers are managed by the system through this service policy, which determines how transit subs are created and removed for that service.

The no form of this command removes the association of the policy to the service.

Default no transit-policy

Parameters *prefix-aasub-policy-id* — Specifies an integer identifying a prefix transit profile entry.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.171 transit-prefix-ipv4-entries

transit-prefix-ipv4-entries

Syntax **transit-prefix-ipv4-entries** *entries*
no transit-prefix-ipv4-entries

Context **[Tree]** (config>isa>aa-grp transit-prefix-ipv4-entries)

Full Context configure isa application-assurance-group transit-prefix-ipv4-entries

Description This command defines the number of transit-prefix IPv4 entries for an ISA.

The **no** form of this command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Default no transit-prefix-ipv4-entries

Parameters *entries* — Specifies an integer that determines the number of transit-prefix-ipv4 entries.

Values 0 to 16383

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.172 transit-prefix-ipv4-remote-entries

transit-prefix-ipv4-remote-entries

Syntax **transit-prefix-ipv4-remote-entries** *entries*
no transit-prefix-ipv4-remote-entries

Context **[Tree]** (config>isa>aa-grp transit-prefix-ipv4-remote-entries)

Full Context configure isa application-assurance-group transit-prefix-ipv4-remote-entries

Description This command configures the ISA-AA-group transit prefix IPv4 remote entry limit. This entry space is allocated on the IOM within a common area with the second MDA/ISA position of the IOM and also used for IPv4filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv4 entries should be set to allow sufficient space on the IOM for SDP IPv4 filters.

The **no** form of this command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Default no transit-prefix-ipv4-remote-entries

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *entries* — Specifies the ISA-AA-Group transit prefix IPv4 remote entry limit.

Values 0 to 2047

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.173 transit-prefix-ipv6-entries

transit-prefix-ipv6-entries

Syntax **transit-prefix-ipv6-entries** *entries*
no transit-prefix-ipv6-entries

Context **[Tree]** (config>isa>aa-grp transit-prefix-ipv6-entries)

Full Context configure isa application-assurance-group transit-prefix-ipv6-entries

Description This command configures the ISA-AA-group transit prefix IPv6 entry limit for each ISA in the group. This entry space is allocated on the IOM within a common area with the second MDA / ISA position of the IOM and also used for ipv6-filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv6 entries should be set to allow sufficient space on the IOM for SDP ipv6-filters.

The **no** form of this command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Default no transit-prefix-ipv6-entries

Parameters *entries* — Specifies the ISA-AA-Group transit prefix IPv6 entry limit.

Values 0 to 8191

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.174 transit-prefix-ipv6-remote-entries

transit-prefix-ipv6-remote-entries

Syntax **transit-prefix-ipv6-remote-entries** *entries*
no transit-prefix-ipv6-remote-entries

Context **[Tree]** (config>isa>aa-grp transit-prefix-ipv6-remote-entries)

Full Context configure isa application-assurance-group transit-prefix-ipv6-remote-entries

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the ISA-AA-group transit prefix IPv6 remote entry limit. This entry space is allocated on the IOM within a common area with the second MDA/ISA position of the IOM and also used for IPv6filter entries for system SDPs. The per-ISA size allocated for transit-prefix-ipv6 entries should be set to allow sufficient space on the IOM for SDP IPv6 filters.

The **no** form of this command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

Default no transit-prefix-ipv6-remote-entries

Parameters *entries* — Specifies the ISA-AA-Group transit prefix IPv6 remote entry limit.

Values 0 to 1023

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.175 transit-prefix-policy

transit-prefix-policy

Syntax **transit-prefix-policy** *prefix-policy-id* [**create**]
no transit-prefix-policy *prefix-policy-id*

Context **[Tree]** (config>app-assure>group transit-prefix-policy)

Full Context configure application-assurance group transit-prefix-policy

Description This command defines a transit aa subscriber prefix policy. Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of this command deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Parameters *prefix-policy-id* — Indicates the transit prefix policy to which this subscriber belongs.

Values 1 to 65535

create — Mandatory keyword used when creating transit prefix policy. The create keyword requirement can be enabled/disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.176 transmission-profile

transmission-profile

Syntax **transmission-profile** *name*
no transmission-profile

Context **[Tree]** (config>system>security>pki>ca-profile>ocsp transmission-profile)

Full Context configure system security pki ca-profile ocsp transmission-profile

Description This command specifies the transmission-profile for OCSP. When specified, this configuration overrides the **service** *service-id* or **service** *service-name* configured in the **config>system>security>pki>ca-profile>ocsp** context.

The **no** form of the command removes the profile name from the configuration.

Default no transmission-profile

Parameters *name* — Specifies the file transmission profile name, up to 32 characters.

Platforms All

transmission-profile

Syntax **transmission-profile** *name*
no transmission-profile

Context **[Tree]** (config>system>security>pki>est-profile transmission-profile)

Full Context configure system security pki est-profile transmission-profile

Description This command specifies the transmission profile name created in the **config**>**system file-transmission-profile** context for the EST profile.

The **no** form of the command removes the name from the EST profile configuration.

Default no transmission-profile

Parameters *name* — Specifies the file transmission profile name, up to 32 characters.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.177 transmit-interval

transmit-interval

Syntax [**no**] **transmit-interval** *interval* [**multiplier** *multiplier*]

Context **[Tree]** (config>port>ethernet>efm-oam transmit-interval)

Full Context configure port ethernet efm-oam transmit-interval

Description This command configures the transmit interval of OAM PDUs.

Default transmit-interval 10 multiplier 5

Parameters *interval* — Specifies the transmit interval, in 100 milliseconds.

Values 1 to 600

multiplier — Specifies the multiplier for transmit-interval to set local link down timer.

Values 2 to 5

Platforms All

transmit-interval

Syntax **transmit-interval** *transmit-interval*
no transmit-interval

Context **[Tree]** (config>lag>bfd>family transmit-interval)

Full Context configure lag bfd family transmit-interval

Description This command specifies the transmit timer used for micro-BFD session over the associated LAG links.

The **no** form of this command removes the transmit timer from the configuration.

Default transmit-interval 100

Parameters *transmit-interval* — Specifies the interval value, in milliseconds.

Values 10 to 100000

Default 100 for CPM3 or later, 1000 for all others

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

transmit-interval

Syntax **transmit-interval** *transmit-interval*
no transmit-interval

Context **[Tree]** (config>router>bfd>bfd-template transmit-interval)

Full Context configure router bfd bfd-template transmit-interval

Description This command specifies the transmit timer used for BFD packets. If the template is used for a BFD session on an MPLS-TP LSP, then this timer is used for CC packets.

The **no** form of this command reverts to the default value.

Default transmit-interval 100

Parameters *transmit-interval* — Specifies the transmit interval. The minimum interval that can be configured is hardware dependent.

Values 10 ms to 100,000 ms in 1 ms intervals

Default 10 ms for CPM3 or higher; 1 second for other hardware

Platforms All

24.178 transmit-period

transmit-period

Syntax **transmit-period** *seconds*
no transmit-period

Context **[Tree]** (config>port>ethernet>dot1x transmit-period)

Full Context configure port ethernet dot1x transmit-period

Description This command configures the period after which the router sends a new EAPOL request message.

The **no** form of this command returns the value to the default.

Default transmit-period 30

Parameters *seconds* — Specifies the server transmit period in seconds.

Values 1 to 3600

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.179 transport

transport

Syntax **transport tcp port** *port*
no transport

Context **[Tree]** (config>aaa>diam-peer-plcy>peer transport)

Full Context configure aaa diameter-peer-policy peer transport

Description This command defines the destination TCP port of the connection channel.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Default transport tcp port 3868

Parameters *port* — Specifies the transport protocol port number used toward this policy peer.

Values 1 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.180 transport-address

transport-address

Syntax **transport-address** {**interface** | **system**}
no transport-address

Context **[Tree]** (config>router>ldp>if-params>if>ipv4 transport-address)
[Tree] (config>router>ldp>if-params>if>ipv6 transport-address)
[Tree] (config>router>ldp>if-params>ipv4 transport-address)
[Tree] (config>router>ldp>if-params>ipv6 transport-address)

Full Context configure router ldp interface-parameters interface ipv4 transport-address
configure router ldp interface-parameters interface ipv6 transport-address
configure router ldp interface-parameters ipv4 transport-address
configure router ldp interface-parameters ipv6 transport-address

Description This command configures the transport address to be used when setting up the LDP TCP sessions. The transport address can be configured as **interface** or **system**. The transport address can be configured globally (applies to all LDP interfaces) or per interface. The most specific value is used.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **config**>**router**>**ldp**>**if-params**>**ipv6**>**transport-address** command is not supported on the 7450 ESS.

With the transport-address command, you can set up the LDP interface to the connection which can be set to the interface address or the system address. However, there can be an issue of which address to use when there are parallel adjacencies. This situation can not only happen with parallel links, it could be a link and a targeted adjacency since targeted adjacencies request the session to be set up only to the system IP address.

The **transport-address** value should not be **interface** if multiple interfaces exist between two LDP neighbors. Depending on the first adjacency to be formed, the TCP endpoint is chosen. In other words, if one LDP interface is set up as **transport-address interface** and another for **transport-address system**, then, depending on which adjacency was set up first, the TCP endpoint addresses are determined. After that, because the hello contains the LSR ID, the LDP session can be checked to verify that it is set up and then match the adjacency to the session.

For any iLDP interface, as the **local-lsr-id** parameters is changed to **interface**, the **transport-address** configuration loses effectiveness. Since it will be ignored and the iLDP session will always use the relevant interface IP address as transport-address even though system is chosen.

The **no** form of this command, at the global level, sets the transport address to the default value.

The **no** form of this command, at the interface level, sets the transport address to the value defined under the global level.

Default system

Parameters **interface** — Specifies the IP interface address is used to set up the LDP session between neighbors. The transport address interface cannot be used if multiple interfaces exist between two neighbors, since only one LDP session is set up between two neighbors.

system — Specifies the system IP address is used to set up the LDP session between neighbors.

Platforms All

24.181 transport-encryption

transport-encryption

Syntax **transport-encryption**

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync transport-encryption)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure redundancy multi-chassis peer sync transport-encryption

Description Commands in this context configure MCS applications that need to encrypt synchronized states for transportation .

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.182 transport-tunnel

transport-tunnel

Syntax **transport-tunnel**

Context **[Tree]** (config>router>bgp>next-hop-res>labeled-routes transport-tunnel)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel

Description Commands in this context configure options for the next-hop resolution of BGP labeled routes (VPN-IP and labeled-unicast) using tunnels in TTM. The context allows the selection of different tunnel resolution options for different types of BGP labeled routes: label-unicast IPv4, label-unicast IPv6, and VPN-IP routes (both VPN-IPv4 and VPN-IPv6).

By default (if this context and the resolution options are not configured), these routes resolve only to LDP tunnels.

If the **resolution** option is explicitly set to **disabled**, the default binding to LDP tunnel resumes. If **resolution** is set to **any**, then any supported tunnel type is allowed and the selection is based on the lowest numerical TTM preference value.

Platforms All

24.183 transport-type

transport-type

Syntax **transport-type** {**ip**}
no transport-type

Context **[Tree]** (config>router>l2tp>l2tpv3 transport-type)
[Tree] (config>service>vprn>l2tp>l2tpv3 transport-type)

Full Context configure router l2tp l2tpv3 transport-type
configure service vprn l2tp l2tpv3 transport-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the transport type to be used to carry the L2TPv3 tunnel. Currently, only IP transport is supported.

The **no** form of this command returns the **transport-type** to the default value.

Default no transport-type

Parameters **ip** — Specifies that IP should be used as the transport type for the L2TPv3 tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.184 trap-gen

trap-gen

Syntax **trap-gen**

Context **[Tree]** (config>saa>test trap-gen)

Full Context configure saa test trap-gen

Description Commands in this context configure trap generation for the SAA test.

Platforms All

24.185 trap-target

trap-target

Syntax **trap-target name address** *ip-address* [**port port**] [**snmpv1** | **snmpv2c** | **snmpv3**] **notify-community** *communityName* | *snmpv3SecurityName* [**security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}] [**replay**]
no trap-target *name*

Context **[Tree]** (config>service>vprn>log>snmp-trap-group trap-target)

Full Context configure service vprn log snmp-trap-group trap-target

Description This command adds/modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the **log-id**, **snmp-trap-group**, and at least one **snmp-trap-group** must be configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **snmp-trap-group** command is used to add or remove a trap receiver from an **snmp-trap-group**. The operational parameters specified in the command include:

- The IP address of the trap receiver
- The UDP port used to send the SNMP trap
- SNMP version
- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

A single **snmp-trap-group** *log-id* can have multiple trap-receivers. Each trap receiver can have different operational parameters.

An address can be configured as a trap receiver more than once as long as a different port is used for each instance.

To prevent resource limitations, only configure a maximum of 10 trap receivers.

If the same **trap-target** *name* **port** *port* parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different *notify-community* value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each router event log when multiple event logs are directed to the same IP address and port destination.

The **no** form of this command removes the SNMP trap receiver from the SNMP trap group.

Default No SNMP trap targets are defined.

Parameters *name* — specifies the name of the trap target up to 28 characters in length

address *ip-address* — The IP address of the trap receiver in dotted decimal notation. Only one IP address destination can be specified per trap destination group.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
	interface: 32 characters maximum, mandatory for link local addresses

The ipv6-address applies to the 7750 SR.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port — Specifies the destination UDP port used to send traps to the destination, expressed as a decimal integer. Only one port can be specified per **trap-target** statement. If multiple traps need to be issued to the same address then multiple ports must be configured.

Values 1 to 65535

Default 162

snmpv1 | *snmpv2c* | *snmpv3* — Specifies the SNMP version format to use for traps sent to the trap receiver.

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv1,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv2c** selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv2c,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv3** selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** must be configured for the SNMP *security-name*. If the SNMP version is changed from **snmpv1** or **snmpv2c** to **snmpv3**, then the **notify-community** parameter must be changed to reflect the *security-name* rather than the community string used by **snmpv1** or **snmpv2c**.

Pre-existing conditions are checked before the snmpv3SecurityName is accepted. These are:

- The username must be configured.
- The v3 access group must be configured.
- The v3 notification view must be configured.

Values snmpv1, snmpv2c, snmpv3

Default snmpv3

notify-community community | *security-name* — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** *security-name*. If no **notify-community** is configured, then no alarms nor traps will be issued for the trap destination. If the SNMP version is modified, the **notify-community** must be changed to the proper form for the SNMP version.

community — The community string as required by the **snmpv1** or **snmpv2c** trap receiver. Allowed values are any string up to 31 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

security-name — The *security-name* as defined in the config>system>security>user context for SNMP v3. The *security-name* can be an ASCII string up to 31 characters in length.

security-level {no-auth-no-privacy | auth-no-privacy | privacy} — Specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies authentication is required but no privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies both authentication and privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication** and **privacy**.

Values no-auth-no-privacy, auth-no-privacy, privacy

Default no-auth-no-privacy. This parameter can only be configured if SNMPv3 is also configured.

replay — Enable replay of missed events to target. If replay is applied to an SNMP trap target address, the address is monitored for reachability. Reachability is determined by whether or not there is a route in the routing table by which the target address can be reached. Before sending a trap to a target address, the SNMP module asks the PIP module if there is either an in-band or out-of-band route to the target address. If there is no route to the SNMP target address, the SNMP module saves the sequence-id of the first event that will be missed by the trap target. When the routing table changes again so that there is now a route by which the SNMP target address can be reached, the SNMP module replays (for example, retransmits) all events generated to the SNMP notification log while the target address was removed from the route table. Because of route table change convergence time, it is possible that one or more events may be lost at the beginning or end of a replay sequence. The cold-start-wait and route-recovery-wait timers under config>log>app-route-notifications can help reduce the probability of lost events.

Platforms All

trap-target

Syntax **trap-target** *name* [**address** *ip-address*] [**port** *port*] [**snmpv1** | **snmpv2c** | **snmpv3**] **notify-community** *communityName* | *snmpv3SecurityName* [**security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}] [**replay**]

no trap-target *name*

Context **[Tree]** (config>log>snmp-trap-group trap-target)

Full Context configure log snmp-trap-group trap-target

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the **log-id**, **snmp-trap-group** and at least one **trap-target** must be configured.

The **trap-target** command is used to add/remove a trap receiver from an **snmp-trap-group**. The operational parameters specified in the command include:

- The IP address of the trap receiver
- The UDP port used to send the SNMP trap
- SNMP version
- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

A single **snmp-trap-group** *log-id* can have multiple trap-receivers. Each trap receiver can have different operational parameters.

An address can be configured as a trap receiver more than once as long as a different port is used for each instance.

To prevent resource limitations, only configure a maximum of 10 trap receivers.

Note: If the same **trap-target** *name* **port** *port* parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different *notify-community* value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each router event log when multiple event logs are directed to the same IP address and port destination.

The **no** form of this command removes the SNMP trap receiver from the SNMP trap group.

Parameters *name* — Specifies the name of the trap target, up to 28 characters.

ip-address — Specifies the IP address of the trap receiver in dotted decimal notation. Only one IP address destination can be specified per trap destination group. ipv6 applies to the 7750 SR only.

Values

ipv4-address	a.b.c.d (host bits must be 0)
ipv6-address	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0..FFFF]H
	d: [0..255]D
	interface: 32 characters maximum, mandatory for link local addresses

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

port — Specifies the destination UDP port used for sending traps to the destination, expressed as a decimal integer. Only one port can be specified per **trap-target** statement. If multiple traps need to be issued to the same address then multiple ports must be configured.

Default 162

Values 1 **to** 65535

snmpv1 | *snmpv2c* | *snmpv3* — Specifies the SNMP version format to use for traps sent to the trap receiver.

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv1,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv2c** selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv2c,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv3** selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** must be configured for the SNMP *security-name*. If the SNMP version is changed from **snmpv1** or **snmpv2c** to **snmpv3**, then the **notify-community** parameter must be changed to reflect the *security-name* rather than the community string used by **snmpv1** or **snmpv2c**.

Pre-existing conditions are checked before the snmpv3SecurityName is accepted. These are:

The user name must be configured.

The v3 access group must be configured.

The v3 notification view must be configured.

Default snmpv3

Values snmpv1, snmpv2c, snmpv3

community | *security-name* — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** *security-name*. If the **notify-community** is not configured, then no alarms or traps will be issued for the trap destination. If the SNMP version is modified, the **notify-community** must be changed to the proper form for the SNMP version.

community-name — Specifies the community string as required by the **snmpv1** or **snmpv2c** trap receiver. Allowed values are any string up to 31 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

security-name — Specifies the *security-name* as defined in the **config>system> security>user** context for SNMP v3. The *security-name* can be an ASCII string up to 31 characters in length.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

security-level {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**} — Specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies authentication is required but no privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies both authentication and privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication** and **privacy**.

Default **no-auth-no-privacy**. This parameter can only be configured if SNMPv3 is also configured.

Values no-auth-no-privacy, auth-no-privacy, privacy

replay — Enables the replay of missed events to target. If replay is applied to an SNMP trap target address, the address is monitored for reachability. Reachability is determined by whether or not there is a route in the routing table by which the target address can be reached. Before sending a trap to a target address, the SNMP module asks the PIP module if there is either an in-band or out-of-band route to the target address. If there is no route to the SNMP target address, the SNMP module saves the sequence-id of the first event that will be missed by the trap target. When the routing table changes again so that there is now a route by which the SNMP target address can be reached, the SNMP module replays (for example, retransmits) all events generated to the SNMP notification log while the target address was removed from the route table.

Note: Due to route table change convergence time, it is possible that one or more events may be lost at the beginning or end of a replay sequence. The cold-start-wait and route-recovery-wait timers under the **config>log>app-route-notifications** context can help reduce the probability of lost events.

Platforms All

24.186 tree

tree

Syntax **tree** [**detail**] [**flat**]

Context **[Tree]** (global tree)

Full Context global tree

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command displays the command hierarchy structure of the current working context.

Parameters **detail** — Displays parameter information for each command shown in the tree output.

flat — Displays the full context on each line.

24.187 trigger

trigger

Syntax **trigger** *trigger-type*

Context **[Tree]** (config>subscr-mgmt>shcv-policy trigger)

Full Context configure subscriber-mgmt shcv-policy trigger

Description This command enables to context to configure SHCV triggers.

Parameters *trigger-type* — Specifies the trigger SHCV properties for the subscriber management group-interface.

Values

ip-conflict — Upon detecting an IP conflict for the new host, a trigger SHCV is sent using a unicast ARP/NS. The request verifies the old host's connectivity to the BNG. An unresponsive host is removed from the system, allowing the new host to connect. The new host must resend its address request in order to be created as an ESM host in the system.

host-limit-exceeded — Upon exceeding the limit for (**sla-profile host-limits** or **session-limits**, **sub-profile host-limits** or **session-limits**, **ipoe-session sap-session-limit**, **ipoe-session session-limit**, and **arp-host host-limit**), a trigger SHCV is sent. The request verifies the old host's connectivity to the BNG. An unresponsive host is removed from the system, allowing the new host to connect. The new host must resend its address request in order to be created as an ESM host in the system.

inactivity — A trigger SHCV is sent to the idle host to verify the host's connectivity to the BNG. An unresponsive host is removed from the system.

mobility — Detects an IP or MAC conflict between different SAPs. Upon detecting a MAC or an IP conflict, a trigger SHCV is sent. The request verifies the old host's connectivity to the BNG. An unresponsive host is removed from the system, allowing the new host to connect. The new host must resend its address request in order to be created as an ESM host in the system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mac-learning — Specifies the trigger SHCV properties to learn the MAC address of static hosts. Upon a **no shutdown**, a trigger SHCV is sent to the host to learn the host's MAC address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

trigger

Syntax **trigger** [**data**] [**iapp**] [**control**]
no trigger

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>mobility trigger)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>mobility trigger)

Full Context configure service ies subscriber-interface group-interface wlan-gw mobility trigger
configure service vprn subscriber-interface group-interface wlan-gw mobility trigger

Description This command specifies the type of packet used as a mobility trigger.

The **no** form of this command removes the parameters from the configuration and disables data-plane mobility.

Parameters **data** — Specifies that data traffic be used as a trigger.

iapp — Specifies that Inter Access Point Protocol (IAPP) messages be used as a trigger.

control — Specifies that control traffic can be used as a trigger.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

trigger

Syntax [**no**] **trigger** [**neighbor** *ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>rip trigger)

Full Context debug router rip trigger

Description This command enables debugging for RIP trigger updates.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP updates sent on the neighbor IP address or interface.

Platforms All

trigger

Syntax [**no**] **trigger** [**neighbor** *ip-int-name* | *ipv6-address*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (debug>router>ripng trigger)

Full Context debug router ripng trigger

Description This command enables debugging for RIP trigger updates.

Parameters *ip-int-name* | *ipv6-address* — Debugs the RIP updates sent on the neighbor IP address or interface.

Platforms All

24.188 trigger-alarm-msg

trigger-alarm-msg

Syntax **trigger-alarm-msg** *message-string*
no trigger-alarm-msg

Context [Tree] (config>system>alarm-contact-input trigger-alarm-msg)

Full Context configure system alarm-contact-input trigger-alarm-msg

Description This command configures a message string to send with SNMP trap and log event messages that are generated when the system generates an alarm. The system generates the default message “Alarm Input Triggered” if no message is configured. The **trigger-alarm-msg** string is included in the log event when the pin changes from the normal state.

The **no** form of this command reverts to the default message “Alarm Input Triggered”.

Default no-trigger-alarm-msg

Parameters *message-string* — Specifies a printable character string, up to 160 characters.

Platforms 7750 SR-a

24.189 trigger-entry

trigger-entry

Syntax [**no**] **trigger-entry** *entry-id*

Context [Tree] (config>log>event-trigger>event trigger-entry)

Full Context configure log event-trigger event trigger-entry

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures an instance of a trigger for an EHS handler. A trigger entry binds a set of matching criteria for a log event to a particular handler. If the log event occurs in the system and matches the criteria configured in the associated log filter then the handler will be executed.

The **no** form of this command removes the specified trigger entry.

Parameters *entry-id* — Specifies the identifier of the EHS event trigger entry.

Values 1 to 1500

Platforms All

24.190 trigger-fault

trigger-fault

Syntax **trigger-fault** {**dying-gasp** | **critical-event**}
no trigger-fault

Context **[Tree]** (config>port>ethernet>efm-oam trigger-fault)

Full Context configure port ethernet efm-oam trigger-fault

Description This command configures the appropriate flag field in the Information OAM PDU, bursting three consecutive packets during the off cycle. If the local port state is operational, this command changes the local port state to “Link Up”. If the local port state is not operational, this configuration is installed as an EFM reason to prevent the port from returning to an Up operational state. This command can be used as a precursor to a port shutdown. This terminates the peering relationship without having to wait for protocol timeouts, assuming the peer supports the necessary action when receiving the dying gasp or critical event flag setting.

The **no** form of this command disables this functionality.

Default no trigger-fault

Parameters **dying-gasp** — Keyword to set the dying gasp flag.

critical-event — Keyword to set the critical event flag.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.191 trigger-packet

trigger-packet

Syntax **trigger-packet** [**dhcp**] [**pppoe**] [**arp**] [**dhcp6**] [**ppp**] [**rtr-solicit**] [**data**]
no trigger-packet

Context **[Tree]** (config>service>vpls>sap trigger-packet)

Full Context configure service vpls sap trigger-packet

Description This command enables triggering packet to initiate RADIUS authentication that provides a service context. The authentication, together with the service context for this request, creates a managed SAP. The VLAN is the same as the triggering packet. This SAP behaves as a regular SAP but the configuration is not user-editable and not maintained in the configuration file. The managed SAP remains active as long as the session is active.

The **no** form of this command reverts to the default.

Parameters **dhcp** — Specifies whether the receipt of DHCP trigger packets on this VPLS SAP when the keyword **capture-sap** is specified in the **sap** command creation string, will result in a RADIUS authentication that will provide a service context and the creation of a SAP with a value of managed.

pppoe — Specifies whether the receipt of PPPoE trigger packets on this VPLS SAP when the keyword **capture-sap** is specified in the **sap** command creation string, will result in a RADIUS authentication that will provide a service context and the creation of a SAP with a value of managed.

arp — Indicates that ARP is the type of trigger packets for this entry.

dhcp6 — Indicates that DHCP6 is the type of trigger packets for this entry.

ppp — Indicates that PPP is the type of trigger packets for this entry.

rtr-solicit — Indicates that router solicit is the type of trigger packets for this entry.

data — Indicates that data is the type of trigger packets for this entry.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.192 triggered-policy

triggered-policy

Syntax [**no**] **triggered-policy**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router triggered-policy)

Full Context configure router triggered-policy

Description This command triggers route policy re-evaluation.

By default, when a change is made to a policy in the **config router policy options** context and then committed, the change is effective immediately. There may be circumstances when the changes should or must be delayed; for example, if a policy change is implemented that would affect every BGP peer on a router, the consequences could be dramatic. It is more effective to control changes on a peer by peer basis.

If the **triggered-policy** command is enabled, and a given peer is established, and you want the peer to remain up, then, in order for a change to a route policy to take effect, a **clear** command with the *soft* or *soft-inbound* option must be used. In other words, when a **triggered-policy** is enabled, any routine policy change or policy assignment change within the protocol will not take effect until the protocol is reset or a clear command is issued to re-evaluate route policies; for example, **clear router bgp neighbor x.x.x.x soft**. This keeps the peer up and the change made to a route policy is applied only to that peer, or group of peers.

Default no triggered-policy

Platforms All

24.193 triggered-updates

triggered-updates

Syntax **triggered-updates**

Context [Tree] (config>subscr-mgmt>acct-plcy triggered-updates)

Full Context configure subscriber-mgmt radius-accounting-policy triggered-updates

Description Commands in this context configure non-periodic accounting updates that are triggered by specific events.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.194 trust-anchor

trust-anchor

Syntax [**no**] **trust-anchor** *ca-profile-name*

Context **[Tree]** (config>ipsec>trust-anchor-profile trust-anchor)

Full Context configure ipsec trust-anchor-profile trust-anchor

Description This command specifies a CA profile as a trust anchor CA. Up to 8 multiple trust anchors can be specified in a single trust anchor profile.

The **no** form of this command removes the name from the configuration.

Parameters *ca-profile-name* — Specifies the name of the trust anchor profile, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

trust-anchor

Syntax [**no**] **trust-anchor** *ca-profile-name*

Context **[Tree]** (config>system>security>tls>trust-anchor-profile trust-anchor)

Full Context configure system security tls trust-anchor-profile trust-anchor

Description This command configures a trust anchor with a CA profile used by the TLS profile. Up to eight CA profiles can be configured under the trust anchor. TLS will read the CA profiles one by one to try to authenticate the server certificate.

Parameters *ca-profile-name* — Specifies the name of the TLS trust anchor, up to 32 characters.

Platforms All

24.195 trust-anchor-profile

trust-anchor-profile

Syntax **trust-anchor-profile** *name* [**create**]
no trust-anchor-profile *name*

Context **[Tree]** (config>ipsec trust-anchor-profile)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure ipsec trust-anchor-profile

Description This command specifies the trust anchor profile name for the IPsec tunnel or IPsec GW.

Default no trust-anchor-profile

Parameters *name* — Specifies the name of trust anchor profile up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

trust-anchor-profile

Syntax **trust-anchor-profile** *name*
no trust-anchor-profile

Context **[Tree]** (config>service>ies>if>ipsec>ipsec-tunnel>dyn>cert trust-anchor-profile)
[Tree] (config>service>vprn>if>ipsec>ipsec-tunnel>dyn>cert trust-anchor-profile)
[Tree] (config>service>ies>if>sap>ipsec-gw>cert trust-anchor-profile)
[Tree] (config>service>vprn>if>sap>ipsec-gw>cert trust-anchor-profile)
[Tree] (config>service>vprn>if>sap>ipsec-tunnel>cert trust-anchor-profile)
[Tree] (config>router>if>ipsec>ipsec-tunnel>dyn>cert trust-anchor-profile)
[Tree] (config>ipsec>trans-mode-prof>dyn>cert trust-anchor-profile)

Full Context configure ipsec ipsec-transport-mode-profile dynamic-keying cert trust-anchor-profile
configure router interface ipsec ipsec-tunnel dynamic-keying cert trust-anchor-profile
configure service ies interface ipsec ipsec-tunnel dynamic-keying cert trust-anchor-profile
configure service ies interface sap ipsec-gw cert trust-anchor-profile
configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert trust-anchor-profile
configure service vprn interface sap ipsec-gw cert trust-anchor-profile
configure service vprn interface sap ipsec-tunnel cert trust-anchor-profile

Description This command specifies the name of trust anchor profile used for certificate authentication.

The **no** form of this command removes the name from the configuration.

Default no trust-anchor-profile

Parameters *name* — Specifies the name of trust anchor profile, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn interface sap ipsec-gw cert trust-anchor-profile
- configure service ies interface sap ipsec-gw cert trust-anchor-profile
- configure ipsec ipsec-transport-mode-profile dynamic-keying cert trust-anchor-profile

VSR

- configure router interface ipsec ipsec-tunnel dynamic-keying cert trust-anchor-profile
- configure service ies interface ipsec ipsec-tunnel dynamic-keying cert trust-anchor-profile

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface ipsec ipsec-tunnel dynamic-keying cert trust-anchor-profile

trust-anchor-profile

Syntax **trust-anchor-profile** *name*
no trust-anchor-profile

Context **[Tree]** (config>system>security>tls>client-tls-profile trust-anchor-profile)
[Tree] (config>system>security>tls>server-tls-profile>authenticate-client trust-anchor-profile)

Full Context configure system security tls client-tls-profile trust-anchor-profile
configure system security tls server-tls-profile authenticate-client trust-anchor-profile

Description This command assigns the trust anchor used by this TLS profile to authenticate the server or client.

The **no** form of the command removes the configured trust anchor profile.

Parameters *name* — Specifies the name of the trust anchor profile.

Platforms All

trust-anchor-profile

Syntax **trust-anchor-profile** *name* [**create**]
no trust-anchor-profile *name*

Context **[Tree]** (config>system>security>tls trust-anchor-profile)

Full Context configure system security tls trust-anchor-profile

Description This command configures a trust anchor profile to be used in the TLS profile. The trust anchor is used for authentication of the server certificate.

Parameters *name* — Specifies the name of the trust anchor profile, up to 32 characters.

create — Keyword used to create the trust anchor profile.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.196 trusted

trusted

Syntax [**no**] **trusted**

Context **[Tree]** (config>router>if>dhcp trusted)
[Tree] (config>service>ies>if>dhcp trusted)
[Tree] (config>service>vprn>if>dhcp trusted)
[Tree] (config>service>ies>sub-if>grp-if>dhcp trusted)

Full Context configure router interface dhcp trusted
configure service ies interface dhcp trusted
configure service ies subscriber-interface group-interface dhcp trusted
configure service vprn interface dhcp trusted

Description This command enables relaying untrusted packets. According to RFC 3046, *DHCP Relay Agent Information Option*, a DHCP request where the giaddr is 0.0.0.0 and which contains an Option 82 field in the packet, should be discarded, unless it arrives on a “trusted” circuit. If the **trusted** mode is enabled on an IP interface, the Relay Agent (the router) modifies the requested giaddr to be equal to the ingress interface and forward the request.

The **no** form of this command reverts to the default.

Default no trusted

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface dhcp trusted

All

- configure router interface dhcp trusted
- configure service ies interface dhcp trusted
- configure service vprn interface dhcp trusted

24.197 ts-list

ts-list

Syntax **ts-list** *list-name* [**create**]
no ts-list *list-name*

Context **[Tree]** (config>ipsec ts-list)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure ipsec ts-list

Description This command creates a new traffic selector (TS).

The **no** form of this command removes the list name from the configuration.

Parameters *list-name* — Specifies the name of the TS-list.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.198 ts-location

ts-location

Syntax **ts-location** *file-url*
no ts-location

Context **[Tree]** (config>system>security>tech-support ts-location)

Full Context configure system security tech-support ts-location

Description The **ts-location** command is used (along with an automatic system generated file name) when no *file-url* parameter is provided for the **admin tech-support** command. If **no ts-location** is defined then the operator must provide a file-url with the **admin tech-support** command itself.

The directory specified for the ts-location is not auto-created by SR OS. The operator must ensure that it exists.

See the **admin tech-support** command for more details about the system generated file name.

Default no ts-location

Parameters *file-url* — Specifies the destination directory for auto-named tech-support files (when no *file-url* is specified with the **admin tech-support** command). The *file-url* for the **ts-location** must be a directory (no filename or extension). The root directory (for example, cf1:\) is blocked for local compact flash destinations. A sub-directory (for example, cf2:\tech-support) must be used if local cf is the location.

Values

local-url | *remote-url*	
local-url	[*cflash-id*/][*file-path*] 200 chars max, including cflash-id directory length 99 chars max each
remote-url	[ftp://*login:pswd@remote-locn*/][*file-path*] 247 chars max

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

	directory length 99 chars max each
remote-locn	[*hostname* | *ipv4-address* | "["*ipv6-address*"]"]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - 32 chars max, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

Platforms All

24.199 ts-negotiation

ts-negotiation

Syntax **ts-negotiation ts-list** *list-name*
no ts-negotiation

Context **[Tree]** (config>ipsec>client-db>client ts-negotiation)

Full Context configure ipsec client-db client ts-negotiation

Description This command specifies the traffic selector (TS) to be used for tunnel setup.

The no form of this command reverts to the default.

Default no ts-negotiation

Parameters *list-name* — Specifies the TS list used by this tunnel, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

ts-negotiation

Syntax **ts-negotiation ts-list** *list-name*
no ts-negotiation

Context **[Tree]** (config>service>ies>if>sap>ipsec-gw ts-negotiation)
[Tree] (config>service>vprn>if>sap>ipsec-gw ts-negotiation)

Full Context configure service ies interface sap ipsec-gw ts-negotiation

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn interface sap ipsec-gw ts-negotiation

Description This command enables the IKEv2 traffic selector negotiation with the specified ts-list.

Parameters *list-name* — Specifies the ts-list name

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.200 ts-sync-loss

ts-sync-loss

Syntax [**no**] **ts-sync-loss**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms ts-sync-loss)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms ts-sync-loss)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms ts-sync-loss)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms ts-sync-loss
configure mcast-management multicast-info-policy bundle channel video analyzer alarms ts-sync-loss
configure mcast-management multicast-info-policy bundle video analyzer alarms ts-sync-loss

Description This command configures the analyzer to check for synchronization loss errors.

Default no ts-sync-loss

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

24.201 ttl

ttl

Syntax **ttl** *value*

Context **[Tree]** (config>subscr-mgmt>pfcp-association>tx ttl)

Full Context configure subscriber-mgmt pfcp-association tx ttl

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures initial TTL value that is sent in the IP header.

Default ttl 255

Parameters *value* — Specifies the TTL value, in seconds.

This value must be identical on both the BNG UPF and CPF. For information about the BNG CUPS CPF configuration, refer to the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide*.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ttl

Syntax **ttl** *hops*
no ttl

Context **[Tree]** (config>router>lmp>peer>control-channel ttl)

Full Context configure router lmp peer control-channel ttl

Description This command configures the time to live (TTL) for all packets (GMPLS RSVP and LMP) on the IP control channel, which allows the TTL to be optimized for multi-hop communication networks between the GMPLS UNI-C and UNI-N.

Default ttl 1

Parameters *hops* — The TTL value for the packets.

Values 1 to 255

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ttl

Syntax **ttl** *label-ttl*
no ttl

Context **[Tree]** (config>saa>test>type-multi-line>lsp-ping>sr-policy ttl)

Full Context configure saa test type-multi-line lsp-ping sr-policy ttl

Description This command configures a time-to-live value for the MPLS label.

The **no** form of this command reverts to the default value.

Default ttl 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *label-ttl* — Specifies the time-to-live value.

Values 1 to 255

Default 255

Platforms All

ttl

Syntax **ttl min-ttl** *min-label-ttl* **max-ttl** *max-label-ttl*
no ttl

Context **[Tree]** (config>saa>test>type-multi-line>lsp-trace>sr-policy ttl)

Full Context configure saa test type-multi-line lsp-trace sr-policy ttl

Description This command configures minimum and maximum time-to-live values.

The **no** form of this command removes the configuration.

Parameters *min-label-ttl* — Specifies the minimum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Values 1 to 255

Default 1

max-label-ttl — Specifies the maximum TTL value in the MPLS label for the LDP treetrace test, expressed as a decimal integer.

Values 1 to 255

Default 30

Platforms All

ttl

Syntax **ttl** *time-to-live*
no ttl

Context **[Tree]** (config>oam-pm>session>ip ttl)

Full Context configure oam-pm session ip ttl

Description This command defines the value of the TTL field of the packet header.

The **no** form of this command restores the default value.

Default ttl 225

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *time-to-live* — Specifies the value to be used in the TTL field.

Values 1 to 255

Default 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ttl

Syntax **ttl** *time-to-live*
no ttl

Context **[Tree]** (config>oam-pm>session>mpls ttl)

Full Context configure oam-pm session mpls ttl

Description This command defines the value of the MPLS TTL for DM packets.

The **no** form of this command reverts the default value.

Default ttl 255

Parameters *time-to-live* — Specifies the value to be used in the TTL field.

Values 1 to 255

Default 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ttl

Syntax **ttl** *value*
no ttl

Context **[Tree]** (config>test-oam>icmp>ping-template ttl)

Full Context configure test-oam icmp ping-template ttl

Description This command configures the TTL value used in the outgoing ping packet. The interface being tested must be directly connected on the same subnet.

The **no** form of this command reinstates the default value for TTL.

Default ttl 1

Parameters *value* — Specifies the value to be used in the TTL field.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ttl

Syntax **ttl** *time-to-live*

Context **[Tree]** (config>test-oam>link-meas>template>twl ttl)

Full Context configure test-oam link-measurement measurement-template twamp-light ttl

Description This command configures the Time to Live (TTL) value in the TWAMP Light test packet.

Default ttl 1

Parameters *time-to-live* — Specifies the value to be used in the TTL field.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

ttl

Syntax **ttl** {**lt** | **gt** | **eq**} *ttl-value*
ttl range *ttl-value ttl-value*
no ttl

Context **[Tree]** (config>filter>ip-filter>entry>match ttl)

Full Context configure filter ip-filter entry match ttl

Description This command configures the Time To Live (TTL) match criteria.

The **no** form of this command removes the configuration.

Default no ttl

Parameters **lt** — Specifies “less than”. The **lt** parameter cannot be used with the lowest possible numerical value for the parameter.

gt — Specifies “greater than”. The **gt** parameter cannot be used with the highest possible numerical value for the parameter.

eq — Specifies “equal to”.

ttl-value — Specifies the maximum TTL value.

Values 0 to 255

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.202 ttl-expired

ttl-expired

Syntax **ttl-expired** *number seconds*
no ttl-expired [*number seconds*]

Context **[Tree]** (config>service>ies>if>icmp ttl-expired)
[Tree] (config>service>ies>sub-if>grp-if>icmp ttl-expired)
[Tree] (config>service>vprn>sub-if>grp-if>icmp ttl-expired)

Full Context configure service ies interface icmp ttl-expired
configure service ies subscriber-interface group-interface icmp ttl-expired
configure service vprn subscriber-interface group-interface icmp ttl-expired

Description This command configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the limiting the rate of TTL expired messages on the router interface and reverts to the default values.

Default ttl-expired 100 10

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the *seconds* parameter.

Values 10 to 2000

seconds — The time frame in seconds used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface icmp ttl-expired
- configure service vprn subscriber-interface group-interface icmp ttl-expired

All

- configure service ies interface icmp ttl-expired

ttl-expired

Syntax **ttl-expired** [**number** *number*] [**seconds** *seconds*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no ttl-expired

Context [Tree] (config>subscr-mgmt>git>ipv4>icmp ttl-expired)

Full Context configure subscriber-mgmt group-interface-template ipv4 icmp ttl-expired

Description This command configures the rate at which ICMP TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables limiting of the rate at which TTL expired messages are generated on the router interface.

Default ttl-expired number 100 seconds 10

Parameters *number* — Specifies the maximum number of ICMP TTL expired messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 to 2000

seconds — Specifies the time, in seconds, used to limit the number of ICMP TTL expired messages that can be generated, expressed as a decimal integer.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ttl-expired

Syntax **ttl-expired** [*number seconds*]
no ttl-expired

Context [Tree] (config>service>vprn>if>icmp ttl-expired)
[Tree] (config>service>vprn>nw-if>icmp ttl-expired)

Full Context configure service vprn interface icmp ttl-expired
configure service vprn network-interface icmp ttl-expired

Description This command configures the rate of Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the limiting the rate of TTL expired messages on the router interface.

Default ttl-expired 100 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *number* — Specifies the maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the *seconds* parameter.

Values 10 to 2000

seconds — Specifies the time frame in seconds used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 to 60

Platforms All

ttl-expired

Syntax **ttl-expired** [*number seconds*]
no ttl-expired

Context **[Tree]** (config>router>if>icmp ttl-expired)

Full Context configure router interface icmp ttl-expired

Description This command configures the rate that Internet Control Message Protocol (ICMP) Time To Live (TTL) expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of TTL expired messages.

Default ttl-expired 100 10 — Maximum of 100 TTL expired message in 10 seconds.

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. The *seconds* parameter must also be specified.

Values 10 to 2000

seconds — The time frame, in seconds, used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 to 60

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.203 ttl-propagate

ttl-propagate

Syntax **ttl-propagate**

Context **[Tree]** (config>service>vprn ttl-propagate)

Full Context configure service vprn ttl-propagate

Description Commands in this context configure TTL propagation for transit and locally generated packets in a given VPRN routing context.

Platforms All

ttl-propagate

Syntax **ttl-propagate**

Context **[Tree]** (config>router ttl-propagate)

Full Context configure router ttl-propagate

Description Commands in this context configure TTL propagation for transit and locally generated packets in the Global Routing Table (GRT) and VPRN routing contexts

Platforms All

24.204 ttl-security

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy ttl-security)

Full Context configure subscriber-mgmt bgp-peering-policy ttl-security

Description This command configures the TTL security parameters for incoming packets.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *min-ttl-value* — Specifies the minimum TTL value for an incoming BGP packet.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context **[Tree]** (config>service>vprn>bgp>group ttl-security)
[Tree] (config>service>vprn>bgp>group>neighbor ttl-security)

Full Context configure service vprn bgp group neighbor ttl-security
configure service vprn bgp group ttl-security

Description Configure TTL security parameters for incoming packets.

Parameters *min-ttl-value* — Specifies the minimum TTL value for an incoming BGP packet.

Values 1 to 255

Default 1

Platforms All

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context **[Tree]** (config>router>bgp>group ttl-security)
[Tree] (config>router>bgp>group>neighbor ttl-security)
[Tree] (config>router>ldp>tcp-session-params>peer-transport ttl-security)
[Tree] (config>system>login-control>ssh ttl-security)
[Tree] (config>system>login-control>telnet ttl-security)

Full Context configure router bgp group neighbor ttl-security
configure router bgp group ttl-security
configure router ldp tcp-session-parameters peer-transport ttl-security
configure system login-control ssh ttl-security
configure system login-control telnet ttl-security

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, LDP will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer. Per-peer-queueing must be enabled in order for TTL protection to operate.

The **no** form of this command disables TTL security.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *min-ttl-value* — Specifies the minimum TTL value for an incoming BGP packet.

Values 1 to 255

Platforms All

24.205 tunnel

tunnel

Syntax **tunnel** *tunnel-name* [**create**]
no tunnel *tunnel-name*

Context **[Tree]** (config>router>l2tp>group tunnel)
[Tree] (config>service>vprn>l2tp>group tunnel)

Full Context configure router l2tp group tunnel
configure service vprn l2tp group tunnel

Description This command configures an L2TP tunnel. A tunnel exists between a LAC-LNS pair and consists of a Control Connection and zero or more L2TP sessions. The tunnel carries encapsulated PPP datagrams and control messages between the LAC and the L2TP Network Server (LNS).

The **no** form of this command removes the tunnel name from the configuration.

Parameters *tunnel-name* — Specifies a valid string to identify an L2TP, up to 32 characters.

create — Mandatory keyword to create a new tunnel.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

tunnel

Syntax **tunnel** *connection-id*

Context **[Tree]** (debug>router>l2tp tunnel)

Full Context debug router l2tp tunnel

Description This command enables debugging for an L2TP tunnel.

Parameters *connection-id* — Specifies the connection ID of the L2TP session associated with this session.

Values 1 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tunnel

Syntax **tunnel** *service-id* **backbone-dest-mac** *mac-name* **isid** *ISID*
tunnel *service-id* **backbone-dest-mac** *ieee-address* **isid** *ISID*
no tunnel

Context **[Tree]** (config>service>epipe>pbb tunnel)

Full Context configure service epipe pbb tunnel

Description This command configures a Provider Backbone Bridging (PBB) tunnel with Backbone VPLS (B-VPLS) service information.

Parameters *service-id* — Specifies the B-VPLS service for the PBB tunnel associated with this service.

Values *service-id*: 1 to 2147483648
svc-name: 64 characters maximum

backbone-dest-mac *mac-name* — Specifies the backbone destination MAC name for PBB packets up to 32 characters in length.

backbone-dest-mac *ieee-address* — Specifies the backbone destination MAC-address for PBB packets as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

isid *ISID* — Specifies a 24 bit service instance identifier for the PBB tunnel associated with this service. As part of the PBB frames, it is used at the destination PE as a demultiplexer field.

Values 0 to 16777215

Platforms All

tunnel

Syntax **tunnel** *ipsec-tunnel-name* [**detail**] [**no-dpd-debug**] [**display-keys**]
no tunnel *ipsec-tunnel-name*

Context **[Tree]** (debug>ipsec tunnel)

Full Context debug ipsec tunnel

Description This command enables debugging for specified IPsec tunnel.

Note: Up to 16 IPsec tunnels are allowed, to enable debugging, at a time.

Parameters *ipsec-tunnel-name* — Specifies the name of ipsec-tunnel, up to 32 characters.

detail — Displays detailed debug information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no-dpd-debug — Stops logging IKEv1 and IKEv2 DPD events for less noise during debug.

display-keys — Specifies the IKE-SA and CHILD-SA keys for inclusion in the debug output.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tunnel

Syntax [**no**] **tunnel** *ip-address*

Context **[Tree]** (debug>router>rib-api tunnel)

Full Context debug router rib-api tunnel

Description This command enables debugging for the specified RIB-API tunnel.

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the RIB-API tunnel.

Values

ipv4-address:	a.b.c.d	
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)	
	x:x:x:x:x:x:d.d.d.d	
	x:	[0 to FFFF]H
	d:	[0 to 255]D

Platforms All

tunnel

Syntax **tunnel** *name* **[create]**
no tunnel *name*

Context **[Tree]** (config>system>grpc-tunnel tunnel)

Full Context configure system grpc-tunnel tunnel

Description Commands in this context configure gRPC tunnel parameters for the specified tunnel. There can be multiple tunnels to one or more destinations.

The **no** form of this command removes the specified gRPC tunnel.

Parameters *name* — Specifies the tunnel name, up to 32 characters.

create — Keyword used to create a tunnel.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.206 tunnel-client-attrs

tunnel-client-attrs

Syntax [**no**] **tunnel-client-attrs**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute tunnel-client-attrs)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute tunnel-client-attrs

Description This command specifies that tunnel attributes should be included into RADIUS accounting messages.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.207 tunnel-dot1q

tunnel-dot1q

Syntax [**no**] **tunnel-dot1q**

Context **[Tree]** (config>port>ethernet>dot1x tunnel-dot1q)

Full Context configure port ethernet dot1x tunnel-dot1q

Description This command configures the tunneling of single tagged (dot1q) dot1x packets arriving on the port. When enabled, the router extracts these packets to the CPM.

The **no** form of this command disables the tunelling of the dot1q dot 1x packets on the port.

Default tunnel-dot1q

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.208 tunnel-down-damp-time

tunnel-down-damp-time

Syntax **tunnel-down-damp-time** *seconds*
no tunnel-down-damp-time

Context **[Tree]** (config>router>ldp tunnel-down-damp-time)

Full Context configure router ldp tunnel-down-damp-time

Description This command specifies the time interval (in s), that LDP waits before posting a tunnel down event to the Tunnel Table Manager (TTM).

When LDP can no longer resolve a FEC and de-activates it, it de-programs the NHLFE in the data path. It will however delay deleting the LDP tunnel entry in the TTM until the tunnel-down-damp-time timer expires. This means users of the LDP tunnel, such as SDPs (all services) and BGP (L3 VPN), will not be notified immediately. Traffic is still blackholed because the forwarding engine NHLFE has been de-programmed.

If the FEC gets resolved before the tunnel-down-damp-time timer expires, then LDP programs the forwarding engine with the new NHLFE and performs a tunnel modify event in TTM updating the dampened entry in TTM with the new NHLFE information. If the FEC does not get resolved and the tunnel-down-damp-time timer expires, LDP posts a tunnel down event to TTM which deletes the LDP tunnel.

When there is an upper layer (user of LDP) which depends of LDP control plane for failover detection then label withdrawal delay and tunnel-down-damp-time options must be set to 0.

An example is pseudowire redundancy where the primary PW does not have its own fast failover detection mechanism and the node depends on LDP tunnel down event to activate the standby PW.

The **no** form of this command resumes the default value of this command.

Default no tunnel-down-damp-time (which equals a value of 3 seconds)

Parameters *seconds* — Specifies the time interval (in s), that LDP waits before posting a tunnel down event to the Tunnel Table Manager.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.209 tunnel-encaps

tunnel-encaps

Syntax **tunnel-encaps**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw tunnel-encaps)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw tunnel-encaps)

Full Context configure service ies subscriber-interface group-interface wlan-gw tunnel-encaps
configure service vprn subscriber-interface group-interface wlan-gw tunnel-encaps

Description Commands in this context configure tunnel encapsulation parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.210 tunnel-endpoint

tunnel-endpoint

Syntax **tunnel-endpoint** [**tunnel-spf**] [**tunnel-leak** *ip-address*]
no tunnel-endpoint

Context **[Tree]** (debug>router>isis tunnel-endpoint)

Full Context debug router isis tunnel-endpoint

Description This command enables debugging for an ISIS tunnel endpoint.

The **no** form of the command disables the debugging.

Parameters **tunnel-spf** — Debugs tunnel SPF information.

ip-address — When specified, only packets with the specified address are debugged.

Platforms All

tunnel-endpoint

Syntax **tunnel-endpoint** [**tunnel-spf** *ip-address*] [**tunnel-leak** *ip-address*]

Context **[Tree]** (debug>router>ospf tunnel-endpoint)
[Tree] (debug>router>ospf3 tunnel-endpoint)

Full Context debug router ospf tunnel-endpoint

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

debug router ospf3 tunnel-endpoint

Description This command enables debugging for OSPF tunnel endpoints.

Parameters **tunnel-spf** — Specifies the tunnel SPF IP address.

tunnel-leak — Specifies the tunnel leak IP address.

ip-address — Specifies the IP address.

Platforms All

24.211 tunnel-endpoint-id

tunnel-endpoint-id

Syntax **tunnel-endpoint-id** *tunnel-endpoint-id*
no tunnel-endpoint-id

Context **[Tree]** (config>test-oam>build-packet>header>gtp-user tunnel-endpoint-id)

Full Context configure test-oam build-packet header gtp-user tunnel-endpoint-id

Description This command defines the GTP tunnel endpoint ID for the GTP user header.

The **no** form of this command removes the tunnel endpoint ID value.

Default tunnel-endpoint-id 0

Parameters *tunnel-endpoint-id* — Specifies the GTP tunnel endpoint ID to be used in the test GTP header.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tunnel-endpoint-id

Syntax **tunnel-endpoint-id** *tunnel-endpoint-id*
no tunnel-endpoint-id

Context **[Tree]** (debug>oam>build-packet>packet>field-override>header>gtp-user tunnel-endpoint-id)

Full Context debug oam build-packet packet field-override header gtp-user tunnel-endpoint-id

Description This command debugs the GTP tunnel endpoint ID for the GTP user header.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the tunnel endpoint ID value.

Default no override

Parameters *tunnel-endpoint-id* — Specifies the GTP tunnel endpoint ID to be used in the test GTP header.

Values 0 to 4294967295

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.212 tunnel-far-end

tunnel-far-end

Syntax **tunnel-far-end** *ip-address* | *ipv6-address*
no tunnel-far-end [*ip-address* | *ipv6-address*]

Context **[Tree]** (config>service>sdp tunnel-far-end)

Full Context configure service sdp tunnel-far-end

Description This command enables the user to specify an SDP tunnel destination address that is different from the configuration in the SDP far-end option. The SDP must be shutdown first to add or change the configuration of the **tunnel-far-end** option.

When this option is enabled, service packets are encapsulated using an LDP LSP with a FEC prefix matching the value entered in ip-address. By default, service packets are encapsulated using an LDP LSP with a FEC prefix matching the address entered in the SDP far-end option.

The T-LDP session to the remote PE is still targeted to the address configured under the **far-end option**. This means that targeted hello messages are sent to the far-end address, which is also the LSR-ID of the remote node. TCP based LDP messages, such as initialization and label mapping messages, are sent to the address specified in the transport-address field of the “hello” message received from the remote PE. This address can be the same as the remote PE LSR-ID, or a different address. This feature works, however, if the signaling option in the SDP is set to off instead of tldp, in which case, the service labels are statically configured.

This feature operates on an SDP of type LDP only. It can be used with VLL, VPLS, and VPRN services when an explicit binding to an SDP with the **tunnel-far-end** is specified. It also operates with a spoke interface on an IES or VPRN service. Finally, this feature operates with a BGP AD based VPLS service when the **use-provisioned-sdp** option is enabled in the pseudowire template.

This feature is not supported in an SDP of type MPLS when an RSVP LSP name is configured under the SDP. It also does not work with a mixed-lsp SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the use of the **tunnel-far-end** option and returns to using the address specified in the far-end.

Default no tunnel-far-end

Parameters *ip-address* **|** *ipv6-address* — Specifies the system address of the far-end router for the SDP in dotted decimal notation.

Platforms All

24.213 tunnel-fault

tunnel-fault

Syntax **tunnel-fault** {**accept** | **ignore**}

Context **[Tree]** (config>service>vpls>eth-cfm tunnel-fault)
[Tree] (config>service>vpls>sap>eth-cfm tunnel-fault)
[Tree] (config>service>epipe>eth-cfm tunnel-fault)
[Tree] (config>service>epipe>sap>eth-cfm tunnel-fault)
[Tree] (config>service>ipipe>eth-cfm tunnel-fault)
[Tree] (config>service>ipipe>sap>eth-cfm tunnel-fault)
[Tree] (config>service>ies>eth-cfm tunnel-fault)
[Tree] (config>service>ies>if>sap>eth-cfm tunnel-fault)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm tunnel-fault)
[Tree] (config>service>vprn>eth-cfm tunnel-fault)
[Tree] (config>service>vprn>if>sap>eth-cfm tunnel-fault)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm tunnel-fault)

Full Context configure service epipe eth-cfm tunnel-fault
configure service epipe sap eth-cfm tunnel-fault
configure service ies eth-cfm tunnel-fault
configure service ies interface sap eth-cfm tunnel-fault
configure service ies subscriber-interface group-interface sap eth-cfm tunnel-fault
configure service ipipe eth-cfm tunnel-fault
configure service ipipe sap eth-cfm tunnel-fault
configure service vpls eth-cfm tunnel-fault
configure service vpls sap eth-cfm tunnel-fault
configure service vprn eth-cfm tunnel-fault
configure service vprn interface sap eth-cfm tunnel-fault
configure service vprn subscriber-interface group-interface sap eth-cfm tunnel-fault

Description Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type, Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an Epipe service as well as setting the operational

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

flag. If AIS generation is the requirement for the Epipe services this command is not required. See the **ais-enable** command under the **config>service>epipe>sap>eth-cfm>ais-enable** context for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is “ignore” and the SAP level command is “accept”. This means simply changing the service level command to “accept” will enable the feature for all SAPs. This is not required for Epipe services that only wish to generate AIS on failure.

Default tunnel-fault ignore (Service Level)

tunnel-fault accept (SAP Level for Epipe and VPLS)

Parameters **accept** — Shares fate with the facility tunnel MEP.

ignore — Does not share fate with the facility tunnel MEP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm tunnel-fault
- configure service ies subscriber-interface group-interface sap eth-cfm tunnel-fault

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service epipe eth-cfm tunnel-fault
- configure service vpls sap eth-cfm tunnel-fault
- configure service ies eth-cfm tunnel-fault
- configure service vprn interface sap eth-cfm tunnel-fault
- configure service ipipe sap eth-cfm tunnel-fault
- configure service ies interface sap eth-cfm tunnel-fault
- configure service vprn eth-cfm tunnel-fault
- configure service ipipe eth-cfm tunnel-fault
- configure service epipe sap eth-cfm tunnel-fault
- configure service vpls eth-cfm tunnel-fault

24.214 tunnel-group

tunnel-group

Syntax **tunnel-group** *tunnel-group-id* [**create**]
tunnel-group *tunnel-group-id* **isa-scale-mode** *isa-scale-mode* [**create**]
no tunnel-group *tunnel-group-id*

Context **[Tree]** (config>isa tunnel-group)

Full Context configure isa tunnel-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows a tunnel group to be created or edited. A tunnel group is a set of one or more MS-ISAs that support the origination and termination of IPsec and IP/GRE tunnels. All of the MS-ISAs in a tunnel group must have **isa-tunnel** as their configured mda-type. On VSR, **isa-scale-mode** must be specified, which defines the number of tunnels on each ISA.

The **no** form of this command deletes the specified tunnel group from the configuration

Parameters *tunnel-group-id* — Identifies the tunnel group.

Values 1 to 16

isa-scale-mode — Defines the maximum number of tunnels (all types combined) which can be established on each ISA of the tunnel group and for the whole tunnel-group.

Values tunnel-limit-32k, where k equals 1024

create — Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tunnel-group

Syntax **tunnel-group** *tunnel-group-id* [**create**]
no tunnel-group *tunnel-group-id*

Context **[Tree]** (config>redundancy>multi-chassis>peer>mc-ipsec tunnel-group)

Full Context configure redundancy multi-chassis peer mc-ipsec tunnel-group

Description This command enables multi-chassis redundancy for specified tunnel-group; or enters an already configured tunnel-group context. The configured tunnel-group could failover independently.

The **no** form of this command removes the tunnel group ID from the configuration.

Parameters *tunnel-group-id* — Specifies the tunnel-group identifier.

Values 1 to 16

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tunnel-group

Syntax **tunnel-group** *tunnel-group-id* **sync-tag** *tag-name* [**create**]
no tunnel-group *tunnel-group-id*

Context **[Tree]** (config>redundancy>multi-chassis>peer>sync tunnel-group)

Full Context configure redundancy multi-chassis peer sync tunnel-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables multi-chassis synchronization of IPsec states of specified tunnel-groups with a peer. The **sync-tag** parameter is used to match corresponding tunnel-group on both peers. IPsec states will be synchronized between tunnel-groups with same sync-tag.

Parameters *tunnel-group-id* — Specifies the ID of the tunnel group.

tag-name — Specifies the name of the sync-tag.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.215 tunnel-id

tunnel-id

Syntax **tunnel-id** *tunnel-id*
no tunnel-id

Context **[Tree]** (config>test-oam>build-packet>header>l2tp tunnel-id)
[Tree] (debug>oam>build-packet>packet>field-override>header>l2tp tunnel-id)

Full Context configure test-oam build-packet header l2tp tunnel-id
debug oam build-packet packet field-override header l2tp tunnel-id

Description This command defines the tunnel ID to be used in the L2TP header.

The **no** form of this command removes the tunnel ID value.

Default tunnel-id 0

Parameters *tunnel-id* — Specifies the L2TP tunnel ID to be used in the L2TP header.

Values 0 to 65535

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.216 tunnel-interface

tunnel-interface

Syntax [**no**] **tunnel-interface** {**rsvp-p2mp** *lsp-name* | **ldp-p2mp** *p2mp-id* **sender** *sender-address* [**root-node**]}

Context **[Tree]** (config>router tunnel-interface)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>router>igmp tunnel-interface)

Full Context configure router igmp tunnel-interface
configure router tunnel-interface

Description This command creates a tunnel interface associated with an RSVP P2MP LSP. IPv4 multicast packets are forwarded over the P2MP LSP at the ingress LER based on a static join configuration of the multicast group against the tunnel interface associated with the originating P2MP LSP. At the egress LER, packets of a multicast group are received from the P2MP LSP via a static assignment of the specific <S,G> to the tunnel interface associated with a terminating LSP.

At ingress LER, the tunnel interface identifier consists of a string of characters representing the LSP name for the RSVP P2MP LSP. The user can create one or more tunnel interfaces and associate each to a different RSVP P2MP LSP.

At egress LER, the tunnel interface identifier consists of a couple of string of characters representing the LSP name for the RSVP P2MP LSP followed by the system address of the ingress LER. The LSP name must correspond to a P2MP LSP name configured by the user at the ingress LER. The LSP name string must not contain "::" (two :s) nor contain a ":" (single ":") at the end of the LSP name. However, a ":" (single ":") can appear anywhere in the string except at the end of the name.

Parameters **rsvp-p2mp** *lsp-name* — Specifies the LSP. The LSP name can be up to 32 characters long and must be unique.

ldp-p2mp *p2mp-id* — Identifier used for signaling MLDP P2MP LSP.

Values 1 to 4294967296 (on leaf node)
1 to 8192 (on root node)

sender *sender-address* — Specifies the sender IP address: a.b.c.d.

Platforms All

tunnel-interface

Syntax **tunnel-interface** [**rsvp-p2mp** *lsp-name*] [**sender** *ip-address*] [**detail**]
tunnel-interface [**ldp-p2mp** *p2mp-id*] [**sender** *ip-address*] [**detail**]
no tunnel-interface [**rsvp-p2mp** *lsp-name*] [**sender** *ip-address*]
no tunnel-interface [**ldp-p2mp** *p2mp-id*] [**sender** *ip-address*]

Context **[Tree]** (debug>router>pim tunnel-interface)

Full Context debug router pim tunnel-interface

Description This command enables debugging for PIM tunnel interfaces.

The **no** form of this command disables debugging for PIM tunnel interfaces.

Parameters *lsp-name* — Specifies the LSP for RSVP P2MP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip-address — Specifies the IP address of the sender.

p2mp-id — Specifies the P2MP ID for LDP P2MP.

detail — Displays detailed information for PIM tunnel interfaces.

Platforms All

tunnel-interface

Syntax [**no**] **tunnel-interface rsvp-p2mp** *lsp-name* **sender** *ip-address*

Context **[Tree]** (config>router>pim tunnel-interface)

Full Context configure router pim tunnel-interface

Description This command creates a tunnel interface associated with an RSVP P2MP LSP. IPv4 multicast packets are forwarded over the P2MP LSP at the ingress LER based on a static join configuration of the multicast group against the tunnel interface associated with the originating P2MP LSP. At the egress LER, packets of a multicast group are received from the P2MP LSP via a static assignment of the specific <S,G> to the tunnel interface associated with a terminating LSP.

At ingress LER, the tunnel interface identifier consists of a string of characters representing the LSP name for the RSVP P2MP LSP. The user can create one or more tunnel interfaces in PIM and associate each to a different RSVP P2MP LSP.

At egress LER, the tunnel interface identifier consists of a couple of string of characters representing the LSP name for the RSVP P2MP LSP followed by the system address of the ingress LER. The LSP name must correspond to a P2MP LSP name configured by the user at the ingress LER. The LSP name string must not contain "::" (two :s) nor contain a ":" (single ":") at the end of the LSP name. However, a ":" (single ":") can appear anywhere in the string except at the end of the name.

The **no** form of this command removes the tunnel parameters.

Parameters *lsp-name* — Specifies the LSP, up to 32 characters.

ip-address — Specifies the sender IP address.

Platforms All

24.217 tunnel-local-address

tunnel-local-address

Syntax **tunnel-local-address** *ip-address*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no tunnel-local-address

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query tunnel-local-address)

Full Context configure subscriber-mgmt wlan-gw ue-query tunnel-local-address

Description This command enables matching on UEs that are active on a tunnel which is connected to the specified IP address on the WLAN-GW.

The **no** form of this command disables matching on the local tunnel address.

Default no tunnel-local-address

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the local tunnel.

Values	
ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.218 tunnel-mtu

tunnel-mtu

Syntax **tunnel-mtu** *mtu-bytes*
no tunnel-mtu

Context **[Tree]** (config>service>vprn>nat>inside>dslite>address tunnel-mtu)

Full Context configure service vprn nat inside dual-stack-lite address tunnel-mtu

Description This command configures the DS-Lite tunnel MTU for this DS-Lite address.

The **no** form of this command reverts the default.

Default tunnel-mtu 1500

Parameters *mtu-bytes* — Specifies the DS-Lite tunnel MTU.

Values 512 to 9212

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tunnel-mtu

Syntax **tunnel-mtu** *mtu-bytes*
no tunnel-mtu

Context **[Tree]** (config>router>nat>inside>dual-stack-lit>address tunnel-mtu)

Full Context configure router nat inside dual-stack-lit address tunnel-mtu

Description This command sets the size of the payload in IPv6 packet in downstream DS-Lite direction. The payload is, in essence, the tunneled IPv4 packet.

tunnel-mtu

Syntax **tunnel-mtu** *bytes*
no tunnel-mtu

Context **[Tree]** (config>router>isis>segment-routing tunnel-mtu)

Full Context configure router isis segment-routing tunnel-mtu

Description This command configures the MTU of all SR tunnels within each IGP instance.

The MTU of a SR tunnel populated into TTM is determined like in the case of an IGP tunnel; for example, LDP LSP, based on the outgoing interface MTU minus the label stack size. Remote LFA can add, at most, one more label to the tunnel for a total of two labels. There is no default value for this command. If the user does not configure an SR tunnel MTU, the MTU is determined by IGP as explained below.

The MTU of the SR tunnel in bytes is then determined as follows:

*SR_Tunnel_MTU = MIN {Cfg_SR_MTU, IGP_Tunnel_MTU- (1+frr-overhead)*4}*

Where:

Cfg_SR_MTU is the MTU configured by the user for all SR tunnels within a given IGP instance using the above CLI. If no value was configured by the user, the SR tunnel MTU will be determined by the IGP interface calculation explained next.

IGP_Tunnel_MTU is the minimum of the IS-IS or OSPF interface MTU among all the ECMP paths or among the primary and LFA backup paths of this SR tunnel.

frr-overhead is set to 1 if **segment-routing** and **remote-lfa** options are enabled in the IGMP instance. Otherwise, it is set to 0.

The SR tunnel MTU is dynamically updated anytime any of the above parameters used in its calculation changes. This includes when the set of the tunnel next-hops changes or the user changes the configured SR MTU or interface MTU value.

Default no tunnel-mtu

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *bytes* — Specifies the size of the Maximum Transmission Unit (MTU) in bytes.

Values 512 to 9786

Platforms All

tunnel-mtu

Syntax **tunnel-mtu** *bytes*
no tunnel-mtu

Context **[Tree]** (config>router>ospf>segm-rtng tunnel-mtu)
[Tree] (config>router>ospf3>segm-rtng tunnel-mtu)

Full Context configure router ospf segment-routing tunnel-mtu
configure router ospf3 segment-routing tunnel-mtu

Description This command configures the MTU of all SR tunnels within each IGP instance.

The MTU of a SR tunnel populated into the TTM is determined as the same as an IGP tunnel; for example, for an LDP LSP, based on the outgoing interface MTU minus the label stack size. Remote LFA can add, at most, one more label to the tunnel for a total of two labels. There is no default value for this command. If the user does not configure an SR tunnel MTU, the MTU will be determined by IGP as follows:

The MTU of the SR tunnel in bytes is then determined as follows:

SR_Tunnel_MTU = MIN {Cfg_SR_MTU, IGP_Tunnel_MTU- (1+frr—overhead)×4}

Where:

- *Cfg_SR_MTU* is the MTU configured by the user for all SR tunnels within an IGP instance using the tunnel-mtu command. If no value is configured by the user, the SR tunnel MTU is determined by the IGP interface calculation explained in the next bullet point.
- *IGP_Tunnel_MTU* is the minimum of the IS-IS or OSPF interface MTU among all the ECMP paths or among the primary and LFA backup paths of this SR tunnel.
- *frr-overhead* is set to 1 if the **segment-routing** and **remote-lfa** options are enabled in the IGMP instance. Otherwise, it is set to 0.

The SR tunnel MTU is dynamically updated whenever any of the above parameters used in its calculation changes. This includes if the set of the tunnel next-hops changes or the user changes the configured SR MTU or interface MTU value.

Default no tunnel-mtu

Parameters *bytes* — Specifies the size of the MTU in bytes.

Values 512 to 9786

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.219 tunnel-nearest-bridge

tunnel-nearest-bridge

Syntax [**no**] **tunnel-nearest-bridge**

Context **[Tree]** (cfg>port>eth>lldp>dstmac tunnel-nearest-bridge)

Full Context configure port ethernet lldp dest-mac tunnel-nearest-bridge

Description This command allows LLDP packets received on the port with the destination address of the nearest bridge to be tunneled without being intercepted on the local port. The dest-mac nearest-bridge must be disabled for tunneling to occur. This is applicable to NULL SAP Epipe and VPLS services only.

Default no tunnel-nearest-bridge

Platforms All

24.220 tunnel-next-hop

tunnel-next-hop

Syntax **tunnel-next-hop**

Context **[Tree]** (config>router>static-route-entry>indirect tunnel-next-hop)

Full Context configure router static-route-entry indirect tunnel-next-hop

Description Commands in this context configure the static route's nexthop to be resolved to an indirect tunnel next-hop.

Platforms All

tunnel-next-hop

Syntax **tunnel-next-hop**

Context **[Tree]** (config>router>isis>igp-shortcut tunnel-next-hop)

Full Context configure router isis igp-shortcut tunnel-next-hop

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the resolution of IGP IPv4 prefix families, IGP IPv6 prefix families, SR-ISIS IPv4 tunnel families, SR-ISIS IPv6 tunnel families, and SR-OSPF IPv4 tunnel families using IGP shortcuts.

The **resolution** node is introduced to provide flexibility in the selection of the tunnel types for each of the IP prefix and SR tunnel families.

The IPv4 **family** option causes the IS-IS or OSPF SPF to include the IPv4 IGP shortcuts in the IP reach calculation of IPv4 nodes and prefixes. RSVP-TE or SR-TE LSPs terminating on a node identified by its router ID can be used to reach IPv4 prefixes owned by this node or for which this node is the IPv4 next hop.

The IPv6 **family** option causes the IS-IS or OSPFv3 SPF to include the IPv4 IGP shortcuts in the IP reach calculation of IPv6 nodes and prefixes. RSVP-TE or SR-TE LSPs terminating on a node identified by its router ID can be used to reach IPv6 prefixes owned by this node or for which this node is the IPv6 next-hop. The resolution of IPv6 prefixes is supported in OSPFv3 and in both IS-IS MT=0 and MT=2.

The IS-IS and OSPFv3 IPv6 routes resolved to IPv4 IGP shortcuts are used to:

- forward packets of IS-IS or OSPFv3 prefixes matching these routes
- forward CPM-originated IPv6 packets
- resolve the BGP next hop of BGP IPv6 prefixes
- resolve the indirect next hop of static IPv6 routes

In the data path, a packet for an IPv6 prefix has a label stack that consists of the IPv6 Explicit-Null label value of 2 at the bottom of the label stack followed by the label stack of the IPv4 RSVP-TE LSP.

There is no default behavior for IPv4 prefixes to automatically resolve to RSVP-TE or SR-TE LSPs used as IGP shortcuts by only enabling the **igp-shortcut** context. Instead, the user must enable the **ipv4 family** or **ipv6 family** and set the resolution to the value of **rsvp-te** to select the RSVP-TE tunnel type, or to the value of **sr-te** to select the SR-TE tunnel type.

Setting the **resolution** to the **any** value means that IGP selects the tunnels used as IGP shortcuts according to the TTM preference for the tunnel type. The RSVP-TE LSP type is of higher priority than the SR-TE LSP type.

An IP prefix of family=ipv4 or family=ipv6 always resolves to a single type of tunnel **rsvp-te** or **sr-te**. **Rsvp-te** type is preferred if both types are allowed by the prefix family resolution and both types exist in the set of tunnel next-hops of the prefix. The feature does not support mixing tunnel types per prefix.

If **resolution** for the IPv4 or IPv6 family is set to **disabled**, the corresponding prefixes are resolved to IP next-hops in the multicast routing table.

The **srv4 family** enables the resolution of SR-OSPF IPv4 tunnels and SR-ISIS IPv4 tunnels in MT=0 over RSVP-TE IPv4 IGP shortcuts. A maximum of 32 ECMP tunnel next-hops can be programmed for an SR-OSPF or an SR-ISIS IPv4 tunnel.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **srv6 family** enables the resolution of SR-ISIS IPv6 tunnels in MT=0 over RSVP-TE IPv4 IGP shortcuts. A maximum of 32 ECMP tunnel next-hops can be programmed for an SR-ISIS IPv6 tunnel.

One or more RSVP-TE LSPs can be selected if **resolution**=**match-family-ip** and the corresponding IPv4 or IPv6 prefix resolves to RSVP-TE LSPs.

Note: An SR tunnel cannot resolve to SR-TE IGP shortcuts.

If **resolution** for the SRv4 or SRv6 tunnel family is set to **disabled**, the corresponding tunnels are resolved to IP next-hops in the multicast routing table.

To enable (disable) IGP shortcuts in the IGP instance, the user must perform a **shutdown** or **no shutdown** in the **igp-shortcut** context.

Platforms All

tunnel-next-hop

Syntax **tunnel-next-hop**

Context **[Tree]** (config>router>ospf>igp-shortcut tunnel-next-hop)
[Tree] (config>router>ospf3>igp-shortcut tunnel-next-hop)

Full Context configure router ospf igp-shortcut tunnel-next-hop
configure router ospf3 igp-shortcut tunnel-next-hop

Description Commands in this context configure the resolution of IGP IPv4 prefix families, IGP IPv6 prefix families, SR-ISIS IPv4 tunnel families, SR-ISIS IPv6 tunnel families, and SR-OSPF IPv4 tunnel families using IGP shortcuts.

The **resolution** node is introduced to provide flexibility in the selection of the tunnel types for each of the IP prefix and SR tunnel families.

The IPv4 **family** option causes the IS-IS or OSPF SPF to include the IPv4 IGP shortcuts in the IP reach calculation of IPv4 nodes and prefixes. RSVP-TE or SR-TE LSPs terminating on a node identified by its router ID can be used to reach IPv4 prefixes owned by this node or for which this node is the IPv4 next hop.

The IPv6 **family** option causes the IS-IS or OSPFv3 SPF to include the IPv4 IGP shortcuts in the IP reach calculation of IPv6 nodes and prefixes. RSVP-TE or SR-TE LSPs terminating on a node identified by its router ID can be used to reach IPv6 prefixes owned by this node or for which this node is the IPv6 next hop. The resolution of IPv6 prefixes is supported in OSPFv3 and in both IS-IS MT=0 and MT=2.

The IS-IS and OSPFv3 IPv6 routes resolved to IPv4 IGP shortcuts are used to:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- forward packets of IS-IS or OSPFv3 prefixes matching these routes
- forward CPM-originated IPv6 packets
- resolve the BGP next hop of BGP IPv6 prefixes
- resolve the indirect next hop of static IPv6 routes

In the data path, a packet for an IPv6 prefix has a label stack that consists of the IPv6 Explicit-Null label value of 2 at the bottom of the label stack followed by the label stack of the IPv4 RSVP-TE LSP.

There is no default behavior for IPv4 prefixes to automatically resolve to RSVP-TE or SR-TE LSPs used as IGP shortcuts by only enabling the **igp-shortcut** context. Instead, the user must enable the **ipv4 family** or **ipv6 family** and set the resolution to the value of **rsvp-te** to select the RSVP-TE tunnel type, or to the value of **sr-te** to select the SR-TE tunnel type.

Setting the **resolution** to the **any** value means that IGP selects the tunnels used as IGP shortcuts according to the TTM preference for the tunnel type. The RSVP-TE LSP type is of higher priority than the SR-TE LSP type.

An IP prefix of family=ipv4 or family=ipv6 always resolves to a single type of tunnel **rsvp-te** or **sr-te**. **Rsvp-te** type is preferred if both types are allowed by the prefix family resolution and both types exist in the set of tunnel next-hops of the prefix. The feature does not support mixing tunnel types per prefix.

If **resolution** for the IPv4 or IPv6 family is set to **disabled**, the corresponding prefixes are resolved to IP next-hops in the multicast routing table.

The **srv4 family** enables the resolution of SR-OSPF IPv4 tunnels and SR-ISIS IPv4 tunnels in MT=0 over RSVP-TE IPv4 IGP shortcuts. A maximum of 32 ECMP tunnel next-hops can be programmed for an SR-OSPF or an SR-ISIS IPv4 tunnel.

The **srv6 family** enables the resolution of SR-ISIS IPv6 tunnels in MT=0 over RSVP-TE IPv4 IGP shortcuts. A maximum of 32 ECMP tunnel next-hops can be programmed for an SR-ISIS IPv6 tunnel.

One or more RSVP-TE LSPs can be selected if **resolution**=**match-family-ip** and the corresponding IPv4 or IPv6 prefix resolves to RSVP-TE LSPs.

Note: An SR tunnel cannot resolve to SR-TE IGP shortcuts.

If **resolution** for the SRv4 or SRv6 tunnel family is set to **disabled**, the corresponding tunnels are resolved to IP next-hops in the multicast routing table.

To enable or disable IGP shortcuts in the IGP instance, the user must perform a **shutdown** or **no shutdown** in the **igp-shortcut** context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.221 tunnel-port-policy

tunnel-port-policy

Syntax **tunnel-port-policy** [*tunnel-port-policy*]
no tunnel-port-policy

Context **[Tree]** (config>isa>wlan-gw-group tunnel-port-policy)

Full Context configure isa wlan-gw-group tunnel-port-policy

Description This command configures the tunnel port policy of this WLAN Gateway ISA group. If a tunnel port policy is associated with a WLAN Gateway ISA group, ports created for this group can take applicable configuration from that policy. This policy is applicable to those ports that take part in the per-tunnel QoS processing.

The **no** form of the command removes the **tunnel-port-policy** name from the configuration.

Default no-tunnel-policy

Parameters *tunnel-port-policy* — Specifies the tunnel port policy of this WLAN Gateway ISA group, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.222 tunnel-qinq

tunnel-qinq

Syntax [**no**] **tunnel-qinq**

Context **[Tree]** (config>port>ethernet>dot1x tunnel-qinq)

Full Context configure port ethernet dot1x tunnel-qinq

Description This command configures the tunneling of double tagged (QinQ) dot1x packets. When enabled, the router extracts the packets to the CPM.

The **no** form of this command disables the tunelling of the QinQ dot1x packets on the port.

Default tunnel-qinq

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.223 tunnel-query

tunnel-query

Syntax **tunnel-query** *query-id* [**name** *name*] [**create**]
no tunnel-query *query-id*

Context **[Tree]** (config>subscr-mgmt>wlan-gw tunnel-query)

Full Context configure subscriber-mgmt wlan-gw tunnel-query

Description This command creates a tunnel query where filter criteria over WLAN-GW tunnels are defined. This query can later be used to retrieve the state of the tunnels and Layer 2 access points (which are modeled as tunnels) matching the configured criteria.

The **no** form of this command removes the query.

Parameters *query-id* — Specifies the ID assigned to a query.

Values 1 to 1024

name — Specifies the name assigned to a query, up to 32 characters.

create — Creates a tunnel query.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.224 tunnel-remote-address

tunnel-remote-address

Syntax **tunnel-remote-address** *ip-address*
no tunnel-remote-address

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query tunnel-remote-address)

Full Context configure subscriber-mgmt wlan-gw ue-query tunnel-remote-address

Description This command enables matching on UEs that are active on a tunnel with the specified source IP address.

The **no** form of this command disables matching on the remote tunnel address.

Default no tunnel-remote-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-address* — Specifies the IPv4 or IPv6 address of the remote tunnel.

Values	
ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.225 tunnel-resource-limit

tunnel-resource-limit

Syntax **tunnel-resource-limit direction** *direction* [**create**]
no tunnel-resource-limit direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter tunnel-resource-limit)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter tunnel-resource-limit

Description This command configures a TCA for the counter capturing the usage of the total number of GTP tunnel resources. A tunnel-resource-limit TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or from the network side (**to-sub**). The **create** keyword is mandatory when creating a TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.226 tunnel-router

tunnel-router

Syntax **tunnel-router** *router-instance*
no tunnel-router

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>wlan-gw>ue-query tunnel-router)

Full Context configure subscriber-mgmt wlan-gw ue-query tunnel-router

Description This command enables matching on UEs that are active on a tunnel which is terminated in the specified router instance.

The **no** form of this command disables matching on the tunnel router instance.

Default no tunnel-router

Parameters *router-instance* — Specifies the routing instance.

Values *router-name* - Base
vprn-svc-id - 1 to 2147483647

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.227 tunnel-selection-blacklist

tunnel-selection-blacklist

Syntax **tunnel-selection-blacklist**

Context [Tree] (config>router>l2tp tunnel-selection-blacklist)
[Tree] (config>service>vprn>l2tp tunnel-selection-blacklist)

Full Context configure router l2tp tunnel-selection-blacklist
configure service vprn l2tp tunnel-selection-blacklist

Description Commands in this context configure L2TP tunnel selection denylist parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.228 tunnel-server-attrs

tunnel-server-attrs

Syntax [**no**] **tunnel-server-attrs**

Context [Tree] (config>subscr-mgmt>auth-policy>include-radius-attribute tunnel-server-attrs)
[Tree] (config>subscr-mgmt>acct-plcy>include-radius-attribute tunnel-server-attrs)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute tunnel-server-attrs
configure subscriber-mgmt authentication-policy include-radius-attribute tunnel-server-attrs

Description This command enables the generation of the tunnel-server RADIUS attribute.

The **no** form of this command disables the generation of the **tunnel-server-attrs** RADIUS attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.229 tunnel-session-limit

tunnel-session-limit

Syntax **tunnel-session-limit** *session-limit*
tunnel-session-limit unlimited
no tunnel-session-limit

Context **[Tree]** (config>router>l2tp tunnel-session-limit)
[Tree] (config>service>vprn>l2tp tunnel-session-limit)

Full Context configure router l2tp tunnel-session-limit
configure service vprn l2tp tunnel-session-limit

Description This command configures the L2TP session limit for each tunnel of the specified router.

The **no** form of this command removes the tunnel session limit value from the configuration.

Default no tunnel-session-limit

Parameters *session-limit* — Specifies the allowed number of sessions within the given context.

Values 1 to 65535

unlimited — Specifies to use the maximum number of sessions available.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.230 tunnel-source-ip

tunnel-source-ip

Syntax **tunnel-source-ip** *ipv6-address/prefix-length*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no tunnel-source-ip

Context [Tree] (config>router>wlan-gw>xconnect tunnel-source-ip)
[Tree] (config>service>vprn>wlan-gw>xconnect tunnel-source-ip)

Full Context configure router wlan-gw xconnect tunnel-source-ip
configure service vprn wlan-gw xconnect tunnel-source-ip

Description This command configures the IPv6 address and prefix for the tunnel source.

The **no** form of this command removes IPv6 address and prefix length from the cross-connect configuration.

Parameters *ipv6-address/prefix-length* — Specifies the tunnel source IPv6 address and prefix length of the cross-connect.

Values ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0..255]D
(no multicast address)
prefix-length [1 to 128]

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.231 tunnel-table

tunnel-table

Syntax **tunnel-table** [*ip-address*] [{**ldp** | **rsvp** [**tunnel-id** *tunnel-id*] | **sdp** [**sdp-id** *sdp-id*}]]

Context [Tree] (debug>router>ip tunnel-table)

Full Context debug router ip tunnel-table

Description This command enables debugging for tunnel tables.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.232 tunnel-table-pref

tunnel-table-pref

Syntax **tunnel-table-pref** *preference*
no tunnel-table-pref

Context **[Tree]** (config>router>ldp tunnel-table-pref)

Full Context configure router ldp tunnel-table-pref

Description This command configures the tunnel table preference for LDP tunnel type away from its default value.

The tunnel table preference applies to the next-hop resolution of BGP routes of the following families: EVPN, IPv4, IPv6, VPN-IPv4, VPN-IPv6, label-IPv4, and label-IPv6 in the tunnel table.

This feature does not apply to a VPRN, VPLS, or VLL service with explicit binding to an SDP that enabled the **mixed-lsp-mode** option. The tunnel preference in such an SDP is fixed and is controlled by the service manager. The configuration of the tunnel table preference parameter does not modify the behavior of such an SDP and the services that bind to it.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

The **no** form of this command reverts to the default value.

Default tunnel-table-pref 9

Parameters *preference* — Specifies the preference value.

Values 1 to 255

Default 9

Platforms All

tunnel-table-pref

Syntax **tunnel-table-pref**

Context **[Tree]** (config>router>mpls tunnel-table-pref)

Full Context configure router mpls tunnel-table-pref

Description Commands in this context configure the tunnel table preference for RSVP-TE LSP and SR-TE LSP tunnel types.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

tunnel-table-pref

Syntax **tunnel-table-pref** *preference-value*
no tunnel-table-pref

Context **[Tree]** (config>router>mpls>fwd-policies>fwd-policy tunnel-table-pref)

Full Context configure router mpls forwarding-policies forwarding-policy tunnel-table-pref

Description This command configures the TTM preference value of an MPLS forwarding policy.

The *preference-value* parameter is used by applications to select one tunnel type to bind to in TTM when multiple tunnel types are enabled for the application.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

The **no** form of this command removes the configured TTM preference parameter value of the MPLS forwarding policy and assigns the default value.

Default no tunnel-table-pref

Parameters *preference-value* — Specifies the preference value.

Values 1 to 255

Default 4

Platforms All

tunnel-table-pref

Syntax **tunnel-table-pref** *preference*
no tunnel-table-pref

Context **[Tree]** (config>router>isis>segment-routing tunnel-table-pref)

Full Context configure router isis segment-routing tunnel-table-pref

Description This command configures the TTM preference of SR tunnels created by the IGP instance. This is used in the case of BGP shortcuts, VPRN auto-bind, or BGP transport tunnel when the new tunnel binding commands are configured to the **any** value which parses the TTM for tunnels in the protocol preference order. The user can choose to either go with the global TTM preference or list explicitly the tunnel types they want to use. When they list the tunnel types explicitly, the TTM preference will still be used to select one type over the other. In both cases, a fallback to the next preferred tunnel type is performed if the selected one fails. Also, a reversion to a more preferred tunnel type is performed as soon as one is available.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The segment routing module adds to TTM a SR tunnel entry for each resolved remote node SID prefix and programs the data path with the corresponding LTN with the push operation pointing to the primary and LFA backup NHLFEs.

The default preference for SR tunnels in the TTM is set lower than LDP tunnels but higher than BGP tunnels to allow controlled migration of customers without disrupting their current deployment when they enable segment routing. The following is the setting of the default preference of the various tunnel types. This includes the preference of SR tunnels based on shortest path (referred to as **SR-ISIS** and **SR-OSPF**).

The global default TTM preference for the tunnel types is as follows:

- ROUTE_PREF_RSVP 7
- ROUTE_PREF_SR_TE 8
- ROUTE_PREF_LDP 9
- ROUTE_PREF_OSPF_TTM 10
- ROUTE_PREF_ISIS_TTM 11
- ROUTE_PREF_BGP_TTM 12
- ROUTE_PREF_GRE 255

The default value for SR-ISIS or SR-OSPF is the same regardless if one or more IS-IS or OSPF instances programmed a tunnel for the same prefix. The selection of a SR tunnel in this case will be based on lowest IGP instance-id.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

Default tunnel-table-pref 11

Parameters *preference* — Specifies the integer value to represent the preference of IS-IS or OSPF SR tunnels in TTM.

Values 1 to 255

Platforms All

tunnel-table-pref

Syntax **tunnel-table-pref** *preference*
no tunnel-table-pref

Context **[Tree]** (config>router>ospf>segm-rtng tunnel-table-pref)
[Tree] (config>router>ospf3>segm-rtng tunnel-table-pref)

Full Context configure router ospf segment-routing tunnel-table-pref
configure router ospf3 segment-routing tunnel-table-pref

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the TTM preference of shortest path SR tunnels created by the IGP instance. This is used for BGP shortcuts, VPRN auto-bind, or BGP transport tunnel when the tunnel binding commands are configured to the **any** value, which parses the TTM for tunnels in the protocol preference order. The user can choose to either accept the global TTM preference or explicitly list the tunnel types they want to use. If the user lists the tunnel types explicitly, the TTM preference is still used to select one type over the other. In both cases, a fallback to the next preferred tunnel type is performed if the selected type fails. A reversion to a more preferred tunnel type is performed as soon as one is available.

The segment routing module adds to the TTM an SR tunnel entry for each resolved remote node SID prefix and programs the data path having the corresponding LTN with the push operation pointing to the primary and LFA backup NHLFEs.

The default preference for shortest path SR tunnels in the TTM is set lower than LDP tunnels but higher than BGP tunnels to allow controlled migration of customers without disrupting their current deployment when they enable segment routing. The following is the value of the default preference for the various tunnel types. This includes the preference of SR tunnels based on shortest path (referred to as SR-ISIS and SR-OSPF).

Note: The preference of an SR-TE LSP is not configurable and is the second most preferred tunnel type after RSVP-TE. The preference is the same whether if the SR-TE LSP was resolved in IS-IS or OSPF.

The global default TTM preference for the tunnel types is as follows:

- ROUTE_PREF_RSVP 7
- ROUTE_PREF_SR_TE 8
- ROUTE_PREF_LDP 9
- ROUTE_PREF_OSPF_TTM 10
- ROUTE_PREF_ISIS_TTM 11
- ROUTE_PREF_BGP_TTM 12
- ROUTE_PREF_GRE 255

The default value for SR-ISIS or SR-OSPF is the same regardless if one or more IS-IS or OSPF instances programmed a tunnel for the same prefix. The selection of a SR tunnel in this case will be based on the lowest IGP instance ID. Similarly, IPv6 SR-ISIS and SR-OSPF3 tunnels are programmed into TTMv6 with the same default preference value as IPv4 SR-ISIS and IPv4 SR-OSPF respectively.

It is recommended to not set two or more tunnel types to the same preference value. In such a situation, the tunnel table prefers the tunnel type which was first introduced in SR OS implementation historically.

Default tunnel-table-pref 10

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *preference* — Specifies the integer value to represent the preference of IS-IS, OSPF, or OSPF3 SR tunnels in the TTM.

Values 1 to 255

Platforms All

24.233 tunnel-template

tunnel-template

Syntax **tunnel-template** *tunnel-template-id*
no tunnel-template

Context **[Tree]** (config>ipsec>client-db>client tunnel-template)

Full Context configure ipsec client-db client tunnel-template

Description This command specifies the tunnel template to be used for tunnel setup.

The **no** form of this command reverts to the default.

Default no tunnel-template

Parameters *tunnel-template-id* — Specifies the identifier of the tunnel template.

Values 1 to 2048

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

tunnel-template

Syntax **tunnel-template** *ipsec-template-identifier* [**create**]
no tunnel-template *ipsec-template-identifier*

Context **[Tree]** (config>ipsec tunnel-template)

Full Context configure ipsec tunnel-template

Description This command creates a tunnel template. Up to 2000 templates are allowed.

Parameters *ipsec-template-identifier* — Specifies the template identifier.

Values 1 to 2048

create — Mandatory keyword used when creating a tunnel-template in the IPsec context. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.234 tunnel-termination

tunnel-termination

Syntax **tunnel-termination** {*ip-address* | *ipv6-address*} **fpe** *fpe-id* [**create**]
no tunnel-termination {*ip-address* | *ipv6-address*}

Context **[Tree]** (config>service>vprn>vxlan tunnel-termination)

Full Context configure service vprn vxlan tunnel-termination

Description This command instructs the system to redirect traffic to the corresponding PXC interface associated with the configured FPE when the destination IP address matches the configured tunnel termination IP address. Because the IP address is registered, the system can respond to ICMP packets directed to it.

The **no** form of this command removes the non-system IP address as the tunnel termination IP address.

Parameters *ip-address* | *ipv6-address* — Specifies the non-system IPv4 or IPv6 address that terminates the VXLAN.

Values ip-address: a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
where:
x: [0 to FFFF]H
d: [0 to 255]D

fpe-id — Specifies the FPE identifier associated with the PXC port or LAG that processes and terminates the VXLAN.

Values 1 to 64

create — Mandatory keyword to create the FPE.

Platforms All

tunnel-termination

Syntax **tunnel-termination** *ip-address* **fpe** *fpe-id* [**create]**
no tunnel-termination *ip-address*

Context **[Tree]** (config>service>system>vxlan tunnel-termination)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service system vxlan tunnel-termination

Description This command instructs the system to redirect traffic to the corresponding PXC interface associated with the configured Forwarding Path Extension (FPE) when the destination IP address matches the configured tunnel-termination IP address. The IP address is also registered, which enables the system to respond to ICMP packets directed to it.

Parameters *ip-address* — Specifies the non-system IPv4 or IPv6 address that terminates the VXLAN.

fpe-id — Specifies the FPE identifier associated with the PXC port or LAG that processes and terminates the VXLAN.

Values 1 to 64

create — Creates the FPE.

Platforms All

tunnel-termination

Syntax **tunnel-termination** [*ip-address* | *ipv6-address*] **fpe** *fpe-id* [**create**]
no tunnel-termination [*ip-address* | *ipv6-address*]

Context **[Tree]** (config>service>system>gre-eth-bridged tunnel-termination)

Full Context configure service system gre-eth-bridged tunnel-termination

Description This command configures an end-point IP address for a GRE tunnel carrying Ethernet payload that is to be terminated on a PW SAP. It also associates this IP address with the FPE object that is providing cross-connect logic between the tunnel and the PW port. This IP address fully supports ICMP protocols such as PING, traceroute, and others.

Parameters *ip-address* — The tunnel end-point IP address in the SR OS node.

ipv6-address — The tunnel end-point IPv6 address in the SR OS node.

fpe *id* — The FPE ID that is providing cross-connect service between the GRE tunnel and the PW port.

Values 1 to 64

Platforms All

24.235 tunnel-type

tunnel-type

Syntax **tunnel-type** {**gre** | **l2tp** | **l2** | **vxlan** | **not-specified**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no tunnel-type

Context [Tree] (config>subscr-mgmt>wlan-gw>ue-query tunnel-type)

Full Context configure subscriber-mgmt wlan-gw ue-query tunnel-type

Description This command enables matching on UEs that are active on a tunnel of the specified type. The **not-specified** value disables matching on the tunnel type.

The **no** form of this command reverts to the default.

Default tunnel-type not-specified

Parameters **gre** — Specifies that the tunnel is of type GRE.

l2tp — Specifies that the tunnel is of type L2TPv3.

l2 — Specifies that the UE is connected over a Layer 2 access point.

vxlan — Specifies that the tunnel is of type VXLAN.

not-specified — Specifies that no tunnel type matches on UEs.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

24.236 tunneling

tunneling

Syntax [**no**] **tunneling**

Context [Tree] (config>port>ethernet>efm-oam tunneling)

Full Context configure port ethernet efm-oam tunneling

Description This command enables EFM OAM PDU tunneling. Enabling tunneling will allow a port mode Epipe SAP to pass OAM frames through the pipe to the far end.

The **no** form of this command disables tunneling.

Default no tunneling

Platforms All

tunneling

Syntax [**no**] **tunneling**

Context [Tree] (config>port>ethernet>dot1x tunneling)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure port ethernet dot1x tunneling

Description This command enables the tunneling of untagged 802.1x frames received on a port and is supported only when **dot1x port-control** is set to **force-auth**. 802.1x tunneling is applicable to both Epipe and VPLS services using either a null SAP or a default SAP on a dot1q port. When configured, untagged 802.1x frames will be switched into the service with the corresponding supported SAP.

The **no** form of this command disables tunneling of untagged 802.1x frames.

Default no tunneling

Platforms All

tunneling

Syntax [**no**] **tunneling**

Context **[Tree]** (config>router>ldp>targ-session>peer tunneling)
[Tree] (config>router>ldp>targ-session>peer-template tunneling)

Full Context configure router ldp targeted-session peer tunneling
configure router ldp targeted-session peer-template tunneling

Description This command enables LDP over tunnels.

The **no** form of this command disables tunneling.

Default no tunneling

Platforms All

tunneling

Syntax [**no**] **tunneling**

Context **[Tree]** (config>router>ldp>targ-session>auto-tx>ipv4 tunneling)
[Tree] (config>router>ldp>targ-session>auto-rx>ipv4 tunneling)

Full Context configure router ldp targeted-session auto-rx ipv4 tunneling
configure router ldp targeted-session auto-tx ipv4 tunneling

Description This command enables the local system to use the targeted LDP session to send FEC/label bindings that it has advertised to other LDP peers. For LDP rLFA, the source node requires the PQ node's label binding information in order to reach the destination. Therefore, this command must be enabled for the **auto-rx** context. However, because **auto-rx** has lower precedence, **tunneling** must be enabled under the **auto-tx** command, in case **auto-rx** is in a **no shutdown** state on the same system.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the local system from sending FEC/label bindings.

Default no tunneling

Platforms All

24.237 twamp

twamp

Syntax **twamp**

Context **[Tree]** (config>test-oam twamp)

Full Context configure test-oam twamp

Description This command enables TWAMP functionality.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.238 twamp-light

twamp-light

Syntax **twamp-light** [**test-id** *test-id*] [**create**]
no twamp-light

Context **[Tree]** (config>oam-pm>session>ip twamp-light)

Full Context configure oam-pm session ip twamp-light

Description This command assigns an identifier to the TWAMP Light test and creates the individual test.

The **no** form of this command removes the TWAMP Light test function from the OAM-PM session.

Parameters *test-id* — Specifies the value of the 4-byte local test identifier not sent in the TWAMP Light packets.

Values 0 to 2147483647

create — Creates the test.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

twamp-light

Syntax **twamp-light**

Context **[Tree]** (config>router twamp-light)
[Tree] (config>service>vprn twamp-light)
[Tree] (config>test-oam>twamp twamp-light)

Full Context configure router twamp-light
configure service vprn twamp-light
configure test-oam twamp twamp-light

Description Commands in this context configure TWAMP Light parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

twamp-light

Syntax **twamp-light**

Context **[Tree]** (config>test-oam>link-meas>template twamp-light)

Full Context configure test-oam link-measurement measurement-template twamp-light

Description Commands in this context configure TWAMP Light test values.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

twamp-light

Syntax **twamp-light**

Context **[Tree]** (config>router>if>if-attr>delay>dyn twamp-light)

Full Context configure router interface if-attribute delay dynamic twamp-light

Description Commands in this context configure TWAMP Light parameters that are used with the **measurement-template** when assigned to IP interfaces.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

twamp-light

Syntax **twamp-light**

Context **[Tree]** (config>router>if>if-attr>delay>dyn twamp-light)

Full Context configure router interface if-attribute delay dynamic twamp-light

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure TWAMP Light parameters that are used with the **measurement-template** when assigned to IP interfaces.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.239 two-way-delay-test

two-way-delay-test

Syntax **two-way-delay-test** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*]

Context **[Tree]** (oam>eth-cfm two-way-delay-test)

Full Context oam eth-cfm two-way-delay-test

Description This command issues an ETH-CFM two-way delay test.

Parameters *mac-address* — Specifies a unicast destination MAC address.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

remote-mepid *mep-id* — Specifies the remote MEP ID of the peer within the association. The domain and association information are derived from the **source mep** for the session. The Layer 2 IEEE MAC address is resolved from previously-learned remote MAC addressing, derived from the reception and processing of the ETH-CC PDU. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

priority — Specifies the priority.

Values 0 to 7

Default 7

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.240 two-way-slm-test

two-way-slm-test

Syntax **two-way-slm-test** {*mac-address* | **remote-mepid** *mep-id*} **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**send-count** *send-count*] [**size** *data-size*] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam>eth-cfm two-way-slm-test)

Full Context oam eth-cfm two-way-slm-test

Description This command configures an Ethernet CFM two-way SLM test in SAA.

Parameters *mac-address* — Specifies a unicast destination MAC address in the format xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

remote-mepid *mep-id* — Specifies the remote MEP ID of the peer within the association. The domain and association information are derived from the **source mep** for the session. The Layer 2 IEEE MAC address is resolved from previously-learned remote MAC addressing, derived from the reception and processing of the ETH-CC PDU. The local MEP must be administratively enabled.

Values 1 to 8191

mep *mep-id* — Specifies the local MEP ID.

Values 1 to 8191

md-index — Specifies the MD index.

Values 1 to 4294967295

ma-index — Specifies the MA index.

Values 1 to 4294967295

priority — Specifies the priority.

Values 0 to 7

Default 7

send-count — Specifies the number of messages to send, expressed as a decimal integer. The count parameter is used to override the default number of message requests sent. The message interval value must be expired before the next message request is sent.

Values 1 to 1000

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

data-size — Specifies the size of the data portion of the data TLV. If 0 is specified, no data TLV is added to the packet.

Values 0 to 1500

Default 0

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of message time out, the requesting router assumes that the message response is not received. Any response received after the request times out is silently discarded. The *timeout* value must be less than the interval.

Values 1 to 10

Default 5

interval — Specifies the **interval** parameter in seconds, expressed as a decimal integer. This parameter is used to configure the spacing between probes within a test run.

Values 0.1 to 0.9, 1 to 10

Default 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.241 tx

tx

Syntax **tx**

Context **[Tree]** (config>subscr-mgmt>pfcp-association tx)

Full Context configure subscriber-mgmt pfcp-association tx

Description Commands in this context configure parameters that determine how PFCP messages are sent.

Default tx

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

tx

Syntax **tx auto-generated**
tx bytes *byte-string* [*byte-string*...(up to 64 byte-strings max, 64 bytes max)]
tx string *identifier*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no tx

Context [Tree] (config>port>otu>pm-tti tx)

Full Context configure port otu pm-tti tx

Description This command enables the user to configure the transmit (tx) trail trace identifier (TTI) for path monitoring (PM) in the ODU overhead. This identifier can be a string or a non-printable sequence of bytes. The length of the string or sequence of bytes cannot exceed 64 bytes.

The **no** form of this command reverts to the default TTI value.

Default Auto-generated in the format of *nodename:iomnum/mdanum/portnum/dwdmchan*

The auto-generated value has five sections:

- Nodename — The first section is the name of the node.
- iomnum — The second section contains the IOM slot number.
- mdanum — The third section contains the MDA slot number.
- portnum — The fourth section contains the port number.
- dwdmchan — The fifth section contains the DWDM channel number (see the table "DWDM Channel Numbers" in the **channel** command [**config>port>dwdm channel**, **config>port>dwdm>coherent channel**, **config>port>dwdm>tdcm channel**]).

Parameters **auto-generated** — Specifies to use the system generated (default) TTI.

identifier — Sets the PM TTI to the string provided by the user. If the string is less than 64 bytes, the remaining bytes will be set to 0.

byte-string — Sets the PM TTI to the sequence of bytes provided by the user. If the user provides less than 64 bytes, the remaining bytes will be set to 0. A 1 byte sequence of 0xFF will set the default strings. Up to 64 byte strings can be specified in a single statement.

Values 0 to FF, in hexadecimal byte notation

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx

Syntax **tx** *byte*
tx auto

Context [Tree] (config>port>otu>psi-payload tx)

Full Context configure port otu psi-payload tx

Description This command allows the user to configure the transmit payload type value in byte 0 of the payload structure identifier (PSI) of the OPU overhead.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default 3 for 10GE-LAN/WAN or OC192 with OTU encapsulation; 5 for GFP framed 10GE-LAN with OTU encapsulation.

Parameters **auto** — Transmits the standard value in the payload type field.

byte — Specifies the transmit payload type value in bytes.

Values [00 to FF] Hexadecimal notation

Default 00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx

Syntax **tx auto-generated**
tx bytes *byte-string* [*byte-string*)]
tx string *identifier*
no tx

Context **[Tree]** (config>port>otu>sm-tti tx)

Full Context configure port otu sm-tti tx

Description This command allows the user to configure the transmit (tx) trail trace identifier (TTI) for section monitoring (SM) in the OTU overhead. This identifier can be a string or a non-printable sequence of bytes. The length of the string or sequence of bytes cannot exceed 64 bytes.

The **no** form of this command reverts to the default TTI value.

Default Auto-generated in the format of *nodename:iomnum/mdanum/portnum/dwdmchan*

The auto-generated value has five sections:

- Nodename — The first section is the name of the node.
- iomnum — The second section contains the IOM slot number.
- mdanum — The third section contains the MDA slot number.
- portnum — The fourth section contains the port number.
- dwdmchan — The fifth section contains the DWDM channel number (see the table “DWDM Channel Numbers” in the **channel** command [**config>port>dwdm channel**, **config>port>dwdm>coherent channel**, **config>port>dwdm>tdcm channel**]).

Parameters **auto-generated** — Specifies to use the system generated (default) TTI.

identifier — Sets the SM TTI to the string provided by the user. If the string is less than 64 bytes, the remaining bytes will be set to 0. Up to 64 byte strings can be specified in a single statement.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

byte-string — Sets the SM TTI to the sequence of bytes provided by the user. If the user provides less than 64 bytes, the remaining bytes will be set to 0. A 1 byte sequence of 0xFF will set the default strings.

Values 0 to FF, in hexadecimal byte notation

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx

Syntax **tx** {**string** *identifier* | **bytes** *byte-sequence* | **auto-generated**}

Context **[Tree]** (config>port>otu>psi-trace tx)

Full Context configure port otu psi-trace tx

Description This command allows the user to configure the transmit trace in bytes 1 to 255 (skipping byte 0) of the payload structure identifier (PSI) of the OPU overhead. This identifier can be a string or a non-printable sequence of bytes. The length of the string or sequence of bytes cannot exceed 255 bytes.

Default Blank (all zeros)

Parameters **auto-generated** — Sets the default PSI trace.

identifier — Sets the PSI trace to the string provided by the user. If the string is less than 255 bytes, the remaining bytes will be set to 0.

byte-sequence — [byte1 byte2 to byte64] Sets the PSI trace to the sequence of bytes provided by the user. If the user provides less than 64 bytes, the remaining bytes will be set to 0. A 1 byte sequence of 0xFF will set the default strings.

Values 0 to FF, in hexadecimal byte notation

24.242 tx-credit-max

tx-credit-max

Syntax **tx-credit-max** *count*
no tx-credit-max

Context **[Tree]** (config>system>lldp tx-credit-max)

Full Context configure system lldp tx-credit-max

Description This command configures the maximum consecutive LLDPDUs transmitted.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no tx-credit-max

Parameters *count* — Specifies the maximum consecutive LLDPDUs transmitted.

Values 1 to 100

Default 5

Platforms All

24.243 tx-dus

tx-dus

Syntax [**no**] **tx-dus**

Context **[Tree]** (config>port>ethernet>ssm tx-dus)
[Tree] (config>port>sonet-sdh tx-dus)

Full Context configure port ethernet ssm tx-dus
configure port sonet-sdh tx-dus

Description This command forces the QL value transmitted from the SSM channel of the SONET/SDH port or the Synchronous Ethernet port to be set to QL-DUS/QL-DNU. This capability is provided to block the use of the interface from the SR/ESS for timing purposes.

This command is supported on TDM satellite.

Default no tx-dus

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh tx-dus

All

- configure port ethernet ssm tx-dus

24.244 tx-eth-ed

tx-eth-ed

Syntax [**no**] **tx-eth-ed**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>eth-ring>path>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>lag>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>port>ethernet>eth-cfm>mep>grace>eth-ed tx-eth-ed)

Full Context configure eth-ring path eth-cfm mep grace eth-ed tx-eth-ed
configure eth-tunnel path eth-cfm mep grace eth-ed tx-eth-ed
configure lag eth-cfm mep grace eth-ed tx-eth-ed
configure port ethernet eth-cfm mep grace eth-ed tx-eth-ed

Description This command enables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP when a system soft reset notification is received for one or more cards.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP.

Default no tx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx-eth-ed

Syntax [**no**] **tx-eth-ed**

Context [Tree] (config>service>epipe>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)

Full Context configure service epipe sap eth-cfm mep grace eth-ed tx-eth-ed
configure service epipe spoke-sdp eth-cfm mep grace eth-ed tx-eth-ed
configure service ipipe sap eth-cfm mep grace eth-ed tx-eth-ed

Description This command enables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP when a system soft reset notification is received for one or more cards.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP.

Default no tx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tx-eth-ed

Syntax [**no**] **tx-eth-ed**

Context **[Tree]** (config>service>vpls>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)

Full Context configure service vpls eth-cfm mep grace eth-ed tx-eth-ed
configure service vpls mesh-sdp eth-cfm mep grace eth-ed tx-eth-ed
configure service vpls sap eth-cfm mep grace eth-ed tx-eth-ed
configure service vpls spoke-sdp eth-cfm mep grace eth-ed tx-eth-ed

Description This command enables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP when a system soft reset notification is received for one or more cards.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP.

Default no tx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx-eth-ed

Syntax [**no**] **tx-eth-ed**

Context **[Tree]** (config>service>ies>if>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)

Full Context configure service ies interface sap eth-cfm mep grace eth-ed tx-eth-ed
configure service ies interface spoke-sdp eth-cfm mep grace eth-ed tx-eth-ed
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed tx-eth-ed

Description This command enables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP when a system soft reset notification is received for one or more cards.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP.

Default no tx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-ed tx-eth-ed

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface spoke-sdp eth-cfm mep grace eth-ed tx-eth-ed
- configure service ies interface sap eth-cfm mep grace eth-ed tx-eth-ed

tx-eth-ed

Syntax [**no**] **tx-eth-ed**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace>eth-ed tx-eth-ed)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-ed tx-eth-ed)

Full Context configure service vprn interface sap eth-cfm mep grace eth-ed tx-eth-ed
configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed tx-eth-ed
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed tx-eth-ed

Description This command enables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP when a system soft reset notification is received for one or more cards.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP.

Default no tx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-ed tx-eth-ed

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm mep grace eth-ed tx-eth-ed
- configure service vprn interface spoke-sdp eth-cfm mep grace eth-ed tx-eth-ed

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tx-eth-ed

Syntax [**no**] **tx-eth-ed**

Context **[Tree]** (config>router>if>eth-cfm>mep>grace>eth-ed tx-eth-ed)

Full Context configure router interface eth-cfm mep grace eth-ed tx-eth-ed

Description This command enables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP when a system soft reset notification is received for one or more cards.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the ITU-T Y.1731 ETH-ED PDU from the MEP.

Default no tx-eth-ed

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.245 tx-eth-vsm-grace

tx-eth-vsm-grace

Syntax [**no**] **tx-eth-vsm-grace**

Context **[Tree]** (config>eth-ring>path>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>eth-tunnel>path>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>lag>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>port>ethernet>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

Full Context configure eth-ring path eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure eth-tunnel path eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure lag eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure port ethernet eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

Description This command enables the transmission of the Nokia ETH-CFM Grace PDU from the MEP when a system soft reset notification is received for one or more cards.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the Nokia ETH-CFM Grace PDU from the MEP.

Default tx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx-eth-vsm-grace

Syntax [**no**] **tx-eth-vsm-grace**

Context **[Tree]** (config>service>epipe>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>epipe>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>ipipe>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

Full Context configure service epipe sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service epipe spoke-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service ipipe sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

Description This command enables the transmission of the Nokia ETH-CFM Grace PDU from the MEP when a system soft reset notification is received for one or more cards.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the Nokia ETH-CFM Grace PDU from the MEP.

Default tx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx-eth-vsm-grace

Syntax [**no**] **tx-eth-vsm-grace**

Context **[Tree]** (config>service>vpls>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>mesh-sdp>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>vpls>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>vpls>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

Full Context
configure service vpls eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service vpls mesh-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service vpls sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service vpls spoke-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

Description
This command enables the transmission of the Nokia ETH-CFM Grace PDU from the MEP when a system soft reset notification is received for one or more cards.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the Nokia ETH-CFM Grace PDU from the MEP.

Default
tx-eth-vsm-grace

Platforms
7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

tx-eth-vsm-grace

Syntax
[**no**] **tx-eth-vsm-grace**

Context
[Tree] (config>service>ies>if>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>ies>if>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>ies>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

Full Context
configure service ies interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service ies interface spoke-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

Description
This command enables the transmission of the Nokia ETH-CFM Grace PDU from the MEP when a system soft reset notification is received for one or more cards.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the Nokia ETH-CFM Grace PDU from the MEP.

Default tx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service ies subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service ies interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
- configure service ies interface spoke-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

tx-eth-vsm-grace

Syntax [**no**] **tx-eth-vsm-grace**

Context **[Tree]** (config>service>vprn>if>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>vprn>if>spoke-sdp>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)
[Tree] (config>service>vprn>sub-if>grp-if>sap>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

Full Context configure service vprn interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service vprn interface spoke-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

Description This command enables the transmission of the Nokia ETH-CFM Grace PDU from the MEP when a system soft reset notification is received for one or more cards.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the Nokia ETH-CFM Grace PDU from the MEP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default tx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure service vprn subscriber-interface group-interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure service vprn interface sap eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace
- configure service vprn interface spoke-sdp eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

tx-eth-vsm-grace

Syntax [**no**] **tx-eth-vsm-grace**

Context **[Tree]** (config>router>if>eth-cfm>mep>grace>eth-vsm-grace tx-eth-vsm-grace)

Full Context configure router interface eth-cfm mep grace eth-vsm-grace tx-eth-vsm-grace

Description This command enables the transmission of the Nokia ETH-CFM Grace PDU from the MEP when a system soft reset notification is received for one or more cards.

The Nokia Grace function is a vendor-specific PDU that informs MEP peers that the local node may be entering a period of expected defect.

The **config**>**eth-cfm**>**system**>**grace-tx-enable** command must be configured to instruct the system that the node is capable of transmitting expected defect windows to the peers. Only one form of ETH-CFM grace (Nokia ETH-CFM Grace or ITU-T Y.1731 ETH-ED) may be transmitted.

The **no** form of this command disables the transmission of the Nokia ETH-CFM Grace PDU from the MEP.

Default tx-eth-vsm-grace

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.246 tx-hold-multiplier

tx-hold-multiplier

Syntax **tx-hold-multiplier** *multiplier*
no tx-hold-multiplier

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>system>lldp tx-hold-multiplier)

Full Context configure system lldp tx-hold-multiplier

Description This command configures the multiplier of the tx-interval.

The **no** form of this command reverts to the default value.

Default no tx-hold-multiplier

Parameters *multiplier* — Specifies the multiplier of the tx-interval.

Values 2 to 10

Default 4

Platforms All

24.247 tx-interval

tx-interval

Syntax **tx-interval** *interval*
no tx-interval

Context [Tree] (config>system>lldp tx-interval)

Full Context configure system lldp tx-interval

Description This command configures the LLDP transmit interval time.

The **no** form of this command reverts to the default value.

Default no tx-interval

Parameters *interval* — Specifies the LLDP transmit interval time.

Values 5 to 32768

Default 30

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.248 tx-mgmt-address

tx-mgmt-address

Syntax **tx-mgmt-address** [**system**] [**system-ipv6**] [**oob**] [**oob-ipv6**]
no tx-mgmt-address

Context **[Tree]** (config>port>ethernet>lldp>dstmac tx-mgmt-address)

Full Context configure port ethernet lldp dest-mac tx-mgmt-address

Description This command specifies which management address to transmit. The operator can choose to send the system IPv4 address, the system IPv6 address, the out-of-band IPv4 address, the out-of-band IPv6 address, or any combination of these. The system address is sent only once. The address must be configured for the specific version of the protocol in order to send the management address.

The **no** form of the command resets value to the default.

Default no tx-mgmt-address

Parameters **system** — Specifies to use the system IP address. The system address will only be transmitted once it has been configured if this parameter is specified.

system-ipv6 — Specifies to use the system IPv6 address. The system address will only be transmitted once it has been configured if this parameter is specified.

oob — Specifies to use the out-of-band IPv4 address for active CPM.

oob-ipv6 — Specifies to use the out-of-band IPv6 address for active CPM.

Platforms All

24.249 tx-timer

tx-timer

Syntax **tx-timer** *seconds*
no tx-timer

Context **[Tree]** (config>subscr-mgmt>diameter-application-policy tx-timer)

Full Context configure subscriber-mgmt diameter-application-policy tx-timer

Description This command defines the time-out period for the application’s request messages (CCR-I/U/T).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **on-failure** configuration determines the action that taken once the message times out.

The **no** form of this command reverts to the default value.

Default tx-timer 10

Parameters *seconds* — Specifies the Tx Timer value (in seconds) for this policy.

Values 10 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

24.250 tx-tlvs

tx-tlvs

Syntax **tx-tlvs** [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**]
no tx-tlvs

Context **[Tree]** (config>port>ethernet>lldp>dstmac tx-tlvs)

Full Context configure port ethernet lldp dest-mac tx-tlvs

Description This command specifies which LLDP TLVs to transmit. The TX TLVs, defined as a bitmap, includes the basic set of LLDP TLVs whose transmission is allowed on the local LLDP agent by the network management. Each bit in the bitmap corresponds to a TLV type associated with a specific optional TLV. Organizationally-specific TLVs are excluded from this bitmap.

There is no bit reserved for the management address TLV type since transmission of management address TLVs are controlled by another object.

The **no** form of this command resets the value to the default.

Default no tx-tlvs

Parameters **port-desc** — Indicates that the LLDP agent should transmit port description TLVs.

sys-name — Indicates that the LLDP agent should transmit system name TLVs.

sys-desc — Indicates that the LLDP agent should transmit system description TLVs.

sys-cap — Indicates that the LLDP agent should transmit system capabilities TLVs.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

24.251 tx-while-sync-uncertain

tx-while-sync-uncertain

Syntax [**no**] **tx-while-sync-uncertain**

Context **[Tree]** (config>system>ptp tx-while-sync-uncertain)

Full Context configure system ptp tx-while-sync-uncertain

Description This command configures the local PTP clock to transmit Announce messages to downstream clocks, indicating it has not yet stabilized on the recovered synchronization source (upstream clocks or GM clock). While the PTP clock is unsynchronized, the SyncUncertain state is true.

The **no** form of this command prevents the local PTP clock from sending Announce messages to downstream clocks to indicate it is not synchronized to a valid timing source. If the **no** form of this command is used while the clock's SyncUncertain state is true, unicast negotiation grant requests are not granted and current grants are canceled.

Default tx-while-sync-uncertain

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

24.252 type

type

Syntax [**no**] **type** {**internal** | **external**}

Context **[Tree]** (config>subscr-mgmt>bgp-prng-plcy type)

Full Context configure subscriber-mgmt bgp-peering-policy type

Description This command designates the BGP peer as type internal or external.

The type of **internal** indicates the peer is an IBGP peer while the type of **external** indicates that the peer is an EBGP peer.

By default, the OS derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered **internal**. If the local AS is different, then the peer is considered **external**.

The **no** form of this command used at the group level reverts to the default value.

Parameters **internal** — Configures the peer as internal.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

external — Configures the peer as external.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

type

Syntax [**no**] **type**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query type)

Full Context configure subscriber-mgmt wlan-gw tunnel-query type

Description This command enables matching on specific tunnel types. If no tunnel type match criteria is specified, type matching is implicitly disabled.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

type

Syntax **type** [*type*] [**vendor-id** *vendor-id*]
no type

Context **[Tree]** (config>router>radius-proxy>server>attribute-matching type)
[Tree] (config>service>vprn>radius-proxy>server>attribute-matching type)

Full Context configure router radius-proxy server attribute-matching type
configure service vprn radius-proxy server attribute-matching type

Description This command specifies the RADIUS VSA type for the entries to be matched with.

Parameters type — Specifies the RADIUS server policy matching attribute-type.

Values 1 to 255

vendor-id — Specifies the vendor ID number.

Values 1 to 16777215, **nokia**

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

type

Syntax [**no**] **type** {**internal** | **external**}

Context **[Tree]** (config>service>vprn>bgp>group type)
[Tree] (config>service>vprn>bgp>group>neighbor type)

Full Context configure service vprn bgp group neighbor type
configure service vprn bgp group type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command designates the BGP peer as type internal or external.

The type of **internal** indicates the peer is an IBGP peer while the type of external indicates that the peer is an EBGP peer.

By default, the OS derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered **internal**. If the local AS is different, then the peer is considered **external**.

The **no** form of this command used at the group level reverts to the default value.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default no type

Parameters **internal** — Configures the peer as internal.

external — Configures the peer as external.

no type — Type of neighbor is derived on the local AS specified.

Platforms All

type

Syntax **type** [**hub** | **spoke** | **subscriber-split-horizon**]
no type

Context **[Tree]** (config>service>vprn type)

Full Context configure service vprn type

Description This command designates the type of VPRN instance being configured for hub and spoke topologies. Use the **no** form to reset to the default of a fully meshed VPRN.

Default no type

Parameters **hub** — Specifies a hub VPRN which allows all traffic from the hub SAPs to be routed to the destination directly, while all traffic from spoke VPRNs or network interfaces can only be routed to a hub SAP.

spoke — Specifies a spoke VPRN which allows traffic from associated SAPs or spoke terminations to only be forwarded through routes learned from separate VPRN, which should be configured as a type Hub VPRN.

subscriber-split-horizon — Controls the flow of traffic for wholesale subscriber applications.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type

Syntax **type** [**head-end** | **tail-end**]

Context **[Tree]** (config>gmpls-tun-grp type)

Full Context configure gmpls-tun-grp type

Description This command configures whether a GMPLS tunnel group is at the head-end or tail-end of the set of member GMPLS LSPs from the perspective of GMPLS LSP setup. It can only configured if the GMPLS tunnel group has no members; for example, if none have yet been configured.

Default type head-end

Parameters **head-end** — Sets the GMPLS tunnel group to operate as a head-end.

tail-end — Sets the GMPLS tunnel group to operate as a tail-end.

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

type

Syntax [**no**] **type**

Context **[Tree]** (config>saa>test type)

Full Context configure saa test type

Description This command creates the context to provide the test type for the named test. Only a single test type can be configured.

A test can only be modified while the test is in shut down mode.

Once a test type has been configured, the command can be modified by re-entering the command. However, the test type must be the same as the previously entered test type.

To change the test type, the old command must be removed using the **config>saa>test>no type** command.

The **no** form of this command removes the test type parameters from the configuration.

Platforms All

type

Syntax **type** *filter-type*
no type

Context **[Tree]** (config>qos>sap-ingress>ip-criteria type)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>qos>sap-ingress>ipv6-criteria type)

Full Context configure qos sap-ingress ip-criteria type
configure qos sap-ingress ipv6-criteria type

Description This command sets the **ip-criteria** and **ipv6-criteria** type to control the type of match entries configurable in this context.

Default type normal

Parameters *filter-type* — Specifies which type of entries that the **ip-criteria** and **ipv6-criteria** statements can contain.

Values **normal** — Regular match criteria are allowed; VXLAN VNI matching is not allowed.

tagged-entries — Specifies that entries within that criteria statement are tagged. Tagged entries are not populated by default, they are only populated when their tag value is activated using the criteria override under an Ethernet SAP.

The **type** can only be changed from **normal** to **tagged-entries** if there are no **ip-criteria** or **ipv6-criteria** entries configured and the SAP ingress QoS policy is not applied to any object.

A SAP ingress QoS policy configured with a criteria statement with **type tagged-entries** is not supported within an SLA profile, sub profile or MSAP policy, or under an IES/VPRN group interface SAP.

The configuration of **type tagged-entries** is mutually exclusive with the configuration of the **match dst-port** in the same criteria statement.

vxlan-vni — Matching is allowed on a VXLAN VNI for VXLAN and VXLAN GPE frames.

The type cannot be changed when **ip-criteria** or **ipv6-criteria** entries are configured. If there are no **ip-criteria** or **ipv6-criteria** entries configured, the type can be changed from **vxlan-vni** to **normal**. The type can only be changed from **normal** to **vxlan-vni** if there are no **ip-criteria** or **ipv6-criteria** entries configured but it is necessary that the SAP ingress QoS policy is also not applied to any object in order to change from **normal** to **vxlan-vni**.

A SAP ingress QoS policy configured with **type vxlan-vni** can be applied to any Ethernet SAPs, except for a PW-SAP, B-VPLS SAP, or CCAG SAP, in any applicable service.

Platforms All

type

Syntax **type** *filter-type*
no type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>qos>sap-ingress>mac-criteria type)

Full Context configure qos sap-ingress mac-criteria type

Description This command sets the mac-criteria type.

Default type normal

Parameters *filter-type* — Specifies which type of entries this MAC filter can contain.

Values **normal** — Regular match criteria are allowed; ISID match not allowed.

vid — Configures the VID filter type used to match on ethernet_II frame types. This allows matching VLAN tags for explicit filtering.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

type

Syntax **type** *redirect-list-type*
no type

Context [Tree] (config>qos>queue-group-redirect-list type)

Full Context configure qos queue-group-redirect-list type

Description This command configures the type of a queue group redirect list. The default value is **vxlan-vni**, which is the only possible value.

Parameters *redirect-list-type* — Specifies the type of the queue group redirect list. The queue group redirect list is used to match VXLAN VNIs in IPv4 and IPv6 VXLAN or VXLAN GPE packets.

Values vxlan-vni

Platforms All

type

Syntax **type** {**normal** | **src-mac** | **packet-length**| **destination-class**}

Context [Tree] (config>filter>ip-filter type)
[Tree] (config>filter>ipv6-filter type)

Full Context configure filter ip-filter type
configure filter ipv6-filter type

Description This command configures the filter policy type. The policy type defines the list of match criteria supported in a filter policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default type normal

Parameters **normal** — Specifies the default filter policy type.

src-mac — Specifies the source MAC filter policy type to match on source MAC addresses in VPLS services.

packet-length — Specifies the packet-length filter policy type to match on the total packet length.

destination-class — Specifies the destination-class filter policy. This filter policy type is supported on egress networks, IES, VPRN, and R-VPLS interfaces.

Platforms All

type

Syntax **type** *filter-type*

Context **[Tree]** (config>filter>mac-filter type)

Full Context configure filter mac-filter type

Description This command configures the MAC Filter Policy type as being either normal, ISID or VID.

Default type normal

Parameters *filter-type* — Specifies which type of entry this MAC filter can contain.

Values **normal** — regular match criteria are allowed; ISID or VID filter match criteria not allowed

isid — only ISID match criteria are allowed

vid — only VID match criteria are allowed on ethernet_II frame types

Platforms All

type

Syntax **type** {**cpm-np**}
no type

Context **[Tree]** (config>router>bfd>bfd-template type)

Full Context configure router bfd bfd-template type

Description This command selects the CPM network processor as the local termination point for the BFD session. This is enabled by default.

The **no** form of this command reverts to the default behavior.

Default no type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

type

Syntax **type** *file-url* [**no-redirect**] [**client-tls-profile** *profile*] [**proxy** *proxy-url*]

Context **[Tree]** (file type)

Full Context file type

Description This command displays the contents of a text file.

Parameters *file-url* — Specifies the file contents to display.

Values

local-url	[*cflash-id/*][*file-path*] up to 200 characters, including cflash-id directory length up to 99 each
remote-url	[{ftp:// | tftp:// | http:// | https://}*login*:*pswd*@*remote-locn*/][*file-path*] up to 247 characters directory length up to 99 characters each
remote-locn	[hostname | ipv4-address | [ipv6-address]]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D interface - up to 32 characters, for link local addresses 255
cflash-id	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

profile — Specifies the TLS client profile configured under **config**>**system**>**security**>**tls**>**client-tls-profile** to use.

proxy-url — Specifies the URL of an HTTP proxy. For example, http://proxy.mydomain.com:8000. This URL must be an HTTP URL and not an HTTPS URL.

no-redirect — Specifies to automatically refuse any HTTP redirects without prompting the user.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type

Syntax **type** *schedule-type*

Context **[Tree]** (config>system>cron>sched type)

Full Context configure system cron schedule type

Description This command specifies how the system should interpret the commands contained within the schedule node.

Default type periodic

Parameters *schedule-type* — Specifies the type of schedule for the system to interpret the commands contained within the schedule node.

Values periodic — Specifies a schedule which runs at a given interval. The interval must be specified for this feature to run successfully.

calendar — Specifies a schedule which runs based on a calendar. The month, weekday, day-of-month, and minute parameters must be specified for this feature to run successfully.

oneshot — Specifies a schedule which runs one time only. As soon as the first event specified in these parameters takes place and the associated event occurs, the schedule enters a shutdown state. The month, weekday, day-of-month, and minute parameters must be specified for this feature to run successfully.

Default periodic

Platforms All

type

Syntax **type** *indicator-type*

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment>progress-indicator type)

Full Context configure system management-interface cli md-cli environment progress-indicator type

Description This command specifies the type of progress indicator used in the MD-CLI.

Default type dots

Parameters *indicator-type* — Specifies the progress indicator type.

Values **dots**: displays the progress indicator as dynamically changing dots

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

type

Syntax **type all**
type [**gnmi-capabilities**] [**gnmi-get**] [**gnmi-set**] [**gnmi-subscribe**] [**gnoi-cert-mgmt-rpcs**]
no type

Context **[Tree]** (debug>system>grpc type)

Full Context debug system grpc type

Description This command enables debugging for all RPCs or a particular RPC.

The **no** form of this command deactivates debugging for all RPCs.

Parameters **all** — Specifies that debugging is enabled for all RPCs.

gnmi-capabilities — Specifies that debugging is enabled for gNMI capability RPC.

gnmi-get — Specifies that debugging is enabled for gNMI get RPC.

gnmi-set — Specifies that debugging is enabled for gNMI set RPC.

gnmi-subscribe — Specifies that debugging is enabled for gNMI subscribe RPC.

gnoi-cert-mgmt-rpcs — Specifies that debugging is enabled for gNOI certificate management RPCs.

Platforms All

type

Syntax [**no**] **type** {**internal** | **external**}

Context **[Tree]** (config>router>bgp>group type)
[Tree] (config>router>bgp>group>neighbor type)

Full Context configure router bgp group neighbor type
configure router bgp group type

Description **This command designates t**he BGP peer as type internal or external.

The type of **internal** indicates the peer is an IBGP peer while the type of external indicates that the peer is an EBGP peer.

By default, the router derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered **internal**. If the local AS is different, then the peer is considered **external**.

The **no** form of this command used at the group level reverts to the default value.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no type

Parameters **internal** — Configures the peer as internal.

external — Configures the peer as external.

Platforms All

type

Syntax **type** {**1** | **2**}
no type

Context **[Tree]** (config>router>policy-options>policy-statement>entry>from type)

Full Context configure router policy-options policy-statement entry from type

Description This command configures an OSPF type metric as a match criterion in the route policy statement entry.

If no type is specified, any OSPF type is considered a match.

The **no** form of this command removes the OSPF type match criterion.

Default no type

Parameters **1** — Matches OSPF routes with type 1 LSAs.

2 — Matches OSPF routes with type 2 LSAs.

Platforms All

type

Syntax **type** {*type* | *param-name*}
no type

Context **[Tree]** (config>router>policy-options>policy-statement>default-action type)
[Tree] (config>router>policy-options>policy-statement>entry>action type)

Full Context configure router policy-options policy-statement default-action type
configure router policy-options policy-statement entry action type

Description This command sets the subtype for the Type 5 LSA (external LSA).

The **no** form of this command disables assigning a type in the route policy entry.

Default type 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *type* — Specifies the type metric.

Values Subtype 1 — The external metric in the external LSA is comparable with the internal metric, and thus one can sum up all the metrics along the path (both internal and external) to get the total cost to the destination.

Subtype 2 — The metric in the external LSA is much more important than the internal metric, so the internal metrics should only be considered when comparing two external routes that have the same external metric.

param-name — The type parameter variable name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Policy parameters must start and end with at-signs (@); for example, “@variable@”.

Platforms All

24.253 type-multi-line

type-multi-line

Syntax [**no**] **type-multi-line**

Context **[Tree]** (config>saa>test type-multi-line)

Full Context configure saa test type-multi-line

Description This command creates the context to configure the OAM probe type and its parameters in a flexible multi-line format.

The **no** form of this command removes the context.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25 u Commands

25.1 udp

udp

Syntax [**no**] **udp**

Context **[Tree]** (config>service>epipe>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter udp)
[Tree] (config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter udp)
[Tree] (config>service>vprn>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter udp)
[Tree] (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel>resolution-filter udp)

Full Context configure service epipe bgp-evpn mpls auto-bind-tunnel resolution-filter udp
configure service vpls bgp-evpn mpls auto-bind-tunnel resolution-filter udp
configure service vprn bgp-evpn mpls auto-bind-tunnel resolution-filter udp
configure service vprn bgp-ipvpn mpls auto-bind-tunnel resolution-filter udp

Description This command selects the MPLS-over-UDP tunnel type programmed in TTM.

The **udp** value instructs BGP EVPN to search for a UDP LSP to the address of the BGP next hop.

The **no** form of this command removes the selected MPLS-over-UDP tunnel type.

Default no udp

Platforms All

udp

Syntax **udp** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no udp

Context **[Tree]** (config>service>nat>nat-policy>timeouts udp)
[Tree] (config>service>nat>firewall-policy>timeouts udp)
[Tree] (config>service>nat>up-nat-policy>timeouts udp)

Full Context configure service nat firewall-policy timeouts udp
configure service nat nat-policy timeouts udp
configure service nat up-nat-policy timeouts udp

Description This command configures the UDP mapping timeout.

Default udp min 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hours* — Specifies the timeout hours field.

Values 1 to 24

minutes — Specifies the timeout minutes field.

Values 1 to 59

seconds — Specifies the timeout seconds field.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy timeouts udp
- configure service nat nat-policy timeouts udp

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts udp

udp

Syntax **udp src** *udp-port* **dest** *udp-port*
no udp

Context **[Tree]** (config>mirror>mirror-dest>encap>layer-3-encap>gateway udp)

Full Context configure mirror mirror-dest encap layer-3-encap gateway udp

Description This command configures the source UDP port and destination UDP port to use in the UDP header part of the routable LI encapsulation.

Parameters *udp-port* — Specifies source UDP port.

Values 1 to 65535

Platforms All

udp

Syntax **udp**

Context **[Tree]** (config>test-oam>build-packet>header udp)
[Tree] (debug>oam>build-packet>packet>field-override>header udp)

Full Context configure test-oam build-packet header udp
debug oam build-packet packet field-override header udp

Description This command creates a UDP header and enables the context to define the associated parameters.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

udp

Syntax [**no**] **udp**

Context **[Tree]**
(config>router>bgp>next-hop-resolution>labeled-routes>transport-tunnel>family>resolution-filter udp)

Full Context configure router bgp next-hop-resolution labeled-routes transport-tunnel family resolution-filter udp

Description This command selects UDP tunnel in TTM for next-hop resolution.

Platforms All

25.2 udp-dns

udp-dns

Syntax **udp-dns** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no udp-dns

Context **[Tree]** (config>service>nat>nat-policy>timeouts udp-dns)
[Tree] (config>service>nat>firewall-policy>timeouts udp-dns)
[Tree] (config>service>nat>up-nat-policy>timeouts udp-dns)

Full Context configure service nat firewall-policy timeouts udp-dns
configure service nat nat-policy timeouts udp-dns
configure service nat up-nat-policy timeouts udp-dns

Description This command configures the timeout applied to a UDP session with destination port 53.

Default udp-dns sec 15

Parameters *hours* — Specifies the timeout hours field.

Values 1 to 24

minutes — Specifies the timeout minutes field.

Values 1 to 59

seconds — Specifies the timeout seconds field.

Values 1 to 59

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy timeouts udp-dns
- configure service nat nat-policy timeouts udp-dns

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts udp-dns

25.3 udp-dst

udp-dst

Syntax **udp-dst** *udp-port*
no udp-dst

Context **[Tree]** (config>li>mirror-dest-template>layer-3-encap udp-dst)

Full Context configure li mirror-dest-template layer-3-encap udp-dst

Description This command configures the destination UDP port to be used in the UDP header of the routable LI encapsulation.

Parameters *udp-port* — Specifies the destination UDP port.

Values 1 to 65535

Platforms All

25.4 udp-dst-port

udp-dst-port

Syntax **udp-dst-port** *port*
no udp-dst-port

Context **[Tree]** (config>mcast-mgmt>mcast-rprt-dest udp-dst-port)

Full Context configure mcast-management mcast-reporting-dest udp-dst-port

Description This command specifies the UDP destination port of the external node to which IGMP events are exported.

The **no** form of this command reverts to the default.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *port* — Specifies the UDP port to send multicast reports.

Values 1 to 65535

Platforms All

25.5 udp-inbound-refresh

udp-inbound-refresh

Syntax [**no**] **udp-inbound-refresh**

Context **[Tree]** (config>service>nat>nat-policy udp-inbound-refresh)
[Tree] (config>service>nat>firewall-policy udp-inbound-refresh)
[Tree] (config>service>nat>up-nat-policy udp-inbound-refresh)

Full Context configure service nat firewall-policy udp-inbound-refresh
configure service nat nat-policy udp-inbound-refresh
configure service nat up-nat-policy udp-inbound-refresh

Description This command enables UDP session timeout extended on inbound traffic.

The **no** form of the command disables UDP session timeout extended on inbound traffic.

Default no udp-inbound-refresh

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy udp-inbound-refresh
- configure service nat up-nat-policy udp-inbound-refresh

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy udp-inbound-refresh

25.6 udp-initial

udp-initial

Syntax **udp-initial** [**min** *minutes*] [**sec** *seconds*]
no udp-initial

Context **[Tree]** (config>service>nat>nat-policy>timeouts udp-initial)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>nat>firewall-policy>timeouts udp-initial)
[Tree] (config>service>nat>up-nat-policy>timeouts udp-initial)

Full Context configure service nat firewall-policy timeouts udp-initial
configure service nat nat-policy timeouts udp-initial
configure service nat up-nat-policy timeouts udp-initial

Description This command configures the UDP mapping timeout applied to new sessions.

Default udp-initial sec 15

Parameters *minutes* — Specifies the timeout minutes field.

Values 1 to 59

seconds — Specifies the timeout seconds field.

Values 1 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat nat-policy timeouts udp-initial
- configure service nat up-nat-policy timeouts udp-initial

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy timeouts udp-initial

25.7 udp-port

udp-port

Syntax **udp-port** *udp-port-number*

Context [Tree] (config>service>vprn>mtrace2 udp-port)
[Tree] (config>router>mtrace2 udp-port)

Full Context configure router mtrace2 udp-port
configure service vprn mtrace2 udp-port

Description This command specifies the destination and listening port for the **mtrace2** command. When it is configured, this command generates Mtrace2 packets with the configured UDP port, and also listens on the same port for any incoming Mtrace2 packets.

Port 33435 is the IANA-assigned port for Mtrace2. On several operating systems (for example, Linux OS, SR OS), this port is also used by traceroute. On SR OS, if port 33435 is configured as the Mtrace2 port, SR OS does not respond to traceroute on this port.

Default 5000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *udp-port-number* — Specifies the UDP port for the test.

Values 1024 to 49151

Platforms All

25.8 udp-return-object

udp-return-object

Syntax **udp-return-object** *ip-address*
no udp-return-object

Context **[Tree]** (config>oam-pm>session>mpls>lsp>rsvp udp-return-object)
[Tree] (config>oam-pm>session>mpls>lsp>rsvp-auto udp-return-object)

Full Context configure oam-pm session mpls lsp rsvp udp-return-object
configure oam-pm session mpls lsp rsvp-auto udp-return-object

Description This command configures the destination IP address used by the far end of the test to send a test response. The UDP port in the UDP-Return Object is set to 64353 for MPLS DM PDUs.

RSVP tunnels are unidirectional and must include a configured local address for the responder can route the response back by the IP control plane. If the configuration is absent, the DN test fails to activate. If the configured IP address is not a local address, the command fails.

The **no** form of this command removes the udp-return-object IP address.

Parameters *ip-address* — Specifies the destination IP.

Values
ipv4-address -a.b.c.d
ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.9 udp-src

udp-src

Syntax **udp-src** *udp-port*
no udp-src

Context **[Tree]** (config>li>mirror-dest-template>layer-3-encap udp-src)

Full Context configure li mirror-dest-template layer-3-encap udp-src

Description This command configures the source UDP port to be used in the UDP header of the routable LI encapsulation.

Parameters *udp-port* — Specifies the source UDP port.

Values 1 to 65535

Platforms All

25.10 ue

ue

Syntax **ue** *ieee-address* [**profile** *trace-profile-name*]
no ue *ieee-address*

Context **[Tree]** (debug>call-trace>wlan-gw ue)

Full Context debug call-trace wlan-gw ue

Description This command starts tracing the UE with the specified MAC address. The trace is started with default parameters or optionally parameters specified in the trace-profile.

The **no** form of this command stops the trace and make sure no new traces are started.

Parameters *ieee-address* — Displays information about the MAC address of this UE.

trace-profile-name — Specifies the name of a configured trace profile.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.11 ue-creation-type

ue-creation-type

Syntax [**no**] **ue-creation-type**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes ue-creation-type)

Full Context configure aaa isa-radius-policy acct-include-attributes ue-creation-type

Description This command enables including the Alc-Wlan-Ue-Creation-Type.

Default no ue-creation-type

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.12 ue-query

ue-query

Syntax **ue-query** *query-id* [**name** *name*] [**create**]
no ue-query *query-id*

Context **[Tree]** (config>subscr-mgmt>wlan-gw ue-query)

Full Context configure subscriber-mgmt wlan-gw ue-query

Description This command creates a UE query where filter criteria over WLAN-GW ISA UEs are defined. This query can later be used to retrieve state of the UEs matching the configured criteria.

The **no** form of this command removes the query.

Parameters *query-id* — Specifies the ID assigned to a query.

Values 1 to 1024

name — Specifies the name assigned to a query, up to 32 characters.

create — Creates a UE query.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.13 ue-state

ue-state

Syntax [**no**] **ue-state**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query ue-state)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ue-state

Description This command enables matching on a specific UE state. Multiple states can be provisioned. If no UE state specifier is configured, UE state matching is disabled (all UEs match).

This match criteria can be combined with minimum and maximum match criteria, which will then apply only to UEs of the specified state.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.14 uli

uli

Syntax [**no**] **uli**

Context **[Tree]** (config>subscr-mgmt>auth-plcy>include-radius-attribute uli)

Full Context configure subscriber-mgmt authentication-policy include-radius-attribute uli

Description This command enables the inclusion of the User Location Information in AAA protocols as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the attribute.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

uli

Syntax [**no**] **uli**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute uli)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute uli

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command, in case of ESM over GTP access, includes the ULI VSA in accounting. This VSA contains the last VSA as received via GTP. To generate a triggered interim update whenever ULI changes, the **config>subscr-mgmt>acct-plcy>triggered-updates>gtp-mobility** command is used.

The **no** form of this command disables inclusion of the ULI VSA.

Default no uli

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.15 umh-pe

umh-pe

Syntax **umh-pe** *ip-address* **standby** *ip-address*
no umh-pe *ip-address*

Context **[Tree]** (config>service>vprn>mvpn>umh-pe-backup umh-pe)

Full Context configure service vprn mvpn umh-pe-backup umh-pe

Description This command assigns a standby PE to each primary PE that must be selected as an alternative PE in case the UFD session on tunnel from primary PE is detected down. Standby for a PE cannot be modified without shutting down the MVPN instance.

If a primary PE is not assigned a standby PE then the UMH selection would fall back to the default method.

Platforms All

25.16 umh-pe-backup

umh-pe-backup

Syntax **umh-pe-backup**

Context **[Tree]** (config>service>vprn>mvpn umh-pe-backup)

Full Context configure service vprn mvpn umh-pe-backup

Description This command enables context to configure primary and standby upstream PE association for the MVPN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

25.17 umh-rate-monitoring

umh-rate-monitoring

Syntax **umh-rate-monitoring**

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive umh-rate-monitoring)
[Tree] (config>service>vprn>mvpn>pt>selective umh-rate-monitoring)

Full Context configure service vprn mvpn provider-tunnel inclusive umh-rate-monitoring
configure service vprn mvpn provider-tunnel selective umh-rate-monitoring

Description Commands in this context configure bandwidth monitoring for UMH redundancy.

Platforms All

25.18 umh-selection

umh-selection

Syntax **umh-selection** {**highest-ip** | **hash-based** | **tunnel-status** | **unicast-rt-pref**}
no umh-selection

Context **[Tree]** (config>service>vprn>mvpn umh-selection)

Full Context configure service vprn mvpn umh-selection

Description This command specifies which UMH selection mechanism to use, highest IP address, hash based or provider tunnel status.

The **no** form of this command resets it back to default.

Default umh-selection highest-ip

Parameters **highest-ip** — Specifies that the highest next-hop IP address is selected as UMH. The RTM may have just one next-hop to the source, but **highest-ip** uses all of the next-hops available to BGP that appear in the BGP database.

hash-based — Specifies that the UMH selection is based on hash-based procedures set out in RFC6513, section 5.1.3. The RTM may have just one next-hop to the source, but **hash-based** uses all of the next-hops available to BGP that appear in the BGP database.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

tunnel-status — Specifies that UMH selection is based on the state of the tunnel as well as the available unicast routes through the tunnel. Not supported for IPv6.

unicast-rt-pref — When selected, best unicast route will decide which UMH is chosen. All PE routers shall prefer the same route to the UMH for the UMH selection criterion (for example BGP path selection criteria must not influence one PE to choose different UMH from another PE).

Platforms All

25.19 unavailability-event

unavailability-event

Syntax **unavailability-event** {**forward** | **backward** | **aggregate**} **threshold** *raise-threshold* [**clear** *clear-threshold*]
no unavailability-event {**forward** | **backward** | **aggregate**}

Context **[Tree]** (config>oam-pm>session>ethernet>slm>loss-events unavailability-event)
[Tree] (config>oam-pm>session>ethernet>lmm>loss-events unavailability-event)
[Tree] (config>oam-pm>session>ip>twamp-light>loss-events unavailability-event)

Full Context configure oam-pm session ethernet lmm loss-events unavailability-event
configure oam-pm session ethernet slm loss-events unavailability-event
configure oam-pm session ip twamp-light loss-events unavailability-event

Description This command sets the threshold to be applied to the overall count of the unavailability indicators, not transitions, per configured direction. This value is compared to the 32 bit unavailability counter specific to the direction which tracks the number of individual delta-ts that have been recorded as unavailable. The aggregate is a function of summing forward and backward. This value is only used as a threshold mechanism and is not part of the stored statistics. If the optional **clear** *clear-threshold* parameter is not specified, the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and regardless of any previous window. Each unique event can only be raised once within measurement interval. If the optional **clear** *clear-threshold* parameter is specified, the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is carried forward to following measurement intervals. If a threshold crossing event is raised another is raised until a measurement interval completes and the clear threshold has not been exceeded. A clear event is raised under that condition.

The **no** form of this command removes the event threshold for frame loss ratio. The direction must be included with the **no** command.

Default no unavailability-event forward

no unavailability-event backward

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no unavailability-event aggregate

Parameters **forward** — Specifies the threshold is applied to the forward direction count.

backward — Specifies the threshold is applied to the backward direction count.

aggregate — Specifies the threshold is applied to the aggregate count (sum of forward and backward).

raise-threshold — Specifies a numerical value compared to the unavailability counter that is the rising threshold that determines when the event is to be generated, when value reached.

Values 1 to 864000

clear-threshold — Specifies an optional value used for stateful behavior that allows the operator to configure a percentage of loss value lower than the rising percentage to indicate when the clear event should be generated.

Values 0 to 863999

A value of zero means that the unavailability counter must be 0.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events unavailability-event

All

- configure oam-pm session ethernet slm loss-events unavailability-event
- configure oam-pm session ethernet lmm loss-events unavailability-event

25.20 uncoloured-octets-offered-count

uncoloured-octets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters uncoloured-octets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters uncoloured-octets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters uncoloured-octets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters uncoloured-octets-offered-count

Description This command includes the uncoloured octets offered in the count.

The **no** form of this command excludes the uncoloured octets offered in the count.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

uncoloured-octets-offered-count

Syntax [**no**] **uncoloured-octets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters uncoloured-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters uncoloured-octets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters uncoloured-octets-offered-count
configure log accounting-policy custom-record ref-policer e-counters uncoloured-octets-offered-count

Description This command includes the uncoloured octets offered count.

The **no** form of this command excludes the uncoloured octets offered count.

Default no uncoloured-octets-offered-count

Platforms All

uncoloured-octets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters uncoloured-octets-offered-count)
[Tree] (config>log>acct-policy>cr>queue>i-counters uncoloured-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters uncoloured-octets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters uncoloured-octets-offered-count)

Full Context configure log accounting-policy custom-record policer i-counters uncoloured-octets-offered-count
configure log accounting-policy custom-record queue i-counters uncoloured-octets-offered-count
configure log accounting-policy custom-record ref-policer i-counters uncoloured-octets-offered-count
configure log accounting-policy custom-record ref-queue i-counters uncoloured-octets-offered-count

Description This command includes the uncoloured octets offered in the count.

The **no** form of this command excludes the uncoloured octets offered in the count.

Default no uncoloured-octets-offered-count

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.21 uncoloured-packets-offered-count

uncoloured-packets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>cr>queue>i-counters uncoloured-packets-offered-count)
[Tree] (config>subscr-mgmt>acct-plcy>cr>ref-queue>i-counters uncoloured-packets-offered-count)

Full Context configure subscriber-mgmt radius-accounting-policy custom-record queue i-counters uncoloured-packets-offered-count
configure subscriber-mgmt radius-accounting-policy custom-record ref-queue i-counters uncoloured-packets-offered-count

Description This command includes the uncoloured packets offered count.

The **no** form of this command excludes the uncoloured packets offered count.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

uncoloured-packets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>e-counters uncoloured-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>e-counters uncoloured-packets-offered-count)

Full Context configure log accounting-policy custom-record policer e-counters uncoloured-packets-offered-count
configure log accounting-policy custom-record ref-policer e-counters uncoloured-packets-offered-count

Description This command includes the uncoloured packets offered count.

The **no** form of this command excludes the uncoloured packets offered count.

Default no uncoloured-packets-offered-count

Platforms All

uncoloured-packets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context **[Tree]** (config>log>acct-policy>cr>policer>i-counters uncoloured-packets-offered-count)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>log>acct-policy>cr>queue>i-counters uncoloured-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-policer>i-counters uncoloured-packets-offered-count)
[Tree] (config>log>acct-policy>cr>ref-queue>i-counters uncoloured-packets-offered-count)

Full Context configure log accounting-policy custom-record policer i-counters uncoloured-packets-offered-count
configure log accounting-policy custom-record queue i-counters uncoloured-packets-offered-count
configure log accounting-policy custom-record ref-policer i-counters uncoloured-packets-offered-count
configure log accounting-policy custom-record ref-queue i-counters uncoloured-packets-offered-count

Description This command includes the uncolored packets offered count.

The **no** form of this command excludes the uncoloured packets offered count.

Default no uncoloured-packets-offered-count

Platforms All

25.22 uncommitted-changes-indicator

uncommitted-changes-indicator

Syntax [**no**] **uncommitted-changes-indicator**

Context [Tree] (config>system>management-interface>cli>md-cli>environment>prompt uncommitted-changes-indicator)

Full Context configure system management-interface cli md-cli environment prompt uncommitted-changes-indicator

Description This command displays the change indicator.

The **no** form of this command suppresses the change indicator.

Default uncommitted-changes-indicator

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.23 unconstrained-bw

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac unconstrained-bw)
[Tree] (config>subscr-mgmt>sub-mcac-plcy unconstrained-bw)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac unconstrained-bw
configure subscriber-mgmt sub-mcac-policy unconstrained-bw

Description This command configures the bandwidth for the interface or subscriber's multicast CAC policy traffic. When disabled (**no unconstrained-bw**), there is no checking of bandwidth constraints on the interface or subscriber level. When enabled and a policy is defined, enforcement is performed. The allocated bandwidth for optional channels should not exceed the **unconstrained-bw** minus the **mandatory-bw** and the mandatory channels have to stay below the specified value for the **mandatory-bw**. After this interface and subscriber check, the bundle checks are performed.

The **no** form of this command reverts to the default.

Parameters *bandwidth* — Specifies bandwidth assigned for interface's MCAC policy traffic, in kilobits per second (kb/s).

Values 0 to 2147483647

mandatory-bw — Specifies the bandwidth pre-reserved for all the mandatory channels on a given interface in kilobits per second (kb/s).

If the *bandwidth* value is 0, no mandatory channels are allowed. If the value of *bandwidth* is '-1', then all mandatory and optional channels are allowed.

If the value of *mandatory-bw* is equal to the value of *bandwidth*, then all the unconstrained bandwidth on a given interface is allocated to mandatory channels configured through multicast CAC policy on that interface and no optional groups (channels) are allowed.

The value of *mandatory-bw* should always be less than or equal to that of *bandwidth*, An attempt to set the value of *mandatory-bw* greater than that of *bandwidth*, will result in inconsistent value error.

Values 0 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s

- configure subscriber-mgmt sub-mcac-policy unconstrained-bw

7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac unconstrained-bw

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping>mcac unconstrained-bw)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping>mcac unconstrained-bw)
[Tree] (config>service>vpls>sap>igmp-snooping>mcac unconstrained-bw)
[Tree] (config>service>vpls>sap>mld-snooping>mcac unconstrained-bw)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping>mcac unconstrained-bw)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping>mcac unconstrained-bw)

Full Context configure service vpls mesh-sdp igmp-snooping mcac unconstrained-bw
configure service vpls mesh-sdp mld-snooping mcac unconstrained-bw
configure service vpls sap igmp-snooping mcac unconstrained-bw
configure service vpls sap mld-snooping mcac unconstrained-bw
configure service vpls spoke-sdp igmp-snooping mcac unconstrained-bw
configure service vpls spoke-sdp mld-snooping mcac unconstrained-bw

Description This command configures the bandwidth for the interface's multicast CAC policy traffic. When disabled (**no unconstrained-bw**) there will be no checking of bandwidth constraints on the interface level. When enabled and a policy is defined, enforcement is performed. The allocated bandwidth for optional channels should not exceed the **unconstrained-bw** minus the **mandatory-bw** and the mandatory channels have to stay below the specified value for the **mandatory-bw**. After this interface check, the bundle checks are performed.

Parameters *bandwidth* — The bandwidth assigned for interface's MCAC policy traffic, in kilobits per second (kb/s)

Values 0 to 2147483647

mandatory-bw *mandatory-bw* — Specifies the bandwidth pre-reserved for all the mandatory channels on a specified interface in kilobits per second (kb/s)

If the *bandwidth* value is 0, no mandatory channels are allowed. If *bandwidth* is not configured, then all mandatory and optional channels are allowed.

If the value of *mandatory-bw* is equal to the value of *bandwidth*, then all the unconstrained bandwidth on a specified interface is allocated to mandatory channels configured through multicast CAC policy on that interface and no optional groups (channels) are allowed.

The value of *mandatory-bw* should always be less than or equal to that of *bandwidth*, An attempt to set the value of *mandatory-bw* greater than that of *bandwidth*, will result in inconsistent value error.

Values 0 to 2147483647

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context [Tree] (config>service>vprn>igmp>grp-if>mcac unconstrained-bw)
[Tree] (config>service>vprn>igmp>if>mcac unconstrained-bw)
[Tree] (config>service>vprn>mld>grp-if>mcac unconstrained-bw)
[Tree] (config>service>vprn>mld>if>mcac unconstrained-bw)
[Tree] (config>service>vprn>pim>if>mcac unconstrained-bw)

Full Context configure service vprn igmp group-interface mcac unconstrained-bw
configure service vprn igmp interface mcac unconstrained-bw
configure service vprn mld group-interface mcac unconstrained-bw
configure service vprn mld interface mcac unconstrained-bw
configure service vprn pim interface mcac unconstrained-bw

Description This command configures the bandwidth for the interface's multicast CAC policy traffic. When disabled (**no unconstrained-bw**) there will be no checking of bandwidth constraints on the interface level. When enabled and a policy is defined, enforcement is performed. The allocated bandwidth for optional channels should not exceed the **unconstrained-bw** minus the **mandatory-bw** and the mandatory channels have to stay below the specified value for the **mandatory-bw**. After this interface check, the bundle checks are performed.

Parameters *bandwidth* — The bandwidth assigned for the interface's MCAC policy traffic in kb/s.

Values 0 to 2147483647

mandatory-bw *mandatory-bw* — Specifies the bandwidth pre-reserved for all the mandatory channels on a given interface, in kb/s.

If the *bandwidth* value is 0, no mandatory channels are allowed. If *bandwidth* is not configured, then all mandatory and optional channels are allowed.

If the value of *mandatory-bw* is equal to the value of *bandwidth*, then all the unconstrained bandwidth on a given interface is allocated to mandatory channels configured through multicast CAC policy on that interface and no optional groups (channels) are allowed.

The value of *mandatory-bw* should always be less than or equal to that of *bandwidth*, An attempt to set the value of *mandatory-bw* greater than that of *bandwidth*, will result in inconsistent value error.

Values 0 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn mld group-interface mcac unconstrained-bw
- configure service vprn igmp group-interface mcac unconstrained-bw

All

- configure service vprn igmp interface mcac unconstrained-bw
- configure service vprn mld interface mcac unconstrained-bw

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn pim interface mcac unconstrained-bw

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context **[Tree]** (config>router>igmp>grp-if>mcac unconstrained-bw)
[Tree] (config>router>igmp>interface>mcac unconstrained-bw)
[Tree] (config>router>mcac>if-policy unconstrained-bw)
[Tree] (config>router>mld>grp-if>mcac unconstrained-bw)
[Tree] (config>router>mld>interface>mcac unconstrained-bw)
[Tree] (config>router>pim>interface>mcac unconstrained-bw)

Full Context configure router igmp group-interface mcac unconstrained-bw
configure router igmp interface mcac unconstrained-bw
configure router mcac if-policy unconstrained-bw
configure router mld group-interface mcac unconstrained-bw
configure router mld interface mcac unconstrained-bw
configure router pim interface mcac unconstrained-bw

Description This command enables MCAC (or HMCAC) function on the corresponding level (subscriber, group-interface or redirected interface). When MCAC (or HMCAC) is enabled and a channel definition policy is referenced, admission control is performed. The allocated bandwidth for optional channels should not exceed the unconstrained-bw minus the mandatory-bw. The mandatory channels have to stay below the specified value for the mandatory-bw.

In HMCAC, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface or the group-interface against the bandwidth limits defined there.

In case that redirection is enabled and HMCAC enabled, the channel definition policy must be referenced under the redirected interface level. If it is referenced under the group-interface level, it will be ignored.

Subscriber MCAC (only subscriber is checked for available resources) is supported only with direct subscriber replication (no redirection). In this case the channel definition policy must be referenced under the group-interface.

If the redirection is enabled but the policy is referenced only under the group-interface, no admission control is executed (HMCAC or MCAC).

The **no** form of this command removes the values from the configuration.

Default no unconstrained-bw

Parameters *bandwidth* — Specifies the unconstrained bandwidth in kb/s for the MCAC policy.

Values 0 to 2147483647

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

mandatory-bw — Specifies the mandatory bandwidth in kb/s for the MCAC policy.

Values 0 to 2147483647

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface mcac unconstrained-bw
- configure router mld group-interface mcac unconstrained-bw

All

- configure router igmp interface mcac unconstrained-bw
- configure router mcac if-policy unconstrained-bw
- configure router mld interface mcac unconstrained-bw
- configure router pim interface mcac unconstrained-bw

25.24 unconsumed-agg-rate

unconsumed-agg-rate

Syntax **unconsumed-agg-rate percent** *percent-of-unconsumed-agg-rate*
no unconsumed-agg-rate

Context **[Tree]**
(config>qos>adv-config-policy>child-control>bandwidth-distribution>above-offered-allowance unconsumed-agg-rate)

Full Context configure qos adv-config-policy child-control bandwidth-distribution above-offered-allowance unconsumed-agg-rate

Description This command configures the percentage of the unconsumed aggregate rate that can be given to a queue at the end of an H-QoS below CIR pass and above CIR pass. This command is only applicable when the port scheduler is configured to use the **above-offered-allowance-control** algorithm, otherwise it is ignored.

The **no** form of this command reverts the **unconsumed-agg-rate percent** to its default value.

Default unconsumed-agg-rate 100.00

Parameters *percent-of-unconsumed-agg-rate* — Specifies the percentage of the unconsumed aggregate rate that can be given to a queue.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.25 unconsumed-higher-tier-rate

unconsumed-higher-tier-rate

Syntax **unconsumed-higher-tier-rate percent** *percent-of-unconsumed-higher-tier-rate*
no unconsumed-higher-tier-rate

Context **[Tree]**
(config>qos>adv-config-policy>child-control>bandwidth-distribution>above-offered-allowance unconsumed-higher-tier-rate)

Full Context configure qos adv-config-policy child-control bandwidth-distribution above-offered-allowance unconsumed-higher-tier-rate

Description This command configures the percentage of the unconsumed higher tier rate that can be given to a queue at the end of an H-QoS below CIR pass and above CIR pass. Higher tier refers to the Vport aggregate rate and port scheduler level, group, and maximum rates.

This command is only applicable when the port scheduler is configured to use the **above-offered-allowance-control** algorithm, otherwise it is ignored.

The **no** form of this command reverts the **unconsumed-higher-tier-rate percent** to its default value.

Default unconsumed-higher-tier-rate 100.00

Parameters *percent-of-unconsumed-higher-tier-rate* — Specifies the percentage of the unconsumed higher tier rate that can be given to a queue.

Values 0.00 to 100.00

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

25.26 underflow-limit

underflow-limit

Syntax **underflow-limit** *number* **threshold** *percent* [**bw** *bandwidth-in-mbps*]
no underflow-limit

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth underflow-limit)
[Tree] (config>router>mpls>lsp-template>auto-bandwidth underflow-limit)

Full Context configure router mpls lsp auto-bandwidth underflow-limit
configure router mpls lsp-template auto-bandwidth underflow-limit

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures underflow-triggered auto-bandwidth adjustment. An underflow auto-bandwidth adjustment can occur any time during the adjust-interval; it is triggered when the number of consecutive underflow samples reaches the threshold N configured as part of this command. The new bandwidth of the LSP after a successful underflow adjustment is the maximum data rate observed in the last N consecutive underflow samples.

A sample interval is counted as an underflow if the average data rate during the sample interval is lower than the currently reserved bandwidth by at least the thresholds configured as part of this command.

The **no** form of this command disables underflow-triggered automatic bandwidth adjustment.

Default no underflow-limit

Parameters *number* — Specifies the number of consecutive underflow samples that triggers an underflow auto-bandwidth adjustment attempt.

Values 0 to 10

percent — Specifies the minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as a percentage of the current bandwidth, for counting an underflow sample.

Values 0 to100

bandwidth-in-mbps — Specifies the minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as an absolute bandwidth (Mb/s) relative to the current bandwidth, for counting an underflow sample.

Values 0 to 6400000

Platforms All

25.27 undet-availability-event

undet-availability-event

Syntax **undet-availability-event** {**forward** | **backward** | **aggregate**} **threshold** *raise-threshold* [**clear** *clear-threshold*]
no undet-availability-event {**forward** | **backward** | **aggregate**}

Context **[Tree]** (config>oam-pm>session>ethernet>slm>loss-events undet-availability-event)
[Tree] (config>oam-pm>session>ethernet>lmm>loss-events undet-availability-event)
[Tree] (config>oam-pm>session>ip>twamp-light>loss-events undet-availability-event)

Full Context configure oam-pm session ethernet lmm loss-events undet-availability-event
configure oam-pm session ethernet slm loss-events undet-availability-event
configure oam-pm session ip twamp-light loss-events undet-availability-event

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command sets the threshold to be applied to the overall count of the undetermined availability indicators, not transitions, per configured direction. This value is compared to the 32 bit unavailability counter specific to the direction which tracks the number of individual delta-ts that have been recorded as undetermined available. The aggregate is a function of summing forward and backward. This value is only used as a threshold mechanism and is not part of the stored statistics. If the optional **clear** *clear-threshold* parameter is not specified, the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and regardless of any previous window. Each unique event can only be raised once within measurement interval. If the optional **clear** *clear-threshold* parameter is specified, the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is carried forward to following measurement intervals. If a threshold crossing event is raised another is raised until a measurement interval completes and the clear threshold has not been exceeded. A clear event is raised under that condition.

The **no** form of this command removes the event threshold for frame loss ratio. The direction must be included with the **no** command.

Default no undet-availability-event forward

no undet-availability-event backward

no undet-availability-event aggregate

Parameters **forward** — Specifies the threshold is applied to the forward direction count.

backward — Specifies the threshold is applied to the backward direction count.

aggregate — Specifies the threshold is applied to the aggregate count (sum of forward and backward).

raise-threshold — Specifies the rising threshold that determines when the event is to be generated, when value reached.

Values 1 to 864000

clear-threshold — Specifies an optional value used for stateful behavior that allows the operator to configure a percentage of loss value lower than the rising percentage to indicate when the clear event should be generated.

Values 0 to 863999

A value of zero means that the undetermined availability counter must be 0.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events undet-availability-event

All

- configure oam-pm session ethernet slm loss-events undet-availability-event
- configure oam-pm session ethernet lmm loss-events undet-availability-event

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.28 undet-unavailability-event

undet-unavailability-event

Syntax **undet-unavailability-event** {**forward** | **backward** | **aggregate**} **threshold** *raise-threshold* [**clear** *clear-threshold*]
no undet-unavailability-event {**forward** | **backward** | **aggregate**}

Context **[Tree]** (config>oam-pm>session>ethernet>slm>loss-events undet-unavailability-event)
[Tree] (config>oam-pm>session>ethernet>lmm>loss-events undet-unavailability-event)
[Tree] (config>oam-pm>session>ip>twamp-light>loss-events undet-unavailability-event)

Full Context configure oam-pm session ethernet lmm loss-events undet-unavailability-event
configure oam-pm session ethernet slm loss-events undet-unavailability-event
configure oam-pm session ip twamp-light loss-events undet-unavailability-event

Description This command sets the threshold to be applied to the overall count of the undetermined unavailability indicators, not transitions, per configured direction. This value is compared to the 32 bit unavailability counter specific to the direction which tracks the number of individual delta-ts that have been recorded as undetermined unavailable. The aggregate is a function of summing forward and backward. This value is only used as a threshold mechanism and is not part of the stored statistics. If the **clear** *clear-threshold* parameter is not specified the traffic crossing alarm is stateless. Stateless means the state is not carried forward to other measurement intervals. Each measurement interval is analyzed independently and without regard to any previous window. Each unique event can only be raised once within measurement interval. If the optional clear threshold is specified the traffic crossing alarm uses stateful behavior. Stateful means each unique previous event state is carried forward to following measurement intervals. If a threshold crossing event is raised another is not raised until a measurement interval completes and the clear threshold has not been exceeded. A clear event is raised under that condition.

The **no** form of this command removes the event threshold for frame loss ratio. The direction must be included with the **no** command.

Default no undet-unavailable-event forward

no undet-unavailable-event backward

no undet-unavailable-event aggregate

Parameters **forward** — Specifies the threshold is applied to the forward direction count.

backward — Specifies the threshold is applied to the backward direction count.

aggregate — Specifies the threshold is applied to the aggregate count (sum of forward and backward).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

raise-threshold — Specifies the rising threshold that determines when the event is to be generated, when value reached.

Values 1 to 864000

clear-threshold — Specifies an optional value used for stateful behavior that allows the operator to configure a percentage of loss value lower than the rising percentage to indicate when the clear event should be generated.

Values 0 to 863999

A value of zero means that the undetermined availability counter must be 0.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure oam-pm session ip twamp-light loss-events undet-unavailability-event

All

- configure oam-pm session ethernet slm loss-events undet-unavailability-event
- configure oam-pm session ethernet lmm loss-events undet-unavailability-event

25.29 undo

undo

Syntax **undo** [*count*]

Context **[Tree]** (candidate undo)

Full Context candidate undo

Description This command removes the most recent change(s) done to the candidate. The changes can be reapplied using the **redo** command. All undo or redo history is lost when the operator exits the **edit-cfg** mode. Undo can not be used to recover a candidate that has been discarded with **candidate discard**.

An **undo** command is blocked if another user has made changes in the same CLI branches that would be impacted during the undo.

Parameters *count* — Specifies the number of previous changes to remove.

Values 1 to 50

Default 1

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.30 uni

uni

Syntax **uni**

Context **[Tree]** (config>system>security>keychain>direction uni)

Full Context configure system security keychain direction uni

Description This command configures keys for send or receive stream directions.

Platforms All

25.31 unicast-address

unicast-address

Syntax [**no**] **unicast-address** *ip-address*

Context **[Tree]** (config>service>vprn>rip>group>neighbor unicast-address)

Full Context configure service vprn rip group neighbor unicast-address

Description This command configures the unicast IPv4 address, RIP updates messages will be sent to if the RIP **send** command is set to **send unicast**.

Multiple unicast-address entries can be configured, in which case unicast messages will be sent to each configured unicast IPv4 address.

The **no** form of this command deletes the specified IPv4 unicast address from the configuration.

Parameters *ip-address* — Specifies the unicast IPv4 address in a.b.c.d format.

Platforms All

unicast-address

Syntax [**no**] **unicast-address** *ipv6-address*

Context **[Tree]** (config>service>vprn>ripng>group>neighbor unicast-address)

Full Context configure service vprn ripng group neighbor unicast-address

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the unicast IPv6 address, RIPng updates messages will be sent to if the RIPng **send** command is set to **send unicast**.

Multiple unicast-address entries can be configured, in which case unicast messages will be sent to each configured unicast IPv6 address.

The **no** form of this command deletes the specified IPv6 unicast address from the configuration.

Parameters *ipv6-address* — Specifies the unicast IPv6 address.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x [0 to FFFF]H
	d [0 to 255]D

Platforms All

unicast-address

Syntax [**no**] **unicast-address** *ipv6-address*

Context **[Tree]** (config>router>rip>group>neighbor unicast-address)
[Tree] (config>router>ripng>group>neighbor unicast-address)

Full Context configure router rip group neighbor unicast-address
configure router ripng group neighbor unicast-address

Description This command configures the unicast IPv6 address that RIP and RIPng update messages will be sent to if the **send** command is set to **send unicast**.

Multiple unicast-address entries can be configured, in which case unicast messages will be sent to each configured unicast IPv6 address.

The **no** form of the command deletes the specified IPv6 unicast address from the configuration.

Parameters *ipv6-address* — Specifies the IPv6 unicast address to which unicast RIP or RIPng updates should be sent.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.32 unicast-import-disable

unicast-import-disable

Syntax [**no**] **unicast-import-disable** [**ipv4**]
[**no**] **unicast-import-disable** [**ipv6**]
[**no**] **unicast-import-disable** [**both**]

Context **[Tree]** (config>service>vprn>isis unicast-import-disable)

Full Context configure service vprn isis unicast-import-disable

Description This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM. Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes will not be imported into RPF RTM as such an import policy must be explicitly configured.

Default no unicast-import-disable

Parameters **ipv4** — Allows importation of IPv4 routes only.

ipv6 — Allows importation of IPv6 routes only.

both — Allows importation of both IPv4 and IPv6 routes.

Platforms All

unicast-import-disable

Syntax [**no**] **unicast-import-disable**

Context **[Tree]** (config>service>vprn>ospf unicast-import-disable)

Full Context configure service vprn ospf unicast-import-disable

Description This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM.

Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes will not be imported into RPF RTM as such an import policy must be explicitly configured

Default no unicast-import-disable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

unicast-import-disable

Syntax [**no**] **unicast-import-disable** [**ipv4**]
[**no**] **unicast-import-disable** [**ipv6**]
[**no**] **unicast-import-disable** [**both**]

Context **[Tree]** (config>router>isis unicast-import-disable)

Full Context configure router isis unicast-import-disable

Description This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM.

Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes are not imported into RPF RTM, thus, an import policy must be explicitly configured.

Default no unicast-import-disable both

Parameters **ipv4** — Allows importation of IPv4 routes only.

ipv6 — Allows importation of IPv6 routes only.

both — Allows importation of both IPv4 and IPv6 routes.

Platforms All

unicast-import-disable

Syntax [**no**] **unicast-import-disable**

Context **[Tree]** (config>router>ospf unicast-import-disable)
[Tree] (config>router>ospf3 unicast-import-disable)

Full Context configure router ospf unicast-import-disable
configure router ospf3 unicast-import-disable

Description This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM. Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes are not imported into RPF RTM as such an import policy must be explicitly configured.

Default no unicast-import-disable

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.33 unicast-rt-test

unicast-rt-test

Syntax [**no**] **unicast-rt-test**

Context **[Tree]** (config>filter>redirect-policy>dest unicast-rt-test)

Full Context configure filter redirect-policy destination unicast-rt-test

Description This command configures a unicast route test for this destination. A destination is eligible for redirect if a valid unicast route to that destination exists in the routing instance specified by **config>filter>redirect-policy>router**. The unicast route test is mutually exclusive with other redirect-policy test types.

The test cannot be configured if **no router** is configured for this redirect policy.

The **no** form of the command disables the test.

Default no unicast-rt-test

Platforms All

25.34 unidirectional-measurement

unidirectional-measurement

Syntax **unidirectional-measurement** *measurement-type*

Context **[Tree]** (config>test-oam>link-meas>template unidirectional-measurement)

Full Context configure test-oam link-measurement measurement-template unidirectional-measurement

Description This command specifies the method used to compute the unidirectional delay value.

Default unidirectional-measurement derived

Parameters *measurement-type* — Specifies the method to compute a unidirectional delay measurement.

Values **actual** — Keyword to use the forward delay as the unidirectional measurement. The forward delay is calculated using T2-T1 timestamps.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

derived — Keyword to compute the unidirectional measurement using the round trip delay divided by two. This option should be used when the nodal clocks are not synchronized using an accurate time synchronization method or protocol, like PTP.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

25.35 unique-sid-per-sap

unique-sid-per-sap

Syntax **unique-sid-per-sap** [**per-msap**]
no unique-sid-per-sap

Context **[Tree]** (config>subscr-mgmt>ppp-policy unique-sid-per-sap)

Full Context configure subscriber-mgmt ppp-policy unique-sid-per-sap

Description This command assigns a unique session ID to each PPPoE session active on a single SAP.

On a capture SAP, a unique session ID is assigned per capture SAP: multiple sessions that are active on the same or different MSAP have a unique session ID per capture SAP.

With the optional parameter **per-msap**, a unique session ID is assigned per MSAP:

- multiple sessions that are active on the same MSAP have a unique session ID per MSAP
- multiple sessions that are active on different MSAPs are not guaranteed to have a unique session ID

The session ID range is 1 to 8191.

By default, all PPPoE sessions with a different client MAC address and active on a given SAP or MSAP have a session ID of 1 (**sid-allocation sequential**) or a random value in the range 1 to 8191 (**sid-allocation random**).

The **no** form of this command reverts to the default.

Parameters **per-msap** — Assigns a unique session ID for PPPoE sessions that are active on the same MSAP. This parameter has no effect on regular SAPs.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.36 unknown-arp-request-flood-evpn

unknown-arp-request-flood-evpn

Syntax [**no**] **unknown-arp-request-flood-evpn**

Context **[Tree]** (config>service>vpls>proxy-arp unknown-arp-request-flood-evpn)

Full Context configure service vpls proxy-arp unknown-arp-request-flood-evpn

Description This command controls whether unknown ARP-requests are flooded into the EVPN network. By default, the system floods ARP-requests, including EVPN (with source squelching), if there is no active proxy-arp entry for the requested IP.

The **no** form of the command will only flood to local SAPs/SDP-bindings and not to EVPN destinations.

Default unknown-arp-request-flood-evpn

Platforms All

25.37 unknown-mac-route

unknown-mac-route

Syntax [**no**] **unknown-mac-route**

Context **[Tree]** (config>service>vpls>bgp-evpn unknown-mac-route)

Full Context configure service vpls bgp-evpn unknown-mac-route

Description This command enables the advertisement of the unknown-mac-route in BGP. This will be coded in an EVPN MAC route where the MAC address is zero and the MAC address length 48. By using this unknown-mac-route advertisement, the user may decide to optionally turn off the advertisement of MAC addresses learned from SAPs and SDP-bindings, hence reducing the control plane overhead and the size of the FDB tables in the data center. All the receiving NVEs supporting this concept will send any unknown-unicast packet to the owner of the unknown-mac-route, as opposed to flooding the unknown-unicast traffic to all other nodes part of the same VPLS. Although the 7750 SR, 7450 ESS, or 7950 XRS can be configured to generate and advertise the unknown-mac-route, the router will never honor the unknown-mac-route and will flood to the vpls flood list when an unknown-unicast packet arrives to an ingress SAP/SDP-binding.

Use of the unknown-mac-route is only supported for BGP-EVPN VXLAN.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no unknown-mac-route

Platforms All

25.38 unknown-message-rate

unknown-message-rate

Syntax **unknown-message-rate** *integer*
no unknown-message-rate

Context **[Tree]** (config>router>pcep>pcc unknown-message-rate)
[Tree] (config>router>pcep>pce unknown-message-rate)

Full Context configure router pcep pcc unknown-message-rate
configure router pcep pce unknown-message-rate

Description This command configures the maximum rate of unknown messages which can be received on a PCEP session.

When the rate of received unrecognized or unknown messages reaches the configured limit, the PCEP speaker closes the session to the peer.

The **no** form of the command returns the unknown message rate to the default value.

Default unknown-message-rate 10

Parameters *integer* — the rate of unknown messages, in messages per minute

Values 1 to 255

Platforms All

25.39 unknown-ns-flood-evpn

unknown-ns-flood-evpn

Syntax [**no**] **unknown-ns-flood-evpn**

Context **[Tree]** (config>service>vpls>proxy-nd unknown-ns-flood-evpn)

Full Context configure service vpls proxy-nd unknown-ns-flood-evpn

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command controls whether unknown Neighbor Solicitation messages are flooded into the EVPN network. By default, the system floods NS (with source squelching) to SAPs/SDP-bindings including EVPN, if there is no active proxy-nd entry for the requested IPv6.

The **no** form of the command will only flood to local SAPs/SDP-bindings but not to EVPN destinations.

Default unknown-ns-flood-evpn

Platforms All

25.40 unknown-policer

unknown-policer

Syntax **unknown-policer** *policer-id* [**fp-redirect-group**]
no unknown-policer

Context **[Tree]** (config>qos>sap-ingress>fc unknown-policer)

Full Context configure qos sap-ingress fc unknown-policer

Description Within a **sap-ingress** QoS policy forwarding class context, the **unknown-policer** command is used to map packets that match the forwarding class and are considered unknown in nature to the specified policer-id. The specified policer-id must already exist within the **sap-ingress** QoS policy. While the system is determining the forwarding class of a packet, it is also looking up its forwarding destination based on the ingress service type and the service instance forwarding records. If the service type is VPLS and the destination MAC address is unicast, but the MAC has not been learned and populated within the VPLS services FDB, the packet is classified into the unknown forwarding type.

Unknown forwarding type packets are mapped to either an ingress multipoint queue (using the **unknown** *queue-id* or **unknown** *queue-id* **group** *ingress-queue-group* commands) or an ingress policer (**unknown-policer** *policer-id*). The **unknown** and **unknown-policer** commands within the forwarding class context are mutually exclusive. By default, the unknown forwarding type is mapped to the SAP ingress default multipoint queue. If the **unknown-policer** *policer-id* command is executed, any previous policer mapping or queue mapping for the unknown forwarding type within the forwarding class is overridden if the policer mapping is successful.

A policer defined within the **sap-ingress** policy is not actually created on an ingress SAP or a subscriber using an **sla-profile** where the policy is applied until at least one forwarding type (unicast, broadcast, unknown, or multicast) from one of the forwarding classes is mapped to the policer. If insufficient policer resources exist to create the policer for a SAP or subscriber or multiservice site, or ingress policing is not supported on the port associated with the SAP or subscriber or multiservice site, the initial forwarding class forwarding type mapping will fail.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **unknown-policer** command is ignored for instances of the policer applied to SAPs or subscribers' multiservice site where unknown packets are not supported.

When the unknown forwarding type within a forwarding class is mapped to a policer, the unknown packets classified to the subclasses within the forwarding class are also mapped to the policer.

The **no** form of this command is used to restore the mapping of the unknown forwarding type within the forwarding class to the default multipoint queue. If all forwarding class forwarding types had been removed from the default multipoint queue, the queue will not exist on the SAPs or subscriber or multiservice site associated with the QoS policy and the **no broadcast-policer** command will cause the system to attempt to create the default multipoint queue on each object. If the system cannot create the queue on each instance, the **no unknown-policer** command will fail and the unknown forwarding type within the forwarding class will continue its mapping to the existing *policer-id*. If the **no unknown-policer** command results in a policer without any current mappings, the policer will be removed from the SAPs and subscribers associated with the QoS policy. All statistics associated with the policer on each SAP and subscriber will be lost.

Parameters *policer-id* — When the forwarding class **unknown-policer** command is executed, a valid *policer-id* must be specified. The parameter *policer-id* references a *policer-id* that has already been created within the **sap-ingress** QoS policy.

Values 1 to 63

fp-redirect-group — Redirects a forwarding class to a forwarding plane queue-group as specified in a SAP QoS policy.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, 7950 XRS, VSR

25.41 unknown-protocol

unknown-protocol

Syntax **unknown-protocol** [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no unknown-protocol

Context **[Tree]** (config>service>nat>firewall-policy>timeouts unknown-protocol)

Full Context configure service nat firewall-policy timeouts unknown-protocol

Description This command configures the timeout interval for unknown protocol mappings.

The **no** form of the command reverts the timeout interval to the default of 5 minutes.

Default unknown-protocol min 5

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *hours* — Specifies the number of hours in the unknown protocol mapping timeout interval.

Values 0 to 24

minutes — Specifies the number of minutes in the unknown protocol mapping timeout interval.

Values 1 to 59

seconds — Specifies the number of seconds in the unknown protocol mapping timeout interval.

Values 0 to 59

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.42 unknown-protocols

unknown-protocols

Syntax **unknown-protocols**

Context **[Tree]** (config>service>nat>firewall-policy unknown-protocols)

Full Context configure service nat firewall-policy unknown-protocols

Description Commands in this context configure the treatment of flows of unknown Layer 4 protocols, which are protocols that cannot be natively handled by the system.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.43 unknown-queue

unknown-queue

Syntax **unknown-queue** *queue-id* [**group** *queue-group-name*]
no unknown-queue

Context **[Tree]** (config>qos>sap-ingress>fc unknown-queue)

Full Context configure qos sap-ingress fc unknown-queue

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command overrides the default unknown unicast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all unknown traffic on a SAP using this policy is forwarded using the *queue-id*.

The unknown forwarding type usually tracks the multicast forwarding type definition. This command overrides that default behavior.

The **no** form of this command sets the unknown forwarding type *queue-id* back to the default of tracking the multicast forwarding type queue mapping.

Parameters *queue-id* — Specifies an existing multipoint queue defined in the **config>qos>sap-ingress** context.

Values Any valid multipoint *queue-id* in the policy including 2 through 32.

Default 11

group *queue-group-name* — This optional parameter is used to redirect the forwarding type within the forwarding class to the specified queue-id within the queue-group-name. When the policy is applied, all packets matching the forwarding class and forwarding type will be redirected to the queue within the specified queue group. The *queue-group-name* are configured in the **config>qos>queue-group-templates** egress and ingress contexts.

Platforms All

unknown-queue

Syntax **unknown-queue** *queue-id*
no unknown-queue

Context **[Tree]** (config>qos>shared-queue>fc unknown-queue)

Full Context configure qos shared-queue fc unknown-queue

Description This command configures the unknown unicast forwarding type queue mapping for **fc** *fc-name*. The specified *queue-id* must exist within the policy as a multipoint queue before the mapping can be made. When the forwarding class mapping is executed, all unknown traffic on a SAP using this policy is forwarded using the *queue-id*.

The unknown forwarding type usually tracks the multicast forwarding type definition. This command overrides that default behavior.

The **no** form of this command sets the unknown forwarding type *queue-id* back to the default of tracking the multicast forwarding type queue mapping.

Parameters *queue-id* — The *queue-id* must be an existing, multipoint queue defined in the **config>qos>sap-ingress** context policer-output-queues profile. For the 7950 XRS, this is not configurable in the policer-output-queues profile.

Values 25 to 32

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

25.44 unnumbered

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]
no unnumbered

Context **[Tree]** (config>service>vprn>sub-if unnumbered)
[Tree] (config>service>ies>sub-if unnumbered)

Full Context configure service ies subscriber-interface unnumbered
configure service vprn subscriber-interface unnumbered

Description This command can be configured only for subscriber interfaces that do not have an IPv4 address explicitly configured and is therefore operationally in a DOWN state. By configuring this command, the subscriber interface borrows the IPv4 address from the referenced interface (directly or indirectly via IP address) that must be operationally UP and located in the same routing instance as the subscriber interface. This allows the subscriber interface to be operationally UP and consequently allow forwarding of the subscriber traffic.

Such interface is referred as unnumbered interface, since it does not have explicitly configured a unique IP address. Subscriber hosts under the unnumbered subscriber interface are installed in the fib as /32 hosts.

Without this command the subscriber interface is operationally DOWN and subscriber-host instantiation is not possible.

This command is mutually exclusive with the allow-unmatched-subnets command under the same CLI hierarchy.

The operation of IPv6 host is not affected by this command.

The **no** form of this command reverts to the default.

Parameters *ip-int-name* — Specifies the interface name from which an IPv4 address is borrowed.

ip-address — Specifies the IP address from an optionally up interface that is used for subscriber interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no unnumbered

Context **[Tree]** (config>service>vprn>sub-if unnumbered)
[Tree] (config>service>ies>sub-if unnumbered)

Full Context configure service ies subscriber-interface unnumbered
configure service vprn subscriber-interface unnumbered

Description This command can be configured only for subscriber interfaces that do not have an IPv4 address explicitly configured and is therefore operationally in a DOWN state. By configuring this command, the subscriber interface borrows the IPv4 address from the referenced interface (directly or indirectly via IP address) that must be operationally UP and located in the same routing instance as the subscriber interface. This allows the subscriber interface to be operationally UP and consequently allow forwarding of the subscriber traffic.

Such interface is referred as unnumbered interface, since it does not have explicitly configured a unique IP address. Subscriber hosts under the unnumbered subscriber interface are installed in the fib as /32 hosts.

Without this command the subscriber interface is operationally DOWN and subscriber-host instantiation is not possible.

This command is mutually exclusive with the allow-unmatched-subnets command under the same CLI hierarchy.

The operation of IPv6 host is not affected by this command.

The **no** form of this command reverts to the default.

Parameters *ip-int-name* — Specifies the interface name from which an IPv4 address is borrowed.

ip-address — Specifies the IP address from an optionally up interface that is used for subscriber interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]
no unnumbered

Context **[Tree]** (config>service>vpls>interface unnumbered)

Full Context configure service vpls interface unnumbered

Description This command configures the interface as an unnumbered interface.

Parameters *ip-int-name* — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes

ip-address — Specifies an IP address which must be a valid address of another interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]
no unnumbered

Context **[Tree]** (config>service>vpls>interface unnumbered)

Full Context configure service vpls interface unnumbered

Description This command configures the interface as an unnumbered interface.

Parameters *ip-int-name* — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes

ip-address — Specifies an IP address which must be a valid address of another interface

unnumbered

Syntax **unnumbered** {*ip-int-name* | *ip-address*}
no unnumbered

Context **[Tree]** (config>service>ies>if unnumbered)

Full Context configure service ies interface unnumbered

Description This command configures the interface as an unnumbered interface. Unnumbered IP interfaces are supported on a SONET/SDH access port with the PPP, ATM, Frame Relay, cisco-HDLC encapsulation. It is not supported on access ports that do not carry IP traffic, but are used for native TDM circuit emulation.

Parameters *ip-int-name* — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

ip-address — Specifies an IP address.

Platforms All

unnumbered

Syntax **unnumbered** {*ip-int-name* | *ip-address*}
no unnumbered

Context **[Tree]** (config>service>ies>if unnumbered)

Full Context configure service ies interface unnumbered

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the interface as an unnumbered interface. Unnumbered IP interfaces are supported on a SONET/SDH access port with the PPP, ATM, Frame Relay, cisco-HDLC encapsulation. It is not supported on access ports that do not carry IP traffic, but are used for native TDM circuit emulation.

Parameters *ip-int-name* — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

ip-address — Specifies an IP address.

Platforms All

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]
no unnumbered

Context **[Tree]** (config>service>vprn>if unnumbered)
[Tree] (config>service>vprn>nw-if unnumbered)

Full Context configure service vprn interface unnumbered
configure service vprn nw-if unnumbered

Description This command configures the interface as an unnumbered interface. An unnumbered IP interface is supported on a SONET/SDH access port with the PPP, ATM, Frame Relay, cisco-HDLC encapsulation. It is not supported on access ports that do not carry IP traffic, but are used for native TDM circuit emulation.

Parameters *ip-int-name* — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

ip-address — Specifies an IP address.

Platforms All

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*]
no unnumbered

Context **[Tree]** (config>service>vprn>if unnumbered)
[Tree] (config>service>vprn>nw-if unnumbered)

Full Context configure service vprn interface unnumbered
configure service vprn nw-if unnumbered

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the interface as an unnumbered interface. An unnumbered IP interface is supported on a SONET/SDH access port with the PPP, ATM, Frame Relay, cisco-HDLC encapsulation. It is not supported on access ports that do not carry IP traffic, but are used for native TDM circuit emulation.

Parameters *ip-int-name* — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

ip-address — Specifies an IP address.

Platforms All

unnumbered

Syntax **unnumbered** [{*ip-int-name* | *ip-address*}]
no unnumbered

Context **[Tree]** (config>router>if unnumbered)

Full Context configure router interface unnumbered

Description This command sets an IP interface as an unnumbered interface and specifies the IP address to be used for the interface.

To conserve IP addresses, unnumbered interfaces can be configured. The address used when generating packets on this interface is the *ip-addr* parameter configured.

An error message will be generated if an **unnumbered** interface is configured, and an IP address already exists on this interface.

The **no** form of this command removes the IP address from the interface, effectively removing the unnumbered property. The interface must be **shutdown** before **no unnumbered** is issued to delete the IP address from the interface, or an error message will be generated.

Default no unnumbered

Parameters *ip-int-name* | *ip-address* — Optional. Specifies the IP address or IP interface name to associate with the unnumbered IP interface in dotted decimal notation. The configured IP address must exist on this node. It is recommended to use the system IP address as it is not associated with a specific interface and is therefore always reachable. The system IP address is the default if no *ip-addr* or *ip-int-name* is configured.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.45 unnumbered-source-ip

unnumbered-source-ip

Syntax **unnumbered-source-ip** {*ip-address*}
no unnumbered-source-ip

Context **[Tree]** (config>subscr-mgmt>shcv-policy>layer-3 unnumbered-source-ip)

Full Context configure subscriber-mgmt shcv-policy layer-3 unnumbered-source-ip

Description This command configures the source IPv4 address (also known as the sender IP address) used in SHCV ARP requests for unnumbered hosts. When unconfigured, 0.0.0.0 is used as the source IPv4 address in SHCV ARP requests.

The **no** form of this command removes the IPv4 address from Layer 3.

Parameters *ip-address* — Specifies the unicast IPv4 address to be used as the source address in SHCV ARP requests for unnumbered hosts.

Values a.b.c.d

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.46 unreachables

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables[*number seconds*]

Context **[Tree]** (config>service>ies>if>icmp unreachables)
[Tree] (config>service>ies>sub-if>grp-if>icmp unreachables)
[Tree] (config>service>vprn>if>icmp unreachables)
[Tree] (config>service>vprn>if>ipv6>icmp6 unreachables)
[Tree] (config>service>vprn>nw-if>icmp unreachables)
[Tree] (config>service>vprn>sub-if>grp-if>icmp unreachables)

Full Context configure service ies interface icmp unreachables
configure service ies subscriber-interface group-interface icmp unreachables
configure service vprn interface icmp unreachables
configure service vprn interface ipv6 icmp6 unreachables
configure service vprn network-interface icmp unreachables
configure service vprn subscriber-interface group-interface icmp unreachables

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachables messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of ICMP destination unreachable messages on the router interface and reverts to the default values.

Default unreachables 100 10

Parameters *number* — Specifies the maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 to 2000

seconds — Specifies the time frame, in seconds, used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies subscriber-interface group-interface icmp unreachables
- configure service vprn subscriber-interface group-interface icmp unreachables

All

- configure service vprn interface icmp unreachables
- configure service ies interface icmp unreachables
- configure service vprn network-interface icmp unreachables
- configure service vprn interface ipv6 icmp6 unreachables

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context **[Tree]** (config>service>ies>if>ipv6>icmp6 unreachables)

Full Context configure service ies interface ipv6 icmp6 unreachables

Description This command specifies that ICMPv6 host and network unreachable messages are generated by this interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When disabled, ICMPv6 host and network unreachable messages are not sent.

The **no** form of this command reverts to the default.

Default unreachables 100 10

Parameters *number* — Specifies the number of destination unreachable ICMPv6 messages are issued in the time frame specified by the *seconds* parameter.

Values 10 to 2000

seconds — Specifies the time frame, in seconds, that is used to limit the number of destination unreachable ICMPv6 messages to be issued.

Values 1 to 60

Platforms All

unreachables

Syntax **unreachables** [**number** *number*] [**seconds** *seconds*]
no unreachables

Context **[Tree]** (config>subscr-mgmt>git>ipv4>icmp unreachables)

Full Context configure subscriber-mgmt group-interface-template ipv4 icmp unreachables

Description This command configures the generation of ICMP destination unreachable messages on the router interface. The rate at which ICMP unreachable messages are issued can be controlled with the optional *number* and *seconds* parameters, which indicate the maximum number of destination unreachable messages that can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachables messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of ICMP destination unreachable messages on the router interface.

Default unreachables number 100 seconds 10

Parameters *number* — Specifies the maximum number of ICMP unreachable messages sent. This parameter must be specified with the *seconds* parameter.

Values 10 to 2000

seconds — Specifies the time frame, in seconds, used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context **[Tree]** (config>router>if>icmp unreachables)

Full Context configure router interface icmp unreachables

Description This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages that can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachables messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the generation of ICMP destination unreachables on the router interface.

Default unreachables 100 10 — Maximum of 100 unreachable messages in 10 seconds.

Parameters *number* — The maximum number of ICMP unreachable messages to send, expressed as a decimal integer. The *seconds* parameter must also be specified.

Values 10 to 2000

seconds — The time frame, in seconds, used to limit the *number* of ICMP unreachable messages that can be issued, expressed as a decimal integer.

Values 1 to 60

Platforms All

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context **[Tree]** (config>router>if>ipv6>icmp6 unreachables)

Full Context configure router interface ipv6 icmp6 unreachables

Description This command configures the rate for ICMPv6 unreachable messages. When enabled, ICMPv6 host and network unreachable messages are generated by this interface.

The **no** form of this command disables the generation of ICMPv6 host and network unreachable messages by this interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default unreachables 100 10 (when IPv6 is enabled on the interface)

Parameters *number* — Determines the number destination unreachable ICMPv6 messages to issue in the time frame specified in *seconds* parameter.

Values 10 to 2000

seconds — Sets the time frame, in seconds, to limit the number of destination unreachable ICMPv6 messages issued per time frame.

Values 1 to 60

Platforms All

25.47 untrusted

untrusted

Syntax **untrusted** [**default-forwarding** *default-forwarding*]
no untrusted

Context **[Tree]** (config>router>if untrusted)

Full Context configure router interface untrusted

Description This command configures the state of untrusted for a network IP interface.

The untrusted state identifies the participating interfaces in the label security feature for prefixes of a VPN family at an inter-AS boundary. The router supports a maximum of 15 network interfaces that can participate in this feature.

The user normally applies this command to an inter-AS interface. PIP keeps track of the untrusted status of each interface. In the data path, such an interface causes the default forwarding to be set to the *default-forwarding* value.

For backward compatibility reasons, the interface **default-forwarding** is set to the **forward** value; this means that labeled packets are checked in the normal way against the table of programmed ILMs to decide if they should be dropped or forwarded in a GRT, a VRF, or a L2 service context.

If the user sets the *default-forwarding* value to **drop**, all labeled packets received on that interface are automatically dropped.

This command sets the default behavior for an untrusted interface in the data path and for all ILMs. When enabling the label security for VPN IPv4 or VPN IPv6 prefixes, BGP programs the data path to provide an exception to the normal way of forwarding handling away from the default for those VPRN ILMs.

The **no** form of this command returns the interface into the default state of trusted.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no untrusted

Parameters *default-forwarding* — Specifies the default forwarding behavior of labeled packets received on this interface.

Values forward, drop

Default forward

Platforms All

25.48 unzip

unzip

Syntax **unzip** *source-file-url* [*dest-file-url*] **list**
unzip *source-file-url dest-file-url* [**create-destination**] [**force**]

Context **[Tree]** (file unzip)

Full Context file unzip

Description This command expands the contents of a ZIP file to the local file system. Any file that is zipped using the store, deflate, or zip64 compression methods can be unzipped. The source ZIP file location can be a locally installed solid-state storage device or a remote FTP or TFTP server. Files can only be unzipped to the active CPM.

Parameters *source-file-url*, *dest-file-url* — Specifies the source or destination file URL.

Values

local-url	[*cflash-id*/]*file-path*
	200 chars max, including cflash-id
	directory length 99 chars max each
remote-url	{ftp | tftp}://[*login*:*pswd*@]
	remote-locn / [*file-path*]
	247 chars max, *file-path* 199 chars max
remote-locn	{*hostname* | *ipv4-address* | "["i*pv6-address*"]" }[:*port*]|
ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x: [0 to FFFF]H
	d: [0 to 255]D
	interface - 32 characters max, for link local addresses
port	[0 to 65535]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

cflash-id cf1: | cf1-A: | cf2: | cf2-A: | cf3: | cf3-A:

create-destination — Specifies that a non-existent directory structure that is explicitly entered as the destination file URL is created as part of the unzip operation. This parameter is required to create new directories.

list — Lists the content of the ZIP file without performing the unzip operation.

force — Overwrites without prompting, any file or directory contained within the ZIP file that already exists in the destination URL. This keyword does not automatically create new directories explicitly specified by *dest-file-url*. To create these directories, use the **create-destination** flag.

Platforms All

25.49 up

up

Syntax **up ip** *seconds*
no up ip
up ipv6 *seconds*
no up ipv6

Context **[Tree]** (config>service>ies>if>hold-time up)
[Tree] (config>service>ies>sub-if>hold-time up)
[Tree] (config>service>ies>red-if>hold-time up)
[Tree] (config>service>vpls>if>hold-time up)
[Tree] (config>service>vprn>if>hold-time up)
[Tree] (config>service>vprn>nw-if>hold-time up)
[Tree] (config>service>vprn>sub-if>hold-time up)
[Tree] (config>service>vprn>red-if>hold-time up)

Full Context configure service ies interface hold-time up
configure service ies redundant-interface hold-time up
configure service ies subscriber-interface hold-time up
configure service vpls interface hold-time up
configure service vprn interface hold-time up
configure service vprn network-interface hold-time up
configure service vprn redundant-interface hold-time up
configure service vprn subscriber-interface hold-time up

Description This command causes a delay in the deactivation of the associated IP interface by the specified number of seconds. The delay is invoked whenever the system attempts to bring the associated IP interface down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the command from the active configuration and removes the delay in deactivating the associated IP interface. If the configuration is removed during a delay period, the currently running delay will continue until it expires.

Default no up ip

Parameters *seconds* — The time delay, in seconds, to make the interface operational.

Values 1 to 1200

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface hold-time up
- configure service vprn redundant-interface hold-time up
- configure service ies subscriber-interface hold-time up
- configure service ies redundant-interface hold-time up

All

- configure service vprn network-interface hold-time up
- configure service vpls interface hold-time up
- configure service vprn interface hold-time up
- configure service ies interface hold-time up

25.50 up-count

up-count

Syntax **up-count** *up-count*
no up-count

Context **[Tree]** (config>port>sonet-sdh>path>cisco-hdlc up-count)
[Tree] (config>port>tdm>ds1>channel-group>cisco-hdlc up-count)
[Tree] (config>port>tdm>ds3>cisco-hdlc up-count)
[Tree] (config>port>tdm>e1>channel-group>cisco-hdlc up-count)
[Tree] (config>port>tdm>e3>cisco-hdlc up-count)

Full Context configure port sonet-sdh path cisco-hdlc up-count
configure port tdm ds1 channel-group cisco-hdlc up-count
configure port tdm ds3 cisco-hdlc up-count
configure port tdm e1 channel-group cisco-hdlc up-count
configure port tdm e3 cisco-hdlc up-count

Description This command configures the number of continual keepalive packets that have to be received in order to declare the link up. It is expected that the nodes at the two endpoints of the cHDLC link are provisioned with the same values.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default up-count 1

Parameters *up-count* — Specifies the number of continual keepalive packets that must be received in order to declare the link up.

Values 1 to 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path cisco-hdlc up-count

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

- configure port tdm ds3 cisco-hdlc up-count
- configure port tdm ds1 channel-group cisco-hdlc up-count
- configure port tdm e1 channel-group cisco-hdlc up-count
- configure port tdm e3 cisco-hdlc up-count

25.51 up-link

up-link

Syntax **up-link gbr** *rate* **mbr** *rate*
no up-link

Context **[Tree]** (config>subscr-mgmt>gtp>peer-profile>ggsn>qos up-link)
[Tree] (config>subscr-mgmt>gtp>peer-profile>pgw>qos up-link)
[Tree] (config>subscr-mgmt>gtp>peer-profile>mme>qos up-link)

Full Context configure subscriber-mgmt gtp peer-profile ggsn qos up-link
configure subscriber-mgmt gtp peer-profile mme qos up-link
configure subscriber-mgmt gtp peer-profile pgw qos up-link

Description This command configures the up-link bitrate in kb/s to be used in the GTP messages.

The **no** form of this command reverts to the default.

Default up-link gbr 5000 mbr 5000 - for ggsn

up-link gbr 0 mbr 0 - for mme and pgw

Parameters **gbr** *rate* — Specifies the uplink Guaranteed Bit Rate (GBR) to be used in the GTP messages as QOS IE (GTPv1) or Bearer QOS (GTPv2).

mbr *rate* — Specifies the uplink Maximum Bit Rate (MBR) to be used in the GTP messages as QOS IE (GTPv1) or Bearer QOS (GTPv2).

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.52 up-nat-policy

up-nat-policy

Syntax **up-nat-policy** *name* [**create**]

Context **[Tree]** (config>service>nat up-nat-policy)

Full Context configure service nat up-nat-policy

Description This command creates a NAT policy template for BNG CUPS UPF. This template is instantiated for a set of subscribers sharing in a NAT pool. The policy includes parameters that define the BNG CUPS UPF NAT behavior, such as, but not limited to, the following:

- ALGs
- filtering mode
- watermarks
- ports and NAT flow limits
- priority NAT flows
- protocol timers

When the BNG CPF does not receive the NAT policy template, a default template takes effect if it is configured on the BNG UPF. The name of the default NAT policy template on the BNG UPF must equal default.

Parameters **create** — Keyword required to create a new NAT policy for BNG CUPS UPF.

name — Specifies the UP NAT policy name, up to 32 characters. The name default has a special meaning representing the default NAT policy template. The system uses the default template when the BNG CPF does not receive a more specific name when the subscriber is instantiated.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.53 up-resiliency

up-resiliency

Syntax **up-resiliency**

Context **[Tree]** (config>subscr-mgmt up-resiliency)

Full Context configure subscriber-mgmt up-resiliency

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure the inter-UPF resiliency in a CUPS system.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

up-resiliency

Syntax **up-resiliency**

Context **[Tree]** (config>service>ies>subscriber-mgmt up-resiliency)
[Tree] (config>service>vprn>subscriber-mgmt up-resiliency)
[Tree] (config>service>vpls>sap>pfcp up-resiliency)

Full Context configure service ies subscriber-mgmt up-resiliency
configure service vpls sap pfcp up-resiliency
configure service vprn subscriber-mgmt up-resiliency

Description Commands in this context configure inter-UPF resiliency service parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.54 up-threshold

up-threshold

Syntax **up-threshold** *percent-change* [**bw** *absolute-change*]

Context **[Tree]** (config>router>rsvp>dbw-accounting up-threshold)

Full Context configure router rsvp dbw-accounting up-threshold

Description This command sets the minimum change (in percent of the latest advertised value) above which an increase in MRLB (IS-IS TE sub-TLV 10) or MRB (OSPF TE sub-TLV 7) triggers an IGP-TE update. This configuration only applies to a change in MRLB or MRB caused by dark bandwidth. Other events affecting MRLB or MRB (such as the change of the subscription factor or the loss of link in a LAG over which the RSVP interface is defined) trigger an immediate TE update, regardless of the importance of the impact.

Optionally, the threshold can also be expressed as an absolute value. In this case, the evaluation of the change is made using the percent change and the absolute change. An IGP-TE update is sent if both of these thresholds are crossed. Changing this parameter in the course of dark bandwidth accounting does not affect the accounting cycle.

Default up-threshold 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *percent-change* — Specifies the minimum increase in MRLB/MRB, expressed in percent.

Values 0 to 100

absolute-change — Specifies the minimum increase in MRLB/MRB, expressed in Mb/s.

Values 0 to 1000000

25.55 update

update

Syntax **update** [**neighbor** *ip-address* | **group** *name*]
no update

Context **[Tree]** (debug>router>bgp update)

Full Context debug router bgp update

Description This command decodes and logs all sent and received update messages in the debug log.

The **no** form of this command disables debugging.

Parameters **neighbor** *ip-address* — Debugs only events affecting the specified BGP neighbor.

Values ipv4-address:
- a.b.c.d (host bits must be 0)

ipv6-address:
- x:x:x:x:x:x:x:x [-interface] (eight 16-bit pieces)
- x:x:x:x:x:x:d.d.d.d [-interface]
- x: [0 to FFFF]H
- d: [0 to 255]D
- interface: up to 32 characters for link local addresses

group *name* — Debugs only events affecting the specified peer group name, up to 64 characters, and associated neighbors.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.56 update-fault-tolerance

update-fault-tolerance

Syntax [**no**] **update-fault-tolerance**

Context **[Tree]** (config>service>vprn>bgp>error-handling update-fault-tolerance)
[Tree] (config>service>vprn>bgp>group>error-handling update-fault-tolerance)
[Tree] (config>service>vprn>bgp>group>neighbor>error-handling update-fault-tolerance)

Full Context configure service vprn bgp error-handling update-fault-tolerance
configure service vprn bgp group error-handling update-fault-tolerance
configure service vprn bgp group neighbor error-handling update-fault-tolerance

Description This command enables **treat-as-withdraw** and other similarly non-disruptive approaches for handling a wide range of UPDATE message errors, as long as there are no length errors that prevent all of the NLRI fields from being correctly identified and parsed.

Default no update-fault-tolerance

Platforms All

update-fault-tolerance

Syntax [**no**] **update-fault-tolerance**

Context **[Tree]** (config>router>bgp>error-handling update-fault-tolerance)
[Tree] (config>router>bgp>group>error-handling update-fault-tolerance)
[Tree] (config>router>bgp>group>neighbor>error-handling update-fault-tolerance)

Full Context configure router bgp error-handling update-fault-tolerance
configure router bgp group error-handling update-fault-tolerance
configure router bgp group neighbor error-handling update-fault-tolerance

Description This command enables **treat-as-withdraw** and other similarly non-disruptive approaches for handling a wide range of UPDATE message errors, as long as there are no length errors that prevent all of the NLRI fields from being correctly identified and parsed.

Default no update-fault-tolerance

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.57 update-interval

update-interval

Syntax **update-interval** [**hrs** *hours*] [**min** *minutes*] [**days** *days*]
no update-interval

Context [Tree] (config>service>dynsvc>acct-1 update-interval)
[Tree] (config>service>dynsvc>acct-2 update-interval)

Full Context configure service dynamic-services dynamic-services-policy accounting-1 update-interval
configure service dynamic-services dynamic-services-policy accounting-2 update-interval

Description This command specifies the interval between each RADIUS Accounting Interim-Update message (minimum 5 minutes; maximum 180 days).

The **no** form of this command disables the sending of Accounting Interim-Update messages.

A RADIUS specified Accounting Interim Interval overrides the CLI configured value.

Default no update-interval (do not send Accounting Interim-Update messages)

Parameters *hrs* — specifies the interval in hours.

Values 1 to 23

min — Specifies the interval in minutes.

Values 1 to 59

days — specifies the interval in days.

Values 1 to 180

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

update-interval

Syntax **update-interval** [**hrs** *hours*] [**min** *minutes*] [**days** *days*]
no update-interval

Context [Tree] (config>service>dynsvc>ladb>user>idx>acct update-interval)

Full Context configure service dynamic-services local-auth-db user-name index accounting update-interval

Description This command specifies the time between each dynamic data service accounting interim update for this accounting destination. This command overrides the local configured value in the dynamic services policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the generation of interim accounting updates to this destination.

The minimum update interval is 5 minutes.

Parameters *hours* — Specifies the interval in hours.

Values 1 to 23

minutes — Specifies the interval in minutes.

Values 1 to 59

days — Specifies the interval in days.

Values 1 to 180

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

update-interval

Syntax **update-interval** *minutes*
no update-interval

Context **[Tree]** (config>subscr-mgmt>acct-plcy update-interval)

Full Context configure subscriber-mgmt radius-accounting-policy update-interval

Description This command specifies the interval at which accounting data of subscriber hosts is updated in a RADIUS Accounting Interim-Update message. Requires interim-update to be enabled when specifying the accounting mode in the radius accounting policy.

A RADIUS specified interim interval (attribute [85] Acct-Interim-Interval) overrides the CLI configured value.

The **no** form of this command reverts to the default.

Parameters *minutes* — Specifies the interval, in minutes, at which accounting data of subscriber hosts is updated.

Values 5 to 259200

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

update-interval

Syntax **update-interval** *minutes* [**jitter** *seconds*]
no update-interval

Context **[Tree]** (config>ipsec>rad-acct-plcy update-interval)

Full Context configure ipsec radius-accounting-policy update-interval

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the system to send RADIUS interim-update packets for IKEv2 remote-access tunnels. The RADIUS attributes in the interim-update packet are the same as acct-start. The value of the Acct-status-type in the interim-update message is 3.

Default update-interval 10

Parameters *minutes* — Specifies the interval in minutes.

Values 5 to 259200

seconds — Specifies the jitter as the number of seconds when the system sends each interim-update packet.

Values 0 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.58 update-interval-jitter

update-interval-jitter

Syntax **update-interval-jitter absolute** *seconds*
no update-interval-jitter

Context **[Tree]** (config>service>dynsvc>acct-1 update-interval-jitter)
[Tree] (config>service>dynsvc>acct-2 update-interval-jitter)

Full Context configure service dynamic-services dynamic-services-policy accounting-1 update-interval-jitter
configure service dynamic-services dynamic-services-policy accounting-2 update-interval-jitter

Description This command specifies the absolute maximum random delay introduced on the update interval between two RADIUS Accounting Interim Update messages. The effective maximum random delay value is the minimum of the configured absolute jitter value and 10% of the configured update-interval.

A value of zero sends the accounting interim update message without introducing an additional random delay.

The **no** form of this command sets the default to 10% of the configured update-interval.

Default no update-interval-jitter (10% of the configured update-interval)

Parameters *seconds* — Specifies the absolute maximum jitter value in seconds.

Values 0 to 3600

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

update-interval-jitter

Syntax **update-interval-jitter absolute** *seconds*
no update-interval-jitter

Context **[Tree]** (config>subscr-mgmt>acct-plcy update-interval-jitter)

Full Context configure subscriber-mgmt radius-accounting-policy update-interval-jitter

Description This command specifies the absolute maximum random delay introduced on the update interval between two accounting interim update messages. The effective maximum random delay value is the minimum of the configured absolute jitter value and 10% of the configured update-interval.

A value of zero will send the accounting interim update message without introducing an additional random delay.

The **no** form of this command sets the default to 10% of the configured update-interval.

Parameters *seconds* — Specifies the absolute maximum jitter value in seconds.

Values 0 to 36000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.59 update-timer

update-timer

Syntax **update-timer** *seconds*
no update-timer

Context **[Tree]** (config>router>rsvp>te-threshold-update update-timer)

Full Context configure router rsvp te-threshold-update update-timer

Description This command is to control timer-based IGP TE updates. Timer-based IGP updates can be enabled by specifying a non-zero time value. Default value of update-timer is 0.

The **no** form of this command should reset update-timer to the default value and disable timer-based IGP update.

Default no update-timer

Parameters *seconds* — Specifies the time in seconds.

Values 0 to 300

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.60 updated-error-handling

updated-error-handling

Syntax [**no**] **updated-error-handling**

Context **[Tree]** (config>service>vprn>bgp>group updated-error-handling)
[Tree] (config>service>vprn>bgp>group>neighbor updated-error-handling)

Full Context configure service vprn bgp group neighbor updated-error-handling
configure service vprn bgp group updated-error-handling

Description This command controls whether SR OS utilizes the new neighbor-complete bit when processing optional transitive path attributes and advertising them to the associated BGP neighbor.

This command also control if SR OS utilizes the error handling mechanism for optional-transitive path attributes.

Default no updated-error-handling

25.61 updates

updates

Syntax [**no**] **updates** [**neighbor** *ip-int-name* | *ip-address*]

Context **[Tree]** (debug>router>rip updates)

Full Context debug router rip updates

Description This command enables debugging for RIP updates.

Parameters *ip-int-name* **|** *ip-address* — Debugs the RIP updates sent on the neighbor IP address or interface.

Platforms All

updates

Syntax [**no**] **updates** [**neighbor** *ip-int-name* | *ipv6-address*]

Context **[Tree]** (debug>router>ripng updates)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context debug router ripng updates

Description This command enables debugging for RIP updates.

Parameters *ip-int-name* | *ipv6-address* — Debugs the RIP updates sent on the neighbor IP address or interface.

Platforms All

25.62 upf-data-endpoint

upf-data-endpoint

Syntax **upf-data-endpoint interface** *interface-name* **fpe** *fep-id*
no upf-data-endpoint

Context **[Tree]** (config>router>gtp upf-data-endpoint)
[Tree] (config>service>vprn>gtp upf-data-endpoint)

Full Context configure router gtp upf-data-endpoint
configure service vprn gtp upf-data-endpoint

Description This command configures the GTP - User Plane (GTP-U) endpoint used by BNG CUPS FWA sessions.

The **no** form of the command disables GTP-U termination for BNG CUPS FWA sessions.

Default no upf-data-endpoint

Parameters *interface-name* — Specifies an interface name on which GTP-U packets terminate. The name must start with a letter and can be up to 32 characters.

fpe-id — Specifies the forwarding path extension (FPE) ID used to encapsulate and decapsulate GTP-U traffic.

Values 1 to 64

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.63 upgrade

upgrade

Syntax **upgrade** *index* **path** *upgrade-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no upgrade *index*

Context [Tree] (config>card upgrade)
[Tree] (config>card>mda upgrade)
[Tree] (config>card>xiom upgrade)

Full Context configure card mda upgrade
configure card upgrade
configure card xiom upgrade

Description This command assigns a license level upgrade to the card, XIOM, or XMA. There can be multiple upgrades applied to a card, XIOM, or XMA. The first upgrade must use index 1 and then next index 2 and so on. Also, when removing upgrades, the largest index must be removed first and then the next largest removed and so on.

The path indicates the starting level and the new level that will apply due to the upgrade. For example, "cr1200g-cr1600g" can be applied to an XMA that is currently at the cr1200g level and after application of the upgrade, the operational level of the XMA shall be cr1600g.

There must be an upgrade license available for the path specified. Available upgrades can be checked using the **show licensing entitlements** command.

Note: Some upgrades require a hard reset of the card or MDA to take effect. In general, this is required when the Full Duplex bandwidth is being changed.

Parameters *index* — Specifies the order of the upgrade.

Values 1 to 6

upgrade-name — Specifies the upgrade name to be applied, up to 32 characters.

Platforms 7450 ESS, 7750 SR

- configure card upgrade

7750 SR-s

- configure card xiom upgrade

7750 SR-s, 7950 XRS

- configure card mda upgrade

upgrade

Syntax **upgrade**

Context [Tree] (admin>app-assure upgrade)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context admin application-assurance upgrade

Description Use this command to load a new isa-aa.tim file as part of a router-independent signature upgrade. An AA ISA reboot is required.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.64 uplink

uplink

Syntax [**no**] **uplink**

Context **[Tree]** (config>router>gtp uplink)
[Tree] (config>service>vprn>gtp uplink)

Full Context configure router gtp uplink
configure service vprn gtp uplink

Description This command enables GTP configuration related to a GTP uplink using the Gn, S2a, or S2b interface.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

uplink

Syntax **uplink arbiter** *arbiter-name*
uplink policer *policer-id*
uplink queue *queue-id*
uplink scheduler *scheduler-name*
no uplink

Context **[Tree]** (config>subscr-mgmt>gtp>apn-policy>apn>ambr-qos-mapping uplink)

Full Context configure subscriber-mgmt gtp apn-policy apn ambr-qos-mapping uplink

Description When enabled, the uplink rate in the APN-AMBR IE in an incoming GTP message is interpreted as a rate override for the specified ingress QoS object. For queues and policers, the PIR is overridden.

This override uses standard SR OS QoS overrides. Therefore, a subsequent Gx/ RADIUS-based override removes this override.

The **no** form of this command disables the override mechanism.

Default no uplink

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *arbiter-name* — Specifies the name of the arbiter to be overridden, up to 32 characters.

policer-id — Specifies the ID of the policer to be overridden.

Values 1 to 63

queue-id — Specifies the ID of the queue to be overridden.

Values 1 to 32

scheduler-name — Specifies the name of the scheduler to be overridden, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

uplink

Syntax **uplink** *port-id*
uplink system-default
uplink none

Context **[Tree]** (config>system>satellite>port-template>port uplink)

Full Context configure system satellite port-template port uplink

Description This command configures the uplink association to be used for the associated satellite port.

Parameters *port-id* — Specifies the satellite physical port ID. This must use the format *slot*/*mda*/*port*. All satellites have a single slot and a single MDA, so these values will always be 1. For example, port 10 would be specified as 1/1/10.

system-default — Specifies that the uplink association is returned to the system default.

none — Clears the uplink association.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

25.65 uplink-forwarding-while-standby

uplink-forwarding-while-standby

Syntax [**no**] **uplink-forwarding-while-standby**

Context **[Tree]** (config>subscr-mgmt>up-resiliency>fsg-template uplink-forwarding-while-standby)

Full Context configure subscriber-mgmt up-resiliency fate-sharing-group-template uplink-forwarding-while-standby

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command allows a standby BNG UPF to forward uplink traffic. To prevent the possibility of packet replication towards the network, this command should only be enabled if the access network is provisioned not to replicate unicast packets to the BNG UPF.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.66 uplink-initial-wait

uplink-initial-wait

Syntax **uplink-initial-wait** *seconds*

Context **[Tree]** (config>subscr-mgmt>vrgw>brg>brg-profile uplink-initial-wait)

Full Context configure subscriber-mgmt vrgw brg brg-profile uplink-initial-wait

Description This command specifies how long to wait for the uplink to fully establish when using a non-routed uplink such as a PPPoE client. During this initial wait time, setup of devices in the home is blocked.

After the timer expires, if an uplink was successful on only one of two IP stacks, devices continue to be configured with the successful IP stack. Control plane message for the failed IP stack are dropped.

Default uplink-initial-wait 30

Parameters *seconds* — Specifies the timeout in seconds.

Values 10 to 300

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.67 uplink-mbr-gbr

uplink-mbr-gbr

Syntax **uplink-mbr-gbr arbiter** *arbiter-name*
uplink-mbr-gbr policer *policer-id*
uplink-mbr-gbr queue *queue-id*
uplink-mbr-gbr scheduler *scheduler-name*
no uplink-mbr-gbr

Context **[Tree]** (config>subscr-mgmt>sla-prof>pfcp>seq uplink-mbr-gbr)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure subscriber-mgmt sla-profile pfcp-mappings session-qer uplink-mbr-gbr

Description This command configures the uplink MBR/GBR to QoS override mapping.

The **no** form of the command disables the uplink MBR/GBR mapping.

Default no uplink-mbr-gbr

Parameters *arbiter-name* — Specifies the arbiter target of the MBR/GBR override. The arbiter name can be up to 32 characters.

policer-id — Specifies the policer ID target of the MBR/GBR override.

Values 1 to 63

queue-id — Specifies the queue ID target of the MBR/GBR override.

Values 1 to 8

scheduler-name — Specifies the scheduler name target of the MBR/GBR override. The scheduler name can be up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.68 upnp

upnp

Syntax **upnp**

Context **[Tree]** (config>service upnp)

Full Context configure service upnp

Description Commands in this context configure UPnP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.69 upnp-mappings

upnp-mappings

Syntax **upnp-mappings** [*upnp-mappings*]
no upnp-mappings

Context **[Tree]** (config>isa>wlan-gw-group>nat>session-limits upnp-mappings)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure isa wlan-gw-group nat session-limits upnp-mappings

Description This command limits the number of Universal Plug 'n Play mappings per member

The **no** form of this command reverts to the default value.

Default upnp-mappings 524288

Parameters *upnp-mappings* — specifies, for each MDA in this ISA group, the maximum number of Universal Plug 'n Play (UPnP) mappings.

Values 1 to 524288

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

upnp-mappings

Syntax **upnp-mappings** *limit* **no upnp-mappings**

Context **[Tree]** (config>isa>nat-group>session-limits upnp-mappings)

Full Context configure isa nat-group session-limits upnp-mappings

Description This command specifies the maximum number of UPnP mappings per ISA.

Default 524288

Parameters *limit* — Specifies the maximum number of UPnP mappings.

Values 1 to 524288

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.70 upnp-policy

upnp-policy

Syntax **upnp-policy** *policy-name* [**create**]
no upnp-policy *policy-name*

Context **[Tree]** (config>service>upnp upnp-policy)

Full Context configure service upnp upnp-policy

Description This command creates a new upnp-policy or enters the configuration context of an existing upnp-policy.

The **no** form of the command removes the upnp-policy policy-name from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default none

Parameters *policy-name* — Specifies the name of the UPnP policy up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

upnp-policy

Syntax **upnp-policy** *policy-name*
no upnp-policy

Context **[Tree]** (config>subscr-mgmt>sub-prof upnp-policy)

Full Context configure subscriber-mgmt sub-profile upnp-policy

Description This command enables UPnP IGD services for the subscriber. All ESM hosts of the subscriber could use the UPnP protocol to create port mapping. This feature only support L2-Aware NAT host.

UPnP parameters are defined in the referenced upnp-policy configured in the **config> service>upnp** context.

Default no upnp-policy

Parameters *policy-name* — Specifies the UPnP policy associated with this subscriber profile up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.71 upstream-ip-filter

upstream-ip-filter

Syntax **upstream-ip-filter** *filter-id*
no upstream-ip-filter

Context **[Tree]** (config>service>vprn>nat>outside upstream-ip-filter)
[Tree] (config>router>nat>outside upstream-ip-filter)

Full Context configure router nat outside upstream-ip-filter
configure service vprn nat outside upstream-ip-filter

Description This command configures the ip-filter for upstream traffic. This filter is applied to the upstream traffic after the NAT function and before it enters the outside virtual router instance; it is useful for traffic that bypasses the ingress filters applied in the inside virtual router instance, such as DS-Lite traffic.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no upstream-ip-filter

Parameters *filter-id* — Specifies the identifier of an IP filter.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.72 upstream-ipv6-filter

upstream-ipv6-filter

Syntax **upstream-ipv6-filter** *filter-id*
no upstream-ipv6-filter

Context **[Tree]** (config>router>nat>outside upstream-ipv6-filter)
[Tree] (config>service>vprn>nat>outside upstream-ipv6-filter)

Full Context configure router nat outside upstream-ipv6-filter
configure service vprn nat outside upstream-ipv6-filter

Description This command configures the ipv6-filter for upstream traffic. This filter is applied to the upstream traffic after the NAT function and before it enters the outside virtual router instance. This is useful for shared v6 filters that apply to all v6 DSM hosts.

Default no upstream-ipv6-filter

Parameters *filter-id* — Specifies the identifier of an ipv6-filter.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.73 url

url

Syntax **url** *rdr-url-sting*
no url

Context **[Tree]** (config>subscr-mgmt>http-rdr-plcy url)

Full Context configure subscriber-mgmt http-redirect-policy url

Description This command configures the HTTP URL to re-direct the matching traffic to. It also can specify inclusion of original URL, MAC address and IP address of the subscriber in the redirect URL.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *rdr-url-sting* — Specifies the URL to redirect to.

Values		
rdr-url-string		Up to 255 characters
macro substitutions:		
	$URL	Request-URI in the HTTP GET Request received
	$MAC	A string that represents the MAC address of the subscriber host
	$IP	A string that represents the IP address of the subscriber host

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

url

Syntax **url** *url-string* [**service-id** *service-id*]
url *url-string* [**service-name** *service-name*]
no url

Context **[Tree]** (config>system>security>pki>ca-profile>cmpv2 url)

Full Context configure system security pki ca-profile cmpv2 url

Description This command specifies HTTP URL of the CMPv2 server. The URL must be unique across all configured ca-profiles.

The URL will be resolved by the DNS server configured (if configured) in the corresponding router context.

If the *service-id* is 0 or omitted, then system will try to resolve the FQDN via DNS server configured in bof.cfg. After resolution, the system will connect to the address in management routing instance first, then base routing instance.

If the service is VPRN, then the system only allows HTTP ports 80 and 8080.

Default no url

Parameters *url-string* — Specifies the HTTP URL of the CMPv2 server up to 180 characters.

service-id *service-id* — Specifies the service instance that used to reach CMPv2 server.

Values Service ID: 1 to 2147483647
base-router: 0

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

url

Syntax **url** *url*
no url

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update>crl-urls>url-entry url)

Full Context configure system security pki ca-profile auto-crl-update crl-urls url-entry url

Description This command specifies the HTTP URL of the CRL file for the **url-entry**. The system supports both IPv4 and IPv6 HTTP connections.

Note: The URL must point to a DER encoded CRL.

Default no url

Parameters *url* — Specifies the URL, which specifies the location, where an updated CRL can be downloaded from.

Platforms All

url

Syntax **url** *url-string* [**service-id** *service-id*]
url *url-string* [**service-name** *service-name*]
no url

Context **[Tree]** (config>system>security>pki>ca-profile>cmp2 url)

Full Context configure system security pki ca-profile cmp2 url

Description This command specifies HTTP URL of the CMPv2 server. The URL must be unique across all configured ca-profiles.

The URL will be resolved by the DNS server configured (if configured) in the corresponding router context.

If the *service-id* is 0 or omitted, then system will try to resolve the FQDN via DNS server configured in bof.cfg. After resolution, the system will connect to the address in management routing instance first, then base routing instance.

Note: If the service is VPRN, then the system only allows HTTP ports 80 and 8080.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *url-string* — Specifies the HTTP URL of the CMPv2 server, up to 180 characters.

service-id *service-id* — Specifies the service instance that used to reach CMPv2 server.

This variant of this command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **url** *url-string* **service-name** *service-name* variant can be used in all configuration modes.

Values service-id: 1 to 2147483647 base-router: 0

service-name *service-name* — Identifies the service, up to 64 characters.

25.74 url-entry

url-entry

Syntax **url-entry** *entry-id* [**create**]
no url-entry *entry-id*

Context **[Tree]** (config>system>security>pki>ca-prof>auto-crl-update>crl-urls url-entry)

Full Context configure system security pki ca-profile auto-crl-update crl-urls url-entry

Description This command creates a new **crl-url** entry with the **create** parameter, or enters an existing url-entry configuration context without **create** parameter.

The **no** form of this command removes the specified entry.

Parameters *entry-id* — Specifies a URL configured on this system.

Values 1 to 8

create — Creates an auto URL entry.

Platforms All

25.75 url-filter

url-filter

Syntax **url-filter** *url-filter-name* [**characteristic** *characteristic-name*]
no url-filter

Context **[Tree]** (config>app-assure>group>aqp>entry>action url-filter)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group app-qos-policy entry action url-filter

Description This command configures a url-filter action for flows matching this entry.

Parameters *url-filter-name* — Specifies the name of the url-filter policy.

characteristic-name — Specifies the name of the characteristic.

url-filter

Syntax **url-filter** *url-filter-name* [**create**]
no url-filter *url-filter-name*

Context **[Tree]** (config>app-assure>group url-filter)

Full Context configure application-assurance group url-filter

Description This command configures a URL filter action for flows of a specific type matching this entry.

If no URL filters are specified then no URL filters will be evaluated.

Parameters *url-filter-name* — Specifies the Application-Assurance URL filter that will be evaluated.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.76 url-list

url-list

Syntax **url-list** *url-list-name* [**create**]
no url-list *url-list-name*

Context **[Tree]** (config>app-assure>group url-list)

Full Context configure application-assurance group url-list

Description This command configures a url-list object. The url-list points to a file containing a list of URLs located on the system Compact Flash. The url-list is then referenced in a url-filter object in order to filter and redirect subscribers when a URL from this file is accessed.

The **no** form of this command removes the url-list object.

Parameters *url-list-name* — Specify the Application-Assurance url-list

create — Keyword used to create the URL list.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

url-list

Syntax **url-list** *url-list-name* **upgrade**

Context **[Tree]** (admin>app-assure>group url-list)

Full Context admin application-assurance group url-list

Description This command upgrades the URL list.

Parameters *url-list-name* — Specifies the application assurance URL list, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.77 urpf-check

urpf-check

Syntax [**no**] **urpf-check**

Context **[Tree]** (config>service>ies>if urpf-check)
[Tree] (config>service>ies>if>ipv6 urpf-check)
[Tree] (config>service>ies>sub-if>grp-if>ipv6 urpf-check)
[Tree] (config>service>vprn>if urpf-check)
[Tree] (config>service>vprn>nw-if urpf-check)
[Tree] (config>service>vprn>if>ipv6 urpf-check)
[Tree] (config>service>vprn>sub-if>grp-if urpf-check)

Full Context configure service ies interface ipv6 urpf-check
configure service ies interface urpf-check
configure service ies subscriber-interface group-interface ipv6 urpf-check
configure service vprn interface ipv6 urpf-check
configure service vprn interface urpf-check
configure service vprn network-interface urpf-check
configure service vprn subscriber-interface group-interface urpf-check

Description This command enables unicast RPF (uRPF) check on this interface.

The **no** form of this command disables unicast RPF (uRPF) Check on this interface.

Default no urpf-check

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface urpf-check
- configure service ies subscriber-interface group-interface ipv6 urpf-check

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service ies interface urpf-check
- configure service vprn network-interface urpf-check
- configure service vprn interface urpf-check
- configure service vprn interface ipv6 urpf-check
- configure service ies interface ipv6 urpf-check

urpf-check

Syntax [**no**] **urpf-check**

Context **[Tree]** (config>subscr-mgmt>git>ipv4 urpf-check)

Full Context configure subscriber-mgmt group-interface-template ipv4 urpf-check

Description This command enables the uRPF check on this interface.

The **no** form of this command disables the uRPF check on this interface.

Default no urpf-check

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

urpf-check

Syntax **urpf-check**
no urpf-check

Context **[Tree]** (config>service>vprn>network>ingress urpf-check)

Full Context configure service vprn network ingress urpf-check

Description This command enables the unicast RPF (uRPF) check of network ingress traffic to include traffic associated with the VPRN if the incoming network interface is configured with the **urpf-selected-vprns** command

If the command is not configured, then traffic associated with this VPRN that arrives on a network interface with **urpf-selected-vprns** configured bypasses the uRPF checking options specified for that network interface.

Default no urpf-check

Platforms All

urpf-check

Syntax [**no**] **urpf-check**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>router>if urpf-check)
[Tree] (config>router>if>ipv6 urpf-check)

Full Context configure router interface ipv6 urpf-check
configure router interface urpf-check

Description This command enables unicast RPF (uRPF) Check on this interface.

The **no** form of this command disables unicast RPF (uRPF) Check on this interface.

Platforms All

25.78 urpf-selected-vprns

urpf-selected-vprns

Syntax [**no**] **urpf-selected-vprns**

Context [Tree] (config>router>if urpf-selected-vprns)

Full Context configure router interface urpf-selected-vprns

Description This command enables uRPF checking of incoming traffic on the network interface for the following packets.

- Packets associated with the global routing table (base router) context.
- Packets associated with VPRNs that have enabled the uRPF check using the **config**>**service**>**vprn**>**network**>**ingress**>**urpf-check** command.

If the command is not configured, the default action is to perform uRPF checks for all ingress traffic on the network interface (associated with the base router and all VPRNs) based on the IPv4 and IPv6 **urpf-check** configuration options of the network interface.

Default no urpf-selected-vprns

Platforms All

25.79 usage-monitoring

usage-monitoring

Syntax [**no**] **usage-monitoring**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>statistics>aa-sub usage-monitoring)

Full Context configure application-assurance group statistics aa-sub usage-monitoring

Description This command enables Gx usage monitoring the given AA group/partition. It can only be enabled if there is enough usage monitoring resources for all existing subs. Once disabled, all monitoring instances for AA subscribers are silently removed (no PCRF notifications) and all subsequent AA Gx usage monitoring messages are ignored.

Default no usage-monitoring.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.80 use-arp

use-arp

Syntax [**no**] **use-arp**

Context [Tree] (config>service>vprn>if>dhcp use-arp)
[Tree] (config>service>ies>if>dhcp use-arp)

Full Context configure service ies interface dhcp use-arp
configure service vprn interface dhcp use-arp

Description This command enables the use of ARP to determine the destination hardware address.

The **no** form of this command disables the use of ARP to determine the destination hardware address.

Platforms All

25.81 use-bgp-routes

use-bgp-routes

Syntax [**no**] **use-bgp-routes**

Context [Tree] (config>service>vprn>bgp>next-hop-res use-bgp-routes)

Full Context configure service vprn bgp next-hop-resolution use-bgp-routes

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the use of BGP routes to resolve BGP next hops. When this command is enabled, any unlabeled IPv4 or IPv6 BGP route received from a VPRN BGP peer becomes resolvable by up to four other BGP routes in order to resolve the route to a VPRN IP interface.

This command also allows unlabeled IPv4 or IPv6 BGP routes leaked from the GRT with unresolved next hops (in the GRT) to be resolvable by BGP-VPN routes (of the VPRN).

The **no** form of this command reverts to the default behavior. By default, a VPRN BGP route is not resolvable by another VPRN BGP route or by a BGP-VPN route.

Default no use-bgp-routes

Platforms All

use-bgp-routes

Syntax [**no**] **use-bgp-routes**

Context **[Tree]** (config>router>bgp>next-hop-res use-bgp-routes)

Full Context configure router bgp next-hop-resolution use-bgp-routes

Description This command specifies whether to use BGP routes to recursively resolve the BGP next-hop of unlabeled IPv4 and unlabeled IPv6 routes. Up to four levels of recursion are supported.

The **no** form of this command reverts to the default behavior. By default, a BGP route is not resolvable by another BGP route.

Default no use-bgp-routes

Platforms All

use-bgp-routes

Syntax **use-bgp-routes**

Context **[Tree]** (config>router>bgp>next-hop-res>lbl-routes use-bgp-routes)

Full Context configure router bgp next-hop-resolution labeled-routes use-bgp-routes

Description Commands in this context configure labeled route options for next-hop resolution.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.82 use-broadcast-address

use-broadcast-address

Syntax [**no**] **use-broadcast-address**

Context **[Tree]** (config>port>ethernet>dwl use-broadcast-address)

Full Context configure port ethernet down-when-looped use-broadcast-address

Description This command specifies whether or not the down when looped destination MAC address is the broadcast address, or the local port MAC address, as specified in the port's MAC address.

Platforms All

25.83 use-broadcast-mac

use-broadcast-mac

Syntax [**no**] **use-broadcast-mac**

Context **[Tree]** (config>service>ipipe>sap use-broadcast-mac)

Full Context configure service ipipe sap use-broadcast-mac

Description This command enables the user of a of broadcast MAC on SAP.

An Ipipe VLL service with the command enabled forwards unicast IP packets using the broadcast MAC address until the ARP cache is populated with a valid entry for the CE IP and MAC addresses.

The **no** form of this command enables the user of a of broadcast MAC on SAP.

Default no use-broadcast-mac

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.84 use-def-mcast

use-def-mcast

Syntax [**no**] **use-def-mcast**

Context **[Tree]** (config>service>vpls>isid-policy>entry use-def-mcast)

Full Context configure service vpls isid-policy entry use-def-mcast

Description The **use-def-mcast** option prevents local installation of the ISIDs in the range in the MFIB and uses the default multicast tree instead for a B-VPLS. In a node that does not have I-VPLS or static-isids, this command prevents the building of an MFIB entry for this ISID when received in a SPBM TLV and allows the broadcast of ISID based traffic on the default multicast tree. If an **isid-policy** exists, the core nodes can have this policy to prevent connectivity problems when some nodes are advertising an ISID and others are not. In a I-VPLS service if the customer MAC (C-MAC) is unknown, a frame will have the Multicast DA for an ISID (PBB-OUI + ISID) flooded on the default multicast tree and not pruned.

Default no use-def-mcast

Platforms All

25.85 use-default-template

use-default-template

Syntax [**no**] **use-default-template**

Context **[Tree]** (config>service>vprn>aaa>remote-servers>radius use-default-template)
[Tree] (config>service>vprn>aaa>rmt-srv>tacplus use-default-template)

Full Context configure service vprn aaa remote-servers radius use-default-template
configure service vprn aaa remote-servers tacplus use-default-template

Description This command specifies whether the RADIUS default user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server. When enabled, the radius_default user-template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server and radius authorization is enabled.

The no form of this command disables the use of the RADIUS default template.

Default no use-default-template

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

use-default-template

Syntax [**no**] **use-default-template**

Context **[Tree]** (config>system>security>tacplus use-default-template)

Full Context configure system security tacplus use-default-template

Description This command specifies whether the **user-template tacplus_default** is actively applied to the TACACS+ user. When enabled, some parameters of the **user-template tacplus_default** are actively applied to all users that authenticate via TACACS+. See the **user-template tacplus_default** command for more details.

When disabled, the parameters of the template are not applied to TACACS+ users, and TACACS+ users can not connect to an SR OS router since the user access parameters are not available. In this case, TACACS+ can only be used for accounting.

Default use-default-template

Platforms All

use-default-template

Syntax [**no**] **use-default-template**

Context **[Tree]** (config>system>security>radius use-default-template)

Full Context configure system security radius use-default-template

Description This command specifies whether the RADIUS default user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server. When enabled, the radius_default user-template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server and radius authorization is enabled.

The **no** form of this command disables the use of the RADIUS default template.

Default no use-default-template

Platforms All

use-default-template

Syntax [**no**] **use-default-template**

Context **[Tree]** (config>system>security>ldap use-default-template)

Full Context configure system security ldap use-default-template

Description This command specifies whether or not the default template is to be actively applied to LDAP users.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default use-default-template

Platforms All

25.86 use-direct-map-as-default

use-direct-map-as-default

Syntax [**no**] **use-direct-map-as-default**

Context **[Tree]** (config>subscr-mgmt>sub-ident-pol>app-profile-map use-direct-map-as-default)

Full Context configure subscriber-mgmt sub-ident-policy app-profile-map use-direct-map-as-default

Description This command enables direct mapping of application profile as default. With this flag, a script returned string is used as the named profile. If the named profiled cannot be found, the default profile is used.

The **no** form of this command disables the direct mapping.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

use-direct-map-as-default

Syntax [**no**] **use-direct-map-as-default**

Context **[Tree]** (config>subscr-mgmt>sub-prof>sla-prof-map use-direct-map-as-default)
[Tree] (config>subscr-mgmt>sub-ident-pol>sla-profile-map use-direct-map-as-default)
[Tree] (config>subscr-mgmt>sub-ident-pol>sub-profile-map use-direct-map-as-default)

Full Context configure subscriber-mgmt sub-ident-policy sla-profile-map use-direct-map-as-default
configure subscriber-mgmt sub-ident-policy sub-profile-map use-direct-map-as-default
configure subscriber-mgmt sub-profile sla-profile-map use-direct-map-as-default

Description This command enables direct mapping of the profiles as default. With this flag, a string returned in authentication is used as the named profile. If the named profiled cannot be found, the default profile is used.

The **no** form of this command disables direct mapping.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.87 use-es-bmac

use-es-bmac

Syntax [**no**] **use-es-bmac**

Context **[Tree]** (config>service>vpls>pbb use-es-bmac)

Full Context configure service vpls pbb use-es-bmac

Description This command is only supported in B-VPLS instances where BGP-EVPN is enabled and controls the source B-MAC used by the system for packets coming from the SAP or spoke-SDPs when they belong to an EVPN Ethernet-Segment.

If enabled, the system will use a source B-MAC derived from the source-bmac (high order four bytes) and the least significant two bytes configured in **config>service>system>bgp-evpn>eth-seg>source-bmac-lsb** for all the packets coming from the local ethernet-segment.

If **no use-es-bmac** is configured, the system will use the regular source-bmac (provided by the **config>service>vpls>pbb>source-bmac** command, or the chassis bmac if the source-bmac is not configured).

Default no use-es-bmac

Platforms All

25.88 use-gi-address

use-gi-address

Syntax **use-gi-address** [**scope** *scope*]

Context **[Tree]** (config>router>dhcp>server use-gi-address)
[Tree] (config>service>vprn>dhcp>server use-gi-address)

Full Context configure router dhcp local-dhcp-server use-gi-address
configure service vprn dhcp local-dhcp-server use-gi-address

Description This command enables the use of gi-address matching. If the gi-address flag is enabled, a pool can be used even if a subnets is not found. If the **local-user-db-name** is not used, the gi-address flag is used and addresses are handed out by GI only. If a user must be blocked from getting an address the server maps to a local user database and configures the user with no address.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

A pool can include multiple subnets. Since the GI is shared by multiple subnets in a subscriber interface the pool may provide IP addresses from any of the subnets included when the GI is matched to any of its subnets. This allows a pool to be created that represents a sub-int.

The **no** form of the reverts to the default.

Parameters *scope* — Specifies if addresses are handed out for a certain subnet where the gi-address belongs to only or for all subnets part of the pool.

Values **subnet** — Addresses are only handed out for the subnet where the gi-address is part.

pool — All subnets part of the pool which contain subnet where the gi-address is part of can hand out addresses.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.89 use-ingress-l2tp-dscp

use-ingress-l2tp-dscp

Syntax [**no**] **use-ingress-l2tp-dscp**

Context **[Tree]** (config>subscr-mgmt>sla-prof>egress use-ingress-l2tp-dscp)

Full Context configure subscriber-mgmt sla-profile egress use-ingress-l2tp-dscp

Description This command enables the use of the DSCP marking taken from the L2TP header received on an L2TP Access Concentrator (LAC) for egress classification for the subscriber host using the associated sla-profile.

This command is ignored if the ingress packet is not identified as an L2TP packet.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.90 use-lag-port-weight

use-lag-port-weight

Syntax [**no**] **use-lag-port-weight**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>subscr-mgmt>msap-policy>vpls-only>igmp-snp>mcac>mc-constraints use-lag-port-weight)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping mcac mc-constraints use-lag-port-weight

Description This command enables port weight to be used when determining available bandwidth per level when LAG ports go down/come up. The command is required for proper operation on mixed port-speed LAGs and can be used for non-mixed port-speed LAGs as well.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

use-lag-port-weight

Syntax **use-lag-port-weight**
no use-lag-port-weight

Context [Tree] (config>service>vpls>sap>igmp-snooping>mcac>mc-constraints use-lag-port-weight)
[Tree] (config>service>vpls>sap>igmp-snooping>mcac>mc-constraints use-lag-port-weight)

Full Context configure service vpls sap igmp-snooping mcac mc-constraints use-lag-port-weight

Description This command enables port weight to be used when determining available bandwidth per level when LAG ports go down/come up. The command is required for correct operation on mixed port-speed LAGs and can be used for non-mixed port-speed LAGs as well.

Default no use-lag-port-weight — The port number is used when determining available BW per level when LAG ports go down/come up.

Platforms All

use-lag-port-weight

Syntax [**no**] **use-lag-port-weight**

Context [Tree] (config>service>vprn>igmp>if>mcac>mc-constraints use-lag-port-weight)
[Tree] (config>service>vprn>mld>if>mcac>mc-constraints use-lag-port-weight)
[Tree] (config>service>vprn>pim>if>mcac>mc-constraints use-lag-port-weight)

Full Context configure service vprn igmp interface mcac mc-constraints use-lag-port-weight
configure service vprn mld interface mcac mc-constraints use-lag-port-weight
configure service vprn pim interface mcac mc-constraints use-lag-port-weight

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the port weight to be used when determining available bandwidth per level when LAG ports go down or come up. This command is required for proper operation on mixed port-speed LAGs and can also be used for non-mixed port-speed LAGs. The port number is used when determining available the bandwidth per level when LAG ports go down or come up.

Default no use-lag-port-weight

Platforms All

use-lag-port-weight

Syntax [**no**] **use-lag-port-weight**

Context **[Tree]** (config>router>igmp>interface>mcac>mc-constraints use-lag-port-weight)
[Tree] (config>router>mld>interface>mcac>mc-constraints use-lag-port-weight)
[Tree] (config>router>pim>interface>mcac>mc-constraints use-lag-port-weight)
[Tree] (config>router>mcac>policy>bundle>mc-constraints use-lag-port-weight)

Full Context configure router igmp interface mcac mc-constraints use-lag-port-weight
configure router mcac policy bundle mc-constraints use-lag-port-weight
configure router mld interface mcac mc-constraints use-lag-port-weight
configure router pim interface mcac mc-constraints use-lag-port-weight

Description This command enables port weight to be used when determining available bandwidth per level when LAG ports go down/come up. The command is required for proper operation on mixed port-speed LAGs and can be used for non-mixed port-speed LAGs as well.

The port number is used when determining available BW per level when LAG ports go down/come up.

The **no** form of this command disables the port weight.

Default no use-lag-port-weight

Platforms All

25.91 use-last-adj-bw

use-last-adj-bw

Syntax [**no**] **use-last-adj-bw**

Context **[Tree]** (config>router>mpls>lsp>auto-bandwidth use-last-adj-bw)

Full Context configure router mpls lsp auto-bandwidth use-last-adj-bw

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command enables the carryover of the last adjusted bandwidth from the previous path to the new path, whether primary or secondary, when the LSP switches between paths. It also creates a context for the configuration of the retry limit for secondary paths.

The **no** form of this command disables the carryover of the last adjusted bandwidth from the previous path to the new path.

Default no use-last-adj-bw

Platforms All

25.92 use-link-address

use-link-address

Syntax **use-link-address** [**scope** *scope*]
no use-link-address

Context **[Tree]** (config>router>dhcp6>server use-link-address)
[Tree] (config>service>vprn>dhcp6>server use-link-address)

Full Context configure router dhcp6 local-dhcp-server use-link-address
configure service vprn dhcp6 local-dhcp-server use-link-address

Description This command configures the local pool selection for IPv6 address or prefix assignment for the configured link-address under relay configuration. The selected pool will contain a prefix covering the link-address. The scope option defines the scope for the match. With scope **subnet**, the prefix or address selection is limited to the prefix in the pool that covers the link-address. With scope **pool**, all the prefixes in the selected pool are eligible for assignment.

The **no** form of the reverts to the default.

Default scope subnet

Parameters *scope* — Specifies the scope of the IP address selection.

Values **subnet** — Specifies that the prefix or address selection is limited to the prefix in the pool that covers the link address.

pool — Specifies that all prefixes in the selected pool are eligible for assignment.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.93 use-outside-ip-address

use-outside-ip-address

Syntax [**no**] **use-outside-ip-address**

Context **[Tree]** (config>li use-outside-ip-address)

Full Context configure li use-outside-ip-address

Description This command enables LI to be performed on an L2-Aware NAT subscriber after NAT. The LI traffic will contain the subscriber's outside public IP address instead of the default private IP address.

The **no** form of this command disables the use of the outside public IP address for the L2-Aware NAT subscriber.

Platforms All

25.94 use-pool-from-client

use-pool-from-client

Syntax **use-pool-from-client delimiter** *delimiter*
use-pool-from-client
no use-pool-from-client

Context **[Tree]** (config>router>dhcp>server use-pool-from-client)
[Tree] (config>service>vprn>dhcp>server use-pool-from-client)

Full Context configure router dhcp local-dhcp-server use-pool-from-client
configure service vprn dhcp local-dhcp-server use-pool-from-client

Description This command enables the use of the pool indicated by DHCP client. When enabled, the IP address pool to be used by this server is the pool is indicated by the vendor-specific sub-option 13 of the DHCP option 82. When disabled or if there is no sub-option 13 in the DHCP message, the pool selection falls back to the **use-gi-address** configuration.

The **no** form of this command disables the use of the pool indicated by DHCP client.

Parameters *delimiter* — A single ASCII character specifies the delimiter of separating primary and secondary pool names in Option82 VSO.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.95 use-sap-bmac

use-sap-bmac

Syntax [**no**] **use-sap-bmac**

Context **[Tree]** (config>service>vpls>pbb use-sap-bmac)

Full Context configure service vpls pbb use-sap-bmac

Description This command enables on a per BVPLS basis the use of source B-MACs allocated to multi-homed SAPs (assigned to an MC-LAG) in the related IVPLS or Epipe service. The command will fail if the value of the source-bmac assigned to the BVPLS is the hardware (chassis) B-MAC. That is, the **source-bmac** must be a configured one.

Default no use-sap-bmac

Platforms All

25.96 use-sdp-bmac

use-sdp-bmac

Syntax [**no**] **use-sdp-bmac**

Context **[Tree]** (config>service>epipe>spoke-sdp use-sdp-bmac)

Full Context configure service epipe spoke-sdp use-sdp-bmac

Description This command indicates that this spoke SDP is expected to be part of a redundant pseudowire connected to a PBB Epipe service. Enabling this parameter will cause traffic forwarded from this spoke SDP into the B-VPLS domain to use a virtual backbone MAC as its source MAC address when both this, and the control pseudowire, are in the active state on this BEB. This virtual backbone MAC is derived from the SDP source-bmac-lsb configuration.

This command will fail when configuring it under a spoke SDP within a PBB-Epipe that is connected to a B-VPLS with mac-notification enabled.

Default no use-sdp-bmac

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.97 use-virtual-mac

use-virtual-mac

Syntax [**no**] **use-virtual-mac**

Context **[Tree]** (config>service>vprn>router-advert>if use-virtual-mac)

Full Context configure service vprn router-advertisement interface use-virtual-mac

Description This command enables sending router advertisement messages using the VRRP virtual MAC address, provided that the virtual router is currently the master.

If the virtual router is not the master, no router advertisement messages are sent.

The **no** form of this command disables sending router advertisement messages.

Default no use-virtual-mac

Platforms All

use-virtual-mac

Syntax [**no**] **use-virtual-mac**

Context **[Tree]** (config>router>router-advert>if use-virtual-mac)

Full Context configure router router-advertisement interface use-virtual-mac

Description This command enables sending router advertisement messages using the VRRP virtual MAC address, provided that the virtual router is currently the master.

If the virtual router is not the master, no router advertisement messages are sent.

The **no** form of this command disables sending router advertisement messages.

Default no use-virtual-mac

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.98 use-vrtr-if-index

use-vrtr-if-index

Syntax [**no**] **use-vrtr-if-index**

Context **[Tree]** (config>cflowd use-vrtr-if-index)

Full Context configure cflowd use-vrtr-if-index

Description This command is used to export flow data using interface indexes (ifIndex values), which can be used directly as the index into the IF-MIB tables for retrieving interface statistics. Specifically, if this command is enabled, the ingressInterface (ID=10) and egressInterface (ID= 14) fields in IP flow templates used to export the flow data to cflowd version 9 and version 10 collectors will be populated with the IF-MIB ifIndex of that interface. In addition, for version 10 templates, two fields are available in the IP flow templates to specify the virtual router ID associated with the ingress and egress interfaces.

The **no** form of this command removes the command from the active configuration and causes cflowd to return to the default behavior of populating the ingress and egress interface ID with the global IF index IDs.

Default no use-vrtr-if-index

Platforms All

25.99 user

user

Syntax [**no**] **user** *user-name*

Context **[Tree]** (config>system>security user)

Full Context configure system security user

Description This command creates a local user and a context to edit the user configuration.

If a new *user-name* is entered, the user is created. When an existing *user-name* is specified, the user parameters can be edited.

When creating a new user and then entering the **info** command, the system displays a password in the output. This is expected behavior in the hash2 scenario. However, when using that user name, there will be no password required. The user can login to the system and then <ENTER> at the password prompt, the user will be logged in.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Unless an administrator explicitly changes the password, it will be null. The hashed value displayed uses the username and null password field, so when the username is changed, the displayed hashed value will change.

The **no** form of this command deletes the user and all configuration data. Users cannot delete themselves.

Parameters *user-name* — Specifies the name of the user up to 32 characters.

Platforms All

25.100 user-db

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host user-db)

Full Context configure subscriber-mgmt local-user-db ppp host user-db

Description This command specifies local user database for PPP PAP/CHAP access.

With this configuration, system will access the specified DB again during PPP PAP/CHAP phase.

This configuration only becomes effective when system is accessing parent DB during PPPoE discovery phase.

The **no** form of this command removes the name from the configuration.

Parameters *local-user-db-name* — Specifies the name of the local user database for PAP/CHAP access.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context **[Tree]** (config>service>ies>sub-if>grp-if>pppoe user-db)
[Tree] (config>service>vprn>sub-if>grp-if>pppoe user-db)
[Tree] (config>service>ies>sub-if>grp-if>ppp user-db)
[Tree] (config>service>vprn>sub-if>grp-if>ppp user-db)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface group-interface ppp user-db
configure service ies subscriber-interface group-interface pppoe user-db
configure service vprn subscriber-interface group-interface ppp user-db
configure service vprn subscriber-interface group-interface pppoe user-db

Description This command configures the local user database to use for PPP PAP/CHAP authentication

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the local user database name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-db-name* [**create**]
no user-db

Context **[Tree]** (config>router>dhcp>server user-db)
[Tree] (config>service>ies>sub-if>grp-if>dhcp user-db)
[Tree] (config>service>ies>sub-if>grp-if>dhcp6 user-db)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 user-db)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 user-db)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp user-db)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp6 user-db)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 user-db)

Full Context configure router dhcp local-dhcp-server user-db
configure service ies subscriber-interface group-interface dhcp user-db
configure service ies subscriber-interface group-interface dhcp6 user-db
configure service ies subscriber-interface group-interface ipv6 dhcp6 user-db
configure service vprn subscriber-interface group-interface dhcp user-db
configure service vprn subscriber-interface group-interface dhcp6 user-db
configure service vprn subscriber-interface group-interface ipv6 dhcp6 user-db

Description This command configures a local user database for authentication.

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the name of a user database, up to 32 characters.

create — Keyword used to create the user database. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-db-name*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no user-db

Context [Tree] (config>service>ies>if>ipv6>dhcp6-relay user-db)
[Tree] (config>service>vprn>if>ipv6>dhcp6-relay user-db)

Full Context configure service ies interface ipv6 dhcp6-relay user-db
configure service vprn interface ipv6 dhcp6-relay user-db

Description This command enables access to the LUDB for DHCPv6 messages under a routed interface. The name of this LUDB must match the name of the LUDB configured by the **config>sub-gmt>local-user-db** command.

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the name of the local user database, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-database-name*
no user-db

Context [Tree] (config>subscr-mgmt>gtp>apn-policy>apn user-db)

Full Context configure subscriber-mgmt gtp apn-policy apn user-db

Description This command configures the LUDB with which the GTP connection is authenticated.

The **no** form of this command removes the user database for authentication with this APN. Only new session setups are affected.

Default no user-db

Parameters *local-user-database-name* — Specifies the name of the LUDB to be used, up to 32 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context [Tree] (config>router>l2tp>group>ppp user-db)
[Tree] (config>router>l2tp>group>tunnel>ppp user-db)
[Tree] (config>service>vprn>l2tp>group>ppp user-db)
[Tree] (config>service>vprn>l2tp>group>tunnel>ppp user-db)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router l2tp group ppp user-db
configure router l2tp group tunnel ppp user-db
configure service vprn l2tp group ppp user-db
configure service vprn l2tp group tunnel ppp user-db

Description This command configures the local user database to use for PPP PAP/CHAP authentication.

Default no user-db

Parameters *local-user-db-name* — Specifies the local user database name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context **[Tree]** (config>service>ies>sub-if>grp-if>wpp user-db)
[Tree] (config>service>vprn>sub-if>grp-if>wpp user-db)

Full Context configure service ies subscriber-interface group-interface wpp user-db
configure service vprn subscriber-interface group-interface wpp user-db

Description This command configures the user database.

Note: If configured, the values configured under grp-if will only be used if there is no corresponding value returned from LUDB lookup.

This command specifies the LUDB system use to lookup while creating initial host before WPP authentication. LUDB could return WPP attributes such as portal name, **initial-sla-profile**, **initial-sub-profile**, and so on LUDB is configured in **config>subscr-mgmt>local-user-db** context.

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the Local User Database name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax [**no**] **user-db**

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>rtr-sol user-db)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-sol user-db)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service ies subscriber-interface group-interface ipv6 router-solicit user-db

Description This command enables the use of the local-user-database for authentication.

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the name of the local-user-database to authenticate the router-solicit. The local-user-database can also return a static prefix or a pool name for address assignment.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-db

Syntax **user-db** *local-user-db-name*
no user-db

Context **[Tree]** (config>service>vpls>sap>ipoe-session user-db)
[Tree] (config>service>ies>sub-if>grp-if>ipoe-session user-db)
[Tree] (config>service>vprn>sub-if>grp-if>ipoe-session user-db)

Full Context configure service ies subscriber-interface group-interface ipoe-session user-db
configure service vpls sap ipoe-session user-db
configure service vprn subscriber-interface group-interface ipoe-session user-db

Description This command configures the local user database to use for IPoE session authentication.

When configured on a capture SAP, the group interface must have the same local user database configured.

On a wlan-gw group interface, the **no** form of this command indicates that the user database is picked from the following sources in the order shown:

1. dhcp
2. ipv6>dhcp6
3. ipv6>router-solicit

If no user database can be found in any of these locations, processing continues as if no user database was configured. This behavior is for backwards compatibility reasons only; when using a LUDB, it should be explicitly added to the IPoE session configuration.

The **no** form of this command reverts to the default.

Parameters *local-user-db-name* — Specifies the local user database name up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

user-db

Syntax **user-db** *name*
no user-db

Context **[Tree]** (config>li>x-interfaces user-db)

Full Context configure li x-interfaces user-db

Description This command configures the location of the data-trigger host for the LIC.

The **no** form of this command reverts to the default.

Parameters *name* — Specifies the local user database name, up to 32 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

25.101 user-equipment-info

user-equipment-info

Syntax **user-equipment-info** [**type** *ue-info-type*]
no user-equipment-info

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp user-equipment-info)
[Tree] (config>subscr-mgmt>diam-appl-plcy>gy>include-avp user-equipment-info)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp user-equipment-info
configure subscriber-mgmt diameter-application-policy gy include-avp user-equipment-info

Description This command includes the **user-equipment-info** in CCR messages.

The **no** form of this command resets the command to the default setting.

Default user-equipment-info type mac

Parameters *ue-into-type* — Specifies what is included in the Diameter User-Equipment-Info attribute if included in Diameter Gx messages.

Values eui64, imeisv, mac, modified-eui64

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt diameter-application-policy gx include-avp user-equipment-info

7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure subscriber-mgmt diameter-application-policy gy include-avp user-equipment-info

25.102 user-ident

user-ident

Syntax **user-ident** *user-ident*
no user-ident

Context [Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6 user-ident)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6 user-ident)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 user-ident
configure service vprn subscriber-interface group-interface ipv6 dhcp6 user-ident

Description This feature is only applicable when DHCPv6-snooping is enabled. The Ethernet header MAC address on DHCPv6 is used as the default key host identification. This command allows addition the keys for identifying the DHCPv6 host. The *interface-id* can be included in addition to the MAC key to further differentiate each DHCPv6 host.

The **no** form of this command reverts to the default.

Default user-ident mac

Parameters *user-ident* — Specifies the DHCP6 user-identification for this interface.

Values **mac** — Specifies to use only the Ethernet MAC of the DHCPv6 message to identify the host.

mac-interface-id — Specifies to additionally use the interface-id to identify the DHCPv6 host.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-ident

Syntax **user-ident** *user-ident*
no user-ident

Context [Tree] (config>router>dhcp>server user-ident)
[Tree] (config>service>vprn>dhcp>server user-ident)

Full Context configure router dhcp local-dhcp-server user-ident
configure service vprn dhcp local-dhcp-server user-ident

Description This command configures the user identification method for the DHCPv4 server.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of the reverts to the default.

Default user-ident mac-circuit-id

Parameters *user-ident* — Specifies the user identification method

Values
- **client-id** — Specifies to use the DHCPv4 client identifier as the user identification method.
- **circuit-id** — Specifies to use the circuit identifier of the DHCPv4 client as the user identification method.
- **mac** — Specifies to use the MAC address of the DHCPv4 client as the user identification method.
- **mac-circuit-id** — Specifies to use the MAC address and circuit identifier of the DHCPv4 client as the user identification method.
- **remote-id** — Specifies to use the MAC address of the remote end as the user identification method.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-ident

Syntax **user-ident** *user-ident*
no user-ident

Context **[Tree]** (config>router>dhcp6>server user-ident)
[Tree] (config>service>vprn>dhcp6>server user-ident)

Full Context configure router dhcp6 local-dhcp-server user-ident
configure service vprn dhcp6 local-dhcp-server user-ident

Description This command configures the keys for identification of the DHCPv6 lease being held in the lease-database (for configured period after lease timeout). Subscriber requesting a lease via DHCPv6 that matches an existing lease based on this configured key is handed the matched prefix or address. This allows address and prefix “stickiness” for DHCPv6 assigned prefixes (IA_NA or PD).

The **no** form of the reverts to the default.

Default user-ident duid

Parameters *user-ident* — Specifies the user identification method.

Values
- **duid** — Specifies the IPv6 DHCP unique identifier from DHCPv6.
- **interface-id** — Specifies the IPv6 interface-id option.
- **interface-id-link-local** — Specifies the interface-id and link-local address.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.103 user-location-info

user-location-info

Syntax [**no**] **user-location-info**

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gx>include-avp user-location-info)
[Tree] (config>subscr-mgmt>diam-appl-plcy>nasreq>include-avp user-location-info)

Full Context configure subscriber-mgmt diameter-application-policy gx include-avp user-location-info
configure subscriber-mgmt diameter-application-policy nasreq include-avp user-location-info

Description This command enables the inclusion of the 3GPP-User-Location-Information AVP as signaled in the incoming GTP setup message.

The **no** form of this command disables the inclusion of the AVP.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.104 user-name

user-name

Syntax **user-name** *name* [**create**]
no user-name *name*

Context **[Tree]** (config>service>dynsvc>ladb user-name)

Full Context configure service dynamic-services local-auth-db user-name

Description This command creates a user name entry in the local authentication database. The user name entry is used to match with the user name of a local authenticated dynamic service data trigger. The user name of a dynamic service data trigger is fixed to the **sap-id**. When matched, the corresponding authentication data is used to set up the dynamic data services.

The **no** form of this command removes the user name entry from the local authentication database configuration.

Parameters *name* — Specifies the user name entry name, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

user-name

Syntax [**no**] **user-name**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute user-name)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute user-name

Description This command enables the inclusion of the **user-name** attribute.

The **no** form of this command disables the inclusion of the **user-name** attribute.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-name

Syntax **user-name** *user-name*
no user-name

Context **[Tree]** (config>aaa>radius-srv-plcy>servers>health-check>test-account user-name)

Full Context configure aaa radius-server-policy servers health-check test-account user-name

Description This command specifies the username that the test account will use to send its access requests to probe the RADIUS servers.

The no form of this command removes the username from the test-account configuration.

Parameters *user-name* — Specifies the probing username, up to 64 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-name

Syntax [**no**] **user-name**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes user-name)

Full Context configure aaa isa-radius-policy acct-include-attributes user-name

Description This command enables the inclusion of user name attributes.

The **no** form of the command excludes user name attributes.

Default no user-name

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

25.105 user-name-format

user-name-format

Syntax **user-name-format** *format* [**mac-format** *mac-format*]
user-name-format *format* **append** [*domain-name*] [**mac-format** *mac-format*]
user-name-format *format* **append** *domain-name*
user-name-format *format* **default-domain** *domain-name* [**mac-format** *mac-format*]
user-name-format *format* **replace** *domain-name* [**mac-format** *mac-format*]
user-name-format *format* **strip** [**mac-format** *mac-format*]
no user-name-format

Context **[Tree]** (config>subscr-mgmt>auth-policy user-name-format)

Full Context configure subscriber-mgmt authentication-policy user-name-format

Description This command defines the format of the “user-name” field in the session authentication request sent to the RADIUS server.

The **no** form of this command switches to the default format, **mac**.

Default By default, the MAC source address of the DHCPv4 DISCOVER or DCHPv6 SOLICIT message is used in the user-name field.

Parameters *format* — Specifies the user name format in RADIUS message.

Values ascii-converted-circuit-id, ascii-converted-tuple, circuit-id, dhcp-client-vendor-opts, mac, mac-giaddr, tuple

ascii-converted-circuit-id — Identical to circuit-id, but the user name is sent to the RADIUS server as a string of hex digits, for use if there is binary data in the circuit-id

ascii-converted-tuple — Identical to tuple, but the circuit-id part of the user name is sent to the RADIUS server as a string of hex digits, for use if there is binary data in the circuit-id

circuit-id — If the system serves as a DHCP relay server which inserts option 82 info, the user name is formatted as defined under DHCP information option. If the system is not a DHCP relay server, the circuit-id is taken from option 82 in the received DHCP message. If no circuit-id can be found, the DHCP-msg is rejected.

dhcp-client-vendor-opts — IPoEv4 host (IPoE session enabled or disabled on group-interface) — The RADIUS user-name is a concatenation of the DHCPv4 Client Identifier Option 61, an “@” delimiter, and the DHCPv4 Vendor Class Identifier Option 60. Non-printing characters in the DHCP option values are converted as described below.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IPoEv6 host (IPoE session enabled on group-interface) — The RADIUS user-name is a concatenation of the identifier field of a type 2 DUID in the DHCPv6 Client Identifier Option 1, the "@" delimiter, and the opaque data field of the first vendor class data in the DHCPv6 Vendor Class Option 16. Non-printing characters in the DHCP option values are converted as described below.

IPoEv6 host (IPoE session disabled on group-interface) — The MAC source address of the DHCPv6 SOLICIT message.

In the absence of a DHCPv4 Client Identifier Option 61 or a DHCPv6 Client Identifier Option 1 containing a DUID type 2, the DHCP client MAC address is used.

In the absence of a DHCPv4 Vendor Class Identifier Option 60 or a DHCPv6 Vendor Class Option 16, the "@" delimited is omitted and nothing is appended.

Non-printing characters, that is, characters outside the ASCII range hex 21 through hex 7E, are converted into an underscore (hex 5F) character.

mac — The MAC source address of the DHCPv4 DISCOVER or DHCPv6 SOLICIT message is used in the user-name field. The format of the MAC address string used as the user name in the RADIUS authentication requests uses lowercase hex digits, and ":" as the inter-digit separator, for example, 00:11:22:aa:bb:cc is valid but 00-11-22-AA-BB-CC will return an error. The RADIUS server must be configured accordingly, otherwise the authentication request will fail.

mac-giaddr — A concatenation of the MAC address and the Relay Agent IP address (giaddr)

tuple — Specifies that the concatenation of MAC source address and circuit-ID are used in the user-name field

mac-format — Specifies how a MAC address is represented when contacting a RADIUS server. This is only used while the value of is equal to the DHCP client vendor options and if the MAC address is used by default of the DHCP client vendor options.

Examples:	ab:	00:0c:f1:99:85:b8 7xxx style
	XY-	00-0C-F1-99-85-B8 IEEE canonical style
	mmmm.	0002.03aa.abff Cisco style

append — Specifies the data type which is an enumerated integer that indicates what needs to be appended to the user-name sent to the RADIUS server.

Values 1 — nothing 2 — domain name

domain — Specifies to user the domain name. In some instances it is desired to add a domain only to usernames which have omitted the domain (@domain). In these instances a default-domain can be appended to usernames which lack a @domain.

append — Adds a "@" delimiter and the specified string after the PAP/CHAP username. No allowance is made for the presence of an existing domain or @ delimited.

replace — Replaces the character-string after the "@" delimiter with the string specified.

strip — Removes all characters after and including the "@" delimiter.

For example:

```
Command: append
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
String:     domainA-1.com
PAP/CHAP User:    someuser
Resulting User:    someuser@domainA-1.com

Command: append
String:     domainA-1.com
PAP/CHAP User:    someuser@existing-domain.net
Resulting User:    someuser@existing-domain.net@domainA-1.com

Command: strip
String:
PAP/CHAP User:    someuser@existing-domain.net
Resulting User:    someuser

Command: replace
String:     domainA-1.com
PAP/CHAP User:    someuser@existing-domain.net
Resulting User:    someuser@domainA-1.com

Command: default-domain
String:    domainA-1.com
PAP/CHAP User:    someuser@existing-domain.net
Resulting User:    someuser@existing-domain.net

Command: default-domain
String: domainA-1.com
PAP/CHAP User:    someuser
Resulting User:    someuser@domainA-1.com
```

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-name-format

Syntax **user-name-format** *format*
no user-name-format

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>nasreq user-name-format)

Full Context configure subscriber-mgmt diameter-application-policy nasreq user-name-format

Description This command defines the format of the User-Name AVP value in Diameter NASREQ AA-Requests for IPoE hosts.

The **no** form of this command reverts to the default.

Parameters *format* — Specifies the format of the User-Name AVP value.

Values **mac** — Specifies to use the MAC source address of the DHCPv4 DISCOVER or DHCPv6 SOLICIT message in the user-name field. The format of the MAC address string is defined with the **mac-forma**t CLI command.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

circuit-id — Specifies to use the circuit ID to identify the user toward the server. If the system serves as a DHCP relay server which inserts option 82 info, the user name is formatted as defined under DHCP information option. If the system is not a DHCP relay server, the circuit-id is taken from option 82 in the received DHCP message. If no circuit-id can be found, the DHCP-msg is rejected.

tuple — Specifies to use a concatenation of MAC source address and circuit-ID.

ascii-converted-circuit-id — Identical to circuit-id, but the user name is a string of hex digits, for use if there is binary data in the circuit-id.

ascii-converted-tuple — Specifies a string of hex digits, for use if there is binary data in the circuit-id.

dhcp-client-vendor-opts — Specifies to use a concatenation of the DHCPv4 Client Identifier Option 61, the "@" delimiter, and the DHCPv4 Vendor Class Identifier Option 60. Non-printing characters in the DHCP option values are converted as described below.

In the absence of a DHCPv4 Client Identifier Option 61, the DHCP client MAC address is used.

In the absence of a DHCPv4 Vendor Class Identifier Option 60, the "@" delimiter is omitted and nothing is appended.

Non-printing characters, that is, characters outside the ASCII range hex 21 through hex 7E, are converted into an underscore (hex 5F) character.

mac-giaddr — Specifies to use a concatenation of MAC source address and DHCP GI address.

nas-port-id — Specifies to use a value of the nas-port-id with format defined in the include-avp section.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

user-name-format

Syntax **user-name-format** *user-name-format* [**mac-format** *mac-format*]
no user-name-format

Context **[Tree]** (config>aaa>isa-radius-plcy user-name-format)

Full Context configure aaa isa-radius-policy user-name-format

Description This command defines the format of the user-name field in the session authentication request sent to the RADIUS server. For authentication of IPv6 triggers (ICMPv6, DHCPv6, IPv6 data-trigger) the user-name format will always fall back to mac only.

The **no** form of the command switches to the default format, **mac**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default user-name-format mac mac-format alu (the MAC source address of the DHCP DISCOVER message is used in the user-name field)

Parameters *user-name-format* — Specifies the user name format in RADIUS message.

mac-format — Specifies how a MAC address is represented when contacting a RADIUS server. This is only used while the value of is equal to the DHCP client vendor options and if the MAC address is used by default of the DHCP client vendor options.

Examples:	ab:	00:0c:f1:99:85:b8 Nokia 7xxx style
	XY-	00-0C-F1-99-85-B8 IEEE canonical style
	mmmm.	0002.03aa.abff Cisco style

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

25.106 user-name-operation

user-name-operation

Syntax **user-name-operation** *operation* [**domain** *domain-name*]
no user-name-operation

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>nasreq user-name-operation)

Full Context configure subscriber-mgmt diameter-application-policy nasreq user-name-operation

Description This command enables domain name manipulation of the user name, such as append, strip, replace or add as default.

For IPoE, this command only applies when **user-name-format** is configured to **dhcp-client-vendor-opts**.

The **no** form of this command reverts to the default.

Parameters *operation* — Specifies the user name manipulations with respect to domain name values.

Values
- **append-domain** – appends an “@” delimiter with the specified domain-name at the end of the user-name, independent if a domain name was already present
- **strip-domain** – removes all characters after and including the “@” delimiter
- **default-domain** – adds an “@” delimiter and the specified domain name to user-names that have no domain name present
- **replace-domain** – replaces the characters after the “@” delimiter with the specified domain-name

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

domain-name — Specifies the domain name string to be used in the specified operation, up to 128 characters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.107 user-srlg-db

user-srlg-db

Syntax **user-srlg-db** [**enable** | **disable**]

Context **[Tree]** (config>router>mpls user-srlg-db)

Full Context configure router mpls user-srlg-db

Description This command enables the use of CSPF by the user SRLG database. When the MPLS module makes a request to CSPF for the computation of an SRLG secondary path, CSPF will query the local SRLG and compute a path after pruning links that are members of the SRLG IDs of the associated primary path. When MPLS makes a request to CSPF for an FRR bypass or detour path to associate with the primary path, CSPF queries the user SRLG database and computes a path after pruning links that are members of the SRLG IDs of the PLR outgoing interface.

If an interface was not entered into the user SRLG database, it is assumed that it does not have any SRLG membership. CSPF will not query the TE database for IGP advertised interface SRLG information.

The disable keyword disables the use of the user SRLG database. CSPF will then resume queries into the TE database for SRLG membership information. The user SRLG database is maintained.

Default user-srlg-db disable

Platforms All

25.108 user-template

user-template

Syntax **user-template** {**tacplus_default** | **radius_default** | **ldap-default**}

Context **[Tree]** (config>system>security user-template)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system security user-template

Description This command configures default security user template parameters.

Parameters **tacplus_default** — Specifies the default TACACS+ user template. All parameters of the tacplus_default template except the “profile” are actively applied to all TACACS+ users if tacplus **use-default-template** is enabled. The **profile** parameter is used for AAA command authorization if TACACS+ authorization is disabled, or if the TACACS+ server does not return a priv-lvl for a user when **use-priv-lvl** is enabled under **tacplus authorization**. See the **tacplus authorization** command for more details.

radius_default — Specifies the default RADIUS user template. The radius_default template is actively applied to a RADIUS user if radius authorization is enabled, radius **use-default-template** is enabled, and no VSAs are returned with the auth-accept from the RADIUS server.

ldap_default — Specifies the default LDAP user template.

Platforms All

25.109 username

username

Syntax **username** *user-name*
username *user-name* **no-domain**
username *user-name* **domain-only**
no username

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ppp>host>host-ident username)

Full Context configure subscriber-mgmt local-user-db ppp host host-identification username

Description This command specifies the PPPoE username to match for a host lookup. When **no-domain** or **domain-only** is specified, the username "user[@domain]" is converted to a user and a domain entity by splitting it on the first @-sign before matching on the specific entity.

Note: This command is only used when **username** is configured as one of the **match-list** parameters.

The **no** form of this command removes the username from the configuration.

Parameters *username* — Specifies the user name, up to 253 characters, of this host. For example, “jane@nokia.com”.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no-domain — Only the user user part of the username is specified and used for matching. For example "jane".

domain-only — Only the domain part of the username is specified and used for matching, for example, nokia.com.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

username

Syntax [**no**] **username** *username*

Context **[Tree]** (debug>service>id>ppp username)

Full Context debug service id ppp username

Description This command enable PPP debug for the specified username. since not all PPP packets contain username, so a MAC debug filter is created automatically when system sees a PPP packet contain the specified username.

Multiple username filters can be specified in the same debug command.

The **no** form of this command disables debugging.

Parameters *user-name* — Specifies the PPP username.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

25.110 usm-community

usm-community

Syntax **usm-community** *community-string* [**hash** | **hash2** | **custom**] **group** *group-name* [**src-access-list** *list-name*]

no usm-community *community-string* [**hash** | **hash2** | **custom**]

Context **[Tree]** (config>system>security>snmp usm-community)

Full Context configure system security snmp usm-community

Description This command is used to associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Nokia's SR OS implementation of SNMP uses SNMPv3. In order to implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. In order to implement SNMP with security features (Version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views which specify more specific OIDs (MIB objects in the subtree) can be configured.

The **no** form of this command removes a community string.

Parameters *community-string* — Specifies the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used. Allowed values are any string up to 32 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (for example, #, $, spaces), the entire string must be enclosed within double quotes.

group — Specifies the group that governs the access rights of this community string. This group must be configured first in the **config**>**system**>**security**>**snmp**>**access group** context. Nokia does not recommend associating a **usm-community** with an SNMP access group that is configured with the **li** (lawful intercept) context.

list-name — Specifies the usm-community to reference a specific src-access-list that will be used to validate the source IP address of all received SNMP requests that use this usm-community. Multiple **community**, **usm-community**, or **vprn snmp community** instances can reference the same **src-access-list**.

Platforms All

25.111 util-stats-interval

util-stats-interval

Syntax **util-stats-interval** *seconds*

Context **[Tree]** (config>port>ethernet util-stats-interval)

Full Context configure port ethernet util-stats-interval

Description This command configures the interval used to calculate the utilization statistics.

Port utilization statistics are only available for physical Ethernet ports on a host system. These statistics are not available for the following:

- Ethernet ports on an Ethernet satellite
- Ethernet ports on a VSR
- PXC ports
- vsm-cca-xp ports

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the size of the interval, in seconds.

Values 30 to 600

Default 300

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26 v Commands

26.1 v4-routed-override-filter

v4-routed-override-filter

Syntax **v4-routed-override-filter** *ip-filter-id*
no v4-routed-override-filter

Context **[Tree]** (config>service>ies>if>vpls>egress v4-routed-override-filter)

Full Context configure service ies interface vpls egress v4-routed-override-filter

Description This command configures an IPv4 filter ID that are applied to packets egressing the IES R-VPLS interface. The filter overrides existing egress IPv4 filter applied to VPLS service endpoints such as SAPs or SDPs, if configured.

The **no** form of this command removes the IPv4 routed override filter from the egress IES R-VPLS interface. When removed, egress IPv4 packets will use the IPv4 egress filter applied to the VPLS endpoint, if configured.

Parameters *ip-filter-id* — Specifies the IP filter ID. This parameter is required when executing the **v4-routed-override-filter** command. The specified filter ID must exist as an IPv4 filter within the system or the override command fails.

Platforms All

v4-routed-override-filter

Syntax **v4-routed-override-filter** *ip-filter-id*
no v4-routed-override-filter

Context **[Tree]** (config>service>ies>if>vpls>ingress v4-routed-override-filter)

Full Context configure service ies interface vpls ingress v4-routed-override-filter

Description This command configures an IPv4 filter ID that is applied to all ingress packets entering the VPLS or I-VPLS service. The filter overrides any existing ingress IPv4 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed. The IPv4 routed packets use any existing ingress IPv4 filter on the VPLS virtual port.

The **no** form of this command removes the IPv4 routed override filter from the ingress IP interface. When removed, the IPv4 ingress routed packets within a VPLS service attached to the IP interface use the IPv4 ingress filter applied to the packets virtual port, when defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-filter-id* — Specifies the IP filter ID. This parameter is required when executing the **v4-routed-override-filter** command. The specified filter ID must exist as an IPv4 filter within the system or the override command fails.

Platforms All

v4-routed-override-filter

Syntax **v4-routed-override-filter** *ip-filter-id*
no v4-routed-override-filter

Context **[Tree]** (config>service>vprn>if>vpls>egress v4-routed-override-filter)

Full Context configure service vprn interface vpls egress v4-routed-override-filter

Description This command configures an IPv4 filter ID that is applied to packets egressing the VPRN R-VPLS interface. The filter overrides the existing egress IPv4 filter applied to VPLS service endpoints such as SAPs or SDPs, if configured.

The **no** form of this command removes the IPv4 routed override filter from the egress VPRN R-VPLS interface. When removed, egress IPv4 packets will use the IPv4 egress filter applied to VPLS endpoint, if configured.

Parameters *ip-filter-id* — Specifies the IP filter ID. This parameter is required when executing the **v4-routed-override-filter** command. The specified filter ID must exist as an IPv4 filter within the system or the override command fails.

Platforms All

v4-routed-override-filter

Syntax **v4-routed-override-filter** *ip-filter-id*
no v4-routed-override-filter

Context **[Tree]** (config>service>vprn>if>vpls>ingress v4-routed-override-filter)

Full Context configure service vprn interface vpls ingress v4-routed-override-filter

Description This command configures an IPv4 filter ID that is applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IPv4 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv4 routed packet's will use the any existing ingress IPv4 filter on the VPLS virtual port.

The **no** form of this command removes the IPv4 routed override filter from the ingress IP interface. When removed, the IPv4 ingress routed packets within a VPLS service attached to the IP interface will use the IPv4 ingress filter applied to the packets virtual port, when defined.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *ip-filter-id* — Specifies the IP filter ID. This parameter is required when executing the **v4-routed-override-filter** command. The specified filter ID must exist as an IPv4 filter within the system or the override command fails.

Platforms All

26.2 v6-aggregate-stats

v6-aggregate-stats

Syntax [**no**] **v6-aggregate-stats**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute v6-aggregate-stats)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute v6-aggregate-stats

Description This command enables reporting of IPv6 aggregated forwarded octet and packet counters using RADIUS VSAs. Disabled by default. It requires **stat-mode v4-v6** for policers and queues for which the IPv6 aggregate forwarded packets should be counted.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.3 v6-frag-header

v6-frag-header

Syntax [**no**] **v6-frag-header**

Context **[Tree]** (config>service>nat>map-domain>ip-fragmentation v6-frag-header)

Full Context configure service nat map-domain ip-fragmentation v6-frag-header

Description This command enables and disables the insertion of the fragmentation header in an IPv6 packet when translating non-fragmented IPv4 packet with DF=0. This option is disabled by default and the size of the IPv6 packet is reduced by 8 bytes.

Default no v6-frag-header

Platforms VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.4 v6-routed-override-filter

v6-routed-override-filter

Syntax **v6-routed-override-filter** *ipv6-filter-id*
no v6-routed-override-filter

Context **[Tree]** (config>service>ies>if>vpls>egress v6-routed-override-filter)

Full Context configure service ies interface vpls egress v6-routed-override-filter

Description This command configures an IPv6 filter ID that is applied to packets egressing the IES R-VPLS interface. The filter overrides existing egress IPv6 filter applied to VPLS service endpoints such as SAPs or SDPs, if configured.

The **no** form of this command removes the IPv4 routed override filter from the egress IES R-VPLS interface. When removed, egress IPv6 routed packets uses the IPv6 egress filter applied to VPLS endpoint, if configured

Parameters *ipv6-filter-id* — Specifies the IPv6 filter ID. This parameter is required when executing the **v6-routed-override-filter** command. The specified filter ID must exist as an IPv6 filter within the system or the override command fails.

Platforms All

v6-routed-override-filter

Syntax **v6-routed-override-filter** *ipv6-filter-id*
no v6-routed-override-filter

Context **[Tree]** (config>service>ies>if>vpls>ingress v6-routed-override-filter)

Full Context configure service ies interface vpls ingress v6-routed-override-filter

Description This command configures an IPv6 filter ID that is applied to all ingress packets entering the VPLS or I-VPLS service. The filter overrides any existing ingress IPv6 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv6 routed packets use any existing ingress IPv6 filter on the VPLS virtual port.

The no v6-routed-override-filter command is used to remove the IPv6 routed override filter from the ingress IP interface. When removed, the IPv6 ingress routed packets within a VPLS service attached to the IP interface will use the IPv6 ingress filter applied to the packet's virtual port, when defined.

Parameters *ipv6-filter-id* — Specifies the IPv6 filter ID. This parameter is required when executing the **v6-routed-override-filter** command. The specified filter ID must exist as an IPv6 filter within the system or the override command fails.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

v6-routed-override-filter

Syntax **v6-routed-override-filter** *ipv6-filter-id*
no v6-routed-override-filter

Context **[Tree]** (config>service>vprn>if>vpls>egress v6-routed-override-filter)

Full Context configure service vprn interface vpls egress v6-routed-override-filter

Description This command configures an IPv6 filter ID that is applied to packets egressing the VPRN R-VPLS interface. The filter overrides existing egress IPv6 filter applied to VPLS service endpoints such as SAPs or SDPs, if configured.

The **no** form of the command removes the IPv4 routed override filter from the egress VPRN R-VPLS interface. When removed, egress IPv6 packets will use the IPv6 egress filter applied to the VPLS endpoint, if configured.

Parameters *ipv6-filter-id* — Specifies the IPv6 filter ID. This parameter is required when executing the **v6-routed-override-filter** command. The specified filter ID must exist as an IPv6 filter within the system or the override command fails.

Platforms All

v6-routed-override-filter

Syntax **v6-routed-override-filter** *ipv6-filter-id*
no v6-routed-override-filter

Context **[Tree]** (config>service>vprn>if>vpls>ingress v6-routed-override-filter)

Full Context configure service vprn interface vpls ingress v6-routed-override-filter

Description This command configures an IPv6 filter ID that is applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IPv6 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv6 routed packets use the any existing ingress IPv6 filter on the VPLS virtual port.

The **no** form of the command removes the IPv6 routed override filter from the ingress IP interface. When removed, the IPv6 ingress routed packets within a VPLS service attached to the IP interface uses the IPv6 ingress filter applied to the packet's virtual port, when defined.

Parameters *ipv6-filter-id* — Specifies the IPv6 filter ID. This parameter is required when executing the **v6-routed-override-filter** command. The specified filter ID must exist as an IPv6 filter within the system or the override command fails.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.5 valid-lifetime

valid-lifetime

Syntax **valid-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no valid-lifetime

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>lease-split valid-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>lease-split valid-lifetime)
[Tree] (config>service>ies>sub-if>ipv6>dhcp6>relay>lease-split valid-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>lease-split valid-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay lease-split valid-lifetime
configure service ies subscriber-interface ipv6 dhcp6 relay lease-split valid-lifetime
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay lease-split valid-lifetime
configure service vprn subscriber-interface ipv6 dhcp6 relay lease-split valid-lifetime

Description This command configures the DHCPv6 lease split valid lifetime (short lease time). DHCPv6 lease split is active when enabled and for all IA_NA and IA_PD options in the transaction the configured lease split valid lifetime (short lease time) is less than or equal to the renew time T1 committed by the server (long renew time) or 50 percent of the preferred lifetime committed by the server when T1 committed by the server equals zero.

The **no** form of this command reverts to the default value.

Default valid-lifetime hrs 1

Parameters [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] — Specifies the valid lifetime values

Values

days:	0 to 3650
hours:	0 to 23
minutes:	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

valid-lifetime

Syntax **valid-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
valid-lifetime infinite
no valid-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host>ipv6-lease-times valid-lifetime)
[Tree] (config>subscr-mgmt>loc-user-db>ppp>host>ipv6-lease-times valid-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>dhcp6>proxy-server valid-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>proxy-server valid-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 proxy-server valid-lifetime
configure service vprn subscriber-interface group-interface ipv6 dhcp6 proxy-server valid-lifetime
configure subscriber-mgmt local-user-db ipoe host ipv6-lease-times valid-lifetime
configure subscriber-mgmt local-user-db ppp host ipv6-lease-times valid-lifetime

Description This command configured valid-lifetime for DHCPv6 lease (address/prefix).

The valid lifetime is the length of time an address/prefix remains in the valid state (for example, the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address/prefix becomes invalid and must not be used in communications. RFC 2461, sec 6.2.1 recommends default value of 30 days.

Each address/prefix assigned to the client has associated preferred and valid lifetimes specified by the address assignment authority (DHCP server, RADIUS, ESM). To request an extension of the lifetimes assigned to an address, the client sends a Renew message to the addressing authority. The addressing authority sends a Reply message to the client with the new lifetimes, allowing the client to continue to use the address/prefix without interruption.

The lifetimes are transmitted from the addressing authority to the client in the IA option on the top level (not the address or prefix level).

The **no** form of this command reverts to the default.

Default valid-lifetime days 1

Parameters **infinite** — Specifies that the valid lifetime is infinite.

Values

days:	0 to 49710
hours:	0 to 23
minutes:	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

valid-lifetime

Syntax **valid-lifetime infinite**
valid-lifetime [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no valid-lifetime

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>dhcp6>local-dhcp-server>pool>prefix valid-lifetime)
[Tree] (config>router>dhcp6>server>pool>prefix valid-lifetime)

Full Context configure router dhcp6 local-dhcp-server pool prefix valid-lifetime
configure service vprn dhcp6 local-dhcp-server pool prefix valid-lifetime

Description This command configures the valid lifetime for the IPv6 prefix or address in the option.

The **no** form of this command reverts to the default.

Default valid-lifetime days 1

Parameters **infinite** — Sets the valid lifetime to infinite value.

valid-lifetime — Specifies the valid lifetime

Values

days *days*	0 to 49710
hrs *hours*	0 to 23
min *minutes*	0 to 59
sec *seconds*	0 to 5

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

valid-lifetime

Syntax **valid-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no valid-lifetime

Context [Tree] (config>router>dhcp6>server>defaults valid-lifetime)

Full Context configure router dhcp6 local-dhcp-server defaults valid-lifetime

Description This command configures the valid lifetime.

The **no** form of this command reverts to the default.

Default valid-lifetime days 1

Parameters *valid-lifetime* — Specifies the valid lifetime for a prefix to remain valid.

Values

days:	0 to 3650
hours:	0 to 23
minutes:	0 to 59
seconds	0 to 59

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

valid-lifetime

Syntax **valid-lifetime** *seconds*
valid-lifetime infinite
no valid-lifetime

Context **[Tree]** (config>subscr-mgmt>rtr-adv>pfx-opt>stateful valid-lifetime)
[Tree] (config>subscr-mgmt>rtr-adv>pfx-opt>stateless valid-lifetime)

Full Context configure subscriber-mgmt router-advertisement-policy prefix-options stateful valid-lifetime
configure subscriber-mgmt router-advertisement-policy prefix-options stateless valid-lifetime

Description This command specifies the time for this prefix to remain valid.

The **no** form of this command reverts to the default.

Default valid-lifetime 86400

Parameters *seconds* — Specifies the time, in seconds, for the prefix to remain preferred.

Values 0, 900 to 86400

infinite — Specifies that the time never expires.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

valid-lifetime

Syntax **valid-lifetime** *seconds*
valid-lifetime infinite
no valid-lifetime

Context **[Tree]** (config>service>ies>if>ipv6>dhcp6>pfx-delegate>prefix valid-lifetime)

Full Context configure service ies interface ipv6 dhcp6-server prefix-delegation prefix valid-lifetime

Description This command configures the time, in seconds, that the prefix is valid.

The **no** form of this command reverts to the default value.

Default valid-lifetime 2592000 (30 days)

Parameters *seconds* — Specifies the time, in seconds, that this prefix remains valid.

Values 1 to 4294967294

infinite — Specifies that this prefix remains valid infinitely. The value 4294967295 is interpreted as infinite.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

valid-lifetime

Syntax **valid-lifetime** *seconds*
valid-lifetime infinite
no valid-lifetime

Context **[Tree]** (config>service>ies>sub-if>ipv6>rtr-adv>pfx-opt valid-lifetime)
[Tree] (config>service>ies>sub-if>grp-if>ipv6>rtr-adv>pfx-opt valid-lifetime)
[Tree] (config>service>vprn>sub-if>ipv6>rtr-adv>pfx-opt valid-lifetime)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>rtr-adv>pfx-opt valid-lifetime)

Full Context configure service ies subscriber-interface group-interface ipv6 router-advertisements prefix-options valid-lifetime
configure service ies subscriber-interface ipv6 router-advertisements prefix-options valid-lifetime
configure service vprn subscriber-interface group-interface ipv6 router-advertisements prefix-options valid-lifetime
configure service vprn subscriber-interface ipv6 router-advertisements prefix-options valid-lifetime

Description This command specifies the remaining time for this prefix to be valid for the purpose of on-link determination.

The **no** form of this command reverts to the default.

Default valid-lifetime 86400

Parameters *seconds* — Specifies the time for the prefix to remain valid on this interface in seconds.

Values 0 to 4294967295

infinite — Specifies that the remaining time will never expire. The value 4294967295 is interpreted as infinite.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

valid-lifetime

Syntax **valid-lifetime** {*seconds* | **infinite**}

Context **[Tree]** (config>service>vprn>router-advert>if valid-lifetime)

Full Context configure service vprn router-advert interface valid-lifetime

Description This command specifies the length of time in seconds that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.

The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default valid-lifetime 2592000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be valid.

Values 0 to 429496729

infinite — Specifies that the prefix will always be valid. A value of 4,294,967,295 represents infinity.

valid-lifetime

Syntax **valid-lifetime** {*seconds* | **infinite**}
no valid-lifetime

Context **[Tree]** (config>router>router-advert>if>prefix valid-lifetime)

Full Context configure router router-advertisement interface prefix valid-lifetime

Description This command specifies the length of time in seconds that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.

The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default valid-lifetime 2592000

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be valid.

infinite — Specifies that the prefix will always be valid. A value of 4,294,967,295 represents infinity.

Platforms All

26.6 validate

validate

Syntax **validate** [*file-url*]

Context **[Tree]** (admin>system>license validate)

Full Context admin system license validate

Description This command performs a validation on the license file pointed to by the command line argument. A validation ensures that the license is compatible with the current state of the target system but it does not change the existing license. Aspects that can cause a failure in the validation include:

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- The license file was created for a different target system. The UUID encoded into the file must match that defined by the specific hardware platform.
- The license file does not include license information for the release of software currently running on the system.
- The current date/time reported to system is outside the validity period encoded in the license.
- The system is currently using a hardware upgrade license that is not included in the new file being validated.

Note: If the CLM tool is being used for license management, it shall perform the validation and activation and there is no need to enter these commands manually.

Parameters *file-url* — Specifies the file URL location to read the license file.

Values local-url, remote-url

Note: IPv6 addresses apply only to 7750 SR and 7950 XRS.

Platforms All

validate

Syntax [**no**] **validate**

Context **[Tree]** (configure>system>security>profile>netconf>base-op-authorization validate)

Full Context configure system security profile netconf base-op-authorization validate

Description This command enables the NETCONF validate operation.

The **no** form of this command disables the operation.

Default no validate

Note: The operation is enabled by default in the built-in system-generated administrative profile.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.7 validate-dest-prefix

validate-dest-prefix

Syntax **validate-dest-prefix**
no validate-dest-prefix

Context **[Tree]** (config>service>vprn>bgp>flowspec validate-dest-prefix)

Full Context configure service vprn bgp flowspec validate-dest-prefix

Description This command enables or disables validation of received IPv4 and IPv6 FlowSpec routes that contain a destination-prefix subcomponent.

A FlowSpec route with a destination-prefix subcomponent is considered invalid if both of the following are true:

- it was originated outside the local AS of the receiving BGP router
- the neighbor AS of the FlowSpec route does not match the neighbor AS of the best match BGP (unicast) route for the destination prefix or the neighbor AS of any longer match BGP (unicast) route for the destination prefix

An invalid route is retained in the BGP but it is not used for filtering traffic or propagated to other BGP routers.

The **no** form of this command disables the validation procedure based on destination-prefix.

Default no validate-dest-prefix

Platforms All

validate-dest-prefix

Syntax [**no**] **validate-dest-prefix**

Context **[Tree]** (config>router>bgp>flowspec validate-dest-prefix)

Full Context configure router bgp flowspec validate-dest-prefix

Description This command enables or disables validation of received IPv4 and IPv6 FlowSpec routes that contain a destination-prefix subcomponent.

A FlowSpec route with a destination-prefix subcomponent is considered invalid if both of the following are true:

- it was originated outside the local AS of the receiving BGP router

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- the neighbor AS of the FlowSpec route does not match the neighbor AS of the best match BGP (unicast) route for the destination prefix or the neighbor AS of any longer match BGP (unicast) route for the destination prefix

An invalid route is retained in the BGP but it is not used for filtering traffic or propagated to other BGP routers.

The **no** form of this command disables the validation procedure based on destination-prefix.

Default no validate-dest-prefix

Platforms All

26.8 validate-gtp-tunnels

validate-gtp-tunnels

Syntax **validate-gtp-tunnels direction** *direction* [**create**]
no validate-gtp-tunnels direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter validate-gtp-tunnels)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter validate-gtp-tunnels

Description This command configures a TCA for the counter capturing drops due to the validation of GTP tunnel check. A validate-gtp-tunnels drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a validate-gtp-tunnels TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

validate-gtp-tunnels

Syntax [**no**] **validate-gtp-tunnels**

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>gtp-tunnel-database validate-gtp-tunnels)

Full Context configure application-assurance group gtp gtp-filter gtp-tunnel-database validate-gtp-tunnels

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures GTP tunnel validation. This allows for validation of TEIDs and is a prerequisite for sequence checking and UE IP address validation. This command applies only when AA GTP FW is deployed on S8/S5/Gp/Gn interfaces.

The **gtpc-inspection** command must be enabled before using this command.

The **no** form of this command disables GTP tunnel validation.

Default no validate-gtp-tunnels

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.9 validate-next-hop

validate-next-hop

Syntax [**no**] **validate-next-hop**

Context **[Tree]** (config>service>vprn>static-route-entry>next-hop validate-next-hop)

Full Context configure service vprn static-route-entry next-hop validate-next-hop

Description This optional command tracks the state of the next hop in the IPv4 ARP cache or IPv6 Neighbor Cache. When the next hop is not reachable and is removed from the ARP or Neighbor Cache, the next hop will no longer be considered valid and the associated static route state removed from the active route-table.

When the next hop is reachable again and present in the ARP/Neighbor Cache, the static route is considered valid and is subject to being placed into the active route-table.

Default no validate-next-hop

Platforms All

validate-next-hop

Syntax [**no**] **validate-next-hop**

Context **[Tree]** (config>router>static-route-entry>next-hop validate-next-hop)

Full Context configure router static-route-entry next-hop validate-next-hop

Description This optional command tracks the state of the next-hop in the IPv4 ARP cache or IPv6 Neighbor Cache. When the next-hop is not reachable and is removed from the ARP or Neighbor Cache, the next-hop will no longer be considered valid and the associated static-route state removed from the active route-table.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When the next-hop is reachable again and present in the ARP/Neighbor Cache, the static route is considered valid and is subject to being placed into the active route-table.

Default no validate-next-hop

Platforms All

26.10 validate-redirect-ip

validate-redirect-ip

Syntax **validate-redirect-ip**
no validate-redirect-ip

Context **[Tree]** (config>service>vprn>bgp>flowspec validate-redirect-ip)

Full Context configure service vprn bgp flowspec validate-redirect-ip

Description This command enables procedures to validate the redirect-to-IPv4 action attached to FlowSpec-IPv4 routes received by the BGP instance.

The SR OS FlowSpec implementation supports the redirect-to-IPv4 action encoded as an IPv4-address-specific BGP extended community.

When this command is configured, a FlowSpec-IPv4 route is considered invalid and not installed as a filter rule if the FlowSpec-IPv4 route is deemed to have originated in a different AS than the IP route that resolves the redirection IPv4 address. The originating AS of a flow-spec route is determined from its AS path.

The **no** form of this command disables the check described above.

Default no validate-redirect-ip

Platforms All

validate-redirect-ip

Syntax [**no**] **validate-redirect-ip**

Context **[Tree]** (config>router>bgp>flowspec validate-redirect-ip)

Full Context configure router bgp flowspec validate-redirect-ip

Description This command enables procedures to validate the **redirect-to-IPv4** action attached to FlowSpec IPv4 routes received by the BGP instance.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The SR OS FlowSpec implementation supports the **redirect-to-IPv4** action encoded as an IPv4-address-specific BGP extended community.

When this command is configured, a FlowSpec IPv4 route is considered invalid and not installed as a filter rule if the FlowSpec IPv4 route is deemed to have originated in a different AS than the IP route that resolves the redirection IPv4 address. The originating AS of a FlowSpec route is determined from its AS path.

The **no** form of this command disables the check described above.

Default no validate-redirect-ip

Platforms All

26.11 validate-sequence-number

validate-sequence-number

Syntax **validate-sequence-number direction** *direction* [**create**]
no validate-sequence-number direction *direction*

Context **[Tree]** (config>app-assure>group>statistics>tca>gtp-filter validate-sequence-number)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter validate-sequence-number

Description This command configures a TCA for the counter capturing drops due to the GTP filter invalid GTP sequence number. A validate-sequence-number drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**) or for traffic generated from the network toward the AA subscriber (**to-sub**). The **create** keyword is mandatory when creating a validate-sequence-number TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub, to-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

validate-sequence-number

Syntax [**no**] **validate-sequence-number**

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>gtp-tunnel-database validate-sequence-number)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure application-assurance group gtp gtp-filter gtp-tunnel-database validate-sequence-number

Description This command configures GTP sequence number checking. GTP packets that fail the sequence number check are discarded.

The **validate-gtp-tunnels** command must be enabled before using this command.

The **no** form of this command disables GTP sequence number checking.

Default no validate-sequence-number

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.12 validate-source-ip-addr

validate-source-ip-addr

Syntax [**no**] **validate-source-ip-addr**

Context **[Tree]** (config>app-assure>group>gtp>gtp-fltr>gtp-tunnel-database validate-source-ip-addr)

Full Context configure application-assurance group gtp gtp-filter gtp-tunnel-database validate-source-ip-addr

Description This command configures the checking for spoofed or invalid UE IP addresses. Upstream GTP packets that contain invalid UE IP addresses are discarded. When a packet is dropped due to **source-ip-address** “invalid source IP add”, the statistics counter is updated.

The **validate-gtp-tunnels** command must be enabled before using this command.

The **no** form of this command disables the checking for spoofed or invalid UE IP addresses.

Default no validate-source-ip-addr

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.13 validate-src-ip-addr

validate-src-ip-addr

Syntax **validate-src-ip-addr direction** *direction* [**create**]
no validate-src-ip-addr direction *direction*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>app-assure>group>statistics>tca>gtp-filter validate-src-ip-addr)

Full Context configure application-assurance group statistics threshold-crossing-alert gtp-filter validate-src-ip-addr

Description This command configures a TCA for the counter capturing drops due to the GTP filter anti-spoofing of the UE IP address check. A validate-src-ip-addr drop TCA can be created for traffic generated from the subscriber side of AA (**from-sub**). The **create** keyword is mandatory when creating a validate-src-ip-addr TCA.

Parameters *direction* — Specifies the traffic direction.

Values from-sub

create — Keyword used to create the TCA.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.14 validity-time

validity-time

Syntax **validity-time** *seconds*
no validity-time

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gy>efh>interim-c validity-time)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling interim-credit validity-time

Description This command configures the validity time for the interim credit allocated to rating groups of a Diameter Gy session when Extended Failure Handling (EFH) is active. When either the allocated interim credit is consumed or the validity time expires, a new attempt is made to establish a Diameter Gy session with the Online Charging Server (OCS).The validity time applies to all interim credit allocated via the **config>subscr-mgmt>diam-appl-plcy** *application-policy-name*>**gy>extended-failure-handling>interim-credit>volume** and **config>subscr -mgmt>category-map** *category-map-name*>**category** *category-name*>**default-credit** CLI commands.

A validity time value of 0 (zero) disables the validity time for the assigned interim credit.

The **no** form of this command resets the value to the default value.

Default validity-time 1800

Parameters *seconds* — Specifies the validity time, in seconds, applicable to the interim credit.

Values 0 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.15 value

value

Syntax **value** *value*

Context **[Tree]** (config>service>system>bgp-evpn>eth-seg>service-carving>manual>preference value)

Full Context configure service system bgp-evpn ethernet-segment service-carving manual preference value

Description This command modifies the default preference value used for the PE in the ES. An ES shutdown is not required to modify this value during maintenance operations.

Default value 32767

Parameters *value* — Determines the preference value used in the preference-based DF election algorithm.

Values 0 to 65535

Platforms All

value

Syntax [**no**] **value** *value-name*

Context **[Tree]** (config>app-assure>group>policy>aso>char value)

Full Context configure application-assurance group policy app-service-options characteristic value

Description This command configures a characteristic value.

The **no** form of this command removes the value for the characteristic.

Parameters *value-name* — Specifies a string of up to 32 characters uniquely identifying this characteristic value.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

value

Syntax **value** *value*
no value

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>asel>pref-opt value)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>asel>pref-opt value)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>asel>pref-opt value)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection preference-option value
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection preference-option value
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection preference-option value

Description This command configures the default preference option value. A DHCPv6 preference option with specified value is inserted in the DHCPv6 advertise message for DHCPv6 clients for which no per DHCPv6 server or per client-mac solicit delay or preference option value is configured.

The **no** form of this command removes the configuration.

Parameters *value* — Specifies the default preference option value.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

value

Syntax **value** *value*
no value

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>asel>clnt-mac>pref-opt value)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>asel>clnt-mac>pref-opt value)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>asel>clnt-mac>pref-opt value)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac preference-option value
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection client-mac preference-option value
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection client-mac preference-option value

Description This command configures the preference option value for DHCPv6 clients with an odd or an even source MAC address. A DHCPv6 preference option with specified value is inserted in the DHCPv6 advertise message for these DHCPv6 clients.

The **no** form of this command removes the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *value* — Specifies the preference option value for DHCPv6 clients with an odd or an even source MAC address.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

value

Syntax **value** *value*
no value

Context **[Tree]** (config>service>ies>sub-if>grp-if>ipv6>dhcp6>relay>asel>srvr>pref-opt value)
[Tree] (config>service>vprn>sub-if>ipv6>dhcp6>relay>asel>srvr>pref-opt value)
[Tree] (config>service>vprn>sub-if>grp-if>ipv6>dhcp6>relay>asel>srvr>pref-opt value)

Full Context configure service ies subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server preference-option value
configure service vprn subscriber-interface group-interface ipv6 dhcp6 relay advertise-selection server preference-option value
configure service vprn subscriber-interface ipv6 dhcp6 relay advertise-selection server preference-option value

Description This command configures the preference option value. A DHCPv6 preference option with specified value is inserted in the DHCPv6 advertise message from the server.

The **no** form of this command removes the configuration.

Parameters *value* — Specifies the preference option value for DHCPv6 advertise messages from the server.

Values 0 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.16 vas-filter

vas-filter

Syntax **vas-filter** *name* [**create**]
no vas-filter *name*

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain vas-filter)

Full Context configure subscriber-mgmt isa-service-chaining vas-filter

Description This command configures a Value Added Service filter.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the VAS filter name from the configuration.

Default This command configures a value added service (VAS) filter that can be associated to an L2-aware NAT host, and is matched on the NAT ISA to select flows for a host that needs to be steered to remote value-added services.

Parameters *name* — Specifies a VAS filter name, up to 32 characters.

create — Keyword used to create the VAS filter instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.17 vas-if-type

vas-if-type

Syntax **vas-if-type** {**to-from-access** | **to-from-network** | **to-from-both**}
no vas-if-type

Context **[Tree]** (config>service>ies>if vas-if-type)

Full Context configure service ies interface vas-if-type

Description This command configures the type of a Value Added Service (VAS) facing interface. To change the **vas-if-type**, the **shutdown** command is required. The **vas-if-type** and **loopback** commands are mutually exclusive.

The **no** form of this command removes the VAS interface type configuration.

Default no vas-if-type

Parameters **to-from-access** — Used when two separate (**to-from-access** and **to-from-network**) interfaces are used for VAS connectivity. For service chaining, traffic arriving from access interfaces (upstream) is redirected to a PBR target reachable over this interface for upstream VAS processing. Downstream traffic after VAS processing must arrive on this interface, so that the traffic is subject to regular routing but is not subject to AA divert, nor egress subscriber PBR.

to-from-network — Used when two separate (**to-from-access** and **to-from-network**) interfaces are used for VAS connectivity. For service chaining, traffic arriving from network interfaces (downstream) is redirected to a PBR target reachable over this interface for downstream VAS processing. Upstream traffic after VAS processing must arrive on this interface, so that regular routing can be applied.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

to-from-both — Used when a single interface is used for VAS connectivity (no local-to-local traffic). For service chaining, both traffic arriving from access interfaces and from network interfaces is redirected to a PBR target reachable over this interface for upstream/downstream VAS processing. Traffic after VAS processing must arrive on this interface, so that the traffic is subject to regular routing but is not subject to AA divert, nor egress subscriber PBR.

Platforms All

vas-if-type

Syntax **vas-if-type** {**to-from-access** | **to-from-network** | **to-from-both**}
no vas-if-type

Context **[Tree]** (config>service>vprn>if vas-if-type)

Full Context configure service vprn interface vas-if-type

Description This command configures the type of a Value Added Service (VAS) facing interface. To change the **vas-if-type**, the **shutdown** command is required. The **vas-if-type** and **loopback** commands are mutually exclusive.

The **no** form of this command removes the VAS interface type configuration.

Default no vas-if-type

Parameters **to-from-access** — Used when two separate (**to-from-access** and **to-from-network**) interfaces are used for VAS connectivity. For service chaining, traffic arriving from access interfaces (upstream) is redirected to a PBR target reachable over this interface for upstream VAS processing. Downstream traffic after VAS processing must arrive on this interface, so that the traffic is subject to regular routing but is not subject to AA divert, nor egress subscriber PBR.

to-from-network — Used when two separate (**to-from-access** and **to-from-network**) interfaces are used for VAS connectivity. For service chaining, traffic arriving from network interfaces (downstream) is redirected to a PBR target reachable over this interface for downstream VAS processing. Upstream traffic after VAS processing must arrive on this interface, so that regular routing can be applied.

to-from-both — Used when a single interface is used for VAS connectivity (no local-to-local traffic). For service chaining, both traffic arriving from access and from network is redirected to a PBR target reachable over this interface for upstream/downstream VAS processing. Traffic after VAS processing must arrive on this interface, so that the traffic is subject to regular routing but is not subject to AA divert, nor egress subscriber PBR.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vas-if-type

Syntax **vas-if-type** {**to-from-access** | **to-from-network** | **to-from-both**}
no vas-if-type

Context **[Tree]** (config>router>if vas-if-type)

Full Context configure router interface vas-if-type

Description This command configures the type of a Value Added Service (VAS) facing interface. To change the **vas-if-type**, the **shutdown** command is required. The **vas-if-type** and **loopback** commands are mutually exclusive.

The **no** form of this command removes the VAS interface type configuration.

Default no vas-if-type

Parameters **to-from-access** — Used when two separate (**to-from-access** and **to-from-network**) interfaces are used for VAS connectivity. For service chaining, traffic arriving from access interfaces (upstream) is redirected to a PBR target reachable over this interface for upstream VAS processing. Downstream traffic after VAS processing must arrive on this interface, so that the traffic is subject to regular routing but is not subject to AA divert, nor egress subscriber PBR.

to-from-network — Used when two separate (**to-from-access** and **to-from-network**) interfaces are used for VAS connectivity. For service chaining, traffic arriving from network interfaces (downstream) is redirected to a PBR target reachable over this interface for downstream VAS processing. Upstream traffic after VAS processing must arrive on this interface, so that regular routing can be applied.

to-from-both — Used when a single interface is used for VAS connectivity (no local-to-local traffic). For service chaining, both traffic arriving from access interfaces and from network interfaces is redirected to a PBR target reachable over this interface for upstream/downstream VAS processing. Traffic after VAS processing must arrive on this interface, so that the traffic is subject to regular routing but is not subject to AA divert, nor to egress subscriber PBR.

Platforms All

26.18 vc-id

vc-id

Syntax **vc-id** *vc-id*
no vc-id

Context **[Tree]** (config>service>epipe>sap>l2tpv3-session vc-id)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vpls>sap>l2tpv3-session vc-id)

Full Context configure service epipe sap l2tpv3-session vc-id
configure service vpls sap l2tpv3-session vc-id

Description This command specifies the VC-ID for the L2TPv3 session.

The **no** form of this command deletes the VC-ID configuration.

Parameters *vc-id* — Specifies the VC-ID, up to 64 characters.

Values 1 to 4294967295

Platforms All

26.19 vc-id-range

vc-id-range

Syntax **vc-id-range** *from* [**to** *vc-id*]
no vc-id-range *from*

Context [Tree] (config>service>system>bgp-evpn>ethernet-segment vc-id-range)

Full Context configure service system bgp-evpn ethernet-segment vc-id-range

Description This command determines the VC-IDs associated with the virtual Ethernet Segment on a specific SDP based on the following considerations:

- VC-IDs for manual spoke-SDP and BGP-AD are included in the range.
- Th mesh-sdp VC-IDs are not allowed on a SDP used by a virtual ES.
- A maximum of 8 ranges are allowed.
- A range can be comprised of a single VC-ID.
- A **vc-id-range** can be comprised of a single VC-ID.
- Shutting down the ES is not required prior to making changes.

The **no** form of the command removes the configured range. Only the first VC-ID value is required to remove the range.

Parameters *vc-id* — Specifies the VC-ID. When configuring a range of VC-IDs (and not a single value), the value of the second VC-ID must be greater than the first VC-ID.

Values 1 to 4294967295

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.20 vc-label

vc-label

Syntax **vc-label** *egress-vc-label*
no vc-label [*egress-vc-label*]

Context **[Tree]** (config>service>vprn>if>spoke-sdp>egress vc-label)
[Tree] (config>service>vprn>red-if>spoke-sdp>egress vc-label)

Full Context configure service vprn interface spoke-sdp egress vc-label
configure service vprn redundant-interface spoke-sdp egress vc-label

Description This command configures the egress VC label.

Parameters *vc-label* — A VC egress value that indicates a specific connection.

Values 16 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp egress vc-label

All

- configure service vprn interface spoke-sdp egress vc-label

vc-label

Syntax **vc-label** *ingress-vc-label*
no vc-label [*ingress-vc-label*]

Context **[Tree]** (config>service>vprn>if>spoke-sdp>ingress vc-label)
[Tree] (config>service>vprn>red-if>spoke-sdp>ingress vc-label)

Full Context configure service vprn interface spoke-sdp ingress vc-label
configure service vprn redundant-interface spoke-sdp ingress vc-label

Description This command configures the ingress VC label.

Parameters *vc-label* — A VC ingress value that indicates a specific connection.

Values 2048 to 18431

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn redundant-interface spoke-sdp ingress vc-label

All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn interface spoke-sdp ingress vc-label

vc-label

Syntax **vc-label** *egress-vc-label*
no vc-label [*egress-vc-label*]

Context **[Tree]** (config>service>ies>if>spoke-sdp>egress vc-label)
[Tree] (config>service>ies>red-if>spoke-sdp>egress vc-label)
[Tree] (config>service>vpls>mesh-sdp>egress vc-label)
[Tree] (config>service>vpls>spoke-sdp>egress vc-label)

Full Context configure service ies interface spoke-sdp egress vc-label
configure service ies redundant-interface spoke-sdp egress vc-label
configure service vpls mesh-sdp egress vc-label
configure service vpls spoke-sdp egress vc-label

Description This command configures the static MPLS VC label used by this device to send packets to the far-end device in this service via this SDP.

Parameters *egress-vc-label* — Specifies a VC egress value that indicates a specific connection.

Values 16 to 1048575

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies redundant-interface spoke-sdp egress vc-label

All

- configure service vpls spoke-sdp egress vc-label
- configure service ies interface spoke-sdp egress vc-label
- configure service vpls mesh-sdp egress vc-label

vc-label

Syntax **vc-label** *ingress-vc-label*
no vc-label [*ingress-vc-label*]

Context **[Tree]** (config>service>ies>if>spoke-sdp>ingress vc-label)
[Tree] (config>service>ies>red-if>spoke-sdp>ingress vc-label)
[Tree] (config>service>vpls>mesh-sdp>ingress vc-label)
[Tree] (config>service>vpls>spoke-sdp>ingress vc-label)

Full Context configure service ies interface spoke-sdp ingress vc-label
configure service ies redundant-interface spoke-sdp ingress vc-label
configure service vpls mesh-sdp ingress vc-label
configure service vpls spoke-sdp ingress vc-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the static MPLS VC label used by the far-end device to send packets to this device in this service via this SDP.

Parameters *ingress-vc-label* — A VC ingress value that indicates a specific connection.

Values 2048 to 18431

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service ies redundant-interface spoke-sdp ingress vc-label

All

- configure service vpls mesh-sdp ingress vc-label
- configure service ies interface spoke-sdp ingress vc-label
- configure service vpls spoke-sdp ingress vc-label

vc-label

Syntax [**no**] **vc-label** *egress-vc-label* | *ingress-vc-label*

Context **[Tree]** (config>service>apipe>spoke-sdp>egress vc-label)
[Tree] (config>service>apipe>spoke-sdp>ingress vc-label)
[Tree] (config>service>cpipe>spoke-sdp>egress vc-label)
[Tree] (config>service>cpipe>spoke-sdp>ingress vc-label)
[Tree] (config>service>fpipe>spoke-sdp>egress vc-label)
[Tree] (config>service>fpipe>spoke-sdp>ingress vc-label)
[Tree] (config>service>ipipe>spoke-sdp>egress vc-label)
[Tree] (config>service>ipipe>spoke-sdp>ingress vc-label)

Full Context configure service apipe spoke-sdp egress vc-label
configure service apipe spoke-sdp ingress vc-label
configure service cpipe spoke-sdp egress vc-label
configure service cpipe spoke-sdp ingress vc-label
configure service fpipe spoke-sdp egress vc-label
configure service fpipe spoke-sdp ingress vc-label
configure service ipipe spoke-sdp egress vc-label
configure service ipipe spoke-sdp ingress vc-label

Description This command configures the egress and ingress VC label.

The actual maximum value that can be configured is limited by the **config>router>mpls-labels>static-label-range** command.

Parameters *vc-label* — A VC egress value that indicates a specific connection.

Values for egress: 16 to 1048575

Values for ingress: 32 to 18431

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service fpipe spoke-sdp egress vc-label
- configure service cpipe spoke-sdp egress vc-label
- configure service fpipe spoke-sdp ingress vc-label
- configure service cpipe spoke-sdp ingress vc-label

7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

- configure service apipe spoke-sdp egress vc-label
- configure service apipe spoke-sdp ingress vc-label

All

- configure service ipipe spoke-sdp ingress vc-label
- configure service ipipe spoke-sdp egress vc-label

vc-label

Syntax **vc-label** *vc-label*
no vc-label [*vc-label*]

Context **[Tree]** (config>service>ies>aarp-interface>spoke-sdp>egress vc-label)
[Tree] (config>service>ies>aarp-interface>spoke-sdp>ingress vc-label)

Full Context configure service ies aarp-interface spoke-sdp egress vc-label
configure service ies aarp-interface spoke-sdp ingress vc-label

Description This command configures the egress and ingress VC label.

The **no** version of this command removes the VC label.

Parameters *vc-label* — Specifies a VC egress value that indicates a specific connection.

Values egress: 16 to 1048575
ingress: 32 to 18431

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vc-label

Syntax **vc-label** *vc-label*
no vc-label [*vc-label*]

Context **[Tree]** (config>service>vprn>aarp-interface>spoke-sdp>egress vc-label)
[Tree] (config>service>vprn>aarp-interface>spoke-sdp>ingress vc-label)

Full Context configure service vprn aarp-interface spoke-sdp egress vc-label
configure service vprn aarp-interface spoke-sdp ingress vc-label

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the egress and ingress VC label.

The **no** version of this command removes the VC label.

Parameters *vc-label* — A VC egress value that indicates a specific connection.

Values egress: 16 to 1048575
ingress: 32 to 18431

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vc-label

Syntax **vc-label** *egress-vc-label*
no vc-label [*egress-vc-label*]

Context **[Tree]** (config>mirror>mirror-dest>spoke-sdp>egress vc-label)
[Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp>egress vc-label)

Full Context configure mirror mirror-dest remote-source spoke-sdp egress vc-label
configure mirror mirror-dest spoke-sdp egress vc-label

Description This command configures the spoke SDP egress VC label.

The **no** form of this command removes the egress VC label value from the configuration.

Parameters *egress-vc-label* — Specifies a VC egress value that indicates a specific connection.

Values 16 to 1048575

Platforms All

vc-label

Syntax **vc-label** *ingress-vc-label*
no vc-label [*ingress-vc-label*]

Context **[Tree]** (config>mirror>mirror-dest>spoke-sdp>ingress vc-label)
[Tree] (config>mirror>mirror-dest>remote-src>spoke-sdp>ingress vc-label)
[Tree] (config>service>vprn>ipmirrorif>spoke-sdp vc-label)

Full Context configure mirror mirror-dest remote-source spoke-sdp ingress vc-label
configure mirror mirror-dest spoke-sdp ingress vc-label
configure service vprn ipmirrorif spoke-sdp vc-label

Description This command configures the spoke SDP ingress VC label.

Parameters *vc-label* — Specifies the VC ingress value that indicates a specific connection.

Values 32 to 18431

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure mirror mirror-dest spoke-sdp ingress vc-label

All

- configure mirror mirror-dest remote-source spoke-sdp ingress vc-label

vc-label

Syntax **vc-label** *vc-label*
no vc-label

Context **[Tree]** (config>service>sdp>binding>pw-port>egress vc-label)

Full Context configure service sdp binding pw-port egress vc-label

Description This command configures the egress VC label for the PW representing the PW-port.

Default no vc-label

Parameters *vc-label* — Specifies the VC egress value that indicates a specific connection.

Values 16 to 1048575

Platforms All

vc-label

Syntax **vc-label** *ingress-vc-label*
no vc-label

Context **[Tree]** (config>service>sdp>binding>pw-port>ingress vc-label)

Full Context configure service sdp binding pw-port ingress vc-label

Description This command configures the ingress VC label used for the PW representing the PW port.

Note that the maximum value of the vc-label that may be configured is limited by the **config**>**router**>**mpls-labels**>**static-label-range** command.

Default no vc-label

Parameters *vc-label* — Specifies a VC ingress value that indicates a specific connection.

Values 32 to 18431

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.21 vc-range

vc-range

Syntax **vc-range** *num* **vpi-range** *vpi-range* **vci-range** *vci-range*
no vc-range num

Context **[Tree]** (config>service>vpls>sap>atm vc-range)

Full Context configure service vpls sap atm vc-range

Description This command configures ATM Virtual Circuit ranges and is supported only in max16k-vc ATM MDA mode. An ATM MDA supports a number of passive (or listening) VCs, of which a subset can be simultaneously active.

The **no** form of this command reverts to the default.

Parameters *num* — Specifies the VC range.

Values 1 to 5 (Five ranges are supported to accommodate non-contiguous ranges of VPI/VCI pairs.

vci-range *vci-range* — Specifies the VCI range.

Values 1, 2, 5 to 65535 (Contiguous VCI ranges in the form of x-y.)

vpi-range vpi-range. — Specifies the VPI range.

Values 0 to 255 for UNI
0 to 4095 for NNI
(Contiguous VPI range in the form of x-y)

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

26.22 vc-threshold

vc-threshold

Syntax **vc-threshold** *buffer-threshold*

Context **[Tree]** (config>port>sonet-sdh>path>atm>custom-buffer-mode vc-threshold)

Full Context configure port sonet-sdh path atm custom-buffer-mode vc-threshold

Description This command configures the ATM port VC threshold.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *buffer-threshold* — specifies the VC buffer threshold for all VCs configured on this port.

Values 190 to 117000

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

26.23 vc-type

vc-type

Syntax **vc-type** {**ether** | **vlan**}
no vc-type

Context **[Tree]** (config>service>sdp>binding>pw-port vc-type)

Full Context configure service sdp binding pw-port vc-type

Description This command sets the forwarding mode for the pseudowire port. The vc-type is signaled to the peer, and must be configured consistently on both ends of the pseudowire. vc-type VLAN is only configurable with dot1q encapsulation on the pseudowire port. The tag with vc-type vlan only has significance for transport, and is not used for service delineation or ESM. The top (provider tag) is stripped while forwarding out of the pseudowire, and a configured vlan-tag (for vc-type vlan) is inserted when forwarding into the pseudowire. With vc-type ether, the tags if present (max 2), are transparently preserved when forwarding in our out of the pseudowire.

The **no** form of the command reverts to the default value.

Default vc-type ether

Parameters **ether** — Specifies **ether** as the virtual circuit (VC) associated with the SDP binding.

vlan — Specifies **vlan** as the virtual circuit (VC) associated with the SDP binding.

Platforms All

vc-type

Syntax **vc-type** {**ether** | **vlan**}

Context **[Tree]** (config>service>pw-template vc-type)

Full Context configure service pw-template vc-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command overrides the default VC type signaled for the binding to the far end SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

Parameters **ether** — Defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The top VLAN tag, if a VLAN tag is present, is stripped from traffic received on the pseudowire, and a vlan-tag is inserted when forwarding into the pseudowire. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings.

Note: The system expects a symmetrical configuration with its peer, specifically it expects to remove the same number of VLAN tags from received traffic as it adds to transmitted traffic. As some of the related configuration parameters are local and not communicated in the signaling plane, an asymmetrical behavior cannot always be detected and so cannot be blocked. Consequently, protocol extractions will not necessarily function for asymmetrical configurations as they would with a symmetrical configurations resulting in an unexpected operation.

Platforms All

26.24 vccv-ping

vccv-ping

Syntax **vccv-ping** *sdp-id:vc-id* [**reply-mode** [**ip-routed** | **control-channel**] [**src-ip-address** *ip-addr* **dst-ip-address** *ip-addr* **pw-id** *pw-id*] [**target-fec-type static-pw-fec agi** *attachment-group-identifier* **pw-path-id-saii** *global-id:node-id:ac-id* **pw-path-id-taii** *global-id:node-id:ac-id*]

vccv-ping saii-type2 *global-id:prefix:ac-id* **taii-type2** *global-id:prefix:ac-id* [**reply-mode** [**ip-routed** | **control-channel**] [**src-ip-address** *ip-addr* **dst-ip-address** *ip-addr*]

vccv-ping spoke-sdp-fec *spoke-sdp-fec-id* [**reply-mode** [**ip-routed** | **control-channel**] [**saii-type2** *global-id:prefix:ac-id* **taii-type2** global-id:prefix:ac-id] [**src-ip-address** *ip-addr*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

dst-ip-address *ip-addr*]

vccv-ping static *sdp-id:vc-id* [**assoc-channel** [**ipv4** | **non-ip**] [**dest-global-id** *global-id* **dest-node-id** *node-id*] [**src-ip-address** *ip-addr*] [**target-fec-type pw-id-fec sender-src-address** *ip-addr* **remote-dst-address** *ip-addr* **pw-id** *pw-id* **pw-type** *pw-type*]

NOTE: Options common to all **vccv-ping** cases: [**count** *send-count*] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**interval** *interval*] [**size** *octets*] [**timeout** *timeout*] [**ttl** *vc-label-ttl*]

Context [Tree] (oam vccv-ping)
[Tree] (config>saa>test>type vccv-ping)

Full Context configure saa test type vccv-ping
oam vccv-ping

Description This command configures a Virtual Circuit Connectivity Verification (VCCV) ping test. A vccv-ping test checks connectivity of a VLL inband. It checks to verify that the destination (target) PE is the egress for the Layer 2 FEC. It provides for a cross-check between the dataplane and the control plane. It is inband which means that the **vccv-ping** message is sent using the same encapsulation and along the same path as user packets in that VLL. The **vccv-ping** test is the equivalent of the lsp-ping test for a VLL service. The vccv-ping reuses an lsp-ping message format and can be used to test a VLL configured over both an MPLS and a GRE SDP.

Note that VCCV ping can be initiated on T-PE or S-PE. If initiated on the S-PE, the **reply-mode** parameter must be used with the **ip-routed** value The ping from the T-PE can have either values or can be omitted, in which case the default value is used.

If a VCCV ping is initiated from T-PE to neighboring a S-PE (one segment only), then it is sufficient to only use the **spoke-sdp-fec-id** parameter. However, if the ping is across two or more segments, at least the **spoke-sdp-fec-id**, **src-ip-address** *ip-addr*, **dst-ip-address** *ip-addr*, **ttl** *vc-label-ttl* parameters are used where:

- The **src-ip-address** is system IP address of the router preceding the destination router.
- The *vc-label-ttl* parameter must have a value equal or higher than the number of pseudowire segments.

Note that VCCV ping is a multi-segment pseudowire. For a single-hop pseudowire, only the peer VCCV CC bit of the control word is advertised when the control word is enabled on the pseudowire.

VCCV ping on multi-segment pseudowires require that the control word be enabled in all segments of the VLL. If the control word is not enabled on a spoke SDP, it is signaled peer VCCV CC bits to the far end, consequently the **vccv-ping** cannot be successfully initiated on that specific spoke SDP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

If the **saii-type-2** and **taii-type-2** parameters are specified by the user of this command for a FEC129 pseudowire, then these values are used by the vccv-ping echo request message instead of the saii and taii of the spoke-sdp indexed by the **spoke-sdp-fec** parameter, or any saii and taii received in a switching point TLV for the pseudowire. Furthermore, the user must enter the **saii** and **taii** in accordance with the direction of the pseudowire as seen from the node on which the **vccv-ping** command is executed. However, the values of the **saii** and **taii** sent in the echo request message are swapped with respect to the user-entered values to match the order in the installed FEC on the targeted node. The output of the command for FEC129 type 2 pseudowire reflects the order of the **saii** and **taii** stored on the targeted node.

This command, when used with the **static** option, configures a Virtual Circuit Connectivity Verification (VCCV) ping test for static MPLS-TP pseudowires used in a VLL service. It checks to verify that the destination (target) PE is the egress for the Static PW FEC. It provides for a cross-check between the dataplane and the configuration. The **vccv-ping static** command reuses an **lsp-ping** message format and can be used to test an MPLS-TP pseudowire VLL configured over an MPLS SDP. VCCV Ping for MPLS-TP pseudowires always uses the VCCV control word (associated channel header) with either an IPv4 channel type (0x0021) or on-demand CV message channel type (0x0025).

Note that **vccv-ping static** can only be initiated on a T-PE. Both the echo request and reply messages are send using the same, in-band, encapsulation. If the **target-fec-type** option is not specified, then the target FEC stack contains a static PW FEC TLV. The contents of this TLV are populated based on the source node ID, source global ID, and destination global ID and destination node ID in the **vccv-ping** command (or taken from the pseudowire context if omitted from the command).

The **target-fec-type** option allows the user to test a segment of a MS-PW that does not have the same FEC type as the local segment from the T-PE where the **vccv-ping** command is issued. This is applicable for performing VCCV ping on an MS-PW comprised of static PW FEC segments and dynamically signaled PW ID FEC segments.

The timestamp format to be sent, and to be expected when received in a PDU, is as configured by the **config>test-oam>mpls-time-stamp-format** command. If RFC 4379 (obsoleted by RFC 8029) is selected, then the timestamp is in seconds and microseconds since 1900, otherwise it is in seconds and microseconds since 1970.

Parameters *sdp-id:vc-id* — Specifies that if a FEC 128 PW is tested, then its VC ID must be indicated with this parameter. The VC ID needs to exist on the local router and the far-end peer needs to indicate that it supports VCCV to allow the user to send vccv-ping message.

Values sdp-id: 1 to 32767
vc-id: 1 to 4294967295

reply-mode {ip-routed | control-channel} — Indicates to the far end, the method to send the reply message. The option **ip-routed** indicates an out-of-band reply mode using the vccv control channel. The option **control-channel** indicates an in-band reply mode using the vccv control channel.

Default control-channel

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

src-ip-address *ip-addr* — Specifies the source IP address.

Values a.b.c.d

dst-ip-address *ip-addr* — Specifies the destination IP address.

Values a.b.c.d

src-ip-address *ip-addr* — Specifies the source IP address.

Values a.b.c.d

pw-id — Specifies the pseudowire ID to be used for performing a VCCV ping operation. The pseudowire ID is a non-zero 32-bit connection ID required by the FEC 128, as defined in RFC 8029, Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures.

Values 1 to 4294967295

target-fec-type — Specifies the FEC type for a remote PW segment targeted by a VCCV Ping echo request. This parameter is used if VCCV Ping is used along a MS-PW where a static MPLS-TP PW segment using the static PW FEC is switched to a T-LDP signaled segment using the PW ID FEC (FEC128), or vice versa, thus requiring the user to explicitly specify a target FEC that is different from the local segment FEC.

Values **pw-id-fec** — Indicates that FEC element for the remote target PW 00000000000000000000000000000000000000000000000000000000000000000000000000000000 segment is of type PW ID (FEC128).

static-pw-fec — Indicates that FEC element for the remote target PW segment is of type Static PW FEC.

attachment-group-identifier — Specifies the attachment group identifier for the target FEC. This parameter is only valid in combination with the **target-fec-type** *static-pw-fec*.

Values 0 to 4294967295

pw-path-id-saii *global-id:node-id:ac-id* — Specifies the SAII of the target FEC. This parameter is only valid in combination with the **target-fec-type** *static-pw-fec*.

global-id — Specifies the global ID of the SAII of the targeted static PW FEC element.

Values 0 to 4294967295

node-id — Specifies the node-id on far end T-PE that the pseudowire being tested is associated with.

Values ipv4-formatted address: a.b.c.d

1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique SAII for the pseudowire being tested at the far end T-PE.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pw-path-id-taii *global-id:node-id:ac-id* — Specifies the SAII of the target FEC. This parameter is only valid in combination with the **target-fec-type** *static-pw-fec*.

global-id — Specifies the global ID of the SAII of the targeted static PW FEC element.

Values 0 to 4294967295

node-id — Specifies the node-id on far end T-PE that the pseudowire being tested is associated with.

Values ipv4-formatted address: a.b.c.d
1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique SAII for the pseudowire being tested at the far end T-PE.

Values 1 to 4294967295

saii-type2 *global-id*:*prefix*:*ac-id* — Specifies that if a FEC129 AII Type 2 pseudowire is tested, then the source attachment individual identifier (SAII) must be indicated. The **saii-type2** parameter is mutually exclusive with *sdp-id:vc-id*.

taii-type2 *global-id:prefix:ac-id* — Specifies that if a FEC129 AII Type 2 pseudowire is tested, then the target attachment individual identifier (TAII) must be indicated. The **taii-type2** parameter is mutually exclusive with *sdp-id:vc-id*.

global-id — Specifies the global ID of the far end T-PE of the FEC129 pseudowire.

Values 0 to 4294967295

Default 0

node-id — Specifies the node-id on far end T-PE that the pseudowire being tested is associated with.

Values ipv4-formatted address: a.b.c.d
1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique TAII for the pseudowire being tested at the far end T-PE.

Values 1 to 4294967295

spoke-sdp-fec-id — Specifies that if a FEC 129 PW is tested, then its *spoke-sdp-fec-id* must be indicated with this parameter. The *spoke-sdp-fec-id* must already exist on the local router and the far-end peer must indicate that it supports VCCV to allow the user to send **vccv-ping** message.

spoke-sdp-fec is mutually exclusive with the *sdp-id:vc-id* parameter.

Values 1 to 4294967295

assoc-channel {ipv4 | non-ip} — Specifies the associated channel encapsulation format to use for the VCCV ping echo request and echo reply packet for a PW that uses the static PW FEC. An associated channel type of ipv4 must be used if a vccv-ping is performed to a remote segment of a different FEC type.

Values **ipv4** – IPv4 encapsulation in an IPv4 pseudowire associated channel (channel type 0x0021)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

non-ip –MPLS-TP encapsulation without UDP/IP headers, in pseudowire associated channel using channel type 0x025.

Default non-ip

global-id — Specifies the MPLS-TP global ID for the far end node of the pseudowire under test. If this is not entered, then the *dest-global-id* is taken from the pseudowire context.

Values 0 to 4294967295

Default 0

node-id — Specifies the MPLS-TP node ID of the far end node for the pseudowire under test. If this is not entered, then the *dest-global-id* is taken from the pseudowire context.

Values ipv4-formatted address: a.b.c.d
1 to 4294967295

Default 0

sender-src-address *ip-addr* — Specifies the 4-octet IPv4 address of the node originating the VCCV Ping echo request. This parameter is only valid in combination with the **target-fec-type** *pw-id-fec*.

Values a.b.c.d

remote-dst-address *ip-addr* — Specifies the 4-octet IPv4 address of the far end node that is a target of the VCCV Ping echo request. This parameter is only valid in combination with the **target-fec-type** *pw-id-fec*.

Values a.b.c.d

pw-type — Specifies the PW type value of the PW segment targeted on the far end node. This field must be included to populate the PW type field of the PW ID FEC in the FEC static TLV, when the far end FEC type is different form the local FEC type and the **target-fec-type** *pw-id-fec*.

Values atm-cell (=3), atm-sdu (=2), atm-vcc (=9), atm-vpc (=10), cesopsn (=21), cesopsn-cas (=23), ether (=5), satop-e1 (=17), satop-t1 (=18), 1 to 65535

send-count — Specifies the number of messages to send, expressed as a decimal integer. The count parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message interval value must have expired before the next message request is sent.

Values 1 to 100

Default 1

fc-name — Specifies the **fc** parameter be used to indicate the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The LSP-EXP mappings on the receive network interface controls the mapping back to the internal forwarding class used by the far-end 7750 SR that receives the message request. The egress mappings of the egress network interface on the far-end router controls the forwarding class markings on the return reply message. The LSP-EXP mappings on the receive network interface controls the mapping of the message reply at the originating SR.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

The ToS byte is not modified. Table 187 summarizes this behavior.

Table 187 **vccv-ping Request Packet and Behavior**

CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • packet queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet {tos=1, fc2, profile2}
Outgoing interface (responder node)	Echo reply packet: • packet queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 187 **vccv-ping Request Packet and Behavior**

Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

profile {in | out} — Specifies the profile state of the MPLS echo request encapsulation.

Default out

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the interval is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

octets — Specifies the size, in octets, expressed as a decimal integer, of the MPLS echo request packet, including the IP header but not the label stack. The request pay-load is padded with zeros to the specified size. Note that an OAM command is not failed if the user entered a size lower than the minimum required to build the packet for the echo request message. The payload is automatically padded to meet the minimum size.

Values 1 to 9786

Default 1

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of message time out, the requesting router assumes that the message response is not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

Values 1 to 10

Default 5

vc-label-ttl — Specifies the time-to-live value for the vc-label of the echo request message. The outer label TTL is still set to the default of 255 regardless of this value.

Values 1 to 255

Default 1

Output The following output is an example of VCCV ping information.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Sample Output

```
Ping TPE to SPE on a LDP/GRE tunnel
===================================

*A:Dut-B# oam vccv-ping 3:1
VCCV-PING 3:1 88 bytes MPLS payload
Seq=1, send from intf toSPE1-D-8 to NH 12.1.8.2
       reply from 4.4.4.4 via Control Channel
       udp-data-len=56 rtt=0.689ms rc=8 (DSRtrMatchLabel)

---- VCCV PING 3:1 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 0.689ms, avg = 0.689ms, max = 0.689ms, stddev = 0.000ms


Ping TPE to SPE on a RSVP tunnel
================================

A:Dut-C# oam vccv-ping 5:1
VCCV-PING 5:1 88 bytes MPLS payload
Seq=1, send from intf toSPE2-E-5 to NH 12.3.5.1
       send from lsp toSPE2-E-5
       reply from 5.5.5.5 via Control Channel
       udp-data-len=56 rtt=1.50ms rc=8 (DSRtrMatchLabel)

---- VCCV PING 5:1 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1.50ms, avg = 1.50ms, max = 1.50ms, stddev = 0.000ms


Ping TPE to TPE over multisegment pseudowire
============================================
*A:Dut-C# oam vccv-ping 5:1 src-ip-address 4.4.4.4 dst-ip-address 2.2.2.2 pw-
id 1 ttl 3
VCCV-PING 5:1 88 bytes MPLS payload
Seq=1, send from intf toSPE2-E-5 to NH 12.3.5.1
       send from lsp toSPE2-E-5
       reply from 2.2.2.2 via Control Channel
       udp-data-len=32 rtt=2.50ms rc=3 (EgressRtr)

---- VCCV PING 5:1 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 2.50ms, avg = 2.50ms, max = 2.50ms, stddev = 0.000ms


Ping SPE to TPE (over LDP tunnel)
=================================

Single segment:
---------------

*A:Dut-D# oam vccv-ping 3:1 reply-mode ip-routed
VCCV-PING 3:1 88 bytes MPLS payload
Seq=1, send from intf toTPE1-B-8 to NH 12.1.8.1
       reply from 2.2.2.2 via IP
       udp-data-len=32 rtt=1.66ms rc=3 (EgressRtr)

---- VCCV PING 3:1 Statistics ----
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1.66ms, avg = 1.66ms, max = 1.66ms, stddev = 0.000ms


Multisegment:
-------------
*A:Dut-D>config>router#  oam vccv-ping 4:200 src-ip-address 5.5.5.5 dst-ip-
address 3.3.3.3 pw-id 1 ttl 2 reply-mode ip-routed
VCCV-PING 4:200 88 bytes MPLS payload
Seq=1, send from intf toSPE2-E-5 to NH 12.2.5.2
       reply from 3.3.3.3 via IP
       udp-data-len=32 rtt=3.76ms rc=3 (EgressRtr)

---- VCCV PING 4:200 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 3.76ms, avg = 3.76ms, max = 3.76ms, stddev = 0.000ms


Ping SPE to SPE
===============
*A:Dut-D# oam vccv-ping 4:200 reply-mode ip-routed
VCCV-PING 4:200 88 bytes MPLS payload
Seq=1, send from intf toSPE2-E-5 to NH 12.2.5.2
       reply from 5.5.5.5 via IP
       udp-data-len=56 rtt=1.77ms rc=8 (DSRtrMatchLabel)

---- VCCV PING 4:200 Statistics ----
1 packets sent, 1 packets received, 0.00% packet loss
round-trip min = 1.77ms, avg = 1.77ms, max = 1.77ms, stddev = 0.000ms
```

Platforms All

26.25 vccv-trace

vccv-trace

Syntax **vccv-trace** *sdp-id:vc-id* [**reply-mode** {**ip-routed** | **control-channel**] [**target-fec-type static-pw-fec agi** *attachment-group-identifier* **pw-path-id-saii** *global-id:node-id:ac-id* **pw-path-id-taii** *global-id:node-id:ac-id*]

vccv-trace saii-type2 *global-id:prefix:ac-id* **taii-type2** *global-id:prefix:ac-id* [**reply-mode** {**ip-routed** | **control-channel**}]

vccv-trace spoke-sdp-fec *spoke-sdp-fec-id* [**reply-mode** {**ip-routed** | **control-channel**}] [**saii-type2** *global-id:prefix:ac-id* **taii-type2** *global-id:prefix:ac-id*]

vccv-trace static *sdp-id:vc-id* [**assoc-channel** {**ipv4** | **non-ip**}] [**src-ip-address** *ipv4-address*] [**target-fec-type pw-id-fec sender-src-address** *ipv4-address* **remote-dst-address** *ipv4-address* **pw-id** *pw-id* **pw-type** *pw-type*]

NOTE: Options common to all **vccv-trace** cases: [**fc** *fc-name* [**profile** {**in** | **out**]] [**interval** *interval-value*] [**max-fail** *no-response-count*] [**max-ttl** *max-vc-label-ttl*] [**min-ttl** *min-vc-label-ttl*] [**probe-count** *probe-count*] [**size** *octets*] [**timeout** *timeout-value*]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (oam vccv-trace)
[Tree] (config>saa>test>type vccv-trace)

Full Context configure saa test type vccv-trace
oam vccv-trace

Description This command configures a Virtual Circuit Connectivity Verification (VCCV) automated trace test. The automated VCCV-trace can trace the entire path of a PW with a single command issued at the T-PE or at an S-PE. This is equivalent to LSP-Trace and is an iterative process by which the source T-PE or S-PE node sends successive VCCV-Ping messages with incrementing the TTL value, starting from TTL=1. In each iteration, the T-PE builds the MPLS echo request message in a way like VCCV-Ping. The first message with TTL=1 has the next-hop S-PE T-LDP session source address in the Remote PE Address field in the PW FEC TLV. Each S-PE which terminates and processes the message includes in the MPLS echo reply message the FEC 128 TLV corresponding the PW segment to its downstream node. The source T-PE or S-PE node can then build the next echo reply message with TTL=2 to test the next-next hop for the MS-PW. It copies the FEC TLV it received in the echo reply message into the new echo request message. The process is terminated when the reply is from the egress T-PE or when a time out occurs.

The user can specify to display the result of the VCCV-trace for a fewer number of PW segments of the end-to-end MS-PW path. In this case, the **min-ttl** and **max-ttl** parameters are configured accordingly. However, the T-PE/S-PE node still probes all hops up to **min-ttl** to correctly build the FEC of the desired subset of segments.

Note that if the **saii-type-2** and **taii-type-2** parameters are specified this command for a FEC129 pseudowire, then these values are used by the vccv-ping echo request message instead of the saii and taii of the spoke SDP indexed by the **spoke-sdp-fec** parameter, or any saii and taii received in a switching point TLV for the pseudowire. Furthermore, the use must enter the saii and taii in accordance with the direction of pseudowire as seen from the node on which the **vccv-trace** command is executed. However, the values of the saii and taii sent in the echo request message are swapped with respect to the user-entered values to match the order in the installed FEC on the targeted node. The output of the command for a FEC129 type 2 pseudowire reflects the order of the saii and taii stored on the targeted node.

This command, when used with the **static** option, configures a VCCV-automated trace test for static MPLS-TP pseudowires used in a VLL service. VCCV trace for MPLS-TP pseudowires always uses the VCCV control word (associated channel header) with either an IPv4 channel type (0x0021) or on-demand CV message channel type (0x0025).

Note that **vccv-trace static** can only be initiated on a T-PE. Both the echo request and reply messages are send using the same, in-band, encapsulation. The target FEC stack contains a static PW FEC TLV. The contents of this TLV are populated based on the source Node ID, source global ID, and destination global ID and destination node ID taken from the pseudowire context.

The **target-fec-type** option allows the user to perform a vccv-trace to a segment of a MS-PW that does not have the same FEC type as the local segment from the T-PE where the **vccv-trace** command is issued. This is applicable for performing VCCV ping on an MS-PW comprised of static PW FEC segments and dynamically signaled PW ID FEC segments.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *sdp-id:vc-id* — Specifies that if a FEC 128 PW is being tested, then its VC ID must be indicated with this parameter. The VC ID needs to exist on the local router and the far-end peer needs to indicate that it supports VCCV to allow the user to send vccv-ping message.

Values sdp-id: 1 to 32767
vc-id: 1 to 4294967295

reply-mode {ip-routed | control-channel} — Indicates to the far end, the method to send the reply message. The option **ip-routed** indicates an out-of-band reply mode using the vccv control channel. The option **control-channel** indicates an in-band reply mode using the vccv control channel.

Default control-channel

target-fec-type — Specifies the FEC type for a remote PW segment targeted by a VCCV Ping echo request. This parameter is used if VCCV Ping is used along a MS-PW where a static MPLS-TP PW segment using the static PW FEC is switched to a T-LDP signaled segment using the PW ID FEC (FEC128), or vice versa, thus requiring the user to explicitly specify a target FEC that is different from the local segment FEC.

Values **pw-id-fec** — Indicates that FEC element for the remote target PW 00000000000000000000000000000000000000000000000000000000000000000000000000000000 segment is of type PW ID (FEC128).

static-pw-fec — Indicates that FEC element for the remote target PW segment is of type Static PW FEC.

attachment-group-identifier — Specifies the attachment group identifier for the target FEC. This parameter is only valid in combination with the **target-fec-type static-pw-fec**.

Values 0 to 4,294,967,295

pw-path-id-saii *global-id:node-id:ac-id* — Specifies the SAII of the target FEC. This parameter is only valid in combination with the **target-fec-type** *static-pw-fec*.

global-id — Specifies the global ID of the SAII of the targeted static PW FEC element.

Values 0 to 4294967295

Default 0

node-id — Specifies the node ID on far end T-PE that the pseudowire being tested is associated with.

Values ipv4-formatted address: a.b.c.d
1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique SAII for the pseudowire being tested at the far end T-PE.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pw-path-id-taii *global-id:node-id:ac-id* — Specifies the SAII of the target FEC. This parameter is only valid in combination with the **target-fec-type** *static-pw-fec*.

global-id — Specifies the global ID of the SAII of the targeted static PW FEC element.

Values 0 to 4294967295

Default 0

node-id — Specifies the node ID of the far-end T-PE that the pseudowire being tested is associated with.

Values ipv4-formatted address: a.b.c.d

1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique SAII for the pseudowire being tested at the far end T-PE.

Values 1 to 4294967295

saii-type2 *global-id:prefix:ac-id* — If a FEC129 AII Type 2 pseudowire is being tested, then the source attachment individual identifier (SAII) must be indicated.

The **saii-type2** parameter is mutually exclusive with the **sdp-id:vc-id** parameter.

global-id — Specifies the global ID of this T-PE node.

Values 1 to 4294967295

prefix — Specifies the prefix on this T-PE node that the spoke SDP is associated with.

ac-id — Specifies an unsigned integer representing a locally unique identifier for the spoke SDP.

Values 1 to 4294967295

taii-type2 *global-id:prefix:ac-id* — Specifies that if a FEC129 AII Type 2 pseudowire is being tested, then the target attachment individual identifier (TAII) must be indicated. The **taii-type2** parameter is mutually exclusive with *sdp-id:vc-id*.

global-id — Specifies the global ID of the far end T-PE of the FEC129 pseudowire.

Values 0 to 4294967295

node-id — Specifies the node ID on far end T-PE that the pseudowire being tested is associated with.

Values ipv4-formatted address: a.b.c.d

1 to 4294967295

ac-id — Specifies an unsigned integer representing a locally unique TAII for the pseudowire being tested at the far end T-PE.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

spoke-sdp-fec-id — Specifies that if a FEC 129 PW is being tested, then its *spoke-sdp-fec-id* must be indicated with this parameter. The **spoke-sdp-fec-id** needs to exist on the local router and the far-end peer needs to indicate that it supports VCCV to allow the user to send vccv-ping message.

spoke-sdp-fec is mutually exclusive with the *sdp-id:vc-id* parameter.

Values 1 to 4294967295

assoc-channel {ipv4 | non-ip} — Specifies the associated channel encapsulation format to use for the VCCV trace echo request and echo reply packet for a PW that uses the static PW FEC. An associated channel type of ipv4 must be used if a vccv-ping is performed to a remote segment of a different FEC type.

Values ipv4 – IPv4 encapsulation in an IPv4 pseudowire associated channel (channel type 0x0021)

non-ip – MPLS-TP encapsulation without UDP/IP headers, in pseudowire associated channel using channel type 0x025.

Default non-ip

src-ip-address *ipv4-address* — Specifies the 4-octet IPv4 address of the source node.

Values a.b.c.d

sender-src-address *ipv4-address* — Specifies the 4-octet IPv4 address of the node originating the VCCV trace.

Values a.b.c.d

remote-dst-address *ipv4-address* — Specifies the 4-octet IPv4 address of the far end node that is a target of the VCCV Ping echo request. This parameter is only valid in combination with the **target-fec-type** *pw-id-fec*.

Values a.b.c.d

pw-id — Specifies the pseudowire ID to be used for performing a VCCV ping operation. The pseudowire ID is a non-zero 32-bit connection ID required by the FEC 128, as defined in RFC 8029, Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures.

Values 1 to 4294967295

pw-type — Specifies the PW type of the PW segment targeted on the far end node. This field must be included to populate the PW type field of the PW ID FEC in the FEC static TLV, when the far end FEC type is different form the local FEC type and the **target-fec-type** is **pw-id-fec**.

Values atm-cell (=3), atm-sdu (=2), atm-vcc (=9), atm-vpc (=10), cesopsn (=21), cesopsn-cas (=23), ether (=5), satop-e1 (=17), satop-t1 (=18), 1 to 65535

fc-name — Specifies the FC and profile parameters are used to indicate the forwarding class of the VCCV trace echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The LSP-EXP mappings on the receive network interface controls the mapping back to the internal forwarding class used by the far-end router that receives the message request. The egress mappings of the egress network interface on the far-end router controls the forwarding class markings on the return reply message. The LSP-EXP mappings on the receive network interface controls the mapping of the message reply at the originating router.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

When an MPLS echo request packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the specified FC and profile parameter values. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface. When the MPLS echo request packet is received on the responding node, The FC and profile parameter values are dictated by the LSP-EXP mappings of the incoming interface.

When an MPLS echo reply packet is generated in CPM and is forwarded to the outgoing interface, the packet is queued in the egress network queue corresponding to the FC and profile parameter values determined by the classification of the echo request packet, which is being replied to, at the incoming interface. The marking of the packet's EXP is dictated by the LSP-EXP mappings on the outgoing interface.

The ToS byte is not modified. Table 188 summarizes this behavior.

Table 188 **vccv trace Request Packet and Behavior**

CPM (sender node)	Echo request packet: • packet {tos=1, fc1, profile1} • fc1 and profile1 are as entered by user in OAM command or default values • tos1 as per mapping of {fc1, profile1} to IP precedence in network egress QoS policy of outgoing interface
Outgoing interface (sender node)	Echo request packet: • packet queued as {fc1, profile1} • ToS field=tos1 not remarked • EXP=exp1, as per mapping of {fc1, profile1} to EXP in network egress QoS policy of outgoing interface
Incoming interface (responder node)	Echo request packet: • packet {tos1, exp1} • exp1 mapped to {fc2, profile2} as per classification in network QoS policy of incoming interface
CPM (responder node)	Echo reply packet: • packet{tos=1, fc2, profile2}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Table 188 **vccv trace Request Packet and Behavior**

Outgoing interface (responder node)	Echo reply packet: • packet queued as {fc2, profile2} • ToS filed= tos1 not remarked (reply inband or out-of-band) • EXP=exp2, if reply is inband, remarked as per mapping of {fc2, profile2} to EXP in network egress QoS policy of outgoing interface
Incoming interface (sender node)	Echo reply packet: • packet {tos1, exp2} • exp2 mapped to {fc1, profile1} as per classification in network QoS policy of incoming interface

profile {in | out} — Specifies the profile state of the VCCV trace echo request packet.

Default out

interval-value — Specifies the interval parameter in seconds, expressed as a decimal integer. This parameter is used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the interval is set to 1 second, and the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 255

Default 1

no-response-count — Specifies the maximum number of consecutive VCCV trace echo requests, expressed as a decimal integer that do not receive a reply before the trace operation fails for a given TTL value.

Values 1 to 255

Default 5

max-vc-label-ttl — Specifies the TTL value for the VC label of the echo request message for the last hop of the MS-PW for which the results are to be displayed. This is expressed as a decimal integer. The outer label TTL is still set to the default regardless of the value of the VC label.

Values 1 to 255

Default 8

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

min-vc-label-ttl — Specifies the TTL value for the VC label of the echo request message for the first hop of the MS-PW for which the results are to be displayed. This is expressed as a decimal integer. Note that the outer label TTL is still set to the default regardless of the value of the VC label.

Values 1 to 255

Default 1

probe-count — Specifies the number of VCCV trace echo request messages to send per TTL value.

Values 1 to 10

Default 1

octets — Specifies the size in octets, expressed as a decimal integer, of the MPLS echo request packet, including the IP header but not the label stack. The request pay-load is padded with zeros to the specified size. An OAM command is not failed if the user enters a size lower than the minimum required to build the packet for the echo request message. The payload is automatically padded to meet the minimum size.

Values 1 to 9786

Default 1

timeout-value — Specifies the *timeout* parameter, in seconds, expressed as a decimal integer. This value is used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response are not received. A **request timeout** message is displayed by the CLI for each message request sent that expires. Any response received after the request times out is silently discarded.

Values 1 to 60

Default 3

Output

Sample Output

```
*A:138.120.214.60# oam vccv-trace 1:33
VCCV-TRACE 1:33  with 88 bytes of MPLS payload
1  1.1.63.63  rtt<10ms rc=8(DSRtrMatchLabel)
2  1.1.62.62  rtt<10ms rc=8(DSRtrMatchLabel)
3  1.1.61.61  rtt<10ms rc=3(EgressRtr)
```

Trace with detail:

```
*A:138.120.214.60>oam vccv-trace 1:33 detail

VCCV-TRACE 1:33  with 88 bytes of MPLS payload
1  1.1.63.63  rtt<10ms rc=8(DSRtrMatchLabel)
   Next segment: VcId=34 VcType=AAL5SDU Source=1.1.63.63 Remote=1.1.62.62
2  1.1.62.62  rtt<10ms rc=8(DSRtrMatchLabel)
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
   Next segment: VcId=35 VcType=AAL5SDU Source=1.1.62.62 Remote=1.1.61.61
3  1.1.61.61  rtt<10ms rc=3(EgressRtr)
SAA:

*A:multisim3>config>saa# info
----------------------------------------------
        test "vt1"
            shutdown
            type
                vccv-trace 1:2 fc "af" profile in timeout 2 interval 3 size 200
min-ttl 2 max-ttl 5 max-fail 2 probe-count 3
            exit
        exit
..
----------------------------------------------
*A:multisim3>config>saa#
```

Platforms All

26.26 ve-id

ve-id

Syntax **ve-id** *value*
no ve-id

Context **[Tree]** (config>service>epipe>bgp-vpws>ve-name ve-id)
[Tree] (config>service>epipe>bgp-vpws>remote-ve-name ve-id)

Full Context configure service epipe bgp-vpws remote-ve-name ve-id
configure service epipe bgp-vpws ve-name ve-id

Description This command configures a ve-id for either the local VPWS instance when configured under the ve-name, or for the remote VPWS instance when configured under the remote-ve-name.

A single ve-id can be configured per ve-name or remote-ve-name. The ve-id can be changed without shutting down the VPWS instance. When the ve-name ve-id changes, BGP withdraws the previously advertised route and sends a route-refresh to all the peers which would result in reception of all the remote routes again. The old PWs are removed and new ones are instantiated for the new ve-id value.

When the remote-ve-name ve-id changes, BGP withdraws the previously advertised route and send a new update matching the new ve-id. The old pseudowires are removed and new ones are instantiated for the new ve-id value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

NLRIs received whose advertised ve-id does not match the list of ve-ids configured under the remote ve-id will not have a spoke SDP binding auto-created but will remain in the BGP routing table but not in the Layer 2 route table. A change in the locally configured ve-ids may result in auto-sdp-bindings either being deleted or created, based on the new matching results.

Each ve-id configured within a service must be unique.

The **no** form of this command removes the configured ve-id. It can be used just when the BGP VPWS status is shutdown. The **no shutdown** command cannot be used if there is no ve-id configured.

Default no ve-id

Parameters *value* — A two bytes identifier that represents the local or remote VPWS instance and is advertised through the BGP NLRI.

Values 1 to 65535

Platforms All

ve-id

Syntax **ve-id** *ve-id-value*
no ve-id

Context **[Tree]** (config>service>vpls>bgp-vpls>ve-name ve-id)

Full Context configure service vpls bgp-vpls ve-name ve-id

Description This command configures a ve-id. Just one ve-id can be configured per BGP VPLS instance. The VE-ID can be changed without shutting down the VPLS Instance. When the VE-ID changes, BGP is withdrawing its own previously advertised routes and sending a route-refresh to all the peers which would result in reception of all the remote routes again. The old pseudowires are removed and new ones are instantiated for the new VE-ID value.

The **no** form of this command removes the configured ve-id. It can be used just when the BGP VPLS status is shutdown. The **no shutdown** command cannot be used if there is no ve-id configured.

Default no ve-id

Parameters *value* — Specifies a two-byte identifier that represents the local instance in a VPLS and is advertised through the BGP NLRI. Must be lower or equal with the max-ve-id.

Values 1 to 65535

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.27 ve-name

ve-name

Syntax [**no**] **ve-name** *name*

Context **[Tree]** (config>service>epipe>bgp-vpws ve-name)

Full Context configure service epipe bgp-vpws ve-name

Description This command configures the name of the local VPWS instance in this service.

The **no** form of this command removes the ve-name.

Parameters *name* — Specifies a site name up to 32 characters in length.

Platforms All

ve-name

Syntax **ve-name** *name*
no ve-name

Context **[Tree]** (config>service>vpls>bgp-vpls ve-name)

Full Context configure service vpls bgp-vpls ve-name

Description This command creates or edits a ve-name. Just one ve-name can be created per BGP VPLS instance.

The **no** form of this command removes the configured ve-name from the bgp vpls node. It can be used only when the BGP VPLS status is shutdown. The **no shutdown** command cannot be used if there is no ve-name configured.

Default no ve-name

Parameters *name* — Specifies the A character string to identify the VPLS Edge instance up to 32 characters in length

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.28 vendor-id

vendor-id

Syntax **vendor-id** *vendor-id*
no vendor-id

Context **[Tree]** (config>system>ned>profile vendor-id)

Full Context configure system network-element-discovery profile vendor-id

Description This command configures the vendor ID to be advertised.

The **no** form of this command reverts to the default value.

Default vendor-id "Nokia"

Parameters *vendor-id* — Specifies the vendor ID to be advertised with the profile, up to 255 characters.

Platforms All

26.29 vendor-specific-option

vendor-specific-option

Syntax [**no**] **vendor-specific-option**

Context **[Tree]** (config>service>ies>if>dhcp>option vendor-specific-option)
[Tree] (config>service>ies>sub-if>dhcp vendor-specific-option)
[Tree] (config>service>ies>sub-if>grp-if>dhcp>option vendor-specific-option)
[Tree] (config>service>vprn>if>dhcp>option vendor-specific-option)
[Tree] (config>service>vpls>sap>dhcp>option vendor-specific-option)
[Tree] (config>service>vprn>sub-if>grp-if>dhcp>option vendor-specific-option)
[Tree] (config>subscr-mgmt>msap-policy>vpls-only-sap-parameters>dhcp>option vendor-specific-option)

Full Context configure service ies interface dhcp option vendor-specific-option
configure service ies subscriber-interface dhcp vendor-specific-option
configure service ies subscriber-interface group-interface dhcp option vendor-specific-option
configure service vpls sap dhcp option vendor-specific-option
configure service vprn interface dhcp option vendor-specific-option
configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option

Description This command enables the Nokia vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure service vprn subscriber-interface group-interface dhcp option vendor-specific-option
- configure subscriber-mgmt msap-policy vpls-only-sap-parameters dhcp option vendor-specific-option
- configure service ies subscriber-interface group-interface dhcp option vendor-specific-option

All

- configure service vprn interface dhcp option vendor-specific-option
- configure service vpls sap dhcp option vendor-specific-option
- configure service ies interface dhcp option vendor-specific-option

vendor-specific-option

Syntax [**no**] **vendor-specific-option**

Context **[Tree]** (config>router>if>dhcp>option vendor-specific-option)

Full Context configure router interface dhcp option vendor-specific-option

Description This command configures the Nokia vendor specific suboption of the DHCP relay packet.

Platforms All

26.30 vendor-support

vendor-support

Syntax **vendor-support** [**three-gpp** | **vodafone**]
no vendor-support

Context **[Tree]** (config>subscr-mgmt>diam-appl-plcy>gy vendor-support)
[Tree] (config>aaa>diam-peer-plcy vendor-support)

Full Context configure aaa diameter-peer-policy vendor-support

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure subscriber-mgmt diameter-application-policy gy vendor-support

Description In a diameter peer policy, this command specifies the vendor support announced in the capability exchange. In a Gy diameter application policy, this command specifies the vendor specific attributes for the user sessions.

The **no** form of this command reverts to the default value.

Default vendor-support three-gpp

Parameters **three-gpp** — Specifies the 3GPP diameter policy vendor type.

vodafone — Specifies the vodafone diameter policy vendor type.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.31 version

version

Syntax **version** *version*
no version

Context **[Tree]** (config>subscr-mgmt>igmp-policy version)

Full Context configure subscriber-mgmt igmp-policy version

Description This command configures the version of IGMP.

The **no** form of this command reverts to the default value.

Default version 3

Parameters *version* — Specifies the IGMP version.

Values 1, 2 or 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

version

Syntax **version** *version*
no version

Context **[Tree]** (config>subscr-mgmt>msap-policy>vpls-only-sap-parameters>igmp-snp version)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters igmp-snooping version

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies the version of IGMP which is running on an MSAP. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.

When the **send-query** command is configured, all type of queries generated are of the configured **version**. If a report of a version higher than the configured version is received, the report gets dropped and a new “wrong version” counter is incremented.

If the **send-query** command is not configured, the **version** command has no effect. The version used on that SAP or SDP is the version of the querier. This implies that, for example, when there is a v2 querier, a v3 group or group-source specific query when a host wants to leave a certain group will never be sent.

Default version 3

Parameters *version* — Specifies the IGMP version.

Values 1, 2, 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

version

Syntax **version** *version*
no version

Context **[Tree]** (config>subscr-mgmt>mld-policy version)

Full Context configure subscriber-mgmt mld-policy version

Description This command configures the MLD version.

The **no** form of this command reverts to the default.

Default version 2

Parameters *version* — Specifies the MLD version.

Values 1, 2

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

version

Syntax **version** *version*
no version

Context **[Tree]** (config>router>wpp>portals>portal version)
[Tree] (config>service>vprn>wpp>portals>portal version)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure router wpp portals portal version
configure service vprn wpp portals portal version

Description This command configure the protocol version that is expected by the WPP portal.

The **no** form of this command reverts to the default.

Default version 1

Parameters *version* — Specifies the protocol version.

Values 1, 2

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

version

Syntax **version** *IMA-version*
no version

Context **[Tree]** (config>port>ml-bundle>ima version)

Full Context configure port multilink-bundle ima version

Description This command configures the IMA version for the multilink bundle group. If there is a version mismatch between this IMA group and the far end IMA group, the IMA group becomes operationally down. Automatic version changing is not supported. To change the IMA version, all member links must be removed from the group first.

Default version 1-1

Parameters *IMA-version* — Specifies the IMA version for this group.

Values 1-0: IMA version 1-0 1-1: IMA version 1-1

Platforms 7450 ESS, 7750 SR-7/12/12e

version

Syntax **version** *version*
no version

Context **[Tree]** (config>service>vpls>mesh-sdp>igmp-snooping version)
[Tree] (config>service>vpls>sap>igmp-snooping version)
[Tree] (config>service>vpls>spoke-sdp>igmp-snooping version)
[Tree] (config>service>vpls>mesh-sdp>mld-snooping version)
[Tree] (config>service>vpls>sap>mld-snooping version)
[Tree] (config>service>vpls>spoke-sdp>mld-snooping version)

Full Context configure service vpls mesh-sdp igmp-snooping version

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vpls mesh-sdp mld-snooping version
configure service vpls sap igmp-snooping version
configure service vpls sap mld-snooping version
configure service vpls spoke-sdp igmp-snooping version
configure service vpls spoke-sdp mld-snooping version

Description This command specifies the version of IGMP or MLD which is running on this SAP or SDP. This object can be used to configure a router capable of running either value. For IGMP or MLD to function correctly, all routers on a LAN must be configured to run the same version of IGMP or MLD on that LAN.

When the **send-query** command is configured, all type of queries generate ourselves are of the configured **version**. If a report of a version higher than the configured version is received, the report gets dropped and a new “wrong version” counter is incremented.

If the **send-query** command is not configured, the **version** command has no effect. The version used on that SAP or SDP is the version of the querier. This implies that, for example, when there is a v2 querier, a v3 group or group-source specific query when a host wants to leave a certain group will never be sent.

Parameters *version* — Specifies the IGMP or MLD version

Values 1, 2, 3

Platforms All

version

Syntax **version** *version*
no version

Context **[Tree]** (config>service>vprn>igmp>grp-if version)

Full Context configure service vprn igmp group-interface version

Description This command configures the version of IGMP.

The **no** form of this command removes the version.

Parameters *version* — Specifies the IGMP version.

Values 1, 2, or 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

version

Syntax **version** *version*
no version

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>igmp>if version)

Full Context configure service vprn igmp interface version

Description This command specifies the IGMP version. If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version. For IGMP to function correctly, all routers on a LAN should be configured to run the same version of IGMP on that LAN.

For IGMPv3, a multicast router that is also a group member performs both parts of IGMPv3, receiving and responding to its own IGMP message transmissions as well as those of its neighbors.

Default version 3

Parameters *version* — Specifies the IGMP version number.

Values 1, 2, 3

Platforms All

version

Syntax **version** *version*
no version

Context [Tree] (config>service>vprn>mld>if version)

Full Context configure service vprn mld interface version

Description This command specifies the MLD version. If routers run different versions, they will negotiate the lowest common version of MLD that is supported by hosts on their subnet and operate in that version. For MLD to function correctly, all routers on a LAN should be configured to run the same version of MLD on that LAN.

Default version 2

Parameters *version* — Specifies the MLD version number.

Values 1, 2

Platforms All

version

Syntax **version minimum** *minimum* **maximum** *maximum*
no version

Context [Tree] (config>service>nat>pcp-server-policy version)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service nat pcp-server-policy version

Description This command configures the accepted protocol version range.

Default version minimum 1 maximum 1

Parameters *minimum* — Specifies the minimum protocol version supported by the PCP servers using this PCP policy.

Values 1 to 255

maximum — Specifies the maximum protocol version supported by the PCP servers using this PCP policy.

Values 1 to 255

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

version

Syntax **version** *version*
no version

Context **[Tree]** (config>router>igmp>group-interface version)
[Tree] (config>router>igmp>if version)

Full Context configure router igmp group-interface version
configure router igmp interface version

Description This command specifies the IGMP version. If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version. For IGMP to function correctly, all routers on a LAN should be configured to run the same version of IGMP on that LAN.

For IGMPv3, a multicast router that is also a group member performs both parts of IGMPv3, receiving and responding to its own IGMP message transmissions as well as those of its neighbors.

Default version 3

Parameters *version* — Specifies the IGMP version number.

Values 1, 2, 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router igmp group-interface version

All

- configure router igmp interface version

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

version

Syntax **version** *version*
no version

Context **[Tree]** (config>router>mld>group-interface version)
[Tree] (config>router>mld>interface version)

Full Context configure router mld group-interface version
configure router mld interface version

Description This command specifies the MLD version. If routers run different versions of MLD, they will negotiate the lowest common version of MLD that is supported by hosts on their subnet and operate in that version. For MLD to function correctly, all routers on a LAN should be configured to run the same version of MLD on that LAN.

Default version 2

Parameters *version* — Specifies the MLD version number.

Values 1, 2

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

- configure router mld group-interface version

All

- configure router mld interface version

version

Syntax **version** *version*
no version

Context **[Tree]** (config>service>pw-template>igmp-snooping version)

Full Context configure service pw-template igmp-snooping version

Description This command specifies the version of IGMP. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.

When the **send-query** command is configured, all type of queries generated are of the configured **version**. If a report of a version higher than the configured version is received, the report gets dropped and a new “wrong version” counter is incremented.

If the **send-query** command is not configured, the **version** command has no effect. The version used on that SAP or SDP is the version of the querier. This implies that, for example, when there is a v2 querier, a v3 group or group-source specific query when a host wants to leave a certain group will never be sent.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default version 3

Parameters *version* — Specifies the IGMP version.

Values 1, 2, 3

Platforms All

version

Syntax **version** *file-url* [**check**]

Context **[Tree]** (file version)

Full Context file version

Description This command displays the version of an SR OS *.tim image file.

Parameters *file-url* — Specifies the file name of the target file.

Values

local-url	[*cflash-id*/][*file-path*] up to 200 characters, including *cflash-id* directory length up to 99 characters each
remote-url	[{ftp://| tftp://}*login*:*pswd*@*remote-locn*/ [*file-path*] up to 247 characters directory length 199 characters each
remote-locn	[*hostname* | *ipv4-address* | *ipv6-address*]
ipv4-address	*a.b.c.d*
ipv6-address	*x:x:x:x:x:x:x:x*[-*interface*] *x:x:x:x:x:x:d.d.d.d*[-*interface*] *x* - [0 to FFFF]H *d* - [0 to 255]D *interface* - up to 32 characters, for link local addresses
cflash-id	cf1:, cf1-A:, cf1-B:

check — Validates the SR OS *.tim image file.

Output The following output is an example of SR OS version information.

Sample Output

```
A:Redundancy>file cf3:\ # version  ftp://test:1234@192.0.2.79/usr/global/images/6.1/
R4/cpm.tim
TiMOS-C-6.1.R4 for 7750
Thu Oct 30 14:21:09 PDT 2018 by builder in /relx.1/b1/Rx/panos/main
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
A:Redundancy>file cf3:\ # version check ftp://test:1234@192.0.2.79/usr/global/
images/6.1/R4/cpm.tim
TiMOS-C-6.1.R4 for 7750
Thu Oct 30 14:21:09 PDT 2018 by builder in /relx.1/b1/Rx/panos/main
Validation successful
A:Redundancy>file cf3:\ #
```

Platforms All

version

Syntax **version** *ssh-version*
no version

Context **[Tree]** (config>system>security>ssh version)

Full Context configure system security ssh version

Description This command configures the SSH protocol version that is supported by the SSH server.

The **no** form of this command removes the SSH version from the configuration.

Parameters *ssh-version* — Specifies the SSH version.

Values 1 — Specifies that the SSH server will only accept connections from clients that support SSH protocol version 1 2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 2 1-2 — Specifies that the SSH server will accept connections from clients supporting either SSH protocol version 1, or SSH protocol version 2 or both.

Note: Values “1” and “1-2” are not permitted in FIPS-140-2 mode.

Default 2

Platforms All

26.32 vi

vi

Syntax **vi** *local-url*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (file vi)

Full Context file vi

Description Edit files using the vi editor. For more information, refer to "VI Editor" in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Basic System Configuration Guide*.

Parameters *local-url* — Specifies the local source file or directory.

Values *[cflash-id/]file-path*
cflash-id: cf1:, cf2:, cf3:

Platforms All

26.33 vid-pid-absent

vid-pid-absent

Syntax **vid-pid-absent** *milli-seconds*
no vid-pid-absent

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>video>analyzer>alarms vid-pid-absent)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video>analyzer>alarms vid-pid-absent)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video>analyzer>alarms vid-pid-absent)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video analyzer alarms vid-pid-absent
configure mcast-management multicast-info-policy bundle channel video analyzer alarms vid-pid-absent
configure mcast-management multicast-info-policy bundle video analyzer alarms vid-pid-absent

Description This command configures the analyzer to check for a VID PID within the specified time interval.

Default no vid-pid-absent

Parameters *milli-seconds* — Specifies the time, in milliseconds, for which to check for a VID PID.

Values 100 to 5000

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.34 video

video

Syntax **video**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy>bundle video)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel video)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override video)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video
configure mcast-management multicast-info-policy bundle channel video
configure mcast-management multicast-info-policy bundle video

Description Commands in this context configure video parameters.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

26.35 video-group

video-group

Syntax **video-group** *video-group-id* [**create**]
no video-group *video-group-id*

Context **[Tree]** (config>isa video-group)

Full Context configure isa video-group

Description This command configures an ISA video group.

Parameters *video-group-id* — Specifies a video group ID.

Values 1 to 4

create — Keyword required when first creating the configuration context. Once the context is created, one can navigate into the context without the **create** keyword.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

video-group

Syntax **video-group** *video-group-id*
video-group disable

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no video-group

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>video video-group)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>video video-group)
[Tree] (config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video video-group)

Full Context configure mcast-management multicast-info-policy bundle channel source-override video video-group
configure mcast-management multicast-info-policy bundle channel video video-group
configure mcast-management multicast-info-policy bundle video video-group

Description This command assigns a video group ID to the channel.

Parameters *video-group-id* — specifies the identifier for this video group. The video group must have been configured in the **config>isa** context.

Values 1 to 4

disable — Explicitly disables the video group within the policy.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

26.36 video-interface

video-interface

Syntax **video-interface** *ip-address* [**create**]
no video-interface *ip-address*

Context [Tree] (config>mcast-mgmt>mcast-info-plcy>video-policy video-interface)

Full Context configure mcast-management multicast-info-policy video-policy video-interface

Description This command creates a video interface policy context that correlates to the IP address assigned for a video interface. This interface is created in a subscriber service to which the multicast information policy is assigned. If the specified IP address does not correlate to a video interface ip address, the parameters defined within this context have no effect.

The **no** form of the command deletes the video interface policy context.

Parameters *ip-address* — The IP address of a video interface provisioned within the context of a service to which the Multicast Information Policy is assigned. If the IP address does not match the IP address assigned to a video interface, the parameters defined within this context have no effect.

create — Mandatory keyword needed when creating a new video interface within the video policy.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

video-interface

Syntax **video-interface** *ip-int-name* [**create**]
no video-interface *ip-int-name*

Context **[Tree]** (config>service>ies video-interface)
[Tree] (config>service>vpls video-interface)
[Tree] (config>service>vprn video-interface)

Full Context configure service ies video-interface
configure service vpls video-interface
configure service vprn video-interface

Description This command creates a video interface within the service. The video interface and associated IP addresses are the addresses to which clients within the service will send requests. The video interface must be associated with an ISA group using the video-sap command and have IP addresses for it to be functional.

The **no** form of the command deletes the video interface. The video interface must be administratively shut down before issuing the **no video-interface** command.

Default none

Parameters *ip-int-name* — Specifies the name of the video interface, up to 32 characters. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

create — This keyword is mandatory when creating a video interface.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

video-interface

Syntax [**no**] **video-interface** *video-ip-int-name*

Context **[Tree]** (debug>service>id video-interface)

Full Context debug service id video-interface

Description This command enables debugging for video interfaces.

The **no** form of the command disables the video interface debugging.

Parameters *video-ip-int-name* — Specifies the video interface name.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.37 video-policy

video-policy

Syntax **video-policy**

Context **[Tree]** (config>mcast-mgmt>mcast-info-plcy video-policy)

Full Context configure mcast-management multicast-info-policy video-policy

Description Commands in this context configure video interfaces and video services.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

26.38 video-sap

video-sap

Syntax **video-sap** *video-group-id*
no video-sap

Context **[Tree]** (config>service>ies>video-interface video-sap)
[Tree] (config>service>vpls>video-interface video-sap)
[Tree] (config>service>vprn>video-interface video-sap)

Full Context configure service ies video-interface video-sap
configure service vpls video-interface video-sap
configure service vprn video-interface video-sap

Description This command configures a service video interface association with a video group.

The **no** form of the command removes the video group association.

Default none

Parameters *video-group-id* — Specifies the video group ID number.

Values 1 to 4

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.39 video-template

video-template

Syntax **video-template**

Context **[Tree]** (config>app-assure>group>cflowd>rtp-perf video-template)

Full Context configure application-assurance group cflowd rtp-performance video-template

Description Commands in this context configure the video template for cflowd fields.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.40 view

view

Syntax **view** [*line*]

Context **[Tree]** (candidate view)

Full Context candidate view

Description This command displays the candidate configuration along with line numbers that can be used for editing the candidate configuration.

Parameters *line* — Displays the candidate configuration starting at the point indicated by the following options (the display is not limited to the current CLI context/branch).

Values

line, offset, **first**, **edit-point**, **last**

line	absolute line number
offset	relative line number to current edit point. Prefixed with '+' or '-'
first	keyword - first line
edit-point	keyword - current edit point
last	keyword - last line that is not 'exit'

view

Syntax **view** [*checkpoint-id* | **rescue** | **latest-rb**]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (admin>rollback view)

Full Context admin rollback view

Description This command displays the checkpoint.

Parameters **latest-rb** — Specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file).

checkpoint-id — Indicates rollback checkpoint file to be viewed. Checkpoint-id of 1 corresponds to the file-url.rb.1 rollback checkpoint file. The higher the id, the older the checkpoint. Max is the highest rollback checkpoint supported or configured.

Values 1 to 9

rescue — Displays the rescue configuration.

Platforms All

view

Syntax **view** {**bootup-cfg** | **active-cfg** | **candidate-cfg** | **latest-rb**| *checkpoint-id* | **rescue**}

Context [Tree] (admin view)

Full Context admin view

Description The context to configure administrative system viewing parameters. Only authorized users can execute the commands in the **admin** context.

Parameters **bootup-cfg** — Specifies the bootup configuration.

active-cfg — Specifies current running configuration.

candidate-cfg — Specifies candidate configuration.

latest-rb — Specifies the latest configuration.

checkpoint-id — Specifies a specific checkpoint file configuration.

Values 1 to 9

rescue — Specifies a rescue checkpoint configuration.

Platforms All

view

Syntax **view** *view-name* **subtree** *oid-value*
no view *view-name* [**subtree** *oid-value*]

Context [Tree] (config>system>security>snmp view)

Full Context configure system security snmp view

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a view. Views control the accessibility of a MIB object within the configured MIB view and subtree. Object identifiers (OIDs) uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.

Once the subtree (OID) is identified, a mask can be created to select the portions of the subtree to be included or excluded for access using this particular view. See the **mask** command.

The view(s) configured with this command can subsequently be used in read, write, and notify commands which are used to assign specific access group permissions to created views and assigned to particular access groups.

Multiple subtrees can be added or removed from a view name to tailor a view to the requirements of the user access group.

A subtree statement matches (covers) any OID that is a descendant of the specified OID value. For example, the subtree 1.3.6.1 matches 1.3.6.1.x (for any value of x), 1.3.6.1.x.y (for any values of x & y), and so on.

Subtrees that are not covered by **view** statements are not accessible in the view.

Per RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP),* each MIB view is defined by two sets of view subtrees, the included view subtrees, and the excluded view subtrees (see the **included** and **excluded** parameters of the **mask** command). Every such view subtree, both the included and the excluded ones, are defined in this table. To determine if a particular object instance is in a particular MIB view, compare the object instance's OID with each of the MIB view's active entries in this table. If none match, then the object instance is not in the MIB view. If one or more match, then the object instance is included in, or excluded from, the MIB view according to the value of vacmViewTreeFamilyType in the entry whose value of vacmViewTreeFamilySubtree has the most sub-identifiers.

The **no view** *view-name* command removes a view and all subtrees.

The **no view** *view-name* **subtree** *oid-value* removes a sub-tree from the view name.

Parameters *view-name* — Specifies a view name, up to 32 characters.

oid-value — Specifies the object identifier (OID) value for the *view-name*. This value, for example, 1.3.6.1.6.3.11.2.1, combined with the mask and include and exclude statements, configures the access available in the view.

It is possible to have a view with different subtrees with their own masks and include and exclude statements. This allows for customizing visibility and write capabilities to specific user requirements**.**

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.41 virtual-chassis-identifier

virtual-chassis-identifier

Syntax **virtual-chassis-identifier** *dual-homing-key*
no virtual-chassis-identifier

Context **[Tree]** (config>subscr-mgmt>wlan-gw virtual-chassis-identifier)

Full Context configure subscriber-mgmt wlan-gw virtual-chassis-identifier

Description This command specifies a virtual chassis identifier that can link two wlan-gws together.

The **no** form of this command removes the dual-homing-key.

Parameters *dual-homing-key* — Specifies the name of the dual homing key, up to 16 characters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.42 virtual-link

virtual-link

Syntax [**no**] **virtual-link** *router-id* **transit-area** *area-id*

Context **[Tree]** (config>service>vprn>ospf>area virtual-link)
[Tree] (config>service>vprn>ospf3>area virtual-link)

Full Context configure service vprn ospf area virtual-link
configure service vprn ospf3 area virtual-link

Description This command configures a virtual link to connect area border routers to the backbone via a virtual link.

The *router-id* specified in this command must be associated with the virtual neighbor. The transit area cannot be a stub area or a Not So Stubby Area (NSSA).

The **no** form of this command deletes the virtual link.

Default No virtual link is defined.

Parameters *router-id* — The router ID of the virtual neighbor in IP address dotted decimal notation.

transit-area *area-id* — The area-id specified identifies the transit area that links the backbone area with the area that has no physical connection with the backbone.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

virtual-link

Syntax [**no**] **virtual-link** *router-id* **transit-area** *area-id*

Context **[Tree]** (config>router>ospf>area virtual-link)
[Tree] (config>router>ospf3>area virtual-link)

Full Context configure router ospf area virtual-link
configure router ospf3 area virtual-link

Description This command configures a virtual link to connect area border routers to the backbone via a virtual link.

The *router-id* specified in this command must be associated with the virtual neighbor. The transit area cannot be a stub area or a Not So Stubby Area (NSSA).

The **no** form of this command deletes the virtual link.

By default, no virtual link is defined.

Default no virtual-link

Parameters *router-id* — Specifies the router ID of the virtual neighbor in IP address dotted decimal notation.

area-id — Specifies the area-id that identifies the transit area that links the backbone area with the area that has no physical connection with the backbone.

Platforms All

26.43 virtual-neighbor

virtual-neighbor

Syntax **virtual-neighbor** [*router-id*]
no virtual-neighbor

Context **[Tree]** (debug>router>ospf virtual-neighbor)
[Tree] (debug>router>ospf3 virtual-neighbor)

Full Context debug router ospf virtual-neighbor
debug router ospf3 virtual-neighbor

Description This command enables debugging for an OSPF virtual neighbor.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *router-id* — Specifies the router ID of the virtual neighbor.

Platforms All

26.44 virtual-scheduler-adjustment

virtual-scheduler-adjustment

Syntax **virtual-scheduler-adjustment**

Context **[Tree]** (config>card virtual-scheduler-adjustment)

Full Context configure card virtual-scheduler-adjustment

Description Commands in this context configure the virtual scheduler processing on the card. This is only applicable to queues and to policers parented to a scheduler.

Platforms All

26.45 virtual-subnet

virtual-subnet

Syntax [**no**] **virtual-subnet**

Context **[Tree]** (config>service>ies>sub-if>dhcp virtual-subnet)
[Tree] (config>service>vprn>sub-if>dhcp virtual-subnet)

Full Context configure service ies subscriber-interface dhcp virtual-subnet
configure service vprn subscriber-interface dhcp virtual-subnet

Description This command enables a virtual-subnet for DHCPv4 hosts under the subscriber interface. With this command configured, the system will snoop and record the default router address in the DHCP ACK message for the DHCPv4 ESM host. The system could answer ping or traceroute request even if the default router address is not configured on the subscriber-interface.

The **no** form of this command reverts to the default.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.46 vlan

vlan

Syntax **vlan** [*vlan-encap*]

Context **[Tree]** (config>redundancy>mc>peer>mcr>l3ring>node>cv vlan)

Full Context configure redundancy multi-chassis peer mc-ring l3-ring ring-node connectivity-verify vlan

Description This command specifies the VLAN tag of the SAP used for ring-node connectivity verification of this ring node. It is only meaningful if the value of is not zero.

The **no** form of this command reverts to the default.

Parameters *vlan-encap* — Specifies the node cc VLAN IP.

Platforms All

vlan

Syntax **vlan** *tag*
no vlan

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query vlan)

Full Context configure subscriber-mgmt wlan-gw ue-query vlan

Description This command enables matching on UEs, based on the VLAN tag within the tunnel, which typically used to indicate an SSID.

The **no** form of this command disables matching on the VLAN.

Default no vlan

Parameters *tag* — Specifies the VLAN tag.

Values 0 to 4096

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vlan

Syntax **vlan start** [*value*] **end** [*value*] **retail-svc-id** *service-id*
no vlan start [*value*] **end** [*value*]

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>retailer vlan)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>retailer vlan)

Full Context configure service ies subscriber-interface group-interface wlan-gw retailer vlan
configure service vprn subscriber-interface group-interface wlan-gw retailer vlan

Description This command creates a mapping from a range of VLANs (appearing in the wlan-gw encapsulated Layer 2 frame) to a retail service ID.

The **no** form of this command removes the parameters from the configuration.

Parameters **start** — Specifies the start VLAN tag of this range.

Values 0 to 4095

end — Specifies the end VLAN tag of this range.

Values 0 to 4095

retail-svc-id *service-id* — Specifies the identifier of the retail service to be used by default of a value in the retail service map of this interface.

Values 1 to 2147483650
svc-name: up to 64 characters

vlan

Syntax **vlan** *vlan-encap*
no vlan

Context [Tree] (config>redundancy>mc>peer>mcr>node>cv vlan)

Full Context configure redundancy multi-chassis peer mc-ring ring ring-node connectivity-verify vlan

Description This command specifies the VLAN tag used for the Ring-node Connectivity Verification of this ring node. It is only meaningful if the value of service ID is not zero. A zero value means that no VLAN tag is configured.

Default no vlan

Parameters *vlan-encap* — Specifies the VLAN tag.

Values

vlan-encap:	dot1q	qtag, *
	qinq	qtag1.qtag2, qtag1.*, 0.*
	qtag	0 to 4094
	qtag1	1 to 4094
	qtag2	0 to 4094

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vlan

Syntax **vlan** *vlan-id*
no vlan

Context **[Tree]** (cfg>eth-cfm>domain>assoc>bridge vlan)

Full Context configure eth-cfm domain association bridge-identifier vlan

Description This command configures the bridge identifier primary VLAN ID. This is informational only, and no verification is done to ensure MEPs on this association are on the configured VLAN.

The **no** form of this command reverts to the default value.

Default no vlan

Parameters *vlan-id* — Specifies a VLAN ID monitored by MA.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

26.47 vlan-id

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context **[Tree]** (config>app-assure>group>evt-log>syslog vlan-id)

Full Context configure application-assurance group event-log syslog vlan-id

Description This command configures the service port VLAN ID to be used by application assurance to inject the syslog events inband. This VLAN ID needs also to be configured for application assurance interface.

Default no vlan-id

Parameters *service-port-vlan-id* — Specifies the service port VLAN identifier.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context **[Tree]** (config>app-assure>group>http-redirect>captive-redirect vlan-id)

Full Context configure application-assurance group http-redirect captive-redirect vlan-id

Description This command configures the VLAN ID for captive redirect. Captive redirect uses the provisioned VLAN ID to send the HTTP response to subscribers; therefore this VLAN ID must be properly assigned in the same VPN as the subscriber.

Parameters *service-port-vlan-id* — Specifies the VLAN ID.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context **[Tree]** (config>app-assure>group>url-filter>icap vlan-id)

Full Context configure application-assurance group url-filter icap vlan-id

Description This command configures the VLAN ID on which the ISA-AA is expected to be emitting traffic mapping to a pre-configured aa-interface.

Default no vlan-id

Parameters *service-port-vlan-id* — Specifies the VLAN ID.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vlan-id

Syntax **vlan-id** *vlan-id*
no vlan-id

Context **[Tree]** (config>app-assure>group>url-filter>web-service vlan-id)

Full Context configure application-assurance group url-filter web-service vlan-id

Description This command configures the VLAN ID on which the AA ISA emits the traffic mapping to a preconfigured AA interface.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command removes the VLAN ID configuration.

Default no vlan-id

Parameters *vlan-id* — Specifies the VLAN ID to connect to the web service.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vlan-id

Syntax **vlan-id** *vlan-id*
no vlan-id

Context **[Tree]** (config>test-oam>build-packet>header>dot1q vlan-id)
[Tree] (debug>oam>build-packet>packet>field-override>header>dot1q vlan-id)

Full Context configure test-oam build-packet header dot1q vlan-id
debug oam build-packet packet field-override header dot1q vlan-id

Description This command defines the Dot1Q VLAN ID to be used in the test Dot1Q header.

The **no** form of this command removes the VLAN ID value.

Parameters *vlan-id* — Specifies the Dot1Q VLAN ID to be used in the test Dot1Q header.

Values 0 to 4095

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

vlan-id

Syntax **vlan-id** *service-port-vlan-id*
no vlan-id

Context **[Tree]** (config>app-assure>group>cflowd>dir-exp vlan-id)

Full Context configure application-assurance group cflowd direct-export vlan-id

Description This command configures the VLAN ID on which the ISA-AA is expected to be emitting traffic.

The **no** form of this command removes the VLAN ID from the configuration.

Default no vlan-id

Parameters *service-port-vlan-id* — Specifies the VLAN ID of the service port.

Values 1 to 4094

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.48 vlan-mismatch-timeout

vlan-mismatch-timeout

Syntax **vlan-mismatch-timeout** *seconds*
no vlan-mismatch-timeout

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>authentication vlan-mismatch-timeout)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>authentication vlan-mismatch-timeout)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication vlan-mismatch-timeout
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range authentication vlan-mismatch-timeout

Description This command configures the timeout value for the RADIUS proxy cache if a packet is received with a non-matching VLAN tag. The new timeout value is the lesser of the **vlan-mismatch-timeout** value and the currently remaining proxy cache timeout value.

The **no** form of this command disables the timeout behavior. The cache timeout value will remain unchanged.

Parameters *seconds* — Specifies the timeout value for the RADIUS proxy cache, in seconds.

Values 5 to 60

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.49 vlan-range

vlan-range

Syntax [**no**] **vlan-range** [*vlan-range*]

Context **[Tree]** (config>service>vpls>stp>mst-instance vlan-range)

Full Context configure service vpls stp mst-instance vlan-range

Description This command specifies a range of VLANs associated with a certain mst-instance. This range applies to all SAPs of the M-VPLS.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Every VLAN range that is not assigned within any of the created **config>service>vpls>stp mst-instance** is automatically assigned to mst-instance 0. This instance is automatically maintained by the software and cannot be modified. Changing the VLAN range value can be performed only when the specified mst-instance is shutdown.

The **no** form of this command removes the **vlan-range** from the specified **config>service>vpls>stp mst-instance**.

Parameters *vlan-range* — The first VLAN range specifies the left-bound (i.e., minimum value) of a range of VLANs that are associated with the M-VPLS SAP. This value must be smaller than (or equal to) the second VLAN range value. The second VLAN range specifies the right-bound (i.e., maximum value) of a range of VLANs that are associated with the M-VPLS SAP.

Values 1 to 4094 to 1 to 4094

Platforms All

vlan-range

Syntax **vlan-range** *from* [**to** *to*]
no vlan-range *from*

Context **[Tree]** (config>connection-profile-vlan vlan-range)

Full Context configure connection-profile-vlan vlan-range

Description This command allows the user to configure different ranges in the connection-profile-vlan. The ranges have the following characteristics:

- Ranges can contain a single VID or start-and-end values. When the *to-vid* is not specified, the end vid value is the same as the start vid value.
- On the fly addition/removal of ranges is allowed.
- When removing an entry, the **no vlan-range** *vid* **to** *vid* must be configured by the user.
- Multiple ranges are allowed under the same connection-profile-vlan. No VLAN values should overlap within the same connection-profile-vlan.
- The index for connection-profile and connection-profile-vlan must be unique between the two. For example, if **connection-profile 100** is present, then **connection-profile-vlan 100** is disallowed.

Each connection-profile-vlan must be explicitly configured.

Parameters *from* — Specifies the beginning of the **vlan-range** associated to the **connection-profile-vlan**.

Values 1 to 4094

to — Specifies the end of the **vlan-range** associated to the **connection-profile-vlan**. If not specified, the **vlan-range** is comprised of only the *from* VLAN ID.

Values 1 to 4094

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

26.50 vlan-tag-ranges

vlan-tag-ranges

Syntax **vlan-tag-ranges**

Context **[Tree]** (config>service>ies>sub-if>grp-if>wlan-gw vlan-tag-ranges)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw vlan-tag-ranges)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges

Description Commands in this context configure VLAN-to-retail-map parameters to map dot1q tags to the retail service ID. The WIFI AP inserts a dot1Q tag in the Layer 2 frame within the GRE tunnel to indicate the retail service provider for the subscriber.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.51 vlan-translation

vlan-translation

Syntax **vlan-translation** {*vlan-id* | **copy-outer**}
no vlan-translation

Context **[Tree]** (config>service>epipe>sap>ingress vlan-translation)
[Tree] (config>service>vpls>sap>ingress vlan-translation)

Full Context configure service epipe sap ingress vlan-translation
configure service vpls sap ingress vlan-translation

Description This command configures ingress VLAN translation. If enabled with an explicit VLAN value, the preserved VLAN ID is overwritten with this value. This setting is applicable to dot1q encapsulated ports. If enabled with the copy-outer keyword, the outer VLAN ID is copied to inner position on QinQ encapsulated ports. The feature is not supported on:

- Dot1q saps
- QinQ saps with qinq-vlan-translation
- Connection profile VLAN SAPs if the **copy-outer** option is configured

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** version of the command disables VLAN translation.

Default no vlan-translation

Parameters *vlan-id* — Specifies the VLAN id.

Values 0 to 4094

copy-outer — Specifies to use the outer VLAN id.

Platforms All

26.52 vlan-vc-etype

vlan-vc-etype

Syntax **vlan-vc-etype** *ethernet-type*
no vlan-vc-etype [*ethernet-type*]

Context **[Tree]** (config>service>sdp vlan-vc-etype)

Full Context configure service sdp vlan-vc-etype

Description This command configures the VLAN VC EtherType.

The **no** form of this command returns the value to the default.

Default no vlan-vc-etype

Parameters *ethernet-type* — Specifies a valid VLAN etype identifier.

Values 0x0600 to 0xffff

Platforms All

26.53 vlan-vc-tag

vlan-vc-tag

Syntax **vlan-vc-tag** *vlan-id*
no vlan-vc-tag [*vlan-id*]

Context **[Tree]** (config>service>vpls>spoke-sdp vlan-vc-tag)
[Tree] (config>service>vpls>mesh-sdp vlan-vc-tag)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service vpls mesh-sdp vlan-vc-tag
configure service vpls spoke-sdp vlan-vc-tag

Description This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.

The **no** form of this command disables the command.

Default no vlan-vc-tag

Parameters *vlan-id* — Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

Values 0 to 4094

Platforms All

vlan-vc-tag

Syntax **vlan-vc-tag** *vlan-id*
no vlan-vc-tag

Context **[Tree]** (config>service>sdp>binding>pw-port vlan-vc-tag)

Full Context configure service sdp binding pw-port vlan-vc-tag

Description This command sets tag relevant for vc-type vlan mode. This tag is inserted in traffic forwarded into the pseudowire.

The **no** form of the command reverts to the default value.

Default no vlan-vc-tag

Parameters *vlan-id* — Specifies the VLAN ID value.

Values 0 to 4094

Platforms All

vlan-vc-tag

Syntax **vlan-vc-tag** *tag*
no vlan-vc-tag *tag*

Context **[Tree]** (config>service>epipe>spoke-sdp vlan-vc-tag)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure service epipe spoke-sdp vlan-vc-tag

Description This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.

The **no** form of this command disables the command.

Default no vlan-vc-tag

Parameters *tag* — Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

Values 0 to 4094

Platforms All

vlan-vc-tag

Syntax **vlan-vc-tag** *vlan-id*
no vlan-vc-tag

Context **[Tree]** (config>service>pw-template vlan-vc-tag)

Full Context configure service pw-template vlan-vc-tag

Description This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.

The **no** form of this command disables the command.

Default no vlan-vc-tag

Parameters *vlan-id* — Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

Values 0 to 4094

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.54 vm

vm

Syntax **vm** *vm-id* [**create**]
no vm *vm-id*

Context **[Tree]** (config>esa vm)

Full Context configure esa vm

Description This command configures or creates an ESA-VM instance.

The **no** form of this command removes the ESA-VM from the system.

Parameters *vm-id* — Specifies the VM identifier.

Values 1 to 4

create — Mandatory keyword used when creating an ESA-VM in the config context

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

26.55 vm-traffic-distribution-by-ip

vm-traffic-distribution-by-ip

Syntax [**no**] **vm-traffic-distribution-by-ip**

Context **[Tree]** (config>isa>aa-grp vm-traffic-distribution-by-ip)

Full Context configure isa application-assurance-group vm-traffic-distribution-by-ip

Description This command enables the distribution of packets by IP address across virtual CPUs of a data plane VM. This allows support for AA subscribers whose bandwidth exceeds the processing throughput of a single vCPU.

The **no** form of this command enables traffic distribution by AA subscriber.

Default no vm-traffic-distribution-by-ip

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.56 vm-traffic-distribution-by-teid

vm-traffic-distribution-by-teid

Syntax [**no**] **vm-traffic-distribution-by-teid**

Context **[Tree]** (config>isa>aa-grp vm-traffic-distribution-by-teid)

Full Context configure isa application-assurance-group vm-traffic-distribution-by-teid

Description This command configures AA in VSR mode to load-balance traffic across different VM cores using TEID. Load-balancing is required when VSR is deployed on 3GPP S5/S8 (Gn/Gp) interfaces to provide GTP firewalling.

The **no** form of this command disables load-balancing of the traffic across the VM cores.

Default no vm-traffic-distribution-by-teid

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.57 vm-type

vm-type

Syntax **vm-type** *vm-type*
no vm-type

Context **[Tree]** (config>esa>vm vm-type)

Full Context configure esa vm vm-type

Description This command configures the type of ESA-VM instance.

The **no** form of this command removes the specified VM type.

Parameters *vm-type* — Specifies the VM type.

Values **aa** — Specifies Application Assurance feature support.
bb — Specifies broadband feature support, such as NAT.
tunnel — Specifies tunnel feature support, such as IPsec tunnels.
video — Specifies video feature support, such as FCC and RET (for 7750 SR and 7750 SR-12e only).

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.58 vmep-filter

vmep-filter

Syntax [**no**] **vmep-filter**

Context **[Tree]** (config>service>vpls>eth-cfm>sap vmep-filter)
[Tree] (config>service>vpls>eth-cfm>spoke-sdp vmep-filter)
[Tree] (config>service>vpls>eth-cfm>mesh-sdp vmep-filter)

Full Context configure service vpls eth-cfm mesh-sdp vmep-filter
configure service vpls eth-cfm sap vmep-filter
configure service vpls eth-cfm spoke-sdp vmep-filter

Description Suppress eth-cfm PDUs based on level lower than or equal to configured Virtual MEP. This command is not supported under a B-VPLS context. This will also delete any MIP configured on the SAP or Spoke-SDP.

The **no** form of this command reverts to the default values.

Default no vmep-filter

26.59 voice-template

voice-template

Syntax **voice template**

Context **[Tree]** (config>app-assure>group>cflowd>rtp-perf voice-template)

Full Context configure application-assurance group cflowd rtp-performance voice-template

Description Commands in this context configure the voice template for cflowd fields.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.60 volume

volume

Syntax **volume** *credits* {**bytes** | **kilobytes** | **megabytes** | **gigabytes**}

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no volume

Context [Tree] (config>subscr-mgmt>diam-appl-plcy>gy>efh>interim-c volume)

Full Context configure subscriber-mgmt diameter-application-policy gy extended-failure-handling interim-credit volume

Description This command configures the default volume interim credit that is allocated to all rating groups of a Diameter Gy session when Extended Failure Handling (EFH) is active and for which no default credit is configured at the category map category level.

The **no** form of this command resets the value to the default value.

Default volume 500 megabytes

Parameters *credits* — Specifies the amount of volume credit that is allocated by default to all rating groups of a Diameter Gy session when EFH is active.

Values 1 to 4294967295

bytes | **kilobytes** | **megabytes** | **gigabytes** — Specifies whether credits are in bytes, kilobytes, megabytes, or gigabytes.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

volume

Syntax **volume**

Context [Tree] (config>app-assure>group>cflowd volume)

Full Context configure application-assurance group cflowd volume

Description This command configures the cflowd volume export.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.61 volume-quota-direction

volume-quota-direction

Syntax **volume-quota-direction {both | ingress | egress}**
no volume-quota-direction

Context [Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range>dsm volume-quota-direction)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range>dsm volume-quota-direction)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt volume-quota-direction
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range distributed-sub-mgmt volume-quota-direction

Description This command specifies whether volume quota is applied in the egress (downstream), ingress (upstream), or both directions. Configuration changes apply only to new DSM UEs and not to existing UEs.

Parameters **both** — Enforces the volume quota on the packets ingressing and egressing the WLAN-GW combined.

ingress — Enforces the volume quota on packets ingressing the WLAN-GW from the UE (upstream).

egress — Enforces the volume quota on packets egressing the WLAN-GW to the UE (downstream).

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

26.62 volume-stats-type

volume-stats-type

Syntax **volume-stats-type** {**ip** | **default**}
no volume-stats-type

Context [Tree] (config>subscr-mgmt>sub-prof volume-stats-type)

Full Context configure subscriber-mgmt sub-profile volume-stats-type

Description This command enables the reporting of Layer 3 (IP) based subscriber host volume accounting data.

By default, subscriber host volume accounting data includes Layer 2 header octets and can be configured to include a fixed packet byte offset or last-mile encapsulation overhead.

The **no** form of this command reverts to the default.

Default volume-stats-type default

Parameters **default** — Specifies that the subscriber host volume accounting data is reported including the Layer 2 header octets and optional delta's introduced by configuration (for example: packet byte offset, last mile aware shaping, and so on).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ip — Specifies that the subscriber host volume accounting data reporting is based on Layer 3 (IP) packet sizes. This includes subscriber host ingress/egress queue and policer stats in snmp, CLI show commands, RADIUS and XML accounting, and Diameter Gx usage monitoring. RADIUS and Diameter (DCCA) based credit control volume quota are interpreted as Layer 3 (IP).

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.63 vpi

vpi

Syntax **vpi** *vpi* **egress-traffic-desc** *atm-td-profile-id*
no vpi *vpi*

Context **[Tree]** (config>port>sonet-sdh>path>atm vpi)

Full Context configure port sonet-sdh path atm vpi

Description This command enables the ATM VP shaper under the ATM port. The type of ATM shaper are CBR or rt/nrt-VBR as defined by the traffic descriptor. It cannot be a UBR service-type.

All VCs within the shaper degrades into a UBR type service class. For example, when a CBR type VC is associated with the shaper, it degrades into a UBR type VC. Scheduling traffic amongst VCs within the shaper is based on WRR using the weight parameter.

If the VP shaper is deleted, the VCs that were under it is restored to their original service category.

The VP shaper is statically configured and instantiated upon configuration.

A VP shaper can be seamlessly added to or removed from the active VCs in the system.

The **no** form of this command reverts to the default.

Parameters *vpi* — Specifies the VP identifier.

Values 0 to 4095

atm-td-profile-id — Specifies the ATM traffic description ID.

Values 1 to 1000

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.64 vpls

vpls

Syntax **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**b-vpls** | **i-vpls**] [**etree**] [**name** *name*]
no vpls *service-id*

Context **[Tree]** (config>service vpls)

Full Context configure service vpls

Description This command creates or edits a Virtual Private LAN Services (VPLS) instance. The **vpls** command is used to create or maintain a VPLS service. If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

A VPLS service connects multiple customer sites together acting like a zero-hop, Layer 2 switched domain. A VPLS is always a logical full mesh.

When a service is created, the **create** keyword must be specified if the **create** command is enabled in the **environment** context. When creating a service, you must enter the **customer** keyword and specify a *customer-id* to associate the service with a customer. The *customer-id* must already exist, having been created using the **customer** command in the **service** context. The *customer-id* must already exist having been created using the **customer** command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and re-created with a new customer association.

To create a management VPLS on the 7450 ESS, the m-vpls keyword must be specified. See section **Hierarchical VPLS Redundancy** for an introduction to the concept of management VPLS.

Once a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified will result in an error.

More than one VPLS service may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The **no** form of this command deletes the VPLS service instance with the specified *service-id*. The service cannot be deleted until all SAPs and SDPs defined within the service ID have been shut down and deleted, and the service has been shut down.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *service-id* — Specifies unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every router on which this service is defined.

Values *service-id*: 1 to 2147483647

svc-name: 64 characters maximum

customer *customer-id* — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number

Values 1 to 2147483647

Default null (0)

create — Keyword used to create the service ID. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

m-vpls — Specifies a management VPLS

e-tree — Specifies a VPLS service as an E-Tree VPLS. E-Tree VPLS services have root and leaf attachment circuit (AC) and root leaf tag SAPs/SDP bindings for E-Tree interconnection. The access root AC SAP behaves as a SAP in non-E-tree VPLS services. The leaf AC SAP communicates only with root-connected services. Leaf and root AC SAPs behave externally the same as SAPs in non-E-Tree VPLS services.

The root AC SDP bind behaves as an SDP bind in non-E-tree VPLS services. The leaf AC SDP bind communicates only with root-connected services.

In the E-Tree VPLS, the root AC SAP/SDP bindings can communicate with other root and leaf AC SAP/SDP bind services locally and remotely. Root-originated traffic is marked internally with a root indication and the root is tagged externally on tag SAP/SDP binds. The leaf AC SAP/SDP bindings can communicate with other root SAP/SDP bindings locally and remotely. Leaf-originated traffic is marked internally with a leaf indication and tagged externally on leaf tag SAP/SDP bindings.

Any number of root or leaf AC SAPs can be used, up to the configured SAP limits in the E-Tree VPLS.

Network-side root leaf tag SAPs use additional SAP resources. These tag SAPs used two tags; one for root and one for leaf. Network-side tag SDPs use a hard coded tag of 1 for root and 2 for leaf. AC SDP bindings are designated as root or leaf SDP bindings but carry no tags marking traffic on the egress frames.

The E-Tree SAP type must be specified when the SAP is created. To change the SAP type, the SAP must be removed and recreated.

b-vpls | i-vpls — Creates a backbone-vpls or ISID-vpls

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

name *name* — Configures an optional service name identifier, up to 64 characters, to a given service. This service name can then be used in configuration references, display, and show commands throughout the system. A defined service name can help the service provider or administrator to identify and manage services within the SR OS platforms.

To create a service, you must assign a service ID; however, after it is created, either the service ID or the service name can be used to identify and reference a service.

If a name is not specified at creation time, then SR OS assigns a string version of the *service-id* as the name.

Platforms All

vpls

Syntax **vpls** *service-name*
no vpls

Context **[Tree]** (config>service>ies>if vpls)

Full Context configure service ies interface vpls

Description The **vpls** command, within the IP interface context, is used to bind the IP interface to the specified service name (VPLS or I-VPLS).

The system does not attempt to resolve the service name provided until the IP interface is placed into the administratively up state (**no shutdown**). Once the IP interface is administratively up, the system will scan the available VPLS services that have the **allow-ip-int-bind** flag set for a VPLS service associated with the name. If the service name is bound to the service name when the IP interface is already in the administratively up state, the system will immediately attempt to resolve the given name.

If a VPLS service is found associated with the name and with the **allow-ip-int-bind** flag set, the IP interface is attached to the VPLS service allowing routing to and from the service virtual ports once the IP interface is operational.

A VPLS service associated with the specified name that does not have the **allow-ip-int-bind** flag set or a non-VPLS service associated with the name is ignored and will not be attached to the IP interface.

If the service name is applied to a VPLS service after the service name is bound to an IP interface and the VPLS service **allow-ip-int-bind** flag is set at the time the name is applied, the VPLS service is automatically resolved to the IP interface if the interface is administratively up or when the interface is placed in the administratively up state.

If the service name is applied to a VPLS service without the **allow-ip-int-bind** flag set, the system will not attempt to resolve the applied service name to an existing IP interface bound to the name. To rectify this condition, the flag must first be set and then the IP interface must enter or reenter the administratively up state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

While the specified service name may be assigned to only one service context in the system, it is possible to bind the same service name to more than one IP interface. If two or more IP interfaces are bound to the same service name, the first IP interface to enter the administratively up state (if currently administratively down) or to reenter the administratively up state (if currently administratively up) when a VPLS service is configured with the name and has the **allow-ip-int-bind** flag set is attached to the VPLS service. Only one IP interface is allowed to attach to a VPLS service context. No error is generated for the remaining non-attached IP interfaces using the service name.

Once an IP interface is attached to a VPLS service, the name associated with the service cannot be removed or changed until the IP interface name binding is removed. Also, the **allow-ip-int-bind** flag cannot be removed until the attached IP interface is unbound from the service name.

Unbinding the service name from the IP interface causes the IP interface to detach from the VPLS service context. The IP interface may then be bound to another service name or a SAP or SDP binding may be created for the interface using the **sap** or **spoke-sdp** commands on the interface.

VPRN Hardware Dependency

When a service name is bound to a VPRN IP interface, all SAPs associated with the VPRN service must be on hardware based on the FlexPath2 forwarding plane. Currently, these include the IOM3-XP and the various IMM modules. If any SAPs are associated with the wrong hardware type, the service name binding to the VPRN IP interface fails. Once an IP interface within the VPRN service is bound to a service name, attempting to create a SAP on excluded hardware fails.

IP Interface MTU and Fragmentation

A VPLS service is affected by two MTU values; port MTUs and the VPLS service MTU. The MTU on each physical port defines the largest Layer 2 packet (including all DLC headers and CRC) that may be transmitted out a port. The VPLS itself has a service level MTU that defines the largest packet supported by the service. This MTU does not include the local encapsulation overhead for each port (QinQ, Dot1Q, TopQ or SDP service delineation fields and headers) but does include the remainder of the packet. As virtual ports are created in the system, the virtual port cannot become operational unless the configured port MTU minus the virtual port service delineation overhead is greater than or equal to the configured VPLS service MTU. Thus, an operational virtual port is ensured to support the largest packet traversing the VPLS service. The service delineation overhead on each Layer 2 packet is removed before forwarding into a VPLS service. VPLS services do not support fragmentation and must discard any Layer 2 packet larger than the service MTU after the service delineation overhead is removed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IP interfaces have a configurable up MTU that defines the largest packet that may egress the IP interface without being fragmented. This MTU encompasses the IP portion of the packet and does not include any of the egress DLC header or CRC. This MTU does not affect the size of the largest ingress packet on the IP interface. If the egress IP portion of the packet is larger than the IP interface MTU and the IP header do not fragment flag is not set, the packet is fragmented into smaller packets that will not exceed the configured MTU size. If the do not fragment bit is set, the packet is silently discarded at egress when it exceeds the IP MTU.

When the IP interface is bound to a VPLS service, the IP MTU must be at least 18 bytes less than the VPLS service MTU. This allows for the addition of the minimal Ethernet encapsulation overhead; 6 bytes for the DA, 6 bytes for the SA, 2 bytes for the Etype and 4 bytes for the trailing CRC. Any remaining egress virtual port overhead (Dot1P, Dot1Q, QinQ, TopQ or SDP) required above the minimum is known to be less than the egress ports MTU since the virtual port would not be operational otherwise.

If the IP interface IP MTU value is too large based on the VPLS service MTU, the IP interface will enter the operationally down state until either the IP MTU is adequately lowered or the VPLS service MTU is sufficiently increased.

The **no** form of this command on the IP interface is used to remove the service name binding from the IP interface. If the service name has been resolved to a VPLS service context and the IP interface has been attached to the VPLS service, the IP interface will also be detached from the VPLS service.

Parameters *service-name* — The service-name parameter is required when using the IP interface vpls command and specifies the service name that the system will attempt to resolve to an **allow-ip-int-bind** enabled VPLS service associated with the name. The specified name is expressed as an ASCII string comprised of up to 32 characters. It does not need to already be associated with a service and the system does not check to ensure that multiple IP interfaces are not bound to the same name.

Platforms All

vpls

Syntax **vpls** *service-id*

Context **[Tree]** (config>subscr-mgmt>shcv-policy vpls)

Full Context configure subscriber-mgmt shcv-policy vpls

Description Commands in this context configure SHCV behavior in VPLS services. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 2 Services and EVPN Guide: VLL, VPLS, PBB, and EVPN* for VPLS service command syntax and descriptions.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.65 vpls-group

vpls-group

Syntax **vpls-group** *vpls-group-id* [**create**]
no vpls-group *vpls-group-id*

Context **[Tree]** (config>service>vpls vpls-group)

Full Context configure service vpls vpls-group

Description This command defines a vpls-group index. Multiple vpls-group commands can be specified to allow the use of different VPLS and SAP templates for different ranges of service ids. A vpls-group can be deleted only in shutdown state. Multiple commands under different vpls-group ids can be issued and can be in progress at the same time.

Default no vpls-group

Parameters *vpls-group-id* — Specifies the ID associated with the VPLS group

Values 1 to 4094

Platforms All

26.66 vpls-id

vpls-id

Syntax **vpls-id** *vpls-id*

Context **[Tree]** (config>service>vpls>bgp-ad vpls-id)

Full Context configure service vpls bgp-ad vpls-id

Description This command configures the VPLS ID component that is signaled in one of the extended community attributes (*ext-comm*).

Values and format (6 bytes, other 2 bytes of type-subtype is automatically generated)

Parameters *vpls-id* — Specifies a globally unique VPLS ID for BGP auto-discovery in this VPLS service

Values vpls-id: <ip-addr:comm-val>| <as-number:ext-comm-val>
ip-addr: a.b.c.d
comm-val: [0 to 65535]

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

as-number: [1 to 65535]
ext-comm-val: [0 to 4294967295]

Platforms All

26.67 vpls-only-sap-parameters

vpls-only-sap-parameters

Syntax **vpls-only-sap-parameters**

Context **[Tree]** (config>subscr-mgmt>msap-policy vpls-only-sap-parameters)

Full Context configure subscriber-mgmt msap-policy vpls-only-sap-parameters

Description Commands in this context configure MSAP VPLS properties.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.68 vpls-sap-template

vpls-sap-template

Syntax **vpls-sap-template** *name/id* **create**
[**no**] **vpls-sap-template** *name/id*

Context **[Tree]** (config>service>template vpls-sap-template)

Full Context configure service template vpls-sap-template

Description This is the command used to create a SAP template to be used in a vpls-template. Only certain existing VPLS SAP attributes can be changed in the vpls-sap-template, not in the instantiated VPLS SAP

The following SAP attributes are set in the instantiated saps (no configuration allowed):

description: “Sap <sap-id> controlled by MVRP service <svc id>” – auto generated

shutdown: no shutdown

Parameters *name/id* — Specifies the name in ASCII or the template ID

Values 1 to 2147483647

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

26.69 vpls-template

vpls-template

Syntax **vpls-template** *name/id* **create**
[**no**] **vpls-template** *name/id*

Context **[Tree]** (config>service>template vpls-template)

Full Context configure service template vpls-template

Description This command is used to create a vpls-template to be used to auto-instantiate a range of VPLS services. Only certain existing VPLS attributes specified in the command reference section can be changed in the vpls-template, not in the instantiated VPLS. The following attributes are automatically set in the instantiated VPLSs (no template configuration necessary) and the operator cannot change these values.

vpn-id: none

description: “Service <svc id> auto-generated by control VPLS <svc-id>”

service-name: “Service <svc id>” (Auto-generated)

shutdown: no shutdown

Following existing attributes can be set by the user in the instantiated VPLSs:

[no] sap

All the other VPLS attributes are not supported.

Parameters *name/id* — Specifies the name in ASCII or the template ID

Values name: ASCII string

Values ID: [1 to 2147483647]

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.70 vpls-template-binding

vpls-template-binding

Syntax **vpls-template-binding** *name/id*
no vpls-template-binding

Context **[Tree]** (config>service>vpls>vpls-group vpls-template-binding)

Full Context configure service vpls vpls-group vpls-template-binding

Description This command configures the binding to a VPLS template to be used to instantiate pre-provisioned data VPLS using as input variables the service IDs generated by the vid-range command.

The **no** form of this command removes the binding and deletes the related VPLS instances. The command will fail if any of the affected VPLS instances have either a provisioned SAP or an active MVRP declaration/registration or if the related vpls-group id is in no shutdown state. Any changes to the vpls-template-binding require the vpls-group to be in shutdown state.

Default no vpls-template-binding

Parameters *name/id* — Specifies the name or the ID of the VPLS template

Values 1 to 1024

Platforms All

26.71 vpn-apply-export

vpn-apply-export

Syntax [**no**] **vpn-apply-export**

Context **[Tree]** (config>router>bgp vpn-apply-export)
[Tree] (config>router>bgp>group vpn-apply-export)
[Tree] (config>router>bgp>group>neighbor vpn-apply-export)

Full Context configure router bgp group neighbor vpn-apply-export
configure router bgp group vpn-apply-export
configure router bgp vpn-apply-export

Description This command causes the base instance BGP export route policies to be applied to vpn-ipv4/6, mvpn-ipv4/6, l2-vpn, mdt-safi, mcast-vpn-ipv4, and evpn routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the application of the base instance BGP route policies to vpn-ipv4/6, mvpn-ipv4/6, l2-vpn, mdt-safi, mcast-vpn-ipv4, and evpn routes.

Default no vpn-apply-export

Platforms All

26.72 vpn-apply-import

vpn-apply-import

Syntax [**no**] **vpn-apply-import**

Context **[Tree]** (config>router>bgp vpn-apply-import)
[Tree] (config>router>bgp>group vpn-apply-import)
[Tree] (config>router>bgp>group>neighbor vpn-apply-import)

Full Context configure router bgp group neighbor vpn-apply-import
configure router bgp group vpn-apply-import
configure router bgp vpn-apply-import

Description This command causes the base instance BGP import route policies to be applied to vpn-ipv4/6, mvpn-ipv4/6, l2-vpn, mdt-safi, mcast-vpn-ipv4, and evpn routes.

The **no** form of this command disables the application of the base instance BGP import route policies to vpn-ipv4/6, mvpn-ipv4/6, l2-vpn, mdt-safi, mcast-vpn-ipv4, and evpn routes.

Default no vpn-apply-import

Platforms All

26.73 vpn-domain

vpn-domain

Syntax **vpn-domain** [*type* {**0005** | **0105** | **0205** | **8005**}] **id** *id*
no vpn-domain

Context **[Tree]** (config>service>vprn>ospf vpn-domain)

Full Context configure service vprn ospf vpn-domain

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command specifies type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object will result in an inconsistent value error when is not a VPRN instance. The parameters are mandatory and can be entered in either order. This command is not applicable in the **config>service>vprn>ospf3** context.

This command is not supported in OSPF3.

Default no vpn-domain

Parameters *id* — Specifies the OSPF VPN domain in the “xxxx.xxxx.xxxx” format. This is exchanged using BGP in the extended community attribute associated with a prefix. This object applies to VPRN instances of OSPF only.

type — Specifies the type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID.

Values 0005, 0105, 0205, 8005

Platforms All

26.74 vpn-family-policy

vpn-family-policy

Syntax **vpn-family-policy** *policy-name*
no vpn-family-policy

Context **[Tree]** (config>router>bgp>next-hop-resolution vpn-family-policy)

Full Context configure router bgp next-hop-resolution vpn-family-policy

Description This command specifies the VPN family policy that is applied when filtering routes for consideration for next-hop resolution process for EVPN and IP-VPN families.

This policy is supported by the following families:

- VPN-IPv4 and VPN-IPv6
- EVPN (all routes types 1-6, although AD per-ES and AD per-EVI routes are always shown as resolved)
- MCAST-VPN-IPv4 and MCAST-VPN-IPv6

In a VPN family policy:

- only prefix-lists are used to match the next hop of a resolving route. No other policy qualifiers are supported.
- the route resolving the next hop is accepted or rejected

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

In other words, if an imported route's next hop is resolved by route N (N is the preferred entry in tunnel-table for MPLS or the longest prefix match in the route-table for VXLAN), and route N is rejected by vpn-family-policy, then the route next hop is unresolved. This is irrespective of the existence of a route M that could potentially resolve the next hop in the tunnel-table or route-table.

The **no** form of this command removes the VPN family policy.

Default no vpn-family-policy

Parameters *policy-name* — Specifies the route policy name. Allowed values are any string up to 64 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

Platforms All

26.75 vpn-gre-source-ip

vpn-gre-source-ip

Syntax **vpn-gre-source-ip** *ip-address*
no vpn-gre-source-ip

Context **[Tree]** (config>service>system vpn-gre-source-ip)

Full Context configure service system vpn-gre-source-ip

Description This command configures a single system-wide alternate source IPv4 address of the GRE tunnels in all VPRN services using the **auto-bind-tunnel** or an explicit SDP binding (**config**>**service**>**vprn**>**spoke-sdp**) with a tunnel of encapsulation GRE.

A change to the value of the **vpn-gre-source-ip** parameter can be performed without disabling the service. Once the new value is configured, the system address is not used in services which bind to the GRE tunnel.

The primary IPv4 address of any local network IP interface, loopback or otherwise, may be used.

The address of the following interfaces are not supported, and the configuration is rejected:

- unnumbered network IP interface
- IES interface
- VPRN interface
- CSC VPRN interface

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **vpn-gre-source-ip** parameter value adheres to the following rules:

- This single source address counts towards the maximum of 15 distinct address values per system that are used by all GRE SDPs under the **config**>**service**>**sdp**>**local-end** context and all L2oGRE SDPs under the **config**>**service**>**system**>**gre-eth-bridged**>**tunnel-termination** context.
- The same source address can be used in both **vpn-gre-source-ip** and **config**>**service**>**sdp**>**local-end** contexts.
- The same source address cannot be used in both **vpn-gre-source-ip** and **config**>**service**>**system**>**gre-eth-bridged**>**tunnel-termination** contexts because an address configured for a L2oGRE SDP matches an internally created interface which is not available to other applications.
- The **vpn-gre-source-ip** address, when different from system, need not match the primary address of an interface which has the MPLS-over-GRE termination subnet configured, unless a GRE SDP or tunnel from the far-end router terminates on this address.

The **no** form of the command reverts to the default value.

Default vpn-gre-source-ip ip-address (System interface primary IPv4 address)

Parameters *ip-address* — Specifies the IPv4 address (a.b.c.d).

Platforms All

26.76 vpn-ipv4

vpn-ipv4

Syntax **vpn-ipv4 send** *send-limit* **receive** [**none**]
vpn-ipv4 send *send-limit*
no vpn-ipv4

Context **[Tree]** (config>router>bgp>add-paths vpn-ipv4)
[Tree] (config>router>bgp>group>add-paths vpn-ipv4)
[Tree] (config>router>bgp>group>neighbor>add-paths vpn-ipv4)

Full Context configure router bgp add-paths vpn-ipv4
configure router bgp group add-paths vpn-ipv4
configure router bgp group neighbor add-paths vpn-ipv4

Description This command configures the add-paths capability for VPN-IPv4 routes. By default, add-paths is not enabled for VPN-IPv4 routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The maximum number of paths per VPN-IPv4 NLRI to send is the configured send-limit, which is a mandatory parameter. The capability to receive multiple paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command the receive capability is enabled by default.

The **no** form of this command disables add-paths support for VPN-IPv4 routes, causing sessions established using add-paths for VPN-IPv4 to go down and come back up without the add-paths capability.

Default no vpn-ipv4

Parameters *send-limit* — Specifies the maximum number of paths per VPN-IPv4 NLRI that are allowed to be advertised to add-paths peers (the actual number of advertised routes may be less depending on the next-hop diversity requirement, other configuration options, route policies, or route advertisement rules). If the value is **multipaths**, then BGP advertises all of the used BGP multipaths for each VPN-IPv4 NLRI if the peer has signaled support for receiving multiple add paths. If the router has not installed any of the routes in its FIB then all BGP add-paths qualify for advertisement.

Values 1 to 16, none, multipaths

receive — Specifies that the router negotiates the add-paths receive capability for VPN-IPv4 routes with its peers.

none — Specifies that the router does not negotiate the add-paths receive capability for VPN-IPv4 routes with its peers.

Platforms All

26.77 vpn-ipv6

vpn-ipv6

Syntax **vpn-ipv6 send** *send-limit* **receive** [**none**]
vpn-ipv6 send *send-limit*
no vpn-ipv6

Context **[Tree]** (config>router>bgp>add-paths vpn-ipv6)
[Tree] (config>router>bgp>group>add-paths vpn-ipv6)
[Tree] (config>router>bgp>group>neighbor>add-paths vpn-ipv6)

Full Context configure router bgp add-paths vpn-ipv6
configure router bgp group add-paths vpn-ipv6
configure router bgp group neighbor add-paths vpn-ipv6

Description This command configures the add-paths capability for VPN-IPv6 routes. By default, add-paths is not enabled for VPN-IPv6 routes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The maximum number of paths per VPN-IPv6 NLRI to send is the configured send-limit, which is a mandatory parameter. The capability to receive multiple paths per prefix from a peer is configurable using the **receive** keyword, which is optional. If the **receive** keyword is not included in the command the receive capability is enabled by default.

The **no** form of this command disables add-paths support for VPN-IPv6 routes, causing sessions established using add-paths for VPN-IPv6 to go down and come back up without the add-paths capability.

Default no vpn-ipv6

Parameters *send-limit* — Specifies the maximum number of paths per VPN-IPv6 NLRI that are allowed to be advertised to add-paths peers (the actual number of advertised routes may be less depending on the next-hop diversity requirement, other configuration options, route policies, or route advertisement rules). If the value is **multipaths**, then BGP advertises all of the used BGP multipaths for each VPN-IPv6 NLRI if the peer has signaled support for receiving multiple add paths. If the router has not installed any of the routes in its FIB then all BGP add-paths qualify for advertisement.

Values 1 to 16, none, multipaths

receive — Specifies that the router negotiates the add-paths receive capability for VPN-IPv6 routes with its peers.

none — Specifies that the router does not negotiate the add-paths receive capability for VPN-IPv6 routes with its peers.

Platforms All

26.78 vpn-tag

vpn-tag

Syntax **vpn-tag** *vpn-tag*
no vpn-tag

Context **[Tree]** (config>service>vprn>ospf vpn-tag)

Full Context configure service vprn ospf vpn-tag

Description This command specifies the route tag for an OSPF VPN on a PE router. This field is set in the tag field of the OSPF external LSAs generated by the PE. This is mainly used to prevent routing loops. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object will result in an inconsistent value error when is not a VPRN instance.

This command is not supported in OSPF3.

Default vpn-tag 0

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

26.79 vport

vport

Syntax **vport** *name* [**create**]
no vport *name*

Context **[Tree]** (config>port>ethernet>access>egress vport)
[Tree] (config>port>sonet-sdh>path>access>egress vport)

Full Context configure port ethernet access egress vport
configure port sonet-sdh path access egress vport

Description This command configures a scheduling node, referred to as virtual port, within the context of an egress Ethernet port. The Vport scheduler operates either like a port scheduler with the difference that multiple Vport objects can be configured on the egress context of an Ethernet port, or it can be an aggregate rate when an egress port-scheduler policy is applied to the port.

The Vport is always configured at the port level even when a port is a member of a LAG.

When a port scheduler policy is applied to a Vport the following command is used:

config>**port**>**ethernet**>**access**>**egress**>**vport**>**port-scheduler-policy** *port-scheduler-policy-name*

The CLI will not allow the user to apply a port scheduler policy to a Vport if one has been applied to the port. Conversely, the CLI will not allow the user to apply a port scheduler policy to the egress of an Ethernet port if one has been applied to any Vport defined on the access egress context of this port. The **agg-rate**, along with an egress port-scheduler, can be used to ensure that a given Vport does not oversubscribe the port's rate.

SAP and subscriber host queues can be port-parented to a Vport scheduler in a similar way they port-parent to a port scheduler or can be port-parented directly to the egress port-scheduler if the **agg-rate** is used.

When the Vport uses an aggregate rate, the following command is used:

configure>port>ethernet>access>egress>vport>agg-rate-limit

The **no** form of this command removes the Vport name from the configuration.

Parameters *name* — Specifies the name of the Vport scheduling node and can be up to 32 ASCII characters. This does not need to be unique within the system but is unique within the port or a LAG.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure port sonet-sdh path access egress vport

All

- configure port ethernet access egress vport

vport

Syntax **vport** *vport-name*
no vport

Context **[Tree]** (config>service>sdp>binding>pw-port>egress>shaper vport)

Full Context configure service sdp binding pw-port egress shaper vport

Description This command configures the name of the Vport to be used for the PW port.

This command is valid for PW ports used for enhanced subscriber management (ESM on pseudowire) and pseudowire SAPs on Ethernet ports.

The **no** form of this command removes the configured Vport name.

Default no vport

Parameters *vport-name* — Specifies a text string, up to 32 characters, representing the name of the Vport.

Platforms All

vport

Syntax **vport** *vport*
no vport

Context **[Tree]** (config>service>epipe>pw-port>egress>shaper vport)

Full Context configure service epipe pw-port egress shaper vport

Description This command configures specifies the virtual port name of the shaper on the egress side for this PW-port entry.

Parameters *vport* — Specifies a virtual port applicable to all PW SAPs.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.80 vport-hashing

vport-hashing

Syntax [**no**] **vport-hashing**

Context **[Tree]** (config>subscr-mgmt>sub-prof vport-hashing)

Full Context configure subscriber-mgmt sub-profile vport-hashing

Description This command enables LAG Vport ID hashing. When enabled, Vport ID hashing can span multiple forwarding complexes on egress LAG. The default is to perform Vport ID hashing on egress and requires all active LAG members to be on the same forwarding complex.

Note: LAG hashing parameters that are configured under **config>lag**, for example, **per-link-hash**, take precedence and are incompatible with the **vport-hashing** command.

The **no** form of this command enables the default behavior.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

26.81 vprn

vprn

Syntax **vprn** *service-id* [**name** *name*] [**customer** *customer-id*] [**create**]
no vprn *service-id*

Context **[Tree]** (config>service vprn)

Full Context configure service vprn

Description This command creates or edits a Virtual Private Routed Network (VPRN) service instance.

If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

VPRN services allow the creation of customer-facing IP interfaces in the same routing instance used for service network core routing connectivity. VPRN services require that the IP addressing scheme used by the subscriber must be unique between it and other addressing schemes used by the provider and potentially the entire Internet.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

IP interfaces defined within the context of an VPRN service ID must have a SAP created as the access point to the subscriber network.

When a service is created, the **customer** keyword and *customer-id* must be specified and associates the service with a customer. The *customer-id* must already exist having been created using the customer command in the service context. When a service is created with a customer association, it is not possible to edit the customer association. The service must be deleted and re-created with a new customer association.

When a service is created, the use of the **customer** *customer-id* is optional to navigate into the service configuration context. If attempting to edit a service with the incorrect *customer-id* results in an error.

Multiple VPRN services are created to separate customer-owned IP interfaces. More than one VPRN service can be created for a single customer ID. More than one IP interface can be created within a single VPRN service ID. All IP interfaces created within an VPRN service ID belongs to the same customer.

The **no** form of this command deletes the VPRN service instance with the specified *service-id*. The service cannot be deleted until all the IP interfaces and all routing protocol configurations defined within the service ID have been shut down and deleted.

Parameters *service-id* — Specifies the unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7750 SR on which this service is defined.

Values

service-id:	1 to 2147483648
svc-name:	64 characters maximum

customer-id — Specifies an existing customer identification number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

name *name* — This parameter configures an optional VPRN name, up to 64 characters, which adds a name identifier to a given vprn to then use that vprn name in configuration references as well as display and use vprn names in show commands throughout the system. This helps the service provider/administrator to identify and manage vprn within the SR OS platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

If a name is not specified at creation time, then SR OS assigns a string version of the service-id as the name.

Service names may not begin with an integer (0 to 9).

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

create — Keyword used to create a service ID. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

Platforms All

vprn

Syntax [**no**] **vprn** *service-id* **interface** *ip-int-name*
[**no**] **vprn** *service-id* **network-interface** *ip-int-name*
[**no**] **vprn** *service-id* **subscriber-interface** *ip-int-name* **group-interface** *ip-int-name*

Context **[Tree]** (config>cflowd>collector>exp-filter>if-list>svc vprn)

Full Context configure cflowd collector export-filter interface-list service vprn

Description This command configures which VPRN service interfaces' flow data is being sent to this collector.

The **no** form of the command removes the values from the configuration.

Parameters *service-id* — Specifies the unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every SR OS on which this service is defined.

Values *service-id*:1 to 2147483647
svc-name:64 characters maximum

interface *ip-int-name* — Specifies the name of an IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters and must start with a letter. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

network-interface *ip-int-name* — Specifies the name of a network interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes and must start with a letter.

subscriber-interface *ip-int-name* — Specifies an interface name of a subscriber interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes and must start with a letter.

group-interface *ip-int-name* — Specifies an interface name of a group interface. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes and must start with a letter.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vprn

Syntax **vprn** *service-id* **ofc-loopback** *ip-address*
no vprn

Context **[Tree]** (config>open-flow>of-switch>of-controller vprn)

Full Context configure open-flow of-switch of-controller vprn

Description This command specifies the *service-id* of the VPRN to use for the OpenFlow control channel. The loopback address for the OF control channel in the VPRN is specified using the **ofc-loopback** option.

The **no** form of this command reverts the control channel to using base routing.

Parameters *service-id* — Specifies the service ID for a VPRN instance.

Values {*service-id* | *service-name*}
service-id: 1 to 2147483647
service-name: up to 64 characters (*service-name* is an alias for input only. The *service-name* gets replaced with an id automatically by SR OS in the configuration).

ip-address — Specifies the loopback IP address in the VPRN for the OpenFlow channel to the controller.

Values ip-address: a.b.c.d

Platforms All

vprn

Syntax **vprn** *service-id*
no vprn

Context **[Tree]** (config>system>security>vprn-aaa-server vprn)

Full Context configure system security vprn-aaa-server vprn

Description This command configures TACACS+ or RADIUS servers in a VPRN to be used for AAA by that VPRN and by sessions in VPRNs without a AAA server configured.

The **no** form of this command disables the use of servers in a VPRN.

Default no vprn

Parameters *service-id* — Specifies the VPRN server for AAA to use for sessions in VPRNs without a AAA server.

Values *service-id*: 1 to 2147483648
svc-name: 64 characters maximum

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

26.82 vprn-aaa-server

vprn-aaa-server

Syntax **vprn-aaa-server**

Context **[Tree]** (config>system>security vprn-aaa-server)

Full Context configure system security vprn-aaa-server

Description Commands in this context configure the use of AAA servers in a VPRN.

Platforms All

26.83 vprn-auto-bind

vprn-auto-bind

Syntax **vprn-auto-bind** [**include** | **exclude**]

Context **[Tree]** (config>router>mpls>lsp vprn-auto-bind)
[Tree] (config>router>mpls>lsp-template vprn-auto-bind)

Full Context configure router mpls lsp vprn-auto-bind
configure router mpls lsp-template vprn-auto-bind

Description This command determines whether the associated names LSP can be used or not as part of the auto-bind feature for VPRN services. By default, a names LSP is available for inclusion to be used for the auto-bind feature.

By configuring the command vprn-auto-bind exclude, the associated LSP will not be used by the auto-bind feature within VPRN services.

The **no** form of this command resets the flag back to the default value.

Default vprn-auto-bind include

Parameters **include** — Allows an associated LSP to be used by auto-bin for vprn services

exclude — Disables the use of the associated LSP to be used with the auto-bind feature for VPRN services.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

26.84 vprn-local

vprn-local

Syntax **vprn-local** [{**none** | **all** | **vc-only**}]

Context **[Tree]** (config>router>ttl-propagate vprn-local)

Full Context configure router ttl-propagate vprn-local

Description This command configures the TTL propagation for locally generated packets which are forwarded over a MPLS LSPs in all VPRN service contexts.

For vpn-ipv4 and vpn-ipv6 packets forwarded in the context of all VPRN services in the system, including 6VPE packets, the all value of the command enables TTL propagation from the IP header into all labels in the stack:

The user can enable the TTL propagation behavior separately for locally generated packets by CPM (vprn-local) and for user and control packets in transit at the node (vprn-transit).

The vc-only value reverts to the default behavior by which the IP TTL is propagated into the VC label but not to the transport labels in the stack. The user can explicitly set the default behavior by configuring the vc-only value. This command does not have a no version.

The value none allows the user to disable the propagation of the IP TTL to all labels in the stack, including the VC label. This is needed for a transparent operation of UDP traceroute in VPRN inter-AS option B such that the ingress and egress ASBR nodes are not traced.

The user can override the global configuration within each VPRN instance using the following commands:

- config service vprn ttl-propagate local [inherit | none | vc-only | all]
- config service vprn ttl-propagate transit [inherit | none | vc-only | all]

The default behavior for a given VPRN instance is to inherit the global configuration for the same command. The user can explicitly set the default behavior by configuring the inherit value.

When a packet is received in a VPRN context but is looked up in the Global Routing Table (GRT), for example, leaking to GRT is enabled, the behavior of the TTL propagation is governed by the RSVP or LDP shortcut configuration when the matching routing is a LSP shortcut route. It is governed by the BGP label route configuration when the matching route is a RFC 3107 label route or a 6PE route.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

When a packet is received on one VPRN instance and is redirected using Policy Based Routing (PBR) to be forwarded in another VPRN instance, the TTL propagation is governed by the configuration of the outgoing VPRN instance.

Default vprn-local vc-only

Parameters **none** — Specifies that the TTL of the IP packet is not propagated into the VC label or labels in the transport label stack

all — Specifies that the TTL of the IP packet is propagated into the VC label and all labels in the transport label stack.

vc-only — Specifies that the TTL of the IP packet is propagated into the VC label and not into the labels in the transport label stack.

Platforms All

26.85 vprn-network-exceptions

vprn-network-exceptions

Syntax **vprn-network-exceptions** *number seconds*
no vprn-network-exceptions

Context **[Tree]** (config>system>security vprn-network-exceptions)

Full Context configure system security vprn-network-exceptions

Description This command configures the rate to limit the processing of packets with label TTL expiry received within an LSP shortcut, or within all VPRN instances in the system, and from all network IP interfaces. This includes labeled user and control plane packets, ping and traceroute packets within GRT and VPRN, and ICMP replies. Packets over the configured rate are dropped.

This feature does not rate limit MPLS and service OAM packets (vprn-ping, vprn-trace, lsp-ping, lsp-trace, vccv-ping, and vccv-trace).

The **no** form of this command disables the rate limiting of the reply to these packets.

Parameters *number* — Specifies the number limit of MPLS exception messages.

Values 10 to 10,000

seconds — Specifies the rate limit of MPLS exception messages, in seconds.

Values 1 to 60

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.86 vprn-ping

vprn-ping

Syntax **vprn-ping** {*service-id* | **service** *service-name*} **source** *ip-address* **destination** *ip-address* [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *size*] [**ttl** *vc-label-ttl*] [**count** *send-count*] [**return-control**] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam vprn-ping)
[Tree] (config>saa>test>type vprn-ping)

Full Context configure saa test type vprn-ping
oam vprn-ping

Description This command performs a VPRN ping and applies only to the 7750 SR and 7950 XRS.

Parameters *service-id* — Specifies the VPRN service ID to diagnose or manage.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **configure saa test type vprn-ping service** *service-name* variant can be used in all configuration modes.

Values 1 to 2147483647

service-name — Specifies the VPRN service name to diagnose or manage, up to 64 characters.

source *ip-address* — Specifies an unused IP address in the same network that is associated with the VPRN.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

destination *ip-address* — Specifies the IP address to be used as the destination for performing a VPRN ping operation.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc-name — Specifies the forwarding class of the MPLS echo request encapsulation.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile state of the MPLS echo request encapsulation.

Default out

size — Specifies the OAM request packet size in bytes, expressed as a decimal integer.

Values 1 to 9786

Default 72

vc-label-ttl — Specifies the TTL value in the VC label for the OAM request, expressed as a decimal integer.

Values 1 to 255

Default 255

send-count — Specifies the number of messages to send. The **count** parameter is used to override the default number of message requests sent. Each message request must either time out or receive a reply before the next message request is sent. The message **interval** value must have expired before the next message request is sent.

Values 1 to 100

Default 1

return-control — Specifies the response to come on the control plane.

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response was not received. Any response received after the request times out is silently discarded.

Values 1 to 100

Default 5

interval — Specifies the interval time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second where the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

Output

Sample Output

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
A:PE_1# oam vprn-ping 25 source 10.4.128.1 destination 10.16.128.0
Sequence Node-id                                Reply-Path Size     RTT
-------------------------------------------------------------------------------
[Send request Seq. 1.]
1        10.128.0.3:cpm                          In-Band   100      0ms
-------------------------------------------------------------------------------
...
A:PE_1#
-------------------------------------------------------------------------------
A:PE_1#
```

Platforms All

26.87 vprn-trace

vprn-trace

Syntax **vprn-trace** {*service-id* | **service** *service-name*} **source** *ip-address* **destination** *ip-address* [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *size*] [**min-ttl** *min-vc-label-ttl*] [**max-ttl** *max-vc-label-ttl*] [**probe-count** *send-count*] [**return-control**] [**timeout** *timeout*] [**interval** *interval*]

Context **[Tree]** (oam vprn-trace)
[Tree] (config>saa>test>type vprn-trace)

Full Context configure saa test type vprn-trace
oam vprn-trace

Description This command is used to perform a VPRN trace.

Parameters *service-id* — Specifies the VPRN service ID to diagnose or manage.

This variant of the command is only supported in 'classic' configuration-mode (**configure system management-interface configuration-mode classic**). The **configure saa test type vprn-trace service** *service-name* variant can be used in all configuration modes.

Values 1 to 2147483647

service-name — Specifies the VPRN service name to diagnose or manage, up to 64 characters.

source *ip-address* — Specifies the IP address for the source IP address in dotted decimal notation.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

x: [0 to FFFF]H
d: [0 to 255]D

destination *ip-address* — Specifies the IP address to be used as the destination for performing an vprn-trace operation.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

fc-name — Specifies the forwarding class of the MPLS echo request encapsulation.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Specifies the profile state of the MPLS echo request encapsulation.

Default out

size — Specifies the OAM request packet size in bytes.

Values 1 to 9786

Default 1

min-vc-label-ttl — Specifies the minimum TTL value in the VC label for the trace test.

Values 1 to 255

Default 1

max-vc-label-ttl — Specifies the maximum TTL value in the VC label for the trace test.

Values 1 to 255

Default 4

send-count — Specifies the number of OAM requests sent for a TTL value.

Values 1 to 10

Default 1

return-control — Specifies the OAM reply to a data plane OAM request be sent using the control plane instead of the data plane.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

timeout — Specifies the time, in seconds, used to override the default *timeout* value and is the amount of time that the router waits for a message reply after sending the message request. Upon the expiration of the message time out, the requesting router assumes that the message response was not received. Any response received after the request times out is silently discarded.

Values 1 to 60

Default 3

interval — Specifies the time, in seconds, used to override the default request message send interval and defines the minimum amount of time that must expire before the next message request is sent.

If the **interval** is set to 1 second where the *timeout* value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of a message reply corresponding to the outstanding message request.

Values 1 to 10

Default 1

Output

Sample Output

```
A:PE_1# oam vprn-trace 25 source 10.4.128.1 destination 10.16.128.0
TTL Seq Reply Node-id         Rcvd-on         Reply-Path RTT
-------------------------------------------------------------------------------
[Send request TTL: 1, Seq. 1.]
1   1   1     10.128.0.4      cpm             In-Band    0ms
  Requestor 10.128.0.1 Route: 0.0.0.0/0
    Vpn Label: 131071 Metrics 0 Pref 170 Owner bgpVpn
    Next Hops: [1] ldp tunnel
    Route Targets: [1]: target:65100:1
  Responder 10.128.0.4 Route: 10.16.128.0/24
    Vpn Label: 131071 Metrics 0 Pref 170 Owner bgpVpn
    Next Hops: [1] ldp tunnel
    Route Targets: [1]: target:65001:100

[Send request TTL: 2, Seq. 1.]
2   1   1     10.128.0.3      cpm             In-Band    0ms
  Requestor 10.128.0.1 Route: 0.0.0.0/0
    Vpn Label: 131071 Metrics 0 Pref 170 Owner bgpVpn
    Next Hops: [1] ldp tunnel
    Route Targets: [1]: target:65100:1
  Responder 10.128.0.3 Route: 10.16.128.0/24
    Vpn Label: 0 Metrics 0 Pref 0 Owner local
    Next Hops: [1] ifIdx 2 nextHopIp 10.16.128.0

[Send request TTL: 3, Seq. 1.]
[Send request TTL: 4, Seq. 1.]
...
-------------------------------------------------------------------------------
A:PE_1#
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

26.88 vprn-transit

vprn-transit

Syntax **vprn-transit** [{**none** | **all** | **vc-only**}]

Context **[Tree]** (config>router>ttl-propagate vprn-transit)

Full Context configure router ttl-propagate vprn-transit

Description This command configures the TTL propagation for in transit packets which are forwarded over a MPLS LSPs in all VPRN service contexts. For vpn-ipv4 and vpn-ipv6 packets forwarded in the context of all VPRN services in the system, including 6VPE packets, the all value of the command enables TTL propagation from the IP header into all labels in the stack:

The user can enable the TTL propagation behavior separately for locally generated packets by CPM (vprn-local) and for user and control packets in transit at the node (vprn-transit).

The vc-only value reverts to the default behavior by which the IP TTL is propagated into the VC label but not to the transport labels in the stack. The user can explicitly set the default behavior by configuring the vc-only value. This command does not have a no version.

The value none allows the user to disable the propagation of the IP TTL to all labels in the stack, including the VC label. This is needed for a transparent operation of UDP trace-route in VPRN inter-AS option B such that the ingress and egress ASBR nodes are not traced.

The user can override the global configuration within each VPRN service instance using the following commands:

- config service vprn ttl-propagate local [inherit | none | vc-only | all]
- config service vprn ttl-propagate transit [inherit | none | vc-only | all]

The default behavior for a given VPRN instance is to inherit the global configuration for the same command. The user can explicitly set the default behavior by configuring the inherit value.

When a packet is received in a VPRN context but is looked up in the Global Routing Table (GRT), for example, leaking to GRT is enabled, the behavior of the TTL propagation is governed by the RSVP or LDP shortcut configuration when the matching routing is a LSP shortcut route. It is governed by the BGP label route configuration when the matching route is a RFC 3107 label route or a 6PE route.

When a packet is received on one VPRN instance and is redirected using Policy Based Routing (PBR) to be forwarded in another VPRN instance, the TTL propagation is governed by the configuration of the outgoing VPRN instance

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default vprn-transit vc-only

Parameters **none** — Specifies that the TTL of the IP packet is not propagated into the VC label or labels in the transport label stack

all — Specifies that the TTL of the IP packet is propagated into the VC label and all labels in the transport label stack.

vc-only — Specifies that the TTL of the IP packet is propagated into the VC label and not into the labels in the transport label stack.

Platforms All

26.89 vrf-export

vrf-export

Syntax **vrf-export** *plcy-or-long-expr* [*plcy-or-expr*]
no vrf-export

Context **[Tree]** (config>service>vprn>bgp-evpn>mpls vrf-export)
[Tree] (config>service>vprn>bgp-ipvpn>mpls vrf-export)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 vrf-export)

Full Context configure service vprn bgp-evpn mpls vrf-export
configure service vprn bgp-ipvpn mpls vrf-export
configure service vprn bgp-ipvpn segment-routing-v6 vrf-export

Description This command configures route policies that control how routes are exported from the local VRF to other VRFs on the same or remote PE routers (using MP-BGP). Route policies are configured in the **config>router>policy-options** context.

The **vrf-export** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine final action to accept or reject the route.

Only one of the 15 objects referenced by the **vrf-export** command can be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters while the remaining 14 objects have a maximum length of 64 characters each.

When multiple **vrf-export** commands are issued, the last command entered overrides the previous command.

Aggregate routes are not advertised using MP-BGP protocols to the other MP-BGP peers.

The **no** form of this command removes all route policy names from the **vrf-export** list.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no vrf-export

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters).

plcy-or-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Up to 14 policies may be entered.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service vprn bgp-ipvpn segment-routing-v6 vrf-export

All

- configure service vprn bgp-ipvpn mpls vrf-export
- configure service vprn bgp-evpn mpls vrf-export

vrf-export

Syntax **vrf-export** {**unicast** | *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]]}
no vrf-export

Context **[Tree]** (config>service>vprn>mvpn vrf-export)

Full Context configure service vprn mvpn vrf-export

Description This command specifies the export policy to control MVPN routes exported from the local VRF to other VRFs on the same or remote PE routers.

Default vrf-export unicast

Parameters **unicast** — Specifies to use unicast VRF export policy for the MVPN.

plcy-or-long-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Allowed values are any string up to 255 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

plcy-or-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Allowed values are any string up to 64 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. Up to 14 policies can be specified in a single statement.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.90 vrf-import

vrf-import

Syntax **vrf-import** *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]]
no vrf-import

Context **[Tree]** (config>service>vprn>bgp-evpn>mpls vrf-import)
[Tree] (config>service>vprn>bgp-ipvpn>mpls vrf-import)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 vrf-import)

Full Context configure service vprn bgp-evpn mpls vrf-import
configure service vprn bgp-ipvpn mpls vrf-import
configure service vprn bgp-ipvpn segment-routing-v6 vrf-import

Description This command configures route policies that control how VPN-IP and EVPN-IFL routes exported by other VRFs, on the same or remote PEs, are imported into the local VRF. Route policies are configured in the **config>router>policy-options** context.

The **vrf-import** command can reference up to 15 objects, where each object is either a policy logical expression or the name of a single policy. The objects are evaluated in the specified order to determine final action to accept or reject the route

Only one of the 15 objects referenced by the **vrf-import** command is allowed to be a policy logical expression consisting of policy names (enclosed in square brackets) and logical operators (AND, OR, NOT). The first of the 15 objects has a maximum length of 255 characters while the remaining 14 objects have a maximum length of 64 characters each.

When multiple **vrf-import** commands are issued, the last command entered overrides the previous command.

The **no** form of this command removes all route policy names from the import list

Note: Unless the preference value is changed by the policy, BGP-VPN and EVPN-IFL routes imported with a **vrf-import** policy have the preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs on the same router.

Default no vrf-import

Parameters *plcy-or-long-expr* — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters).

plcy-or-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters).

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- configure service vprn bgp-ipvpn segment-routing-v6 vrf-import

All

- configure service vprn bgp-evpn mpls vrf-import
- configure service vprn bgp-ipvpn mpls vrf-import

vrf-import

Syntax **vrf-import** {**unicast** | *plcy-or-long-expr* [*plcy-or-expr* [*plcy-or-expr*]}
no vrf-import

Context **[Tree]** (config>service>vprn>mvpn vrf-import)

Full Context configure service vprn mvpn vrf-import

Description This command specifies the import policy to control MVPN routes imported to the local VRF from other VRFs on the same or remote PE routers.

Default vrf-import unicast

Parameters **unicast** — Specifies to use a unicast VRF import policy for the MVPN.

plcy-or-long-expr — Specifies the route policy name (up to 64 characters) or a policy logical expression (up to 255 characters). Allowed values are any string up to 255 characters in length composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes.

plcy-or-expr — Specifies the route policy statement name or a policy logical expression. Allowed values are any string up to 64 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed between double quotes. Up to 14 policies can be specified in a single statement.

Platforms All

26.91 vrf-target

vrf-target

Syntax **vrf-target** {*ext-community* | **export** *ext-community* | **import** *ext-community* | **export** *ext-community* **import** *ext-community*}
no vrf-target

Context **[Tree]** (config>service>vprn>bgp-evpn>mpls vrf-target)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>vprn>bgp-ipvpn>mpls vrf-target)
[Tree] (config>service>vprn>bgp-ipvpn>srv6 vrf-target)

Full Context
configure service vprn bgp-evpn mpls vrf-target
configure service vprn bgp-ipvpn mpls vrf-target
configure service vprn bgp-ipvpn segment-routing-v6 vrf-target

Description
This command provides a simplified method to configure the route target added to advertised routes or compared against received routes from other VRFs on the same or remote PE routers (using MP-BGP).

BGP-VPN and EVPN-IFL routes imported with a VRF target policy use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs in the same router.

Specified VRF import or VRF export policies override the VRF target policy.

The **no** form of this command removes the VRF target policy.

Default
no vrf-target

Parameters
ext-comm — Specifies an extended BGP community in the *type:x:y* format. The value *x* can be an integer or IP address. The *type* can be the target or origin. *y* can be 16-bit integers.

Values

<ext-community>	: target:{<ip-addr:comm-val> | <2byte-asnumber:ext-comm-val> | <4byte-asnumber:comm-val>}
ip-addr:	a.b.c.d
comm-val:	[0 to 65535]
2byte-asnumber:	[0 to 65535]
ext-comm-val:	[0 to 4294967295]
4byte-asnumber:	[0 to 4294967295]

import *ext-community* — Specifies communities allowed to be received from remote PE neighbors.

export *ext-community* — Specifies communities allowed to be sent to remote PE neighbors.

Platforms
7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS, VSR

- configure service vprn bgp-ipvpn segment-routing-v6 vrf-target

All

- configure service vprn bgp-evpn mpls vrf-target
- configure service vprn bgp-ipvpn mpls vrf-target

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vrf-target

Syntax **vrf-target** {**unicast** | *ext-community* | **export unicast** | *ext-community* | **import unicast** | *ext-community*}
no vrf-target

Context **[Tree]** (config>service>vprn>mvpn vrf-target)

Full Context configure service vprn mvpn vrf-target

Description This command specifies the route target to be added to the advertised routes or compared against the received routes from other VRFs on the same or remote PE routers. vrf-import or vrf-export policies override the vrf-target policy.

The **no** form of this command removes the vrf-target.

Default no vrf-target

Parameters **unicast** — Specifies to use unicast vrf-target ext-community for the multicast VPN.

ext-comm — An extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values
target:{*ip-address*:*comm-val* | *2byte-asnumber:ext-comm-val* | 4byte-asnumber:comm-val}

ip-address:	a.b.c.d
comm-val:	0 to 65535
2byte-asnumber:	1 to 65535
4byte-asnumber	0 to 4294967295

import *ext-community* — Specifies communities allowed to be accepted from remote PE neighbors.

export *ext-community* — Specifies communities allowed to be sent to remote PE neighbors.

Platforms All

26.92 vrgw

vrgw

Syntax **vrgw**

Context **[Tree]** (config>subscr-mgmt vrgw)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-ranges>range vrgw)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-ranges range vrgw
configure subscriber-mgmt vrgw

Description Commands in this context configure Virtual Residential Gateway parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

vrgw

Syntax **vrgw**

Context [Tree] (config>router vrgw)

Full Context configure router vrgw

Description Commands in this context configure router Virtual Residential Gateway parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vrgw

Syntax **vrgw**

Context [Tree] (config>service>ies>sub-if>grp-if>wlan-gw>ranges>range vrgw)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>ranges>range vrgw)

Full Context configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range vrgw

Description Commands in this context configure Virtual Residential Gateway parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vrgw

Syntax **vrgw**

Context [Tree] (debug>subscr-mgmt vrgw)

Full Context debug subscriber-mgmt vrgw

Description This command clears vRGW data.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.93 vrrp

vrrp

Syntax **vrrp** *virtual-router-id* [**owner**] [**passive**] [**monitor-oper-group** *group-name*]
no vrrp *virtual-router-id*

Context **[Tree]** (config>service>ies>if vrrp)
[Tree] (config>service>ies>if>ipv6 vrrp)

Full Context configure service ies interface ipv6 vrrp
configure service ies interface vrrp

Description This command configures the router to create or edit a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. The **vrrp** *virtual-router-id* command is used to define the configuration parameters for the VRID.

The **no** form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the VRID. The VRID does not need to be shutdown to remove the virtual router instance.

Special Cases **Virtual Router Instance Owner IP Address Conditions —** The virtual router instance **owner** can be created before assigning the parent IP interface primary or secondary IP addresses. In this case, the virtual router instance is not associated with an IP address. The operational state of the virtual router instance is down.

VRRP Owner Command Exclusions — By specifying the VRRP *vrid* as **owner**, the following commands are no longer available:

- **vrrp priority —** The virtual router instance **owner** is hard-coded with a **priority** value of 255 and cannot be changed.
- **vrrp master-int-inherit** — Owner virtual router instances do not accept VRRP advertisement messages. The advertisement interval field is not evaluated and cannot be inherited.
- **ping-reply**, **telnet-reply,** and **ssh-reply —** The **owner** virtual router instance always allows ping, telnet and SSH if the management and security parameters are configured to accept them on the parent IP interface.
- **vrrp shutdown —** The **owner** virtual router instance cannot be shut down on the **vrrp** node. If this were allowed, VRRP messages would not be sent, but the parent IP interface address would continue to respond to ARPs and forward IP packets. Another virtual router instance may detect the missing master due to the termination of VRRP advertisement messages and become master. This

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

would result in two routers responding to ARP requests for the same IP addresses. To shut down the **owner** virtual router instance, use the **shutdown** command in the parent IP interface context. This prevents VRRP participation, IP ARP reply, and IP forwarding. To continue parent IP interface ARP reply and forwarding without VRRP participation, remove the **vrrp** *vrid* instance.

- **traceroute-reply**

VRRP Passive Command Exclusions — By specifying the VRRP *vrid* as **passive**, the following commands related to the master election and processing of VRRP advertisement messages are no longer available:

- **vrrp priority**
- **policy**
- **preempt**
- **master-int-inherit**
- **standby-forwarding**
- **int-delay**
- **message-interval**
- **authentication-key**
- **bfd-enable**
- **monitor-oper-group**

Parameters *virtual-router-id* — Specifies a virtual router ID or an ID that can be modified on the IP interface.

Values 1 to 255

owner — Keyword used to identify this virtual router instance as owning the virtual router IP addresses. If the **owner** keyword is not specified at the time of *vrid* creation, the **vrrp backup** commands must be specified to define the virtual router IP addresses. The **owner** keyword is not required when entering the *vrid* for editing purposes. When created as **owner**, a *vrid* on an IP interface cannot have the **owner** parameter removed. The *vrid* must be deleted, and then recreated without the **owner** keyword, to remove ownership.

passive — Keyword used to identify this virtual router instance as **passive**, and therefore, owning the virtual router IP addresses. A **passive** *vrid* does not send or receive VRRP advertisement messages, and is always in either the **master** state (if the interface is operationally up), or the **init** state (if the interface is operationally down). The **passive** keyword is not required when entering the *vrid* for editing purposes. When a *vrid* on an IP interface is created as **passive**, the parameter cannot be removed from the *vrid*. The *vrid* must be deleted, and then recreated without the **passive** keyword, to remove parameter.

group-name — Specifies the name of the **oper-group**, up to 32 characters to establish the associated VRRP instance as a following instance to the specified operational group. As a result of this association, the VRRP instance state follows that of the VRRP instance (the lead instance) associated with the specified operation group.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vrrp

Syntax **vrrp** *virtual-router-id* [**owner**] [**passive**] [**monitor-oper-group** *group-name*]
no vrrp *virtual-router-id*

Context **[Tree]** (config>service>vprn>if vrrp)

Full Context configure service vprn interface vrrp

Description This command creates or edits a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. One, both, or none may be defined as owner. The nodal context of **vrrp** *virtual-router-id* is used to define the configuration parameters for the VRID.

The **no** form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the VRID. The VRID does not need to be shut down in order to remove the virtual router instance.

Special Cases **Virtual Router Instance Owner IP Address Conditions —** The virtual router instance **owner** can be created prior to assigning the parent IP interface primary or secondary IP addresses. In this case, the virtual router instance is not associated with an IP address. The operational state of the virtual router instance is down.

VRRP Owner Command Exclusions — By specifying the VRRP *vrid* as **owner**, the following commands are no longer available:

- **vrrp priority —** The virtual router instance **owner** is hard-coded with a **priority** value of 255 and cannot be changed.
- **vrrp master-int-inherit** — Owner virtual router instances do not accept VRRP advertisement messages; the advertisement interval field is not evaluated and cannot be inherited.
- **ping-reply**, **telnet-reply** and **ssh-reply —** The **owner** virtual router instance always allows Ping, Telnet and SSH if the management and security parameters are configured to accept them on the parent IP interface.
- **vrrp shutdown —** The **owner** virtual router instance cannot be shut down on the **vrrp** node. If this was allowed, VRRP messages would not be sent, but the parent IP interface address would continue to respond to ARPs and forward IP packets. Another virtual router instance may detect the missing master due to the termination of VRRP advertisement messages and become master. This would result in two routers responding to ARP requests for the same IP addresses. To shut down the **owner** virtual router instance, use the **shutdown** command in the parent IP interface context. This will prevent VRRP participation, IP ARP reply and IP forwarding. To continue parent IP interface ARP reply and forwarding without VRRP participation, remove the **vrrp** *vrid* instance.
- **traceroute-reply**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

VRRP Passive Command Exclusions — By specifying the VRRP *vrid* as **passive**, the following commands related to the master election and processing of VRRP advertisement messages are no longer available:

- **vrrp priority**
- **policy**
- **preempt**
- **master-int-inherit**
- **standby-forwarding**
- **int-delay**
- **message-interval**
- **authentication-key**
- **bfd-enable**
- **monitor-oper-group**

Parameters *virtual-router-id* — Specifies a new virtual router ID or one that can be modified on the IP interface.

Values 1 to 255

owner — Identifies this virtual router instance as owning the virtual router IP addresses. If the **owner** keyword is not specified at the time of *vrid* creation, the **vrrp backup** commands must be specified to define the virtual router IP addresses. The **owner** keyword is not required when entering the *vrid* for editing purposes. Once created as **owner**, a *vrid* on an IP interface cannot have the **owner** parameter removed. The *vrid* must be deleted, and then recreated without the **owner** keyword, to remove ownership.

passive — Identifies this virtual router instance as **passive**, and therefore, owning the virtual router IP addresses. A **passive** *vrid* does not send or receive VRRP advertisement messages, and is always in either the **master** state (if the interface is operational-up), or the **init** state (if the interface is operational-down). The **passive** keyword is not required when entering the *vrid* for editing purposes. Once a *vrid* on an IP interface is created as **passive**, the parameter cannot be removed from the *vrid*. The *vrid* must be deleted, and then recreated without the **passive** keyword, to remove parameter.

group-name — Specifies the name of the **oper-group**, up to 32 characters to establish the associated VRRP instance as a following instance to the specified operational group. As a result of this association, the VRRP instance state follows that of the VRRP instance (the lead instance) associated with specified operation group.

Platforms All

vrrp

Syntax **vrrp** *virtual-router-id* [**owner**] [**passive**] [**monitor-oper-group** *group-name*]
no vrrp *virtual-router-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>service>vprn>if vrrp)

Full Context configure service vprn interface vrrp

Description This command configures the router to create or edit a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. The **vrrp** *virtual-router-id* command is used to define the configuration parameters for the VRID.

The **no** form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the VRID. The VRID does not need to be shutdown to remove the virtual router instance.

Special Cases

Virtual Router Instance Owner IP Address Conditions — The virtual router instance **owner** can be created before assigning the parent IP interface primary or secondary IP addresses. In this case, the virtual router instance is not associated with an IP address. The operational state of the virtual router instance is down.

VRRP Owner Command Exclusions — By specifying the VRRP *vrid* as **owner**, the following commands are no longer available:

- **vrrp priority —** The virtual router instance **owner** is hard-coded with a **priority** value of 255 and cannot be changed.
- **vrrp master-int-inherit** — Owner virtual router instances do not accept VRRP advertisement messages. The advertisement interval field is not evaluated and cannot be inherited.
- **ping-reply**, **telnet-reply,** and **ssh-reply —** The **owner** virtual router instance always allows ping, telnet and SSH if the management and security parameters are configured to accept them on the parent IP interface.
- **vrrp shutdown —** The **owner** virtual router instance cannot be shut down on the **vrrp** node. If this were allowed, VRRP messages would not be sent, but the parent IP interface address would continue to respond to ARPs and forward IP packets. Another virtual router instance may detect the missing master due to the termination of VRRP advertisement messages and become master. This would result in two routers responding to ARP requests for the same IP addresses. To shut down the **owner** virtual router instance, use the **shutdown** command in the parent IP interface context. This prevents VRRP participation, IP ARP reply, and IP forwarding. To continue parent IP interface ARP reply and forwarding without VRRP participation, remove the **vrrp** *vrid* instance.
- **traceroute-reply**

VRRP Passive Command Exclusions — By specifying the VRRP *vrid* as **passive**, the following commands related to the master election and processing of VRRP advertisement messages are no longer available:

- **vrrp priority**
- **policy**
- **preempt**

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **master-int-inherit**
- **standby-forwarding**
- **int-delay**
- **message-interval**
- **authentication-key**
- **bfd-enable**
- **monitor-oper-group**

Parameters *virtual-router-id* — Specifies a virtual router ID or an ID that can be modified on the IP interface.

Values 1 to 255

owner — Keyword used to identify this virtual router instance as owning the virtual router IP addresses. If the **owner** keyword is not specified at the time of *vrid* creation, the **vrrp backup** commands must be specified to define the virtual router IP addresses. The **owner** keyword is not required when entering the *vrid* for editing purposes. When created as **owner**, a *vrid* on an IP interface cannot have the **owner** parameter removed. The *vrid* must be deleted, and then recreated without the **owner** keyword, to remove ownership.

passive — Keyword used to identify this virtual router instance as **passive**, and therefore, owning the virtual router IP addresses. A **passive** *vrid* does not send or receive VRRP advertisement messages, and is always in either the **master** state (if the interface is operationally up), or the **init** state (if the interface is operationally down). The **passive** keyword is not required when entering the *vrid* for editing purposes. When a *vrid* on an IP interface is created as **passive**, the parameter cannot be removed from the *vrid*. The *vrid* must be deleted, and then recreated without the **passive** keyword, to remove parameter.

group-name — Specifies the name of the **oper-group**, up to 32 characters to establish the associated VRRP instance as a following instance to the specified operational group. As a result of this association, the VRRP instance state follows that of the VRRP instance (the lead instance) associated with the specified operation group.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vrrp

Syntax **vrrp** *virtual-router-id* [**owner**] [**passive**] [**monitor-oper-group** *group-name*]
no vrrp *virtual-router-id*

Context **[Tree]** (config>router>if vrrp)
[Tree] (config>router>if>ipv6 vrrp)

Full Context configure router interface ipv6 vrrp
configure router interface vrrp

Description This command creates the context to configure a VRRP virtual router instance. A virtual router is defined by its virtual router identifier (VRID) and a set of IP addresses.

The optional **owner** keyword indicates that the **owner** controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. The **owner** assumes the role of the master virtual router.

All other virtual router instances participating in this message domain must have the same *vrid* configured and cannot be configured as **owner**. Once created, the **owner** keyword is optional when entering the *vrid* for configuration purposes.

A *vrid* is internally associated with the IP interface. This allows the *vrid* to be used on multiple IP interfaces while representing different virtual router instances.

For IPv4, up to four VRRP VRID nodes can be configured on a router interface. Each virtual router instance can manage up to 16 backup IP addresses. For IPv6, only one VRID can be configured on a router interface.

The optional **passive** keyword indicates that a *vrid* can be configured as **passive**, in which case, the VRRP advertisement messages are suppressed on transmission and reception, and all routers configured with the same *vrid* become master. Passive *VRIDs* can exceed the limit of four VRRP VRID nodes on a router interface.

The **no** form of the command removes the specified *vrid* from the IP interface. This terminates VRRP participation and deletes all references to the *vrid* in conjunction with the IP interface. The *vrid* does not need to be shut down to remove the virtual router instance.

Default no vrrp — No VRRP virtual router instance is associated with the IP interface.

Special Cases **Virtual Router Instance Owner IP Address Conditions —** The virtual router instance **owner** can be created prior to assigning the parent IP interface primary or secondary IP addresses. In this case, the virtual router instance is not associated with an IP address. The operational state of the virtual router instance is down.

VRRP Owner Command Exclusions — By specifying the VRRP *vrid* as **owner**, the following commands are no longer available:

- **vrrp priority —** The virtual router instance **owner** is hard-coded with a **priority** value of 255 and cannot be changed.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- **vrrp master-int-inherit** — Owner virtual router instances do not accept VRRP advertisement messages; the advertisement interval field is not evaluated and cannot be inherited.
- **ntp-reply, ping-reply**, **telnet-reply,** and **ssh-reply —** The **owner** virtual router instance always allows Ping, Telnet and SSH if the management and security parameters are configured to accept them on the parent IP interface.
- **vrrp shutdown —** The **owner** virtual router instance cannot be shut down on the **vrrp** node. If this was allowed, VRRP messages would not be sent, but the parent IP interface address would continue to respond to ARPs and forward IP packets. Another virtual router instance may detect the missing master due to the termination of VRRP advertisement messages and become master. This would result in two routers responding to ARP requests for the same IP addresses. To shut down the **owner** virtual router instance, use the **shutdown** command in the parent IP interface context. This prevents VRRP participation, IP ARP reply and IP forwarding. To continue parent IP interface ARP reply and forwarding without VRRP participation, remove the **vrrp** *vrid* instance.
- **traceroute-reply**

VRRP Passive Command Exclusions — By specifying the VRRP *vrid* as **passive**, the following commands related to the master election and processing of VRRP advertisement messages are no longer available:

- **vrrp priority**
- **policy**
- **preempt**
- **master-int-inherit**
- **standby-forwarding**
- **int-delay**
- **message-interval**
- **authentication-key**
- **bfd-enable**

Parameters *virtual-router-id* — The virtual router ID for the IP interface expressed as a decimal integer.

Values 1 to 255

owner — Keyword used to identify this virtual router instance as owning the virtual router IP addresses. If the **owner** keyword is not specified at the time of *vrid* creation, the **vrrp backup** commands must be specified to define the virtual router IP addresses. The **owner** keyword is not required when entering the *vrid* for editing purposes. When created as **owner**, a *vrid* on an IP interface cannot have the **owner** parameter removed. The *vrid* must be deleted, and then recreated without the **owner** keyword, to remove ownership.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

passive — Keyword used to identify this virtual router instance as **passive**, therefore owning the virtual router IP addresses. A **passive** *vrid* does not send or receive VRRP advertisement messages and is always in either the **master** state (if the interface is operationally up), or the **init** state (if the interface is operationally down). The **passive** keyword is not required when entering the *vrid* for editing purposes. When a *vrid* on an IP interface is created as **passive**, the parameter cannot be removed from the *vrid*. The *vrid* must be deleted, and then recreated without the **passive** keyword, to remove the parameter.

group-name — Specifies the name of the **oper-group**, up to 32 characters to establish the associated VRRP instance as a following instance to the specified operational group. As a result of this association, the VRRP instance state follows that of the VRRP instance (the lead instance) associated with the specified operation group.

Platforms All

26.94 vsd

vsd

Syntax **vsd script** *script*
no vsd

Context **[Tree]** (config>python>py-policy vsd)

Full Context configure python python-policy vsd

Description This command configures scripts to handle VSD messages.

The **no** form of this command removes the script from the Python policy.

Parameters *script* — Specifies the name of the Python script, up to 32 characters, that is used to handle the specified message.

Platforms All

vsd

Syntax **vsd**

Context **[Tree]** (config>service vsd)

Full Context configure service vsd

Description Commands in this context configure the vsd configuration.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

vsd

Syntax [**no**] **vsd**

Context **[Tree]** (config>system vsd)
[Tree] (config>system>security>cli-script>authorization vsd)

Full Context configure system security cli-script authorization vsd
configure system vsd

Description Commands in this context configure authorization for the VSD server.

The **no** form of this command removes all authorizations for the VSD server.

Platforms All

vsd

Syntax **vsd script** *script*
no vsd

Context **[Tree]** (config>python>python-policy vsd)

Full Context configure python python-policy vsd

Description This command defines the python script for the Python policy sent by the VSD.

Parameters *script* — Specifies the VSD script that points at the python-script command.

Platforms All

vsd

Syntax **vsd**

Context **[Tree]** (debug vsd)

Full Context debug vsd

Description Commands in this context provide debug vsd functionality.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.95 vsd-domain

vsd-domain

Syntax **vsd-domain** *name*
no vsd-domain

Context **[Tree]** (config>service>vpls vsd-domain)
[Tree] (config>service>vprn vsd-domain)

Full Context configure service vpls vsd-domain
configure service vprn vsd-domain

Description This command associates a previously configured vsd-domain to an existing VPRN or VPLS service. The vsd-domain is a tag used between the VSD and the 7750 SR, 7450 ESS, or 7950 XRS to correlate configuration parameters to a service.

Parameters *name* — Specifies the vsd-domain name.

Platforms All

26.96 vsd-password

vsd-password

Syntax **vsd-password** *password* [{**hash** | **hash2**}]
no vsd-password

Context **[Tree]** (config>system>security>password vsd-password)

Full Context configure system security password vsd-password

Description This command configures the password required to access the **enable-vsd-config** mode. The **enable-vsd-config** mode allows editing of services provisioned by the VSD in fully dynamic mode (or by the **tools perform service vsd evaluate-script** command.

Parameters *password* — Specifies the password required to login as authorized user in the **enable-vsd-config** mode.

hash — Specifies that the primary hashing sequence should be used.

hash2 — Specifies that the secondary hashing sequence should be used.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.97 vsi-export

vsi-export

Syntax **vsi-export** *policy-name* [*policy-name*]
no vsi-export

Context **[Tree]** (config>service>vpls>bgp-ad vsi-export)
[Tree] (config>service>vpls>bgp vsi-export)

Full Context configure service vpls bgp vsi-export
configure service vpls bgp-ad vsi-export

Description This command specifies the name of the VSI export policies to be used for BGP EVPN, BGP auto discovery, BGP VPLS, BGP VPWS, and BGP multi-homing if these features are configured in this VPLS service.

If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

The **no** form of this command removes the policy from the configuration.

Default no vsi-export

Parameters *policy-name* — Specifies up to five policy names, up to 32 characters.

Platforms All

vsi-export

Syntax **vsi-export** *policy-name* [*policy-name*]
no vsi-export

Context **[Tree]** (config>service>epipe>bgp vsi-export)

Full Context configure service epipe bgp vsi-export

Description This command specifies the name of the VSI export policies to be used for BGP EVPN, BGP VPWS and BGP multi-homing if these features are configured in this Epipe service.

If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

The **no** form of this command removes the policy from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no vsi-export

Parameters *policy-name* — Specifies up to five policy names, up to 32 characters.

Platforms All

26.98 vsi-id

vsi-id

Syntax **vsi-id**

Context **[Tree]** (config>service>vpls>bgp-ad vsi-id)

Full Context configure service vpls bgp-ad vsi-id

Description Commands in this context configure the Virtual Switch Instance Identifier (VSI-ID).

Platforms All

26.99 vsi-import

vsi-import

Syntax **vsi-import** *policy-name* [*policy-name*]
no vsi-import

Context **[Tree]** (config>service>vpls>bgp-ad>vsi-id vsi-import)
[Tree] (config>service>vpls>bgp vsi-import)

Full Context configure service vpls bgp vsi-import
configure service vpls bgp-ad vsi-id vsi-import

Description This command specifies the name of the VSI import policies to be used for BGP EVPN, BGP auto discovery, BGP VPLS, BGP VPWS, and BGP multi-homing if these features are configured in this VPLS service.

If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

The **no** form of this command removes the policy from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no vsi-import

Parameters *policy-name* — Specifies up to five policy names, up to 32 characters.

Platforms All

vsi-import

Syntax **vsi-import** *policy-name* [*policy-name*]
no vsi-import

Context **[Tree]** (config>service>epipe>bgp vsi-import)

Full Context configure service epipe bgp vsi-import

Description This command specifies the name of the VSI import policies to be used for BGP EVPN, BGP VPWS and BGP multi-homing if these features are configured in this Epipe service.

If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

The **no** form of this command removes the policy from the configuration.

Default no vsi-import

Parameters *policy-name* — Specifies up to five policy names, up to 32 characters.

Platforms All

26.100 vxlan

vxlan

Syntax **vxlan vni** *vni*
no vxlan

Context **[Tree]** (config>subscr-mgmt>isa-svc-chain>evpn>export vxlan)

Full Context configure subscriber-mgmt isa-service-chaining evpn export vxlan

Description This command configures a VXLAN VNI that is sent in EVPN routes advertised to the service chaining.

The **no** form of this command removes the VNI from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *vni* — Specifies the VNI of the VXLAN created by the EVPN service.

Values 1 to 16777215

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vxlan

Syntax [**no**] **vxlan**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>type vxlan)

Full Context configure subscriber-mgmt wlan-gw tunnel-query type vxlan

Description This command enables matching on VXLAN tunnels.

The **no** form of this command disables matching on VXLAN tunnels, unless no other tunnel type specifier is configured.

Default no vxlan

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vxlan

Syntax **vxlan** [**bgp** *bgp*] [**vxlan-instance** *vxlan-instance*]
no vxlan [**bgp** *bgp*]

Context **[Tree]** (config>service>epipe>bgp-evpn vxlan)
[Tree] (config>service>vpls>bgp-evpn vxlan)

Full Context configure service epipe bgp-evpn vxlan
configure service vpls bgp-evpn vxlan

Description Commands in this context configure the VXLAN parameters when BGP EVPN is used as the control plane. In VPLS services, instance BGP 1 or BGP 2 can be configured, as well as VXLAN instances 1 or 2. Up to two instances of this command can be configured in the same service, as long as the BGP instance and the VXLAN instance are different in both commands. In Epipe services, only BGP instance 1 and VXLAN instance 1 is supported. If the BGP or VXLAN instance are not specified, the instances are by default set to 1.

The **no** version of this command will remove the vxlan instance from the service.

Parameters **bgp** — Indicates the BGP instance identifier.

Values 1 to 2

vxlan-instance — Indicates the VXLAN instance identifier.

Values 1 to 2

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

vxlan

Syntax **vxlan vni** *vni-id* [**create**] [**instance** *instance-id*]
no vxlan [**vni** *vni-id*] [**instance** *instance-id*]

Context **[Tree]** (config>service>epipe vxlan)

Full Context configure service epipe vxlan

Description This command enables the use of VXLAN in the Epipe service.

The **no** version of this command will remove the VXLAN instance from the service.

Parameters *vni-id* — Specifies the VXLAN network identifier configured in the Epipe service. When EVPN is used in the control plane, the configured VNI is encoded in the MPLS field of the NLRI. The VPLS service is operationally up when the **vxlan vni** *vni-id* is successfully created.

Values 1 to 16777215

Default 1

instance-id — Specifies the VXLAN instance identifier.

Values 1, 2

create — Mandatory keyword that creates a VXLAN instance.

Platforms All

vxlan

Syntax **vxlan vni** *vni-id* [**create**] [**instance** *instance-id*]
no vxlan [**vni** *vni-id*] [**instance** *instance-id*]

Context **[Tree]** (config>service>vpls vxlan)

Full Context configure service vpls vxlan

Description This command enables the use of VXLAN in the VPLS service.

The **no** version of this command will remove the VXLAN instance from the service.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *vni-id* — Specifies the VXLAN network identifier configured in the VPLS service. When EVPN is used in the control plane, the configured VNI is encoded in the MPLS field of the NLRI. The VPLS service is operationally up when the **vxlan vni** *vni-id* is successfully created.

Values 1 to 16777215

Default 1

instance-id — Specifies the VXLAN instance identifier.

Values 1, 2

create — Mandatory keyword that creates a VXLAN instance.

Platforms All

vxlan

Syntax **vxlan**

Context **[Tree]** (config>service>vprn vxlan)

Full Context configure service vprn vxlan

Description Commands in this context configure VXLAN parameters in the VPRN.

Platforms All

vxlan

Syntax **vxlan**

Context **[Tree]** (config>service>system vxlan)

Full Context configure service system vxlan

Description Commands in this context configure the vxlan global parameters.

Platforms All

vxlan

Syntax [**no**] **vxlan vtep** *vtep* **vni** *vni-id*

Context **[Tree]** (debug>service>id>igmp-snooping vxlan)

Full Context debug service id igmp-snooping vxlan

Description This command shows IGMP packets for a specific VXLAN binding.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command disables the debugging for that VXLAN binding.

Parameters **vtep** — IP address of the VXLAN Termination Endpoint

vni — VXLAN Network Identifier of the VXLAN binding

Values 1 to 16777215

Platforms All

vxlan

Syntax [**no**] **vxlan vtep** *vtep* **vni** *vni-id*

Context **[Tree]** (debug>service>id>mld vxlan)

Full Context debug service id mld-snooping vxlan

Description This command shows MLD packets for a specific VXLAN binding.

The **no** form of this command disables the debugging for that VXLAN binding.

Parameters **vtep** — IP address of the VXLAN Termination Endpoint

vni — VXLAN Network Identifier of the VXLAN binding

Values 1 to 16777215

Platforms All

vxlan

Syntax **vxlan** [**router** *router-name*]
vxlan service-name *service-name*
no vxlan

Context **[Tree]** (config>fwd-path-ext>fpe vxlan)

Full Context configure fwd-path-ext fpe vxlan

Description This command informs the system about the cross-connect type that is required for non-system IPv4 and IPv6 VXLAN termination. Internally, it triggers the automatic creation of two internal IP interfaces in the PXC ports and enables those internal interfaces to process and terminate VXLAN.

If no parameters are used, the VXLAN termination occurs in the base router; however, when the FPE is used for static VXLAN termination (no BGP-EVPN services), non-system IPv4 and IPv6 VXLAN can be terminated in a VPRN service. In this case, the VPRN router instance or service name must be configured with the **vxlan-termination** command.

The **no** form of this command disables the cross-connect type from the configuration.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default no vxlan-termination

Parameters *router-name* — Specifies the router instance for VXLAN termination.

Values

router-name: *router-name* or *vprn-svc-id*

router-name	"Base"
vprn-svc-id	1 to 2147483647

Default Base

service-name — Specifies the service name that identifies the VPRN for VXLAN termination, up to 64 characters.

Platforms All

26.101 vxlan-ipv4-tep-ecmp

vxlan-ipv4-tep-ecmp

Syntax [**no**] **vxlan-ipv4-tep-ecmp**

Context **[Tree]** (config>service>vpls>allow-ip-int-bind vxlan-ipv4-tep-ecmp)

Full Context configure service vpls allow-ip-int-bind vxlan-ipv4-tep-ecmp

Description This command enables and disables ECMP on VXLAN IPv4 destinations for R-VPLS services. When this command is enabled, packets entering a VPRN connected to an R-VPLS that is terminating on a VXLAN IPv4 destination are looked up in the routing table. If the next hop is a VXLAN IPv4 TEP, the packets are distributed based on per-flow load-balancing.

This command can only be used in FP3- (or higher) routers. R-VPLS per-flow load-balancing for VXLAN IPv6 destinations works by default without this command.

The **no** version of this command reverts the process to the default behavior of per-remote VTEP load-balancing.

Default no vxlan-ipv4-tep-ecmp

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.102 vxlan-ping

vxlan-ping

Syntax **vxlan-ping test-id** *test-id* **service** *vpls-service-id* **dest-vni** *vxlan-network-id* **outer-ip-destination** *ipv4-address* [**outer-ip-source-udp** *udp-port-number*] [**outer-ip-ttl** *time-to-live*] [**inner-l2** *ieee-address*] [**inner-ip-source** *ipv4-address*] [**inner-ip-destination** *ipv4-address*] [**i-flag-on**] [**end-system** *ieee-address*] [**send-count** *packets*] [**interval** *interval-time*] [**timeout** *timeout-time*] [**padding** *tlv-size* [**reflect-pad**]] [**fc** *fc-name*] [**profile** {**in** | **out**}] [**reply-mode** {**overlay** | **udp**}]

Context **[Tree]** (oam vxlan-ping)

Full Context oam vxlan-ping

Description Operational command used to validate the VXLAN Tunnel Endpoint (VXLAN) connectivity between peers.

Parameters *test-id* — Specifies a value to identify the originator handle of the specific request. Each active test requires a unique test identifier.

Values 1 to 2147483647

vpls-service-id — Specifies the VPLS service used to launch the request and by extension pick up the source VNI information.

Values

service-id: 1 to 2147483647

svc-name: up to 64 characters

vxlan-network-id — Specifies the target Vxlan network identifier on the terminating VTEP.

Values 1 to 16777215

outer-ip-destination *ipv4-address* — Specifies the IPv4 address of the terminating VTEP.

Values a.b.c.d

udp-port-number — Optional outer source UDP port number.

Values 1 to 65535

Default System-generated UDP port number

time-to-live — Specifies the optional outer time to live.

Values 1 to 255

Default 255

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

inner-l2 *ieee-address* — Specifies the destination MAC address used in the inner VXLAN header.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Default 00:00:00:00:00:00

inner-ip-source *ipv4-address* — Specifies the inner source IPv4 address.

Values a.b.c.d

Default System IPv4 Address

inner-ip-destination *ipv4-address* — Specifies the inner destination IPv4 address. Must be in the range 127/8.

Values 127.0.0.0 to 127.0.0.8

Default 127.0.0.1

i-flag-on — Sets the VNI Validation bit to 1, indicating that the OAMPDU contains a valid VNI.

Default i-flag set to “0” which prevents the OAMPDU form being forwarded beyond the terminating VTEP.

end-system *ieee-address* — Optional command to include the sub TLV to validate an end system MAC address in the FDB. Only one MAC address may be included.

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

Default 00:00:00:00:00:00

packets — Specifies the number of VXLAN ping requests to transmit.

Values 1 to 1024

Default 1

interval-time — Specifies the probe interval, in seconds.

Values 0.1, 1 to 10

Default 1

timeout-time — Specifies the packet time out value, in seconds.

Values 1 to 10

Default 5

tlv-size — Specifies whether to include the Pad TLV and specifies the number of octets that defines the entire size of the pad TLV, including the type (2B), the length field (2B), the padding (variable).

Values 0, 5 to 2000

Default 0

reflect-pad — Instructs the responder to include the pad-tlv in the echo response. This option is not supported when the reply mode is “UDP”.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

fc-name — Indicates the forwarding class that is exposed to the QoS policy as input into generating the outer CoS.

Values be, l2, af, l1, h2, ef, h1, nc

Default be

profile {in | out} — Defines the frame's disposition that is exposed to the QoS policy as input into generating the outer CoS.

Default in

reply-mode {overlay | udp} — Instructs the responder how to route the VXLAN response.

Values **udp**: responds using UDP over the IP network. The default must be changed if the VTEP uses anything other than an IPv4 System Address as the source.

overlay: responds using the VXLAN overlay for the service

Default udp

Platforms All

26.103 vxlan-port

vxlan-port

Syntax **vxlan-port** [**4789** | **8472**]
no vxlan-port

Context **[Tree]** (config>router>vrgw>lanext vxlan-port)

Full Context configure router vrgw lanext vxlan-port

Description This command specifies the destination UDP port for both ingress and egress VXLAN packets for HLE services.

The **no** form of this command reverts to the default.

Default vxlan-port 4789

Parameters **4789 | 8472** — Specifies the destination UDP port.

Values 4789, 8472

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

26.104 vxlan-src-vtep

vxlan-src-vtep

Syntax **vxlan-src-vtep** {*ip-address* | *ipv6-address*}
no vxlan-src-vtep

Context **[Tree]** (config>service>epipe vxlan-src-vtep)
[Tree] (config>service>vpls vxlan-src-vtep)

Full Context configure service epipe vxlan-src-vtep
configure service vpls vxlan-src-vtep

Description This command enables the router to use the configured IP address as the tunnel source IP address (source VTEP) when originating VXLAN-encapsulated frames for this service. This IP address is also used to set the BGP NLRI next hop in EVPN route advertisements for the service.

Default no vxlan-src-vtep

Parameters *ip-address* — Specifies the non-system IPv4 address that terminates VXLAN for a service.

ipv6-address — Specifies the IPv6 address that terminates VXLAN for a service.

Platforms All

26.105 vxlan-vni

vxlan-vni

Syntax **vxlan-vni** [**eq** *vxlan-vni-id* | **range** *start end*]
no vxlan-vni

Context **[Tree]** (config>qos>sap-ingress>ip-criteria>entry>match vxlan-vni)
[Tree] (config>qos>sap-ingress>ipv6-criteria>entry>match vxlan-vni)

Full Context configure qos sap-ingress ip-criteria entry match vxlan-vni
configure qos sap-ingress ipv6-criteria entry match vxlan-vni

Description This command configures a VXLAN or VXLAN GPE VNI to be used as a SAP QoS policy match criterion. A range of VNIs to be matched can be specified by including the keyword **range** with a *start* and *end* VNI. This command requires the **type** to be set to **vxlan-vni** in the related **ip-criteria** or **ipv6-criteria** context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

See Virtual Network Identifier (VNI) Classification for the list of restrictions for this command.

Default no vxlan-vni

Parameters **eq** *vxlan-vni-id* — Specifies the VXLAN or VXLAN GPE VNI to be matched in the SAP ingress QoS classification. The VNI can be specified in any of the available formats but is always shown in decimal.

Values 1 to 16777215 (Decimal)
0x1 to 0xFFFFFF (Hexadecimal)
[0b1 to 0b111111111111111111111111] (Binary)

range *start end* — Identifies a range of VNIs to be used as matching criteria. The *start* value must be lower than the *end* value. The VNI can be specified in any of the available formats but is always shown in decimal.

Values 1 to 16777215 (Decimal)
0x1 to 0xFFFFFF (Hexadecimal)
[0b1 to 0b111111111111111111111111] (Binary)

Platforms All

26.106 vxlan-vtep-range

vxlan-vtep-range

Syntax **vxlan-vtep-range start** [*ip-address* | *ipv6-address*] **end** [*ip-address* | *ipv6-address*]
no vxlan-vtep-range

Context **[Tree]** (config>router>isa-svc-chain vxlan-vtep-range)

Full Context configure router isa-service-chaining vxlan-vtep-range

Description This command specifies the address range to be used as the local VXLAN VTEP on the ISA for service chaining. The system allocates one address for each ISA in the NAT group out of the specified range. The allocated address appears as /32 or /128 routes in the global routing table with the route type **nat**.

The **no** form of this command removes the IP or IPv6 addresses from the configuration.

Parameters **start** — Specifies the start address of the VXLAN VTEP range.

end — Specifies the end address of the VXLAN VTEP range.

ip-address — Specifies an IPv4 address start and end range.

Values ipv4-address - a.b.c.d

ipv6-address — Specifies an IPv6 address start and end range

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

ipv6-address: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

vxlan-vtep-range

Syntax **vxlan-vtep-range start** *ip-address* | *ipv6-address* **end** *ip-address* | *ipv6-address*
no vxlan-vtep-range

Context **[Tree]** (config>router>vrgw>lanext vxlan-vtep-range)

Full Context configure router vrgw lanext vxlan-vtep-range

Description This command specifies the address range to be used as the local VXLAN VTEP on the ISA for HLE services. The system allocates one address for each ISA in the WLAN GW group out of the specified range. The allocated address appears as /32 or /128 routes in the global routing table with the route type **nat**.

The **no** form of this command removes the values from the configuration.

Parameters **start** — Specifies the start of the VXLAN VTEP range.

end — Specifies the end of the VXLAN VTEP range.

ip-address **|** *ipv6-address* — Specifies the range of VXLAN VTEP addresses.

Values <ip-address| ipv6-address : ipv4-address - a.b.c.d
ipv6-address - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x - [0..FFFF]H
d - [0..255]D

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27 w Commands

27.1 wa-shared-high-wmark

wa-shared-high-wmark

Syntax **wa-shared-high-wmark** *percent*
no wa-shared-high-wmark

Context **[Tree]** (config>isa>aa-grp>qos>egress>from-sub wa-shared-high-wmark)
[Tree] (config>isa>aa-grp>qos>egress>to-sub wa-shared-high-wmark)

Full Context configure isa application-assurance-group qos egress from-subscriber wa-shared-high-wmark
configure isa application-assurance-group qos egress to-subscriber wa-shared-high-wmark

Description This command configures the high watermark for the weighted average utilization of the shared buffer space in the **from-subscriber** buffer pool for each ISA. When a buffer pool is not in the overload state and the wa-shared buffer utilization for an ISA crosses above the high watermark value in the ISA **from-subscriber** buffer pool enters an overload state and an overload notification is raised.

The **no** form of this command reverts to the default.

Default wa-shared-high-wmark max

Parameters *percent* — Specifies the weighted average shared buffer utilization high watermark.

Values 1 to 100, **max** percent (disabled)

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

27.2 wa-shared-low-wmark

wa-shared-low-wmark

Syntax **wa-shared-low-wmark** *percent*
no wa-shared-low-wmark

Context **[Tree]** (config>isa>aa-grp>qos>egress>from-sub wa-shared-low-wmark)
[Tree] (config>isa>aa-grp>qos>egress>to-sub wa-shared-low-wmark)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure isa application-assurance-group qos egress from-subscriber wa-shared-low-wmark
configure isa application-assurance-group qos egress to-subscriber wa-shared-low-wmark

Description This command configures the low watermark for the weighted average utilization of the shared buffer space in the **from-subscriber** buffer pool. When a buffer pool is in an overloaded state and the wa-shared buffer utilization for an ISA drops below low watermark value ISA **from-subscriber** buffer pool leaves the overload state and a is sent to indicate the overload state has cleared.

The **no** form of this command reverts to the default.

Default wa-shared-low-wmark 0

Parameters *percent* — Specifies the weighted average shared buffer utilization low watermark.

Values 0 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

27.3 wait

wait

Syntax **wait** *seconds*

Context **[Tree]** (bof wait)

Full Context bof wait

Description This command configures a pause, in seconds, at the start of the boot process which allows system initialization to be interrupted at the console.

When system initialization is interrupted the operator is allowed to manually override the parameters defined in the boot option file (BOF).

Only one **wait** command can be defined in the BOF.

Default wait 3

Parameters *seconds* — Specifies the time to pause at the start of the boot process, in seconds.

Values 1 to10

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.4 wait-for-up-timer

wait-for-up-timer

Syntax **wait-for-up-timer** *seconds*
no wait-for-up-timer

Context **[Tree]** (config>router>mpls>lsp>bfd wait-for-up-timer)
[Tree] (config>router>mpls>lsp>primary>bfd wait-for-up-timer)
[Tree] (config>router>mpls>lsp>secondary>bfd wait-for-up-timer)
[Tree] (config>router>mpls>lsp-template>bfd wait-for-up-timer)

Full Context configure router mpls lsp bfd wait-for-up-timer
configure router mpls lsp primary bfd wait-for-up-timer
configure router mpls lsp secondary bfd wait-for-up-timer
configure router mpls lsp-template bfd wait-for-up-timer

Description This command configures the time to wait for a BFD to come up in seconds. This timer is applicable to SR-TE LSPs, including auto-LSPs and PCE-initiated LSPs, as well as RSVP-TE LSPs. In case of SR-TE LSPs, this timer takes effect if BFD does not come up, or BFD goes from up to down. The timer is started when BFD is first enabled on a path or BFD transitions from up to down. When the timer expires if BFD is not yet come up, then the path is torn down by removing it from the TTM and the IOM and the retry timer is started.

In case of RSVP-TE LSPs, the timer controls the following:

- a path undergoing MBB when BFD is up on the original path
- the initial administrative enable of an LSP
- signaling retry of non-standby secondary paths

The **no** form of this command sets the timer to its default value.

Default no wait-for-up-timer

Parameters *seconds* — Specifies the BFD wait for up timer in seconds.

Values 0 to 60

Default 4

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

- configure router mpls lsp-template bfd wait-for-up-timer

All

- configure router mpls lsp primary bfd wait-for-up-timer
- configure router mpls lsp bfd wait-for-up-timer
- configure router mpls lsp secondary bfd wait-for-up-timer

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

wait-for-up-timer

Syntax **wait-for-up-timer** *seconds*
no wait-for-up-timer

Context **[Tree]** (config>service>epipe>spoke-sdp>bfd wait-for-up-timer)
[Tree] (config>service>ies>interface>spoke-sdp>bfd wait-for-up-timer)
[Tree] (config>service>vpls>spoke-sdp>bfd wait-for-up-timer)
[Tree] (config>service>vprn>interface>spoke-sdp>bfd wait-for-up-timer)

Full Context configure service epipe spoke-sdp bfd wait-for-up-timer
configure service ies interface spoke-sdp bfd wait-for-up-timer
configure service vpls spoke-sdp bfd wait-for-up-timer
configure service vprn interface spoke-sdp bfd wait-for-up-timer

Description This command configures the time interval, in seconds, that is used to wait for a BFD session to come up.

This command is triggered when a spoke-SDP is first administratively enabled and a VCCV BFD session transitions from up to down. The command is required to allow time for BFD sessions to come up, and for BFD to settle before selecting the active spoke-SDP to use in a redundant set. In the case where a VCCV BFD session is bouncing, the timer prevents excessive flapping of the operational state of a spoke-SDP.

The **no** form of this command disables the timer.

Default no wait-for-up-timer

Parameters *seconds* — Specifies the wait interval, in seconds, for the BFD up timer.

Values 1 to 60

Platforms All

27.5 wait-to-restore

wait-to-restore

Syntax **wait-to-restore** *interval*
no wait-to-restore

Context **[Tree]** (config>router>mpls>mpls-tp>protection-template wait-to-restore)

Full Context configure router mpls mpls-tp protection-template wait-to-restore

Description This command configures the WTR timer. It determines how long to wait until the active path of an MPLS-TP LSP is restored to the working path following the clearing of a defect on the working path. It is applicable to revertive mode, only.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Default wait-to-restore 300

Parameters *interval* — Specifies the WTR timer interval in 1 second increments.

Values 0 to 720 seconds

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

wait-to-restore

Syntax **wait-to-restore** *minutes*
no wait-to-restore

Context **[Tree]** (config>system>sync-if-timing wait-to-restore)

Full Context configure system sync-if-timing wait-to-restore

Description This command configures the time for the Wait to Restore timer. A previously failed input reference must be valid for the time specified before it is used for either the BITSout or the central clock input reference.

The **no** form of this command disables the timer.

Default no wait-to-restore

Parameters *minutes* — Specifies a value representing the number of minutes for the wait to restore timeout.

Values 1 to 12

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

27.6 wap1x

wap1x

Syntax **wap1x**

Context **[Tree]** (config>app-assure>group wap1x)

Full Context configure application-assurance group wap1x

Description This command configures the Wireless Application Protocol (WAP) 1.X.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.7 warm-standby

warm-standby

Syntax **warm-standby**

Context **[Tree]** (config>redundancy>multi-chassis>peer warm-standby)

Full Context configure redundancy multi-chassis peer warm-standby

Description This command enables Oversubscribed Multi-Chassis Redundancy (OMCR) model where subscriber hosts are synchronized between the two chassis only in the control plane and are kept there (as part of the Multi-Chassis Synchronization (MCS) state) until the switchover occurs. Link or nodal failure will trigger the switchover at which point the subscriber hosts are being fully instantiated in the control and the forwarding plane. This approach allows oversubscription of the resources in the central standby (or protecting) node that is backing-up several active nodes. The total number of protected subscribers in the OMCR cluster exceeds the forwarding capacity of the protecting node. This is achievable by not fully occupying the resources for the subscriber hosts until the failure occurs.

The restoration times depend on the amount of the subscriber hosts that are affected by the switchover and it is related to the time needed for the full instantiation of the subscribers in the forwarding plane.

Although this command is configured on a peer level, the warm-standby property is a nodal characteristic. In other words, mixing of N:1 and 1:1 (hot standby) mode in the central standby node is not supported. Consequently all peers on the central standby node must be configured for warm-standby (N:1), or all peers must be configured for hot-standby (1:1) by omitting the warm-standby keyword from the configuration.

The peer of the central backup node is not aware of the redundancy model supported. In in other words, the peer of the central-backup node does not know whether it peers with a warm-standby peer or host-standby-peer.

Platforms 7750 SR

27.8 warnings

warnings

Syntax [**no**] **warnings**

Context **[Tree]** (debug>dynsvc>scripts>event warnings)
[Tree] (debug>dynsvc>scripts>inst>event warnings)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (debug>dynsvc>scripts>script>event warnings)

Full Context debug dynamic-services scripts event warnings
debug dynamic-services scripts instance event warnings
debug dynamic-services scripts script event warnings

Description This command enables/disables the generation of a specific dynamic data service script debugging event output: warnings.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

warnings

Syntax [**no**] **warnings**

Context [Tree] (debug>vsd>scripts>event warnings)
[Tree] (debug>vsd>scripts>instance>event warnings)

Full Context debug vsd scripts event warnings
debug vsd scripts instance event warnings

Description This command enables/disables the generation of a specific script debugging event output: **warnings**.

Platforms All

27.9 watchdog-timer

watchdog-timer

Syntax **watchdog-timer** *seconds*
no watchdog-timer

Context [Tree] (config>aaa>diam-peer-plcy watchdog-timer)
[Tree] (config>aaa>diam-peer-plcy>peer watchdog-timer)

Full Context configure aaa diameter-peer-policy peer watchdog-timer
configure aaa diameter-peer-policy watchdog-timer

Description This command configures the interval between consecutive watchdog messages. On the first timeout of the DWR, the SR OS node will resend the DWR message. The peer is still operational during this time. On the second timeout, the peer transitions into a suspended mode and the peer-failover procedure is initiated (if the peer-failover is enabled by configuration). In this state the peer is not used for new transactions. At the same time, the cooldown procedure is started which means that it would take three successful DWR/DWA message exchanges to reinstate the peer in a fully operation state.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

On the third timeout, the peer is removed and its connection is closed.

This command is applicable only to legacy implementations of Diameter base in the SR OS.

The **no** form of this command reverts to the default.

Default watchdog-timer 30

Parameters *seconds* — Specifies the device watchdog timer, in seconds, used by this policy peer.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

watchdog-timer

Syntax **watchdog-timer** *seconds*
no watchdog-timer

Context **[Tree]** (config>aaa>diam>node>peer watchdog-timer)

Full Context configure aaa diameter node peer watchdog-timer

Description Watchdog messages are used to verify liveliness of a Diameter peer. A single watchdog messages will be sent to a peer in case that no traffic is received from it within a configured watchdog-timer. This watchdog request message will solicit a watchdog answer message from the peer. If no traffic (watchdog answer or otherwise) is received from the peer in response to watchdog request while the watchdog timer is running, the peer will be put in suspicious state and a peer failover routine will be triggered.

The peer will be closed after it has been in suspicious mode for the duration of one more watchdog-timer interval without receiving any traffic from it.

Once the peer is recovered, it will take 3 successful exchanges of diameter watchdog messages (DWR/DWA) for the peer to becomes used again in Diameter forwarding. This behavior is described in RFC 3539, §3.4.1, *Authentication, Authorization and Accounting (AAA) Transport Profile*).

This command is not applicable to legacy implementations of Diameter base in the SR OS.

The **no** form of this command removes the watchdog timer value from the configuration.

Default watchdog-timer 30

Parameters *seconds* — Specifies the device watchdog timer, in seconds, used on all connections by this peer.

Values 1 to 1000

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.10 watermark

watermark

Syntax **watermark**

Context **[Tree]** (config>isa>video-group watermark)

Full Context configure isa video-group watermark

Description Commands in this context configure watermark parameters.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

27.11 watermarks

watermarks

Syntax **watermarks**

Context **[Tree]** (config>isa>wlan-gw-group watermarks)

Full Context configure isa wlan-gw-group watermarks

Description Commands in this context configure ISA watermark notifications.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

watermarks

Syntax **watermarks high** *high-percentage* **low** *low-percentage*
no watermarks

Context **[Tree]** (config>service>vprn>sub-if>wlan-gw>pool-manager watermarks)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager watermarks)

Full Context configure service ies subscriber-interface wlan-gw pool-manager watermarks
configure service vprn subscriber-interface wlan-gw pool-manager watermarks

Description This command configures the watermarks used to determine if a new prefix should be allocated or an old prefix should be removed. A new prefix is allocated when the total usage level for the ISA reaches the high watermark. A prefix is freed if no addresses are currently in use and the usage level without this prefix would be below the low watermark.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** form of this command resets the watermarks to its default values of 95% high and 90% low.

Default watermarks high 95 low 90

Parameters *high-percentage* — Specifies the high watermark.

Values 80 to 99

low-percentage — Specifies the low watermark. The value must be lower than the high percentage value.

Values 50 to 98

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

watermarks

Syntax **watermarks high** *percentage-high* **low** *percentage-low*
no watermarks

Context **[Tree]** (config>service>vprn>nat>outside>pool watermarks)
[Tree] (config>router>nat>outside>pool watermarks)

Full Context configure router nat outside pool watermarks
configure service vprn nat outside pool watermarks

Description This command configures the watermarks for this NAT pool.

Default no watermarks

Parameters *high percentage-high* — Specifies the high percentage.

Values 1 to 100

low percentage-low — Specifies the low percentage.

Values 0 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

watermarks

Syntax **watermarks high** *percentage* **low** *percentage*
no watermarks

Context **[Tree]** (config>isa>nat-group>session-limits watermarks)
[Tree] (config>service>nat watermarks)
[Tree] (config>isa>wlan-gw-group>nat>session-limits watermarks)

Full Context configure isa nat-group session-limits watermarks
configure isa wlan-gw-group nat session-limits watermarks

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service nat watermarks

Description This command configures the ISA NAT or WLAN-GW group watermarks.

Default no watermarks

Parameters **high** *percentage* — Specifies the high watermark of the number of sessions for each MDA in this NAT ISA or WLAN-GW group.

Values 1 to 100

low *percentage* — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA or WLAN-GW group.

Values 0 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure isa nat-group session-limits watermarks

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure isa wlan-gw-group nat session-limits watermarks

watermarks

Syntax **watermarks high** *percentage-high* **low** *percentage-low*
no watermarks

Context **[Tree]** (config>service>nat>nat-policy>port-limits watermarks)
[Tree] (config>service>nat>up-nat-policy>port-limits watermarks)

Full Context configure service nat nat-policy port-limits watermarks
configure service nat up-nat-policy port-limits watermarks

Description This command configures the port usage watermarks for the NAT policy.

Default no watermarks

Parameters *percentage-high* — Specifies the high percentage.

Values 1 to 100

percentage-low — Specifies the low percentage.

Values 0 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

watermarks

Syntax **watermarks high** *percentage-high* **low** *percentage-low*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no watermarks

Context [Tree] (config>service>nat>firewall-policy>session-limits watermarks)
[Tree] (config>service>nat>nat-policy>session-limits watermarks)
[Tree] (config>service>nat>up-nat-policy>session-limits watermarks)

Full Context configure service nat firewall-policy session-limits watermarks
configure service nat nat-policy session-limits watermarks
configure service nat up-nat-policy session-limits watermarks

Description This command configures the session watermarks for the NAT or residential firewall policy.

Default no watermarks

Parameters *percentage-high* — Specifies the high percentage.

Values 1 to 100

percentage-low — Specifies the low percentage.

Values 0 to 99

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat up-nat-policy session-limits watermarks
- configure service nat nat-policy session-limits watermarks

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure service nat firewall-policy session-limits watermarks

27.12 web-service

web-service

Syntax **web-service**

Context [Tree] (config>app-assure>group>url-filter web-service)

Full Context configure application-assurance group url-filter web-service

Description Commands in this context configure the URL filter policy using web-service filtering. The operator must configure the web service, host name, DNS server to use, the AA interface VLAN ID, and provision the category profiles.

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.13 web-service-url-filter

web-service-url-filter

Syntax **web-service-url-filter** *size*

Context **[Tree]** (config>isa>aa-grp>shared-resources web-service-url-filter)

Full Context configure isa application-assurance-group shared-resources web-service-url-filter

Description This command configures the amount of shared memory to be used by the web service URL filter cache.

Default web-service-url-filter 100

Parameters *size* — Specifies the amount of shared memory as a percentage.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

27.14 weekday

weekday

Syntax **weekday** {*weekday-number* [..*weekday-number*] | *day-name* [..*day-name*] | **all**}
no weekday

Context **[Tree]** (config>system>cron>sched weekday)

Full Context configure system cron schedule weekday

Description This command specifies which days of the week that the schedule will fire on. Multiple days of the week can be specified. When multiple days are configured, each of them will cause the schedule to occur. If a weekday is configured without configuring the month, weekday, day-of-month, and minute, the event will not execute.

Using the **weekday** command as well as the **day-of month** command will cause the script to run twice. For example, consider that today is Monday January 1. If Tuesday January 5 is configured, the script will run on Tuesday (tomorrow) as well as January 5 (Friday).

The **no** form of this command removes the specified weekday from the configuration.

Default no weekday

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *weekday-number* — Specifies a weekday number.

Values 1 to 7 (maximum 7 weekday-numbers)

day-name — Specifies a day by name.

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday (maximum 7 weekday names)

all — Specifies all days of the week.

Platforms All

27.15 weight

weight

Syntax **weight** *initial-weight-percentage weight-change-percentage*
no weight

Context **[Tree]** (config>subscr-mgmt>sla-profile>egress>bonding-selection weight)

Full Context configure subscriber-mgmt sla-profile egress bonding-selection weight

Description This command configures the initial (and also the maximum) weight of the preferred connection and the value with which it can change.

The **no** form of this command resets the weight to the default.

Default weight 100 5

Parameters *initial-weight-percentage* — Specifies the initial or maximum weight, as a percentage of the offered weight.

Values 1 to 100

weight-change-percentage — Specifies the weight change, as a percentage.

Values 0 to 10

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

weight

Syntax **weight** *weight*
no weight

Context **[Tree]** (config>qos>atm-td-profile weight)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure qos atm-td-profile weight

Description VCs within the VP tunnel are serviced by a single scheduler assigned to each VP tunnel. VCs within the shaped VP tunnel are degraded from the originally assigned service category to a common UBR service category (default traffic descriptor). Scheduling between VCs are based on WRR with a weight parameter that can be explicitly configured in the ATM traffic descriptor profile. If weight is not specifically configured, the defaults are taken.

The explicitly configured weight parameter is honored only on the ATM MDA in the max16k-vc mode. On all other ATM capable MDAs (ASAP or ATM MDA in max8k-vc mode), the weight parameter is ignored.

The **no** form of this command reverts to the default.

Default VC degraded from CBR = weight 10

VC degraded from rt-VBR = weight 7

VC degraded from nrt-VBR = weight 5

VC degraded from UBR+ = weight 2

VC degraded from UBR = weight 1

Parameters *weight* — Specifies the weight parameter value.

Values 1 to 255

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e, 7950 XRS

weight

Syntax **weight** *weight-value*
no weight

Context **[Tree]** (config>qos>mlppp-profile-egress>class weight)

Full Context configure qos mlppp-profile-egress class weight

Description This command configures the WRR weight scheduling parameter for each MLPPP class queue for this profile.

Parameters *weight-value* — Specifies the weight scheduling parameter.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

weight

Syntax **weight** *weight*
no weight

Context **[Tree]** (config>qos>mc-fr-profile-egress>class weight)

Full Context configure qos mc-fr-profile-egress class weight

Description This command configures the WRR weight scheduling parameter for each Frame Relay scheduling class queue for this profile.

The weight parameter is not applicable to class 0 because the class 0 queue is serviced by the scheduler with the highest priority all the time over all other class queues.

After Class 0 queue packets are serviced, Class 1 queue packets are the next priority up to a rate of MIR. Beyond MIR, Class1, Class2, and Class 3 queues are serviced in proportion to the configured weights.

Parameters *weight* — Specifies the weight schedule.

Values 1 to 100

Default weight 1 — class 1 (not configurable)
weight 90 — class 2
weight 10 — class 3

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

weight

Syntax **weight** *weight*
no weight

Context **[Tree]** (config>router>segment-routing>sr-policies>static-policy>segment-list weight)

Full Context configure router segment-routing sr-policies static-policy segment-list weight

Description This command associates a weight value with a segment list of a statically-defined segment routing policy in order to achieve weighted ECMP behavior. Weight is an optional parameter.

When any segment-list in the active policy has a weight greater than 1, traffic matching the policy will be load-balanced across the segment lists according to their relative weight values.

The **no** form of this command reverts to the default value.

Default weight 1

Parameters *weight* — Specifies the weight value.

Values 1 to 4294967295

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

27.16 weight-down

weight-down

Syntax [**no**] **weight-down** *lag-ports-down-weight*

Context **[Tree]** (config>vrrp>policy>priority-event>lag-port-down weight-down)

Full Context configure vrrp policy priority-event lag-port-down weight-down

Description This command creates a context to configure an event set threshold within a lag-port-down priority control event. The weight-down command defines a sub-node within the lag-port-down event and is uniquely identified with the lag-ports-down-weight parameter. Each weight-down node within the same lag-port-down event node must have a unique lag-ports-down-weight value. Each weight-down node has its own priority command that takes effect whenever that node represents the current threshold. A single LAG can use either weight-threshold or port threshold. The command is required for correct operation on mixed port-speed LAGs and can be used for non-mixed port-speed LAGs as well.

The total number of sub-nodes (uniquely identified by the lag-ports-down-weight parameter) allowed in the system is 2048.

A **weight-down** node is not required for each possible number of ports that could be down. The active threshold is always the closest lower threshold.

The **no** form of the command deletes the event set threshold. The threshold may be removed at any time. If the removed threshold is the current active threshold, the event set thresholds must be re-evaluated after removal.

Default no weight-down

Parameters *lag-ports-down-weight* — The total weight of LAG ports down to create a set event threshold. This is the active threshold when the weight of down ports in the LAG equals or exceeds *lag-ports-down-weight*, but does not equal or exceed the next highest configured *lag-ports-down-weight*.

Values 1 to 64

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.17 weight-threshold

weight-threshold

Syntax **weight-threshold** *value* [**action** {**dynamic-cost** | **static-cost** | **down**}] [**cost** *static-cost*]
no weight-threshold

Context **[Tree]** (config>lag weight-threshold)

Full Context configure lag weight-threshold

Description This command configures the behavior for the Link Aggregation Group (LAG) if the total weight of operational links is equal to or below the configured threshold level. The command can be used for mixed port-speed LAGs and for LAGs with all ports of equal speed.

The **no** form of this command disables the weight-threshold operation in LAG.

Default weight-threshold 0 action down

Parameters *value* — The decimal integer threshold number of operational links for the LAG at or below which the configured action will be invoked. If the number of operational links exceeds the **weight-threshold** value, any action taken for being below the threshold value will cease.

Values 0 to 63

action — Specifies the action to take if the number of active links in the LAG is at or below the threshold value.

dynamic-cost — Specifies that dynamic costing is activated. As a result the LAG remains operationally up with a cost relative to the number of operational links. The link is only regarded as operationally down when all links in the LAG are down.

static-cost — Specifies that static costing will be activated. As a result, the LAG will remain operationally up with the configured cost, regardless of the number of operational links. The link will only be regarded as operationally down when all links in the LAG are down.

down — Specifies the LAG is brought operationally down if the number of operational links is equal to or less than the configured threshold value. The LAG is only regarded as up once the number of operational links exceeds the configured threshold value.

static-cost — The decimal integer static cost of the LAG.

Values 1 to 16777215

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.18 weighted-ecmp

weighted-ecmp

Syntax [**no**] **weighted-ecmp**

Context **[Tree]** (config>service>vprn>bgp-ipvpn>mpls>auto-bind-tunnel weighted-ecmp)

Full Context configure service vprn bgp-ipvpn mpls auto-bind-tunnel weighted-ecmp

Description This command enables weighted ECMP for packets using tunnels that a VPRN automatically binds to. When weighted ECMP is enabled, packets are sprayed across LSPs in the ECMP according to the outcome of the hash algorithm and the configured load balancing weight of each LSP.

The **no** form of this command disables weighted ECMP for next hop tunnel selection.

Default no weighted-ecmp

Platforms All

weighted-ecmp

Syntax **weighted-ecmp** [**strict**]
no weighted-ecmp

Context **[Tree]** (config>service>vprn weighted-ecmp)

Full Context configure service vprn weighted-ecmp

Description This command enables weighted load-balancing for IS-IS, OSPF, and static ECMP routes in the VPRN instance. Weighted ECMP can be performed when all next hops are configured with non-zero load-balancing weights. Weighted ECMP support for IS-IS, OSPF and static ECMP routes applies to both IPv4 and IPv6.

The **no** form of this command restores regular ECMP spraying of packets to IS-IS, OSPF and static route destinations.

Default no weighted-ecmp

Parameters **strict** — Enables strict enforcement for a load balancing weight to be configured on each interface withing a wECMP interface bundle before the interface is taken into wECMP operation. However, when **strict** enforcement is not enabled, then, when **load-balancing-weight** is not configured on one or more interfaces within the wECMP interface bundle, the wECMP load-balancing falls back to classic ECMP operation and equally share the traffic load across the ECMP interface bundle. A special case is when none of the available paths or next-hops have a load balancing weight associated. Then, the load balancing falls back to classic ECMP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Strict load balancing is only applied on IS-IS, OSPF, and static route entries.

Platforms All

weighted-ecmp

Syntax [**no**] **weighted-ecmp**

Context **[Tree]** (config>router>ldp weighted-ecmp)

Full Context configure router ldp weighted-ecmp

Description This command enables weighted ECMP on LDP using RSVP LSPs or SR-TE LSPs. LDP labeled packets are sprayed across the RSVP or SR-TE LSP ECMP in proportion to the configured **load-balancing-weight** of LSPs.

The **no** form of this command removes weighted ECMP.

Default no weighted-ecmp

Platforms All

weighted-ecmp

Syntax **weighted-ecmp** [**strict**]
no weighted-ecmp

Context **[Tree]** (config>router weighted-ecmp)

Full Context configure router weighted-ecmp

Description This command enables the weighted load-balancing, or weighted ECMP, over MPLS LSP.

When this command is enabled, packets of IGP, BGP, and static route prefixes resolved to a set of ECMP tunnel next-hops are sprayed proportionally to the weights configured for each MPLS LSP in the ECMP set.

Weighted load-balancing over MPLS LSP is supported in the following forwarding contexts:

- IGP prefix resolved to IGP shortcuts in RTM (**igp-shortcut** or **advertise-tunnel-link** enabled in the IGP instance).
- BGP prefix with the BGP next-hop resolved to IGP shortcuts in RTM (**igp-shortcut** or **advertise-tunnel-link** enabled in the IGP instance).
- Static route prefix resolved to an indirect next-hop, which itself is resolved to a set of equal-metric MPLS LSPs in TTM. The user can allow automatic selection or specify the names of the equal-metric MPLS LSPs in TTM to be used in the ECMP set.
- Static route prefix resolved to an indirect next-hop, which is resolved to IGP shortcuts in RTM.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- BGP prefix with a BGP next-hop resolved to a static route, which resolves to a set of tunnel next-hops toward an indirect next-hop in RTM or TTM.
- BGP prefix resolving to another BGP prefix, whose next-hop is resolved to a set of ECMP tunnel next-hops with a static route in RTM or TTM or to IGP shortcuts in RTM.

IGP computes the normalized weight for each prefix tunnel next-hop. IGP updates the route in RTM with the set of tunnel next-hops and normalized weights. RTM downloads the information to IOM for inclusion in the FIB.

If one or more LSPs in the ECMP set of a prefix do not have a weight configured, the regular ECMP spraying for the prefix will be performed.

The weight assigned to an LSP impacts only the forwarding decision, not the routing decision. In other words, it does not change the selection of the set of ECMP tunnel next-hops of a prefix when more next-hops exist than the value of the router **ecmp** option. Once the set of tunnel next-hops is selected, the LSP weight is used to modulate the amount of packets forwarded over each next-hop. It also does not change the hash routine, but only the spraying of the flows over the tunnel next-hops is modified to reflect the normalized weight of each tunnel next-hop.

The **no** form of this command resumes regular ECMP spraying of packets of IGP, BGP, and static route prefixes over MPLS LSP.

Default no weighted-ecmp

Parameters **strict** — Enables strict enforcement for a load balancing weight to be configured on each interface withing a wECMP interface bundle before the interface is taken into wECMP operation. However, when **strict** enforcement is not enabled, then, when **load-balancing-weight** is not configured on one or more interfaces within the wECMP interface bundle, the wECMP load-balancing falls back to classic ECMP operation and equally share the traffic load across the ECMP interface bundle. A special case is when none of the available paths or next-hops have a load balancing weight associated. Then, the load balancing falls back to classic ECMP.

Strict load balancing is only applied on IS-IS, OSPF, and static route entries.

Platforms All

weighted-ecmp

Syntax [**no**] **weighted-ecmp**

Context **[Tree]** (config>service>sdp weighted-ecmp)

Full Context configure service sdp weighted-ecmp

Description This command enables weighted ECMP on an SDP. When weighted ECMP is enabled, packets from services using the SDP are sprayed across LSPs in the ECMP set to the SDP far end according to the outcome of the hash algorithm and the configured load-balancing weight of each LSP.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The **no** version of this command disables weighted ECMP for next-hop tunnel selection.

Default no weighted-ecmp

Platforms All

weighted-ecmp

Syntax [**no**] **weighted-ecmp**

Context **[Tree]** (config>router>bgp>next-hop-res weighted-ecmp)

Full Context configure router bgp next-hop-resolution weighted-ecmp

Description This command enables weighted ECMP for next-hop tunnel selection for 6PE. When weighted ECMP is enabled, the RSVP-TE tunnel used to forward 6PE packets to the ECMP next hop is chosen according to the outcome of the hash on the packet at the normalized load-balancing weight of the tunnel.

The **no** version of this command disables weighted ECMP for next-hop tunnel selection for 6PE.

Default no weighted-ecmp

Platforms All

27.19 wide-metrics-only

wide-metrics-only

Syntax [**no**] **wide-metrics-only**

Context **[Tree]** (config>service>vprn>isis>level wide-metrics-only)

Full Context configure service vprn isis level wide-metrics-only

Description This command enables the exclusive use of wide metrics in the LSPs for the level number. Narrow metrics can have values between 1 and 63. IS-IS can generate two TLVs, one for the adjacency and one for the IP prefix. In order to support traffic engineering, wider metrics are required. When wide metrics are used, a second pair of TLVs are added, again, one for the adjacency and one for the IP prefix.

By default, both sets of TLVs are generated. When wide-metrics-only is configured, IS-IS only generates the pair of TLVs with wide metrics for that level.

The **no** form of this command reverts to the default value.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

wide-metrics-only

Syntax [**no**] **wide-metrics-only**

Context **[Tree]** (config>router>isis>level wide-metrics-only)

Full Context configure router isis level wide-metrics-only

Description This command enables the exclusive use of wide metrics in the LSPs for the level number. Narrow metrics can have values between 1 and 63. IS-IS can generate two TLVs, one for the adjacency and one for the IP prefix. In order to support traffic engineering, wider metrics are required. When wide metrics are used, a second pair of TLVs are added, again, one for the adjacency and one for the IP prefix.

By default, both sets of TLVs are generated. When wide-metrics-only is configured, IS-IS only generates the pair of TLVs with wide metrics for that level.

The **no** form of this command reverts to the default value.

Default no wide-metrics-only

Platforms All

27.20 width

width

Syntax **width** *width*

Context **[Tree]** (environment>terminal width)

Full Context environment terminal width

Description This command determines display terminal width.

Default width 80

Parameters *width* — Sets the width of the display terminal.

Values 1 to 512

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

width

Syntax **width** *width*

Context **[Tree]** (config>system>management-interface>cli>md-cli>environment>console width)

Full Context configure system management-interface cli md-cli environment console width

Description This command configures the set number of columns displayed on screen.

Default width 80

Parameters *width* — Specifies the number of columns displayed in the console window.

Values 80 to 512

Platforms All

27.21 wifi-num-attached-ues

wifi-num-attached-ues

Syntax [**no**] **wifi-num-attached-ues**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include wifi-num-attached-ues)
[Tree] (config>subscr-mgmt>auth-plcy>include wifi-num-attached-ues)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute wifi-num-attached-ues
configure subscriber-mgmt authentication-policy include-radius-attribute wifi-num-attached-ues

Description When enabled, this command indicates the number of UEs connected to the tunnel to which the radius message applies to. For session/host accounting this is the tunnel of the associated UE. For queue-instance accounting this attribute will not be included.

The **no** form of this command disables including the RADIUS Alc-Num-Attached-UEs VSA.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.22 wifi-rssi

wifi-rssi

Syntax [**no**] **wifi-rssi**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute wifi-rssi)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute wifi-rssi

Description This command enables the inclusion of the 802.11 Received Signal Strength Indication attribute.

The **no** form of this command reverts to the default.

Default no wifi-rssi

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

wifi-rssi

Syntax [**no**] **wifi-rssi**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes wifi-rssi)

Full Context configure aaa isa-radius-policy acct-include-attributes wifi-rssi

Description This command enables including the Alc-RSSI.

Default no wifi-rssi

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

27.23 wifi-ssid-vlan

wifi-ssid-vlan

Syntax [**no**] **wifi-ssid-vlan**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include wifi-ssid-vlan)
[Tree] (config>subscr-mgmt>auth-plcy>include wifi-ssid-vlan)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes wifi-ssid-vlan)
[Tree] (config>aaa>isa-radius-plcy>acct-include-attributes wifi-ssid-vlan)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa isa-radius-policy acct-include-attributes wifi-ssid-vlan
configure aaa isa-radius-policy auth-include-attributes wifi-ssid-vlan
configure subscriber-mgmt radius-accounting-policy include-radius-attribute wifi-ssid-vlan
configure subscriber-mgmt authentication-policy include-radius-attribute wifi-ssid-vlan

Description This command enables including the per-SSID VLAN ID in a Alc-Wlan-SSID-VLAN VSA.

The **no** form of this command disables including the per-SSID VLAN ID in Alc-Wlan-SSID-VLAN VSA.

Default no wifi-ssid-vlan

Platforms 7450 ESS, 7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure aaa isa-radius-policy auth-include-attributes wifi-ssid-vlan
- configure aaa isa-radius-policy acct-include-attributes wifi-ssid-vlan

7750 SR, 7750 SR-e, 7750 SR-s, VSR

- configure subscriber-mgmt radius-accounting-policy include-radius-attribute wifi-ssid-vlan
- configure subscriber-mgmt authentication-policy include-radius-attribute wifi-ssid-vlan

27.24 wildcard-spmsi

wildcard-spmsi

Syntax **wildcard-spmsi**
no wildcard-spmsi

Context **[Tree]** (config>service>vprn>mvpn>pt>inclusive wildcard-spmsi)

Full Context configure service vprn mvpn provider-tunnel inclusive wildcard-spmsi

Description This command enables RFC 6625 (C-*, C-*) S-PMSI functionality for NG-MVPN. When enabled, (C-*, C-*) S-PMSI is used instead of I-PMSI for this MVPN. Wildcard S-PMSI uses the I-PMSI LSP template.

auto-rp-discovery cannot be enabled together with **mdt-type sender-only** or **mdt-type receiver-only**, or **wildcard-spmsi** configurations.

The **no** form disables the (C-*, C-*) S-PMSI functionality.

Default no wildcard-spmsi

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.25 window

window

Syntax **window** *minutes*

Context **[Tree]** (config>card>mda>egress-xpl window)

Full Context configure card mda egress-xpl window

Description This command configures the Error Window value used by the fail-on-error feature.

Default window 60

Parameters *minutes* — Specifies the time, in minutes, that the MDA can experience frequent Egress XPL Errors. When **fail-on-error** is enabled, if more than *xpl-errors* Egress XPL errors per minute occur on the MDA for the specified number of consecutive minutes, the MDA will be put in the failed state.

The window value cannot be changed while **fail-on-error** is enabled for this MDA.

Values 1 to 1440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

window

Syntax **window** *minutes*

Context **[Tree]** (config>card>mda>ingress-xpl window)

Full Context configure card mda ingress-xpl window

Description This command configures the Error Window value used by the **fail-on-error** feature.

Default window 60

Parameters *minutes* — Specifies the time, in minutes, that the MDA can experience frequent Ingress XPL Errors. When **fail-on-error** is enabled, if more than *xpl-errors* Ingress XPL errors per minute occur on the MDA for the specified number of consecutive minutes, the MDA will be put in the *failed* state.

The window value cannot be changed while **fail-on-error** is enabled for this MDA.

Values 1 to 1440

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

window

Syntax **window** *deciseconds*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame window)

Full Context configure port ethernet efm-oam link-monitoring errored-frame window

Description This command defines the size of the window using a 100ms base *deciseconds*. Errors are accumulated until the end of the window. At the end of the window the actual errors are compared to the thresholds to determine if a threshold has been crossed. There is no mid-window threshold checking. The window represents a unique non-overlapping period of time.

Default window 10

Parameters *deciseconds* — The number of 100ms increments. Must be specified in increments of 10 (full seconds).

Values 10 to 600

Platforms All

window

Syntax **window** *packets*

Context **[Tree]** (config>port>ethernet>efm-oam>link-mon>errored-frame-period window)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-period window

Description This command defines the size of the window based on a packet receive rate. The minimum serviceable rate is the number of minimum size packets that can be received in one second. The window receive count value will be polled at a minimum one second intervals to see if the window size has been reached. Errors are accumulated until the end of the window. At the end of the window the actual errors are compared to the thresholds to determine if a threshold has been crossed. There is no mid-window threshold checking. The window represents a unique non-overlapping period of time.

Parameters *packets* — Specifies the number of received packets in one second.

Values 1 to 4294967295

Default 1488095

Platforms All

window

Syntax **window** *deciseconds*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Context [Tree] (config>port>ethernet>efm-oam>link-mon>errored-frame-seconds window)

Full Context configure port ethernet efm-oam link-monitoring errored-frame-seconds window

Description This command defines the size of the window using a 100ms base *deciseconds*. Errored seconds are accumulated until the end of the window. At the end of the window, the actual errors are compared to the thresholds to determine if a threshold has been crossed. There is no mid-window threshold checking. The window represents a unique non-overlapping period of time.

Parameters *deciseconds* — Specifies the number of 100 ms increments. Must be specified in increments of 10 (full seconds).

Values 100 to 9000

Default 600

Platforms All

window

Syntax **window** *deciseconds*

Context [Tree] (config>port>ethernet>efm-oam>link-mon>errored-symbols window)

Full Context configure port ethernet efm-oam link-monitoring errored-symbols window

Description This command defines the size of the window using a 100ms base *deciseconds*. The time value is converted to a number of symbols for the underlying medium. Errors are accumulated until the end of the window. At the end of the window, the actual errors are compared to the thresholds to determine if a threshold has been crossed. There is no mid-window threshold checking. The window represents a unique non-overlapping period of time.

Parameters *deciseconds* — Specifies the number of 100ms increments in increments of 10 (full seconds).

Values 10 to 600

Default 10

Platforms All

27.26 window-integrity

window-integrity

Syntax **window-integrity** *percentage*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no window-integrity

Context [Tree] (config>oam-pm>streaming>delay-template window-integrity)

Full Context configure oam-pm streaming delay-template window-integrity

Description This command specifies the integrity of the sample window. A percentage value that suggests the measurement has enough samples (integrity) to be considered representative for that sample window. The configured percentage considers the interval of the test PDUs, and the length of the sample window to determine the number of packets required in the sample.

(((window-integrity %) x (sample-window length (s) x pps per test (interval)).

Ensure that the percentage and the combination of sample window and packet per second per test interval produces the desired results.

If the number of samples in the sample window are equal to or greater than the computed number of required samples, then the value has integrity and the suspect flag is set to false for that streamed result.

If the count is less than the computed number of required samples, then the suspect flag is set to true for that streamed result.

Regardless of the integrity, the average values are streamed. It is up to the higher level systems to interrogate the suspect flag and determine if the value that is set should be used, discarded, or reported separately.

The **no** form of this command reverts to the default.

Default window-integrity 50

Parameters *percentage* — Specifies the window integrity percentage.

Values 1 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

window-integrity

Syntax **window-integrity** *percent*
no window-integrity

Context [Tree] (config>test-oam>link-meas>template>asw window-integrity)

Full Context configure test-oam link-measurement measurement-template aggregate-sample-window window-integrity

Description This command determines whether the aggregate sample window is integral based on the number of samples received from the sample window, comparing the number of samples to the percentage configured.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The configured percentage translates to a required sample window count that must be included in the aggregate sample window. The range is from 0 to 100. The number of samples is computed as follows:

(window-integrity (%)) x (((aggregate-sample-window length (s)) / (sample-window length (s)))

For an aggregate sample window that does not reach the integrity, the value is not considered as representative and is used for threshold comparison.

If the number of samples in the aggregate sample window are equal to or greater than the computed number of required samples, the sample window has integrity and the aggregate sample window result is compared to configured sample window thresholds.

If the count is less than the computed number of required samples, the aggregate sample window does not have integrity and the aggregate sample window results are compared to configured sample window thresholds.

If this parameter is not configured, integrity checking is disabled and all results are compared to the configured thresholds.

The **no** form of this command disables integrity checking.

Default window-integrity 0

Parameters *percent* — Specifies the percentage of successful sent and received request-response pairs.

Zero indicates any amount of integrity is acceptable for report to the routing engine.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

window-integrity

Syntax **window-integrity** *percent*
no window-integrity

Context **[Tree]** (config>test-oam>link-meas>template>sw window-integrity)

Full Context configure test-oam link-measurement measurement-template sample-window window-integrity

Description This command specifies the integrity of the sample window. A percentage value indicates when the sample window has enough samples to be considered representative for that window (integrity). The configured percentage considers the interval of probes and the length of the sample window to determine the number of packets required in the sample:

(window-integrity (%)) x (((sample-window length (s)) / pps per test (interval)))

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Ensure that the percentage and the combination of sample window and the packet-per-second per test interval produces the desired results.

If the number of samples in the sample window are equal to or greater than the computed number of required samples, the sample window has integrity and the sample window result is compared to the configured sample window thresholds.

If the count is less than the computed number of required samples, the sample window does not have integrity and the sample window results are not compared to configured sample window thresholds.

If this parameter is not configured, integrity checking is disabled and all results are compared to the configured thresholds.

The **no** form of this command disables integrity checking.

Default window-integrity 0

Parameters *percent* — Specifies the percentage of successful sent and received request-response pairs.

A value of 0 indicates any amount of integrity acceptable for report to the routing engine.

Values 0 to 100

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

27.27 window-size

window-size

Syntax **window-size** *seconds*
no window-size

Context **[Tree]** (config>port>ethernet>sym-mon window-size)

Full Context configure port ethernet symbol-monitor window-size

Description This command specifies sliding window size over which the symbols are sampled to detect signal failure or signal degraded conditions.

Default window-size 10

Parameters *seconds* — Specifies the size of the sliding window in seconds over which the errors are measured.

Values 5 to 60

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

window-size

Syntax **window-size** *seconds*
no window-size

Context **[Tree]** (config>port>ethernet>crc-monitor window-size)

Full Context configure port ethernet crc-monitor window-size

Description This command specifies sliding window size over which the Ethernet frames are sampled to detect signal fail or signal degrade conditions. The command is used jointly with the sf-threshold and the sd-threshold to configure the sliding window size.

The **no** version of this command reverts to the default value of 10 seconds.

Default no window-size

Parameters *seconds* — The size of the sliding window in seconds over which the errors are measured.

Values 5 to 60

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

27.28 wlan-gw

wlan-gw

Syntax **wlan-gw**

Context **[Tree]** (config>router wlan-gw)
[Tree] (config>service>ies>sub-if>grp-if wlan-gw)
[Tree] (config>service>vprn wlan-gw)
[Tree] (config>service>vprn>sub-if>grp-if wlan-gw)
[Tree] (config>subscr-mgmt wlan-gw)
[Tree] (config>service>vprn>radius-proxy>server wlan-gw)
[Tree] (config>router>radius-proxy>server wlan-gw)
[Tree] (config>service>vpls wlan-gw)

Full Context configure router radius-proxy server wlan-gw
configure router wlan-gw
configure service ies subscriber-interface group-interface wlan-gw
configure service vpls wlan-gw
configure service vprn radius-proxy server wlan-gw

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

configure service vprn subscriber-interface group-interface wlan-gw
configure service vprn wlan-gw
configure subscriber-mgmt wlan-gw

Description Commands in this context configure WLAN GW parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw

Syntax [**no**] **wlan-gw**

Context **[Tree]** (debug wlan-gw)

Full Context debug wlan-gw

Description This node contains all the parameters to set up specific call-trace debug sessions for WLAN-GW. The **no** form of this command will stop all configured WLAN-GW traces.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw

Syntax **wlan-gw**

Context **[Tree]** (config>li>li-source wlan-gw)

Full Context configure li li-source wlan-gw

Description This command enables the **wlan-gw** context to configure li-source related parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

27.29 wlan-gw-group

wlan-gw-group

Syntax **wlan-gw-group** *nat-group-id*
no wlan-gw-group

Context **[Tree]** (config>router>wlan-gw>xconnect wlan-gw-group)
[Tree] (config>service>vprn>wlan-gw>xconnect wlan-gw-group)

Full Context configure router wlan-gw xconnect wlan-gw-group
configure service vprn wlan-gw xconnect wlan-gw-group

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures the identifier of the WLAN Gateway ISA group that processes the cross-connect.

The **no** form of this command removes the NAT group IP from the cross-connect configuration.

Parameters *nat-group-id* — Specifies the identifier of the ISA group.

Values 1 to 4

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw-group

Syntax **wlan-gw-group** *group-id*
no wlan-gw-group

Context **[Tree]** (config>router>vrgw>lanext wlan-gw-group)

Full Context configure router vrgw lanext wlan-gw-group

Description This command specifies the WLAN GW group that is used for HLE services.

The **no** form of this command removes the group from the configuration.

Parameters *group-id* — Specifies the WLAN GW group ID.

Values 1 to 4

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw-group

Syntax **wlan-gw-group** *wlan-gw-group-id* [**member** *member-id*]
no wlan-gw-group

Context **[Tree]** (config>subscr-mgmt>wlan-gw>ue-query wlan-gw-group)

Full Context configure subscriber-mgmt wlan-gw ue-query wlan-gw-group

Description This command enables matching on UEs, based on the WLAN-GW group ID and, optionally, the specific ISA member they are installed on.

The **no** form of this command disables matching on the WLAN-GW group.

Default no wlan-gw-group

Parameters *wlan-gw-group-id* — Specifies the WLAN-GW group ID.

Values 1 to 4

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

member-id — Specifies the ISA member ID within the group.

Values 1 to 255

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw-group

Syntax **wlan-gw-group** *group-id* [**create**] [**redundancy** *unit*]
no wlan-gw-group *group-id*

Context **[Tree]** (config>isa wlan-gw-group)

Full Context configure isa wlan-gw-group

Description This command creates a WLAN GW group that contains a set of ISAs to be used in WLAN-GW functionality. A WLAN-GW group can also be used where a NAT group is expected. The WLAN-GW group ID shares the same number space with the NAT group.

At most, one WLAN-GW group may be configured.

The optional redundancy parameter determines the provisioning and redundancy mode.

- IOM mode

  A whole IOM is added to the group. The IOM must be fully provisioned with BB ISA modules. In IOM mode, when a single ISA fails, the entire IOM is considered to have failed and all subscribers are recovered on a backup IOM.
- ISA mode

  BB ISA modules are added separately with no restriction put on other MDAs in the IOM. When a single ISA fails, a backup ISA will try to recover as many subscribers as possible but may run out of resources (for example, queues, policers, host entries) during the recovery process. It is recommended to pair ISAs with MDAs and services that do not consume many IOM resources.

The **no** form of this command removes the group.

Parameters *group-id* — Specifies WLAN Gateway Integrated Service Adaptor (ISA) Groups.

Values 1 to 4

unit — Specifies the provisioning and redundancy mode.

Values mda or iom

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw-group

Syntax **wlan-gw-group** *group-id*

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

no wlan-gw-group

Context [Tree] (config>service>ies>sub-if>grp-if>wlan-gw wlan-gw-group)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw wlan-gw-group)

Full Context configure service ies subscriber-interface group-interface wlan-gw wlan-gw-group
configure service vprn subscriber-interface group-interface wlan-gw wlan-gw-group

Description This command specifies the ID of the **wlan-gw-group** that the **wlan-gw** gateway binds to.

The **no** form of this command removes the value from the **wlan-gw** configuration.

Parameters *group-id* — Specifies the ISA WLAN-GW group.

Values 1 to 4

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

wlan-gw-group

Syntax **wlan-gw-group** *nat-group-id*
no wlan-gw-group

Context [Tree] (config>service>vprn>sub-if>wlan-gw>pool-manager wlan-gw-group)
[Tree] (config>service>ies>sub-if>wlan-gw>pool-manager wlan-gw-group)

Full Context configure service ies subscriber-interface wlan-gw pool-manager wlan-gw-group
configure service vprn subscriber-interface wlan-gw pool-manager wlan-gw-group

Description This command specifies the ISA WLAN gateway group.

Parameters *nat-group-id* — Specifies the identifier of the WLAN gateway group.

Values 1 to 4

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

27.30 working-bundle

working-bundle

Syntax [**no**] **working-bundle** *bundle-id*

Context [Tree] (config>port>multilink-bundle working-bundle)

Full Context configure port multilink-bundle working-bundle

Description This command configures a working bundle that is part of this BPGrp.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *bundle-id* — Specifies the working multilink bundle in the bundle protection group. The command syntax must be configured as follows:

Values bundle-*type-slot/mda.bundle-num*

bundle-PPP or IMA-*slot/mda.bundle-num*	Creates an MLPPP or IMA bundle.
where:	**bundle**: keyword *slot*: IOM/MDA slot numbers *bundle-num*: 1 to 336

For example: router1>config>port>ml-bundle> working-bundle bundle-ima-1/1.1

Platforms 7450 ESS, 7750 SR-7/12/12e

27.31 working-circuit

working-circuit

Syntax **working-circuit** *port-id* [**number** *number*]
no work-circuit [**number** *number*]

Context **[Tree]** (config>port>aps working-circuit)

Full Context configure port aps working-circuit

Description This command configures a physical port that will act as the working circuit for this APS group. The working circuit port must contain only the default configuration and cannot be part of another APS group. The working circuit must be created before the protection circuit.

When a port is a working circuit of an APS group, the configuration available under **config>port** *port-id* context (including submenus) is not allowed for that port unless it is a part of the noted exceptions.

When a port is being configured as a working circuit of an APS group, all common configuration as described above and all service configurations related to the APS port is operationally inherited by the working circuit from the aps-*group-id*. If the working circuit cannot inherit that configuration, for example, due to resource limitations, the configuration attempt fails and an error is returned to the user.

Before a working circuit can be removed from an APS group, the working circuit port must be shutdown. The inherited configuration for the circuit and APS operational commands for that circuit are not preserved when the circuit is removed from the APS group.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Note that all configurations for aps-*group-id* under the **config>port** context and its submenus and all configuration for services that use this aps-*group-id* is preserved as a non-activated configuration since the APS group no longer has any physical circuits assigned.

The **no** form of this command removes the working-circuit. The working circuit can only be removed from the configuration after the protect circuit has been removed.

Parameters *port-id* — Specifies the physical port that will act as the working circuit for this APS group in the following format:

port-id	*slot*/*mda*/*port*		
	eth-sat-id	esat-*id*/*slot*/*port*	
		esat	keyword
		id	1 to 20
	pxc-id	pxc-*id*.*sub-port*	
		pxc	keyword
		id	1 to 64
		sub-port	a, b

number — Specifies the APS channel number; value is 1 or 2.

Modifying Hold-Down Timer Values

Note that for APS configurations, the **config>port>sonet-sdh hold-time down** and **config>port>sonet-sdh hold-time up** default values are 100 ms and 500 ms respectively. But, if there is a large difference in the transmission delay between the APS working (**working-circuit**) and protect line (**config>port>aps protect-circuit**), it is highly recommended that you increase the default timer on the working line accordingly with the transmission delay present on the protect line.

The following output shows an example of the timers on POS interfaces.

```
A:NS044050253# show port aps-1
===============================================================================
SONET/SDH Interface
===============================================================================
Description        : APS Group
Interface          : aps-1                  Speed               : oc3
Admin Status       : up                     Oper Status         : up
Physical Link      : Yes                    Loopback Mode       : none
Single Fiber Mode  : No
Clock Source       : node                   Framing             : sonet
Last State Change  : 04/11/2007 13:53:01    Port IfIndex        : 1358987264
J0 String          : 2/1/5 7750-SR-7        Section Trace Mode  : string
Rx S1 Byte         : 0x00 (stu)             Rx K1/K2 Byte       : 0x00/0x00
Tx S1 Byte         : 0x0f (dnu)             Tx DUS/DNU          : disabled
Rx J0 String (Hex) : 81 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Cfg Alarm          : loc lais lrdi ss1f lb2er-sd lb2er-sf slof slos lrei
Alarm Status       :
Hold time up       : 500 milliseconds
Hold time down     : 100 milliseconds
===============================================================================
Port Statistics
```


© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

```
===============================================================================
Input                 Output
-------------------------------------------------------------------------------
Packets                                          6670498                3804661
Discards                                               0                      0
Unknown Proto Discards                                 0
===============================================================================
A:NS044050253#


For unprotected port these timer are different:
A:NS044050253# show port 2/2/2
===============================================================================
SONET/SDH Interface
===============================================================================
Description        : OC-48 SONET/SDH
Interface          : 2/2/2                   Speed                : oc48
Admin Status       : up                      Oper Status          : up
Physical Link      : Yes                     Loopback Mode        : none
Single Fiber Mode  : No
APS Group          : none                    APS Role             : none
Clock Source       : loop                    Framing              : sonet
Last State Change  : 04/11/2007 14:53:53     Port IfIndex         : 37814272
J0 String          : 0x01                    Section Trace Mode   : byte
Rx S1 Byte         : 0x00 (stu)              Rx K1/K2 Byte        : 0x00/0x00
Tx S1 Byte         : 0x0f (dnu)              Tx DUS/DNU           : disabled
Rx J0 String (Hex) : af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Cfg Alarm          : loc lrdi lb2er-sf slof slos
Alarm Status       :
Hold time up       : 500 milliseconds
Hold time down     : 0 milliseconds
Transceiver Data

Transceiver Type   : SFP
Model Number       : SFP-OC48-SR1
Transceiver Code   : OC48 SR
Laser Wavelength   : 1310                    Diag Capable         : yes
Connector Code     : LC                      Vendor OUI           : 00:01:9c
Manufacture date   : 2004/08/20 00:00:00     Media                : SONET/SDH
Serial Number      : 6331000705
Part Number        : CT2-MS1LBTD32Z2
Optical Compliance*: 00:01:00:00:00:00:00:00
Link Len 9u        : 2 kms                   Link Len Cu          : 0 m
Link Len 9u        : 20 * 100m               Link Len 62.5u       : 0 * 10m
Link Len 50u       : 0 * 10m
===============================================================================
Port Statistics
===============================================================================
                                                    Input                 Output
-------------------------------------------------------------------------------
Packets                                          3870094                6656408
Discards                                               0                      0
Unknown Proto Discards                                 0
===============================================================================
A:NS044050253#
```

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.32 working-path

working-path

Syntax **working-path** *path-name*
no working-path

Context **[Tree]** (config>router>gmpls>lsp working-path)

Full Context configure router gmpls lsp working-path

Description This command specifies the working path for a GMPLS LSP. One working path must be specified for each GMPLS LSP. The path-name parameter must correspond to a path defined under **config>router>gmpls>path**.

The **no** form of the command removes the working-path definition.

Default no working-path

Parameters *path-name* — Specifies the name of the path used by the working path.

Values 32 characters maximum text string

Platforms 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

27.33 working-tp-path

working-tp-path

Syntax [**no**] **working-tp-path**

Context **[Tree]** (config>router>mpls>lsp working-tp-path)

Full Context configure router mpls lsp working-tp-path

Description This command creates or edits the working path for an MPLS-TP LSP. At least one working path (but not more than one working path) must be created for an MPLS-TP LSP. If MPLS-TP linear protection is also configured, then this is the path that is used as the default working path for the LSP, and it must be created prior to the protect path. The working-tp-path can only be deleted if no protect-tp-path exists for the LSP.

The following commands are applicable to the working-tp-path: **lsp-num, in-label, out-label, mep, shutdown**.

Default no working-tp-path

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

27.34 wpp

wpp

Syntax **wpp**

Context **[Tree]** (config>subscr-mgmt>loc-user-db>ipoe>host wpp)

Full Context configure subscriber-mgmt local-user-db ipoe host wpp

Description Commands in this context configure WPP parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

wpp

Syntax **wpp**
no wpp

Context **[Tree]** (config>aaa wpp)
[Tree] (config>service>ies>sub-if>grp-if wpp)
[Tree] (config>service>vprn>sub-if>grp-if wpp)

Full Context configure aaa wpp
configure service ies subscriber-interface group-interface wpp
configure service vprn subscriber-interface group-interface wpp

Description Commands in this context configure Wireless Portal Protocol (WPP) parameters.

The **no** form of the command removes configuration under WPP.

Default no wpp

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

wpp

Syntax [**no**] **wpp**

Context **[Tree]** (debug>router wpp)

Full Context debug router wpp

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description Commands in this context configure WPP debugging parameters.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, VSR

27.35 wrap-around

wrap-around

Syntax [**no**] **wrap-around**

Context **[Tree]** (config>filter>log wrap-around)

Full Context configure filter log wrap-around

Description This command configures a memory filter log to log until full or to store the most recent log entries (circular buffer).

Specifying **wrap-around** configures the memory filter log to store the most recent filter log entries (circular buffer). When the log is full, the oldest filter log entries are overwritten with new entries.

The **no** form of the command configures the memory filter log to accept filter log entries until full. When the memory filter log is full, filter logging for the log filter ID ceases.

Default wrap-around

Platforms All

27.36 wred-queue

wred-queue

Syntax **wred-queue** [**policy** *slope-policy-name*] [**mode** *mode*] [**slope-usage** *slope-usage*]
no wred-queue

Context **[Tree]** (config>qos>sap-egress>queue wred-queue)

Full Context configure qos sap-egress queue wred-queue

Description This command allows the configuration of WRED per queue with the following options:

- Native hardware WRED

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

This uses the hardware per queue WRED capabilities of FP3- and higher-based hardware and is configured with the **native** keyword.

- Pool per queue WRED

  This implements each queue in its own pool and uses the WRED capabilities of the pool to provide WRED per queue. This is configured with the **pool-per-queue** keyword.

Native Hardware WRED

When the **wred-queue mode native** command is configured, the queue uses the WRED capabilities of FP3- and higher-based hardware. In this case, the out-of-profile and exceed-profile traffic map to the low and exceed WRED slopes specified within the slope policy, and the inplus-profile and in-profile traffic uses the MBS drop tail; this requires the **slope-usage** to be configured as **exceed-low**. The instantaneous queue depth is compared against the low and exceed slopes so the time average factor in the slope policy is ignored.

When a policy is not explicitly defined, the default slope policy is used.

When **native** mode is enabled for a queue, the **pool** and **drop-tail** commands are ignored; traffic mapped to a slope that is shut down will use the MBS drop tail.

This is only supported on FP3 hardware.

The **no** form of this command restores the queue default congestion control behavior to the queue.

Pool-per-queue WRED

When the **wred-queue mode pool-per-queue** command is defined and the queue ID is created, a buffer pool is created specifically for the queue and the queue obtains all buffers from that pool. The size of the pool is the same as the size of the queue. In this manner, the WRED slopes that operate based on the pool's buffer utilization are also reacting to the congestion depth of the queue.

The size of the buffer pool is dictated by the queue's MBS parameter. The size of the reserved CBS portion of the buffer pool is dictated by the queue's CBS parameter. The provisioning characteristics of the **mbs** and **cbs** commands are not changed.

In the case where this is applied with WRED queue support shutdown (**config>card>fp>egress>wred-queue-control>shutdown**), the queue will continue to map to its default pool. If the **no shutdown** command is executed in the **wred-queue-control** context, the queue is automatically moved to its own WRED pool.

Each pool created for a queue using the **wred-queue** command shares buffers with all other **wred-queue** enabled queues on the same forwarding plane. The WRED pool buffer management behavior is defined within the **config>card>fp>egress>wred-queue-control** CLI context.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The WRED slopes within the pool are defined by the slope policy associated with the queue. When a policy is not explicitly defined, the default slope policy is used. The slope policy enables, disables, and defines the relative geometry of the highplus, high, low, and exceed WRED slopes in the pool. The policy also specifies the time average factor used by the pool when calculating the weighted average pool depth.

As packets attempt to enter the egress queue, they are associated with the highplus, high, low, or exceed WRED slope based on the packet's profile. If the packet is inplus-profile, the highplus slope is used. If the packet is in-profile, the high slope is used. If the packet is out-of-profile, the low slope is used. If the packet is exceed-profile, the exceed slope is used. This mapping of packet profile to slope is enabled using the **slope-usage default** parameter. Each WRED slope performs a probability discard based on the current weighted average pool depth.

When **wred-queue** is enabled for a SAP egress queue, the queue **pool** and **drop-tail** commands are ignored; traffic mapped to a slope that is shut down will use the MBS drop tail.

The resource usage for the WRED queue pool-per-queue per forwarding plane can be seen in the **tools dump resource-usage card** [*slot-num*] **fp** [*fp-number*] output under *Dynamic Q2 Wred Pools*.

The **no** form of this command restores the generic buffer pool behavior to the queue. The WRED pool is removed from the system. The queue will be moved to the default buffer pool. The queue then uses the default congestion control behavior.

Default no wred-queue

Parameters *slope-policy-name* — Specifies an existing slope policy that is used to override the default WRED slope policy.

mode — Specifies whether the WRED per queue is using the native FP3- and higher-based hardware WRED capabilities or pool per queue.

Values **native** — uses the hardware per queue WRED capabilities of the FP3- and higher-based hardware and requires **slope-usage exceed-low**.

pool-per-queue — each queue uses its own pool and the WRED capabilities of the pool to provide WRED per queue. This is supported on both FP2- and higher-based hardware and requires **slope-usage default**.

Default native

slope-usage — Specifies congestion control to be used.

Values **default** — maps the inplus, in, out, and exceed-profile traffic to the highplus, high, low, and exceed WRED slopes, respectively; this is only supported for **pool-per-queue** mode.

exceed-low — maps the out and exceed-profile traffic to the low and exceed WRED slopes with the inplus and in-profile traffic using the MBS drop tail. This is only supported for **native** mode.

Default exceed-low

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Platforms All

wred-queue

Syntax **wred-queue** [**policy** *slope-policy-name*] [**mode** {**native** | **pool-per-queue**}] [**slope-usage** {**default** | **exceed-low**}]
no wred-queue

Context **[Tree]** (config>qos>qgrps>egr>qgrp>queue wred-queue)

Full Context configure qos queue-group-templates egress queue-group queue wred-queue

Description This command allows the configuration of WRED per queue with the following options:

- Native hardware WRED
  This uses the hardware per queue WRED capabilities of FP3- and higher-based hardware and is configured with the **native** keyword.
- Pool per queue WRED
  This implements each queue in its own pool and uses the WRED capabilities of the pool to provide WRED per queue. This is configured with the **pool-per-queue** keyword.

Native Hardware WRED

When the **wred-queue mode native** command is configured, the queue uses the WRED capabilities of FP3- and higher-based hardware. In this case, the out and exceed-profile traffic map to the low and exceed WRED slopes specified within the slope policy, and the inplus and in-profile traffic uses the MBS drop tail; this requires the **slope-usage** to be configured as **exceed-low**. The instantaneous queue depth is compared against the low and exceed slopes so the time average factor in the slope policy is ignored.

When a policy is not explicitly defined, the default slope policy is used.

When **native** mode is enabled for a queue, the drop-tail commands are ignored; traffic mapped to a slope that is shut down will use the MBS drop tail.

Native hardware WRED is supported on FP3- and higher-based hardware and is ignored on FP2 hardware.

The **no** form of this command restores the queue default congestion control behavior to the queue.

Pool-per-queue WRED

When the **wred-queue mode pool-per-queue** command is defined and the queue ID is created, a buffer pool is created specifically for the queue and the queue obtains all buffers from that pool. The size of the pool is the same as the size of the queue. In this manner, the WRED slopes that operate based on the pool's buffer utilization are also reacting to the congestion depth of the queue.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

The size of the buffer pool is dictated by the queue's **mbs** parameter. The size of the reserved CBS portion of the buffer pool is dictated by the queue's **cbs** parameter. The provisioning characteristics of the **mbs** and **cbs** commands are not changed.

In the case where this is applied with WRED queue support shut down (**config>card>fp>egress>wred-queue-control>shutdown**), the queue will continue to map to its default pool. If the **no shutdown** command is executed in the **wred-queue-control** context, the queue will be automatically moved to its own WRED pool.

Each pool created for a queue using the **wred-queue** command shares buffers with all other **wred-queue** enabled queues on the same forwarding plane. The WRED pool buffer management behavior is defined within the **config>card>fp>egress>wred-queue-control** CLI context.

The WRED slopes within the pool are defined by the slope policy associated with the queue. When a policy is not explicitly defined, the default slope policy is used. The slope policy enables, disables, and defines the relative geometry of the highplus, high, low, and exceed WRED slopes in the pool. The policy also specifies the time average factor used by the pool when calculating the weighted average pool depth.

As packets attempt to enter the egress queue, they are associated with the highplus, high, low, or exceed WRED slope based on the packet's profile. If the packet is inplus-profile, the highplus slope is used. If the packet is in-profile, the high slope is used. If the packet is out-of-profile, the low slope is used, and if the packet is exceed-profile, the exceed slope is used. This mapping of packet profile to slope is enabled using the **slope-usage default** parameter. Each WRED slope performs a probability discard based on the current weighted average pool depth.

When **wred-queue** is enabled for an egress queue group queue, the queue pool and drop-tail commands are ignored; traffic mapped to a slope that is shut down will use the MBS drop tail.

The resource usage for the wred-queue pool-per-queue per forwarding plane can be seen in the **tools dump resource-usage card** [*slot-num*] **fp** [*fp-number*] output under *Dynamic Q2 Wred Pools*.

The **no** form of this command restores the generic buffer pool behavior to the queue. The WRED pool is removed from the system. The queue will be moved to the default buffer pool. The queue then uses the default congestion control behavior.

Default no wred-queue

Parameters *slope-policy-name* — Specifies an existing slope policy that is used to override the default WRED slope policy.

mode {native | pool-per-queue} — Specifies whether the WRED per queue is using the native FP3- and higher-based hardware WRED capabilities or pool per queue.

Values **native** - Each queue uses the hardware per queue WRED capabilities of the FP3- and higher-based hardware and requires **slope-usage exceed-low**.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

pool-per-queue - Each queue uses its own pool and the WRED capabilities of the pool to provide WRED per queue. This requires **slope-usage default**.

Default native

slope-usage {default | exceed-low} — Specifies the type of congestion control to be used.

Values **default** - Maps the inplus-profile, in-profile, out-of-profile, and exceed-profile traffic to the highplus, high, low, and exceed WRED slopes, respectively; this is only supported for **pool-per-queue** mode.

exceed-low - Maps the out-of-profile and exceed-profile traffic to the low and exceed WRED slopes, with the inplus-profile and in-profile traffic using the MBS drop tail. This option is only supported for **native** mode.

Default exceed-low

Platforms All

27.37 wred-queue-control

wred-queue-control

Syntax **wred-queue-control**

Context **[Tree]** (config>card>fp>egress wred-queue-control)

Full Context configure card fp egress wred-queue-control

Description Commands in this context configure the aggregate WRED queue parameters for all WRED queues on an egress forwarding plane.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

27.38 writable-running

writable-running

Syntax [**no**] **writable-running**

Context **[Tree]** (config>system>netconf>capabilities writable-running)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure system netconf capabilities writable-running

Description This command enables support of the writable-running capability in the SR OS NETCONF server. If writable-running is disabled then requests that reference the running datastore as a target return an error, and when a NETCONF client establishes a new session the writable-running capability is not advertised in the SR OS <hello>.

When **management-interface configuration-mode** is set to **model-driven**, then the writable-running capability is disabled, even if **writable-running** is configured.

The **no** form of the command disables of the writable-running capability in the SR OS NETCONF server.

Default no writable-running

Platforms All

27.39 write

write

Syntax **write** {*user-name* | *broadcast*} *message*

Context **[Tree]** (global write)

Full Context global write

Description This command sends a console message to a specific user or to all users with active console sessions.

Parameters *user-name* — Specifies the name of a user, up to 32 characters, with an active console session to which to send a console message.

Values any valid CLI username

broadcast — Sends the *message-string* to all users logged into the router.

message — Specifies the message string to send. Allowed values are any string, up to 256 characters, composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.40 write-algorithm

write-algorithm

Syntax **write-algorithm** {**hash** | **hash2** | **custom** | **cleartext**}
no write-algorithm

Context **[Tree]** (config>system>security>management-interface>classic-cli write-algorithm)

Full Context configure system security management-interface classic-cli write-algorithm

Description This command specifies how encrypted configuration secrets are output from the system. For example, how encrypted secrets are displayed in the output of the info command, and how they are written to the saved configuration file.

The **no** form of this command reverts to the default value.

Default write-algorithm hash2

Parameters **hash** — Specifies hash. Use this option to transport a phrase between modules and nodes. In this case the read-algorithm should be **hash** as well.

hash2 — Specifies hash2 which is module-specific.

custom — Specifies the custom encryption to management interface.

cleartext — Specifies that the phrase is displayed as clear text everywhere.

Platforms All

27.41 wrr-group

wrr-group

Syntax **wrr-group** *group-id* **sched-class** *class-id*
wrr-group *group-id* **unattached**
no wrr-group *group-id*

Context **[Tree]** (config>qos>hs-attachment-policy wrr-group)

Full Context configure qos hs-attachment-policy wrr-group

Description This command defines how the specified group ID is attached to the scheduler. A WRR group may have one of two attachment states:

- directly attached to a scheduler class

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

- unattached

A WRR group provides a weighted scheduling context for its member queues, collapsing the queues into a single scheduling class.

The following WRR membership restrictions apply:

- Two groups are supported: WRR-group 1 and WRR-group 2.
- Up to six of the eight queues can become members of WRR groups (the sum of the membership of both groups cannot exceed six queues). All six queues can be placed in a single WRR group or they can be spread between the two groups.
- All queues within a group must have contiguous queue IDs.
- When both groups are configured to have queue members, the queue IDs in group 1 must be lower than the queue IDs in group 2.

The **queue** *queue-id* attachment command is used to define WRR group membership.

The **no** form of the command reverts to the default unattached attachment state for the group ID.

Default wrr-group group-id unattached

Parameters *group-id* — Specifies the WRR group identifier. The *group-id* parameter is required when executing the **wrr-group** attachment command.

Values 1, 2

sched-class — Specifies a direct attachment between the WRR group and one of the six scheduling classes. The **sched-class** and **unattached** keywords are mutually exclusive. One of the keywords must be specified when the **wrr-group** attachment command is executed.

class-id — Specifies the scheduling class associated with this WRR group. The **sched-class** keyword specifies the attachment between the group ID and one of the six scheduling classes. A value of 1 through 6 must accompany the **sched-class** keyword representing the WRR group's attached scheduling class. Only one queue or WRR group can be attached to a given scheduling class. If another queue or a WRR group is currently attached to the specified scheduling class, the **wrr-group** attachment command fails and the current attachment for the *group-id* is unchanged.

Values 1 to 6

unattached — Indicates that the group ID is not attached to any scheduling class or WRR group. Queues that are members of the unattached WRR group do not forward any packets. The **sched-class** and **unattached** keywords are mutually exclusive. One of the keywords must be specified when the **wrr-group** attachment command is executed.

Platforms 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

27.42 wtr-annexb

wtr-annexb

Syntax **wtr-annexb** *minutes*

Context **[Tree]** (config>port>aps wtr-annexb)

Full Context configure port aps wtr-annexb

Description This command waits to restore for Annex B mode operation. The delay after which the newly active section becomes the primary section after a switch-over from the primary section to the secondary section occurs and the switch request clears normally.

Parameters *minutes* — Specifies the time, in minutes, to wait to restore for Annex B mode operation.

Values 0 to 60

Default 5

Platforms 7450 ESS, 7750 SR-7/12/12e, 7750 SR-a, 7750 SR-e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

28 x Commands

28.1 x-interfaces

x-interfaces

Syntax x-interfaces

Context **[Tree]** (config>li x-interfaces)

Full Context configure li x-interfaces

Description Commands in this context configure LI X1, X2, and X3 interfaces.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

28.2 x1

x1

Syntax **x1**

Context **[Tree]** (config>li>x-interfaces x1)

Full Context configure li x-interfaces x1

Description Commands in this context configure the LI X1 interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

28.3 x2

x2

Syntax **x2**

Context **[Tree]** (config>li>x-interfaces x2)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure li x-interfaces x2

Description Commands in this context configure the LI X2 interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

28.4 x3

x3

Syntax **x3**

Context **[Tree]** (config>li>x-interfaces x3)

Full Context configure li x-interfaces x3

Description Commands in this context configure the LI X3 interface.

Platforms 7450 ESS, 7750 SR, 7750 SR-a, 7750 SR-e, 7750 SR-s, 7950 XRS

28.5 xc

xc

Syntax **xc** [**detail**]
no xc

Context **[Tree]** (debug>router>mpls>event xc)

Full Context debug router mpls event xc

Description This command debugs cross connect events.

The **no** form of the command disables the debugging.

Parameters **detail** — Displays detailed information about cross connect events.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

28.6 xcon

xcon

Syntax [**no**] **xcon**

Context **[Tree]** (config>subscr-mgmt>wlan-gw>tunnel-query>ue-state xcon)

Full Context configure subscriber-mgmt wlan-gw tunnel-query ue-state xcon

Description This command enables matching on tunnels with cross-connect UEs.

The **no** form of this command disables matching on cross-connect UEs, unless UE state matching is disabled altogether.

Default no xcon

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

28.7 xconnect

xconnect

Syntax **xconnect**

Context **[Tree]** (config>router>wlan-gw xconnect)
[Tree] (config>service>vprn>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range xconnect)
[Tree] (config>service>ies>sub-if>grp-if>wlan-gw>vlan-tag-ranges>range xconnect)

Full Context configure router wlan-gw xconnect
configure service ies subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect
configure service vprn subscriber-interface group-interface wlan-gw vlan-tag-ranges range xconnect

Description Commands in this context configure WLAN-GW cross-connect UE-related parameters.

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

xconnect

Syntax **xconnect**

Context **[Tree]** (config>card>mda xconnect)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

[Tree] (config>card>xiom>mda xconnect)

Full Context configure card mda xconnect
configure card xiom mda xconnect

Description This command creates a loopback (cross-connect) in the MAC chip and does not require a faceplate port.

Platforms 7450 ESS, 7750 SR, 7750 SR-s, 7950 XRS

- configure card mda xconnect

7750 SR-s

- configure card xiom mda xconnect

28.8 xconnect-tunnel-home-address

xconnect-tunnel-home-address

Syntax [**no**] **xconnect-tunnel-home-address**

Context **[Tree]** (config>subscr-mgmt>acct-plcy>include-radius-attribute xconnect-tunnel-home-address)
[Tree] (config>subscr-mgmt>auth-plcy>include xconnect-tunnel-home-address)

Full Context configure subscriber-mgmt radius-accounting-policy include-radius-attribute xconnect-tunnel-home-address
configure subscriber-mgmt authentication-policy include-radius-attribute xconnect-tunnel-home-address

Description This command enables the generation of the Cross Connect Tunnel Home Address RADIUS attribute.

The **no** form of the command reverts to the default value.

Default no xconnect-tunnel-home-address

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

xconnect-tunnel-home-address

Syntax [**no**] **xconnect-tunnel-home-address**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes xconnect-tunnel-home-address)
[Tree] (config>aaa>isa-radius-plcy>auth-include-attributes xconnect-tunnel-home-address)

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Full Context configure aaa isa-radius-policy acct-include-attributes xconnect-tunnel-home-address
configure aaa isa-radius-policy auth-include-attributes xconnect-tunnel-home-address

Description This command enables the cross connect tunnel home address RADIUS attribute.

Default no xconnect-tunnel-home-address

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

28.9 xconnect-tunnel-local-ipv6-address

xconnect-tunnel-local-ipv6-address

Syntax [**no**] **xconnect-tunnel-local-ipv6-address**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes xconnect-tunnel-local-ipv6-address)

Full Context configure aaa isa-radius-policy acct-include-attributes xconnect-tunnel-local-ipv6-address

Description This command enables the generation of the cross connect tunnel local IPv6 address RADIUS attribute.

Default no xconnect-tunnel-local-ipv6-address

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

28.10 xconnect-tunnel-remote-ipv6-address

xconnect-tunnel-remote-ipv6-address

Syntax [**no**] **xconnect-tunnel-remote-ipv6-address**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes xconnect-tunnel-remote-ipv6-address)

Full Context configure aaa isa-radius-policy acct-include-attributes xconnect-tunnel-remote-ipv6-address

Description This command enables the generation of the cross connect tunnel remote IPv6 address RADIUS attribute.

Default no xconnect-tunnel-remote-ipv6-address

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

28.11 xconnect-tunnel-service

xconnect-tunnel-service

Syntax [**no**] **xconnect-tunnel-service**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes xconnect-tunnel-service)

Full Context configure aaa isa-radius-policy acct-include-attributes xconnect-tunnel-service

Description This command enables the generation of the cross connect tunnel service RADIUS attribute.

Default no xconnect-tunnel-service

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

28.12 xconnect-tunnel-type

xconnect-tunnel-type

Syntax [**no**] **xconnect-tunnel-type**

Context **[Tree]** (config>aaa>isa-radius-plcy>acct-include-attributes xconnect-tunnel-type)

Full Context configure aaa isa-radius-policy acct-include-attributes xconnect-tunnel-type

Description This command enables the generation of the cross connect tunnel type RADIUS attribute.

Default no xconnect-tunnel-type

Platforms 7750 SR, 7750 SR-e, 7750 SR-s, VSR

28.13 xgig

xgig

Syntax **xgig** {**lan** | **wan**}

Context **[Tree]** (config>port>ethernet xgig)

Full Context configure port ethernet xgig

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command configures a 10 Gb/s interface to be in Local or Wide Area Network (LAN or WAN) mode. When configuring the port to be in WAN mode certain SONET/SDH parameters can be changed to reflect the SONET/SDH requirements for this port.

When the port is configured for LAN mode, all SONET/SDH parameters are pre-determined and not configurable.

Default xgig lan

Parameters **lan** — Sets the port to operate in LAN mode.

wan — Sets the port to operate in WAN mode.

Platforms All

28.14 xiom

xiom

Syntax [**no**] **xiom**

Context **[Tree]** (config>card xiom)

Full Context configure card xiom

Description This command configures an XIOM in one of the slots of an XCM. An XIOM can be used instead of an XMA and operates as a carrier module to support MDA-s modules.

Parameters *xiom-slot* — Specifies the XIOM identifier.

Values x1 or x2

Platforms 7750 SR-s

28.15 xiom-type

xiom-type

Syntax **xiom-type** *xiom-type* [**level** *xiom-level*]
no xiom-type

Context **[Tree]** (config>card>xiom xiom-type)

Full Context configure card xiom xiom-type

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Description This command adds an XIOM to the device configuration for the slot. The XIOM type can be preprovisioned, which means that the XIOM does not have to be installed in the chassis.

An XIOM must be provisioned before an MDA-s, connector, or port can be configured.

An XIOM can only be provisioned in a slot that is vacant. No other XIOM or XMA can be provisioned (configured) for that particular slot. To reconfigure a slot position, use the **no** form of this command to remove the current information.

An XIOM can only be provisioned in a slot if the XIOM type is allowed in the slot. An error message is generated if an attempt is made to provision an XIOM type that is not allowed.

If an XIOM is inserted that does not match the configured XIOM type for the slot, then a log event and a facility alarm are raised. The alarm is cleared when the correct XIOM type is installed or the configuration is modified.

A log event and a facility alarm are raised if an administratively enabled XIOM is removed from the chassis. The alarm is cleared when the correct XIOM type is installed or the configuration is modified. A log event is issued when a XIOM is removed that is administratively disabled.

XIOMs are controlled by hardware and software licensing. For these cards, the license level must be provisioned in addition to the XIOM type. An XIOM cannot become operational unless the provisioned license level matches the license level of the card installed into the slot. The set of license levels varies by XIOM type.

The provisioned license level controls aspects related to connector provisioning and the consumption of hardware egress queues and egress policers. Changes to the provisioned license level may be blocked if a configuration exists that would not be permitted with the new target license level.

If the license level is not specified, the level is set to the highest license level for that XIOM.

The **no** form of this command removes the XIOM from the configuration.

Parameters *xiom-type* — Specifies the type of XIOM to be configured and installed in the slot. Values for this attribute vary by platform and release. The release notes include a listing of all supported xiom-types and their CLI strings. In addition, the command can be queried to check which xiom-types are relevant for the active platform type.

xiom-level — Specifies the license level of the XIOM, up to 32 characters. Possible values vary by XIOM type.

Platforms 7750 SR-s

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

28.16 xmpp

xmpp

Syntax **xmpp**

Context **[Tree]** (config>system xmpp)

Full Context configure system xmpp

Description Commands in this context configure xmpp.

Platforms All

xmpp

Syntax **xmpp** [**connection**] [**gateway**] [**message**] [**vsd**] [**iq**] [**all**]
no xmpp

Context **[Tree]** (debug>system xmpp)

Full Context debug system xmpp

Description This command enables the debug for XMPP messages sent or received by the 7750 SR, 7450 ESS, or 7950 XRS.

Parameters **connection** — Filters only the messages related to the XMPP connection.

gateway — Filters the messages related to the gateway.

message — Filters only the messages.

vsd — Filters the VSD messages.

iq — Filters the IQ messages between the gateway and the VSD.

all — Includes all the above.

Platforms All

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

29 y Commands

29.1 yang-modules

yang-modules

Syntax **yang-modules**

Context **[Tree]** (config>system>management-interface yang-modules)

Full Context configure system management-interface yang-modules

Description Commands in this context configure YANG module parameters.

The **yang-modules** settings affect the data sent in a NETCONF <hello>, data populated in the RFC 6022 /netconf-state/schemas list, data returned in a <get-schema> request, and data populated in the RFC 8525 /yang-library. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, sections “NETCONF Monitoring” and “YANG Library” for more information.

Platforms All

29.2 yellow-differential-delay

yellow-differential-delay

Syntax **yellow-differential-delay** *yellow-diff-delay*
no yellow-differential-delay

Context **[Tree]** (config>port>multilink-bundle yellow-differential-delay)

Full Context configure port multilink-bundle yellow-differential-delay

Description This command sets the yellow warning threshold for the differential delay for members within a multilink bundle. If circuit’s delay exceeds the yellow-differential delay value, a log message and SNMP trap is sent. This command is only valid for MLPPP bundles. The differential delay is calculated as the round-trip differential delay for MLPPP bundles.

The **no** form of this command removes the yellow-differential-delay.

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Parameters *yellow-diff-delay* — Specifies the maximum yellow differential delay threshold value, in milliseconds.

Values 1 to 25

Platforms 7450 ESS, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

30 z Commands

30.1 zone

zone

Syntax **zone** {*std-zone-name* | *non-std-zone-name*} [*hh* [*:mm*]]
no zone

Context **[Tree]** (config>system>time zone)

Full Context configure system time zone

Description This command sets the time zone and/or time zone offset for the device.

The SR-series router OS supports system-defined and user-defined time zones. The system-defined time zones are listed in the Time Zones section.

For user-defined time zones, the zone and the UTC offset must be specified.

The **no** form of the command reverts to the default of Coordinated Universal Time (UTC). If the time zone in use was a user-defined time zone, the time zone will be deleted. If a **dst-zone** command has been configured that references the zone, the summer commands must be deleted before the zone can be reset to UTC.

Default zone UTC 00

Parameters *std-zone-name* — Specifies the standard time zone name. The standard name must be a system-defined zone in the Time Zones section. For zone names in the table that have an implicit summer time setting, for example MDT for Mountain Daylight Saving Time, the remaining **start-date**, **end-date** and **offset** parameters do not need to be provided unless it is necessary to override the system defaults for the time zone.

For system-defined time zones, a different offset cannot be specified. If a new time zone is needed with a different offset, the user must create a new time zone. Note that some system-defined time zones have implicit summer time settings which causes the switchover to summer time to occur automatically; configuring the **config>system>time dst-zone** command is not required.

A user-defined time zone name is case-sensitive and can be up to 5 characters in length.

Values A user-defined value can be up to 5 characters or one of the following values: GMT, WET, CET, EET, EEST, MSK, MSD, AST, NST, EST, CST, MST, PST, HST, AKST, AWST, ACST, AEST, NZST, UTC

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

non-std-zone-name — Specifies the non-standard time zone name. The name can be up to 5 characters.

hh [:mm] — Specifies the hours and minutes offset from UTC time, expressed as integers. Some time zones do not have an offset that is an integral number of hours. In these instances, the *minutes-offset* must be specified. For example, the time zone in Pirlanngimpi, Australia UTC + 9.5 hours.

Values hours: -11 to 12 minutes: 0 to 59

Default hours: 0 minutes: 0

Platforms All

30.2 zone-channel

zone-channel

Syntax **zone-channel** *mcast-address* **source** *ip-address* **adi-channel-name** *channel-name*
no zone-channel *mcast-address* **source** *ip-address*

Context **[Tree]** (config>service>ies>video-interface>channel zone-channel)
[Tree] (config>service>vprn>video-interface>channel zone-channel)

Full Context configure service ies video-interface channel zone-channel
configure service vprn video-interface channel zone-channel

Description This command configures zone-channel parameters or ad insertion. The channel configuration along with the zone-channel configuration associates a network channel to a zone-channel and builds the store and forward relationship.

Parameters *mcast-address* — Specifies the IP multicast group address for which this entry contains information.

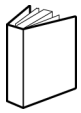
source *ip-address* — Specifies the type of address to be used for a source address.

adi-channel-name *channel-name* — Specifies the name for this zone channel.

Platforms 7450 ESS, 7750 SR-14s, 7750 SR-7/12/12e

© 2022 Nokia.
Use subject to Terms available at: www.nokia.com

Customer Document and Product Support



Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback

© 2022 Nokia.
3HE 18381 AAAA TQZZA 01